Universal Management Suite (UMS)

IGEL Universal Management Suite (UMS) is the management software for the secure central remote administration of IGEL OS devices. With the UMS, you can configure endpoint devices in the same way as locally on the device. For a basic overview of the UMS, see Overview of the IGEL UMS (see page 661).

Installation and Configuration

UMS Installation and Update (see page 4), Installation and Sizing Guidelines for IGEL UMS (see page 231), Connecting to the UMS (see page 134), User Management (see page 1003), UMS Administration (see page 868)

Licenses

Automatic License Deployment, UMS Licenses (see page 884), Device Licenses (see page 886)

Endpoint Devices Deployment

Registering Devices (see page 1134)

User Assistance

Support Information (see page 680), Messages in the IGEL UMS Console (see page 688), Logging (see page 987)

Endpoint Configuration

Using Profiles (see page 700), Priority Profiles (see page 744), Template Profiles in the IGEL UMS (see page 746), Effectiveness of Settings (see page 743)

Firmware Management

Firmware Update (see page 856), Check for New Firmware Updates (see page 857)

Custom Design

Themes (see page 677), Firmware Customizations (see page 764)

Views and Searches

Quick Search (see page 693), Views (see page 818), Search with Regular Expressions (see page 650)

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 10)
- Guidelines and recommendations for setting up your UMS environment: Sizing Guidelines for IGEL UMS 12 and IGEL OS 12 (see page 5)

You can find detailed instructions to perform the following:

- Installation of the standard UMS with embedded database: IGEL UMS Installation under Linux (see page 17) and IGEL UMS Installation under Windows (see page 48)
- Installing the Distributed IGEL UMS (see page 59)
- IGEL UMS Update (see page 204)
- Connecting External Database Systems to UMS (see page 63)

Further information on specific topics can be found in the articles under UMS Installation (see page 396) and IGEL UMS Environment (see page 426).

Sizing Guidelines for IGEL UMS 12 and IGEL OS 12

The following sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite (UMS) 12 environment to manage IGEL OS 12 devices. The UMS environment includes the UMS Server, UMS Console & UMS Web App, database, and, if required, reverse proxy or IGEL Cloud Gateway (ICG) instances.

For information on sizing guidelines for UMS environments managing IGEL OS 11 devices, see Installation and Sizing Guidelines for IGEL UMS Environments Managing IGEL OS 11[1] .

General Prerequisites

The sizing guidelines describe the most common UMS environments. The individual exceptions or requirements may not be covered by these scenarios.

The following prerequisites apply for the IGEL UMS environments described in the sizing guidelines:

System Requirements

- UMS version 12.01.100 or higher
- ICG version 12.01 or higher
- IGEL OS 12.01 or higher

UMS Console Requirements

- 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[2].
- The UMS Console can be installed on single instances or separately, if required.

IGEL OS 12 Devices

- 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[3].
- Devices outside of the internal LAN can be connected through external reverse proxy solutions. As an alternative you can use ICG. For information on network configuration and reverse proxies, see IGEL Universal Management Suite Network Configuration[4].
- Devices are booted/rebooted once a day on average.

1. https://kb.igel.com/en/universal-management-suite/current/installation-and-sizing-guidelines-for-igel-ums
2. https://kb.igel.com/en/universal-management-suite/current/igel-ums-communication-ports
3. https://kb.igel.com/en/universal-management-suite/current/igel-ums-communication-ports
4. https://kb.igel.com/en/universal-management-suite/current/igel-universal-management-suite-network-configurat#id-(12.07.100-en)IGELUniversalManagementSuiteNetworkConfiguration-UMSEndpointPathsforReverseProxyIntegration

UMS Server Requirements

- Not more than 10 base system version and 40 apps or app versions are 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[5]): The DNS alias `igelrmserver` or the DHCP tag can only point to ONE UMS installation. Therefore, the installation of several separate UMS Servers in one network is not recommended.

IGEL UMS Environment Sizing

The size and structure of the recommended UMS setup is mainly defined by the following:

- Number of managed IGEL OS 12 devices
- UMS installation type - Standard UMS or Distributed UMS
- ICG / reverse proxy connection for devices outside of your company network
- Use of UMS as Update Proxy

> **Recommendation for Large Installations**
>
> Large installations should always use the Distributed UMS. It is also recommended to use cluster FQDN for load balancing (see Server Network Settings in the IGEL UMS[6]) or DNS-Round-Robin load balancing or ICG.

Sizing Overview

In the table below you can find the recommended UMS installation type and database type per number of managed device with the basic installation requirements.

> **Installation Requirements**
> The documented installation requirements are purely for the UMS / ICG services. Please check the documentation of your host OS on details about the OS requirements.
> The installation requirements are specified with the understanding that the UMS Server setup includes the UMS Server, the UMS Console, and the UMS Web App.
> For detailed installation requirements, see:
> - Installation Requirements for the IGEL UMS[7]
> - Prerequisites for Installing IGEL Cloud Gateway[8]

5. https://kb.igel.com/en/universal-management-suite/current/registering-devices-automatically-on-the-igel-ums
6. https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums#id-(12.07.100-en)ServerNetworkSettingsintheIGELUMS-ClusterAddress
7. https://kb.igel.com/en/universal-management-suite/current/installation-requirements-for-the-igel-ums
8. https://kb.igel.com/en/igel-cloud-gateway/current/prerequisites-for-installing-igel-cloud-gateway

Installation Type	Number of Managed Devices	Database Type	Number of Servers	Installation Requirements
Standard UMS	**up to 5.000** simultaneously connected devices **up to 2.000** simultaneously booting devices	**Embedded database**	**1 UMS server**	UMS server with UMS Console and Web App • 10 GB RAM • 4 CPUs • 50 GB free disk space / Enough disk space to store app binaries if UMS is used as update proxy.
	up to 25.000 simultaneously connected devices **up to 2.000** simultaneously booting devices	**External database**		
Standard UMS with ICG	**up to 5.000** simultaneously connected devices **up to 2.000** simultaneously booting devices	**Embedded database**	**1 UMS server** **1 ICG server** *(The installation of more ICGs is supported, but it will not have a significant impact on throughput.)*	Requirements for UMS server + ICG server **UMS server with UMS Console and Web App:** • 10 GB RAM • 4 CPUs • 50 GB free disk space / Enough disk space to store app binaries if UMS is used as update proxy. **ICG server:** • 4 GB RAM • 2 CPUs • 2 GB free disk space
	up to 25.000 simultaneously connected devices **up to 2.000** simultaneously booting devices	**External database**		

Installation Type	Number of Managed Devices	Database Type	Number of Servers	Installation Requirements
Distributed UMS	**for 50.000** simultaneously connected devices **up to 4.000** simultaneously booting devices	**External database**	**2 UMS servers**	Requirements for UMS server with UMS Console and Web App for each server • 10 GB RAM • 4 CPUs • 50 GB free disk space / Enough disk space to store app binaries if UMS is used as update proxy.
	Above 50.000 devices When using distributed UMS, there is no fixed upper limit to the number of managed devices. The server requirements of large installations depend heavily on the use cases, as a general guideline, you should plan for approximately one additional UMS server for every 25.000 devices. For example, managing 300.000 simultaneously connected devices may require up to 12 UMS servers, depending on the environment and use case.			

Embedded Database vs External Database

The embedded DB is a supported productive database for small environments, but it is always preferred to use external databases for production environments.
The benefits of an embedded DB are reduced costs and easy management, but it has limitations regarding performance and scalability (e.g. if the database grows big, it gets very slow and UMS updates might take hours).
If required, a standard UMS installation can be extended 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).

Using ICG with IGEL OS 12

When managing IGEL OS 12 devices, the ICG provides a similar solution compared to an external reverse proxy solution. For an overview, see IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices[9] .
There might be advantages regarding the security footprint when using an ICG. However, the security footprint of the reverse proxy setup can be mitigated with decent firewall rules. Paths for firewall setup can be found in IGEL Universal Management Suite Network Configuration[10].

9. https://kb.igel.com/en/universal-management-suite/current/igel-cloud-gateway-vs-reverse-proxy-for-the-commun

UMS as Update Proxy and Disk Space Requirements

You need to have enough disk space in your UMS server to store app binaries to use the UMS as the update proxy for app distribution. The disk space is required for every installation type (Standard UMS, Distributed UMS) and applies to every UMS server.
IGEL recommends a minimum of 50 GB disk space, but the required space also depends on the stored apps and follows the size of apps shown in IGEL App Portal[11] (e.g. 1,24 GB for a base system or 381 MB for Citrix Workspace App).
If the UMS server runs out of disk space, it can have serious effects. To prevent this, admins should monitor disk usage with the help of UMS notifications, see How to Configure Notifications in the IGEL UMS[12].
You can also set the IGEL App Portal as the app repository, for details, see Configuring Global Settings for the Update of IGEL OS Apps[13].

10. https://kb.igel.com/en/universal-management-suite/current/igel-universal-management-suite-network-configurat#id-(12.07.100-en)IGELUniversalManagementSuiteNetworkConfiguration-UMSEndpointPathsforReverseProxyIntegration
11. http://app.igel.com
12. https://kb.igel.com/en/universal-management-suite/current/how-to-configure-notifications-in-the-igel-ums#id-(12.07.100-en)HowtoConfigureNotificationsintheIGELUMS-DiskUsage
13. https://kb.igel.com/en/universal-management-suite/current/configuring-global-settings-for-the-update-of-igel

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 661).

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 (see page 1440)

> Only run the IGEL UMS on a server that has no other server-based, database, or web applications installed. IGEL does not support installations that have other applications installed on the server.

Standard UMS Installation Requirements

Network Topology

Ensure that only one IGEL UMS instance is located in one subnet. This is true for standard UMS installations and Distributed UMS or UMS HA installations.

Background: The UMS uses a default DNS alias (`igelrmserver`) for automatic device registration, and this alias can only point to one UMS instance at a time. Running multiple, unlinked UMS servers could create conflicts, particularly when devices are set up for automatic registration, as devices might not reliably connect to the intended UMS instance.

Installation Requirements

> The documented installation requirements are purely for the UMS services. Please check the documentation of your host OS on details about the OS requirements.

Standard UMS means that you have a single UMS Server. You can host the **UMS Server** with the **UMS Administrator**, **UMS Console**, **UMS Web App**, and optionally, an **Embedded Database** hosted on the same machine. In this case, your hardware and software must meet the following minimum requirements:

- At least **10 GB of RAM**
- At least **50 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

The UMS components on the same host as the UMS Server and UMS Administrator have the following minimum requirements:

- **UMS Web App**
  - At least 2 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

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 (see page 1440). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

Browser Requirements

As of UMS 12.08.100, the login procedure to the IGEL UMS has been changed and requires now a modern browser on the system. For the supported browsers, see the “Supported Environment” section of the release notes[14].

For the login requirements, see UMS Login Requirements[15].

14. https://kb.igel.com/en/universal-management-suite/current/ums-release-notes
15. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

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 (see page 1387).

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 (see page 256).
- The network configuration on Windows Servers must have the TCP/IPv6 option enabled for UMS 12.
- 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

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 231).

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

The single-instance installation is called a **Standard UMS**. In the Standard UMS installation 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.

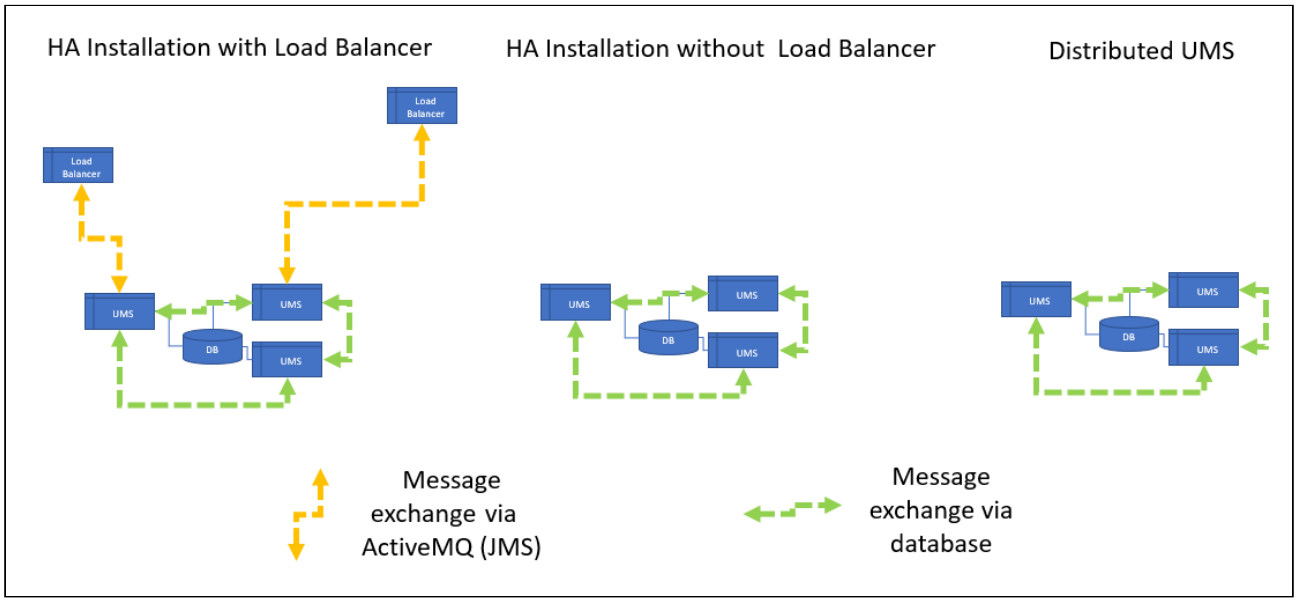
> Alternatively, you can use a reverse proxy / external load balancer for load distribution as of UMS 12; the FQDN and port of the external load balancer / reverse proxy must be specified as a Cluster Address, see Server Network Settings in the IGEL UMS (see page 909).
> Note the following:
> - The Cluster Address is only for communication via the web server port (see page 1038) (default: 8443).
> - SSL can be terminated at the reverse proxy / external load balancer or at the UMS Server. For more information, see IGEL Universal Management Suite Network Configuration (see page 265).

- **UMS High Availability (HA) Extension**
  The UMS HA (see page 1387) 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 (see page 1420).

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 (see page 256).



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 (see page 514), 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 the IGEL Cloud Gateway.
See also Installation and Sizing Guidelines for IGEL UMS (see page 231).

- 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 (see page 1407)) 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 (see page 1155).
- 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 661).

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 17)
- IGEL UMS Installation under Windows (see page 48)

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 (see page 1391).

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 10).

For the supported operating systems, see the "Supported Environment" section of the release notes (see page 1440).

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

1. Familarize yourself with security recommendations on user access under Best Practices for User Access to IGEL UMS Server (see page 408) and create the user to run the UMS Tomcat Server.

2. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[16].

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

3. Open a terminal emulator such as xterm and switch to the directory in which the installation file `setup-igel-ums-linux-[Version].bin` is located.

4. Check whether the installation file is executable. If not, it can be made executable with the following command:
   `chmod u+x setup*.bin`

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

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

5. 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.

6. Start the installation procedure by pressing **Enter**.

   You can cancel the installation at any time by pressing the [Esc] key twice.

7. Read and confirm the license agreement.

8. Under **Destination directory**, select the directory in which the UMS is to be installed. (Default: `/opt/IGEL/RemoteManager`)

9. 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 206).

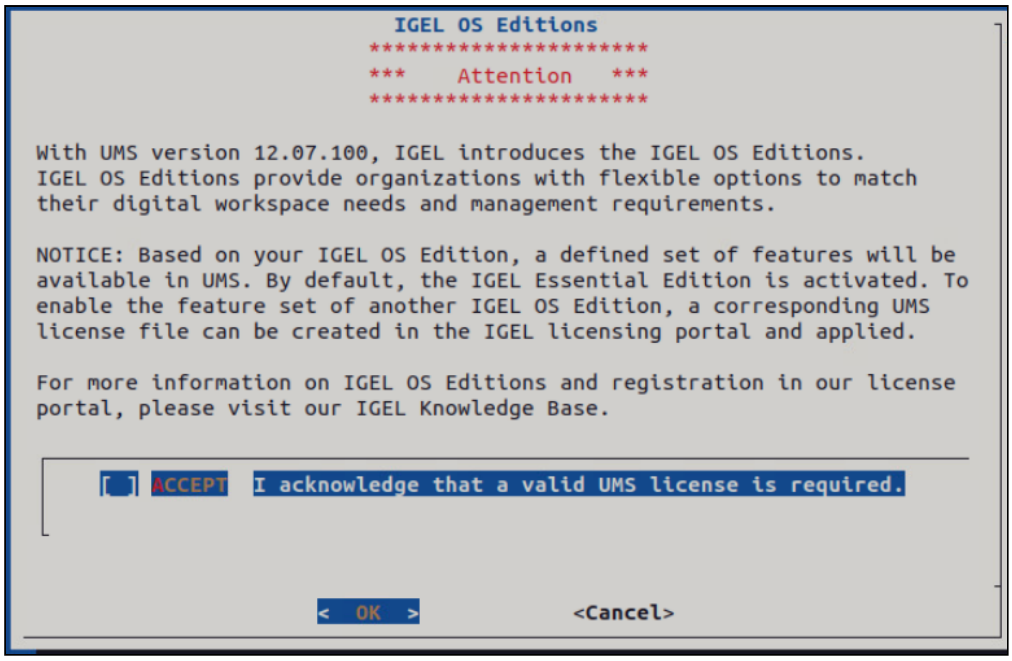
For Update Installations Only
As of UMS 12, the MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:
Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others 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.

10. Under **Installation type**, select the scope of installation:
    - **Complete**: UMS Server and UMS Console
    - **Distributed UMS**: Distributed UMS installation
    - **HA Net**: High Availability configuration
    - **Client only**: UMS Console only

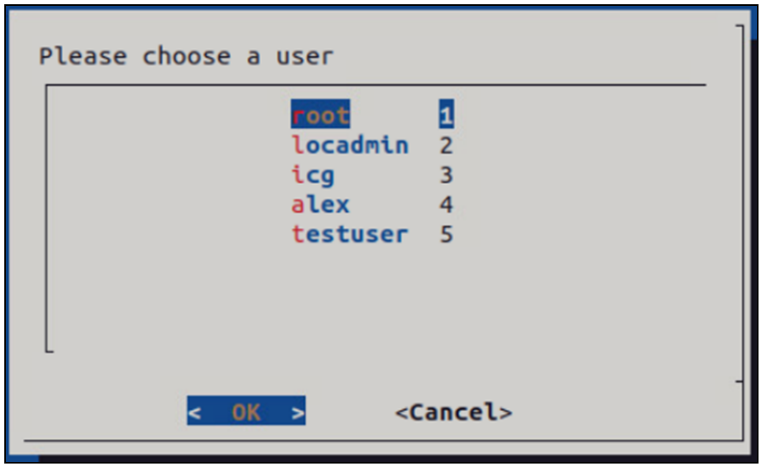
    For more information on installation types, see IGEL UMS Installation[17].

11. Read and confirm the information regarding IGEL OS Editions and UMS Licenses[18] and click **Next**.

17. https://kb.igel.com/en/universal-management-suite/current/igel-ums-installation



12. Select the user to run the UMS Tomcat Server. The user needs to be created before the installation, so if the user is not yet configured, cancel the installation and restart once the user is created.



We strongly recommend using a user with minimal authorizations in order to follow the principle of least privilege and increase system security. For details on why the root user is not recommended, see Best Practices for User Access to IGEL UMS Server (see page 408).

13. Enter the user password and click **Next**.

18. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums

For password verification, the module “pamtester” is required on your system. This module will be automatically downloaded as part of the installation process after confirmation. If you choose not to install it, the installation will only be functional for the root user.

14. Choose whether the **IGEL UMS Web App** (see page 1154) should be installed. See Important Information for the IGEL UMS Web App (see page 1155).

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

16. 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 Troubleshooting Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux (see page 404).

17. 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.

18. 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 63).

19. 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 1070).

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

21. 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.

22. 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`.

23. Connect the UMS Console to the UMS Server by entering the login data for the database that you specified during the installation. See Connecting the UMS Console to the IGEL UMS Server[19].

> 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 (see page 1425).
> - there are problems when connecting the UMS Console to the UMS Server

> **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 Universal Management Suite Network Configuration (see page 265)) or at the UMS Server.

19. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-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 (see page 256).

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 909).

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 668).

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

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 17).

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 (see page 1391)), 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 (see page 256)):

   ```
   # 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 17).

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 (see page 256).
2. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

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 (see page 256).
2. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

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 (see page 256).

5. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

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 17).

1. Adjust the Oracle Linux Server firewall settings to allow the network ports used by the UMS, see IGEL UMS Communication Ports (see page 256).
2. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

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 (see page 256).
2. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

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 (see page 256).
5. Complete the installation as described in IGEL UMS Installation under Linux (see page 17).

Installing IGEL UMS on Microsoft Azure

This article describes a standard IGEL Universal Management Suite (UMS) single server installation (not High Availability (see page 1387)) along with IGEL Cloud Gateway (ICG). The database is reachable via Azure or is hosted in Azure.

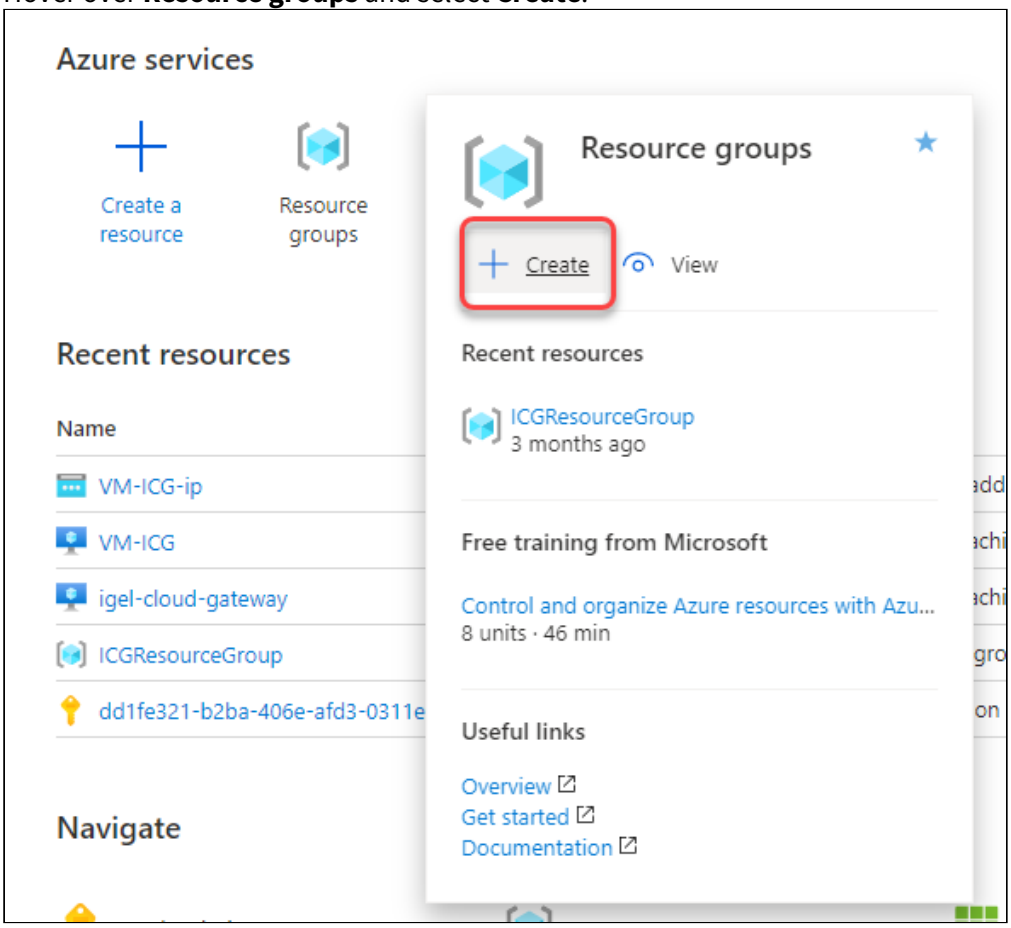
> **High Availability (HA)**
> IGEL UMS Server HA is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks.

IGEL Requirements

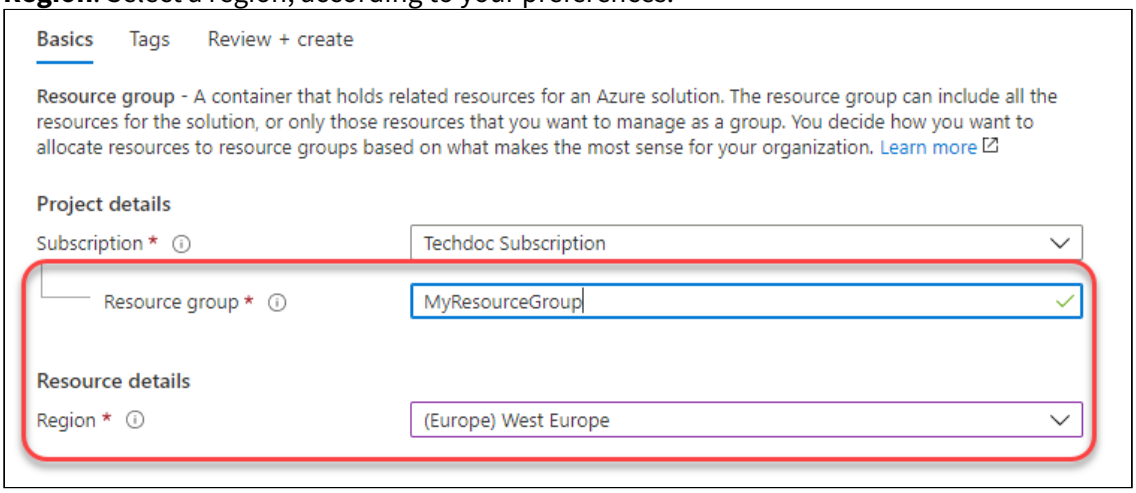
- Microsoft Azure account
- UMS 6.07.100 or higher

Creating a Virtual Machine for the IGEL UMS

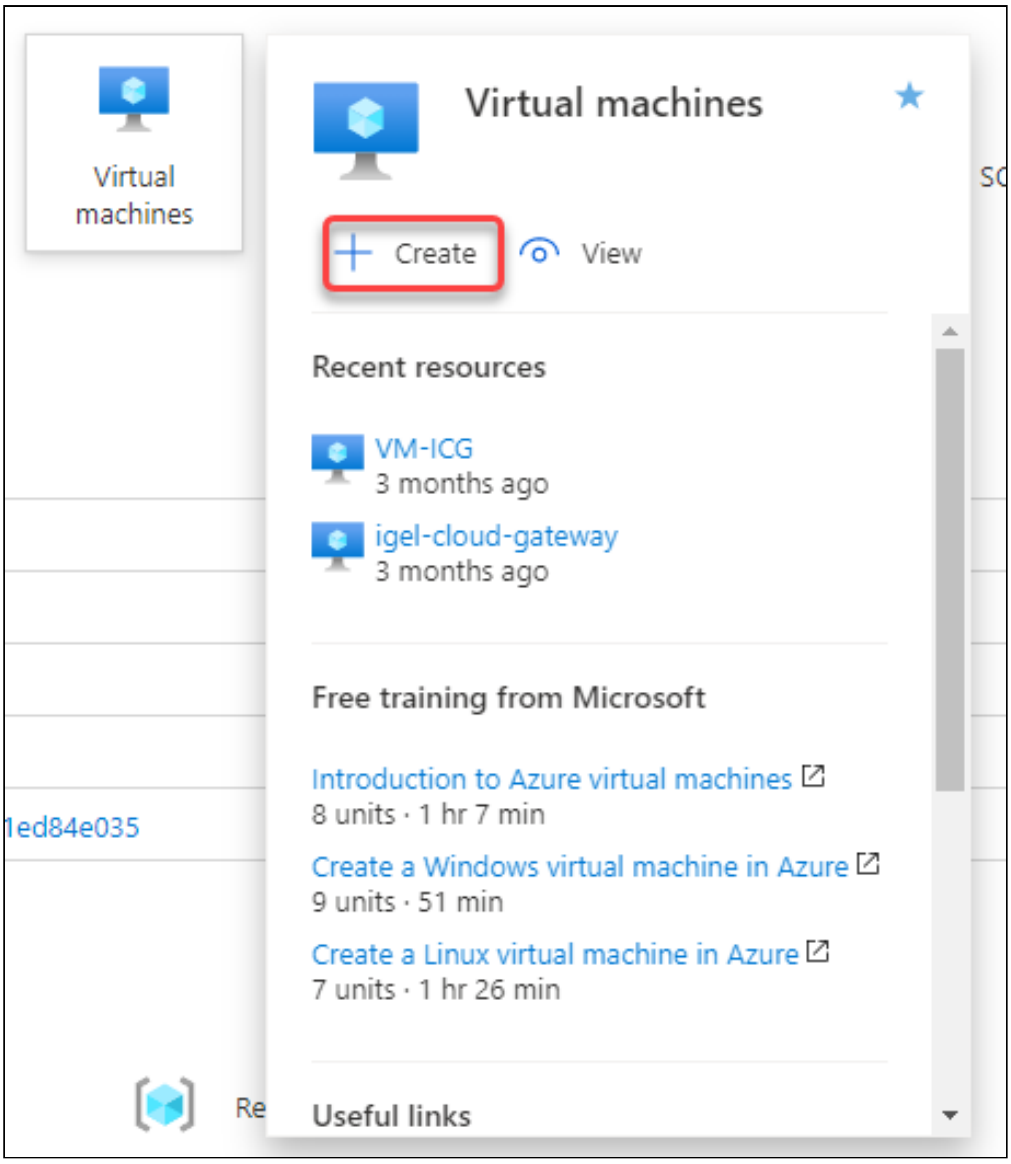
1. Log in to Microsoft Azure.
2. Hover over **Resource groups** and select **Create**.



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.



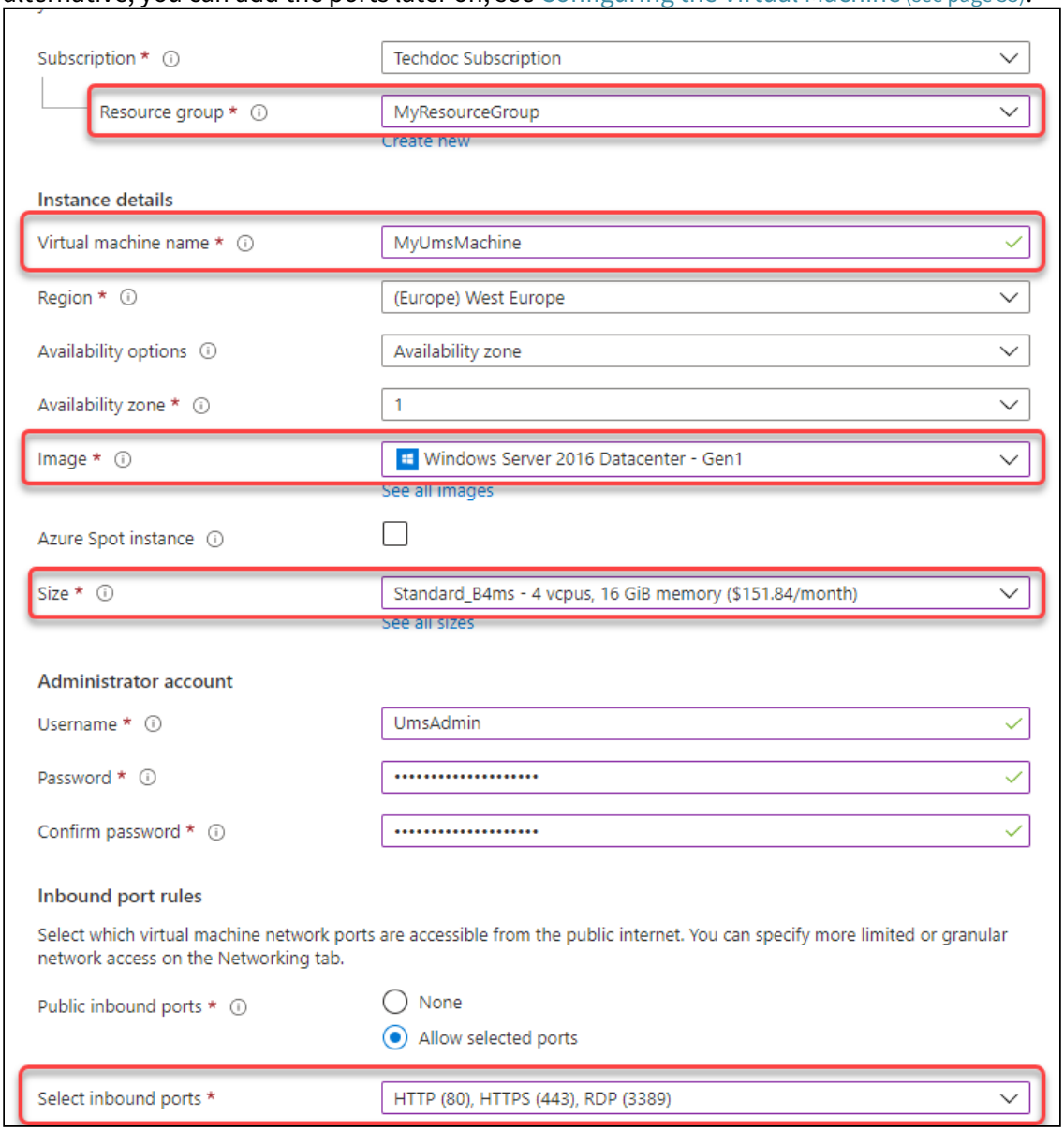
4. Click **Review + create**.
   Your resource group is validated.
5. Click **Create**.
   Your resource group is created.
6. Click **Home** to get to the overview.
7. Hover over **Virtual machines** and select **Create**.



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

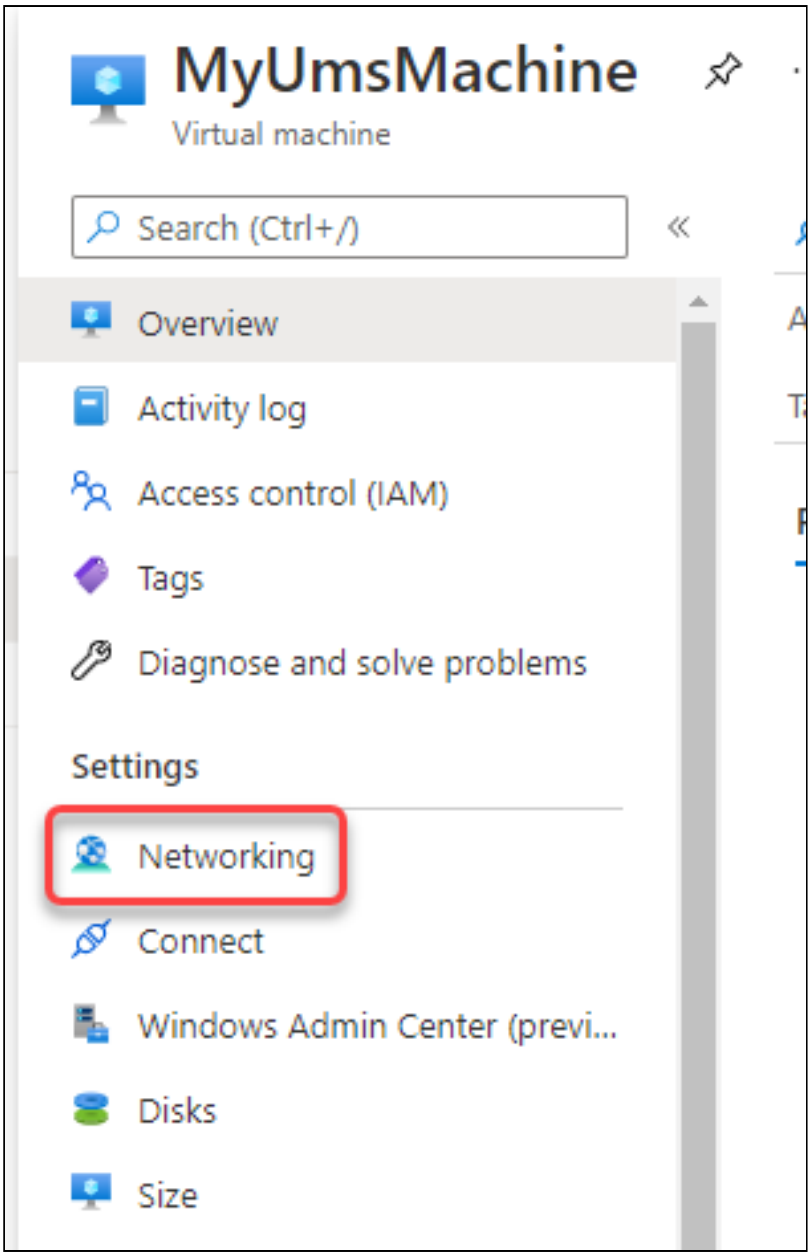
- **Select inbound ports**: Select "HTTP (80)", "HTTPS (443)", and "RDP (3389". As an alternative, you can add the ports later on; see Configuring the Virtual Machine (see page 33).



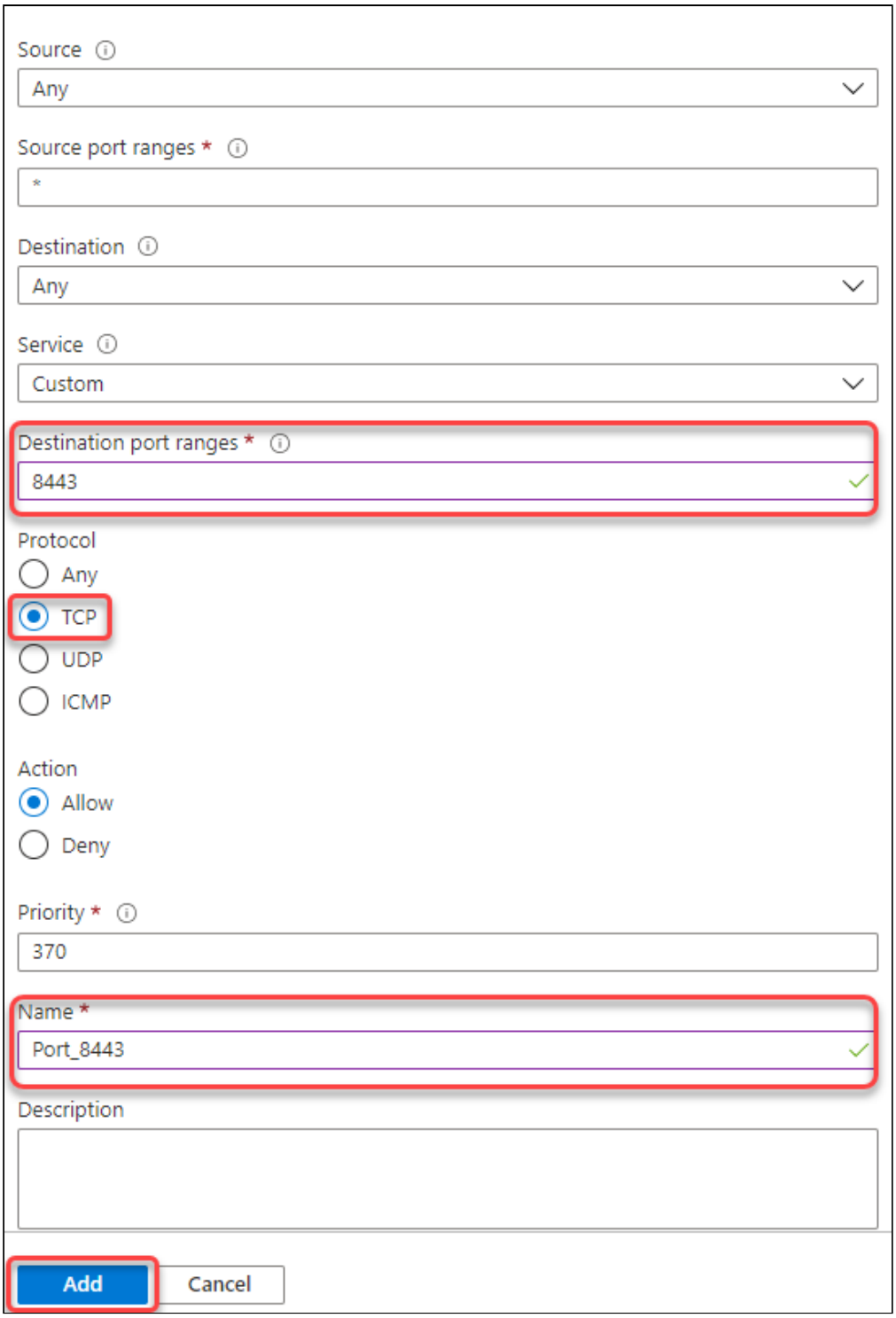
9. Click **Review + create**.
10. Click **Create**.

Configuring the Virtual Machine

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

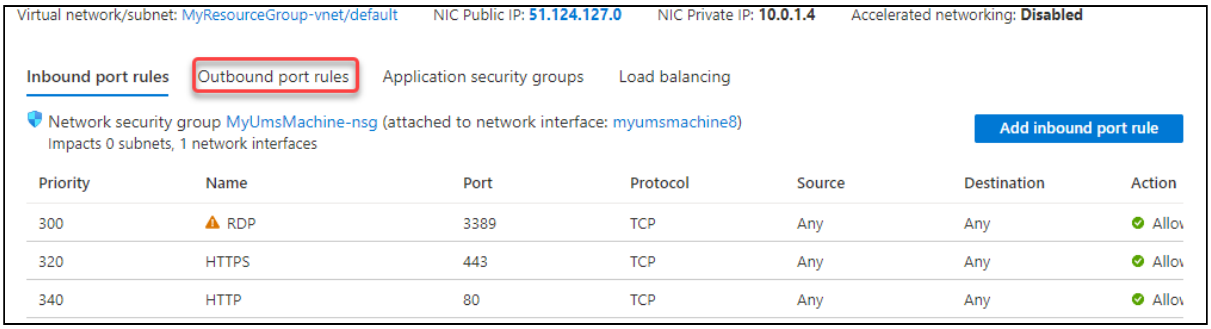


2. Click **Add inbound port rule**.
3. Edit the data as follows:
   - Destination port ranges: Enter "8443".
   - Protocol: Select **TCP**.
   - Name: Change to "Port_8443".
4. Click **Add**.

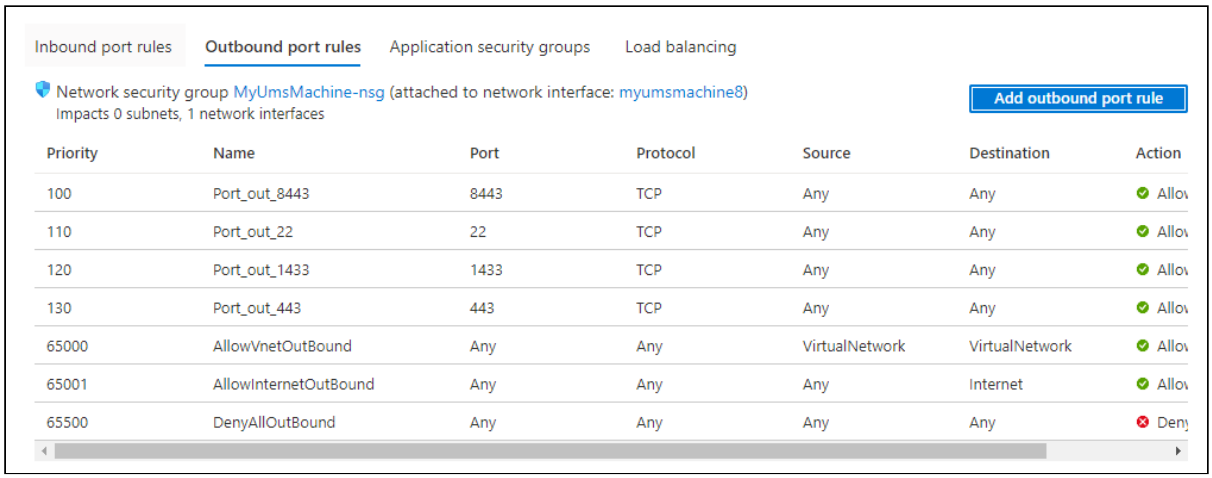


After the installation is complete, do not forget to disable ports 3389 and 22!

5. Select **Outbound port rules**.

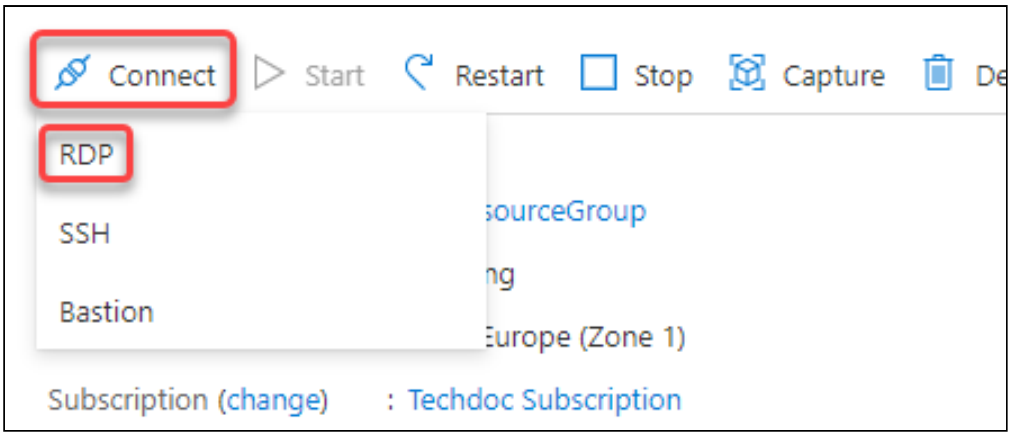


6. Click **Add outbound port rule**.
7. Using the procedure described in steps 2 and 3, add the following ports:
   - 8443 (TCP)
   - 22 (TCP)
   - Database port: The port that will be used for communication with the database. For more information, see UMS with External Database (see page 352).
   - 443 (TCP)
8. Review your settings.



Installing the IGEL UMS

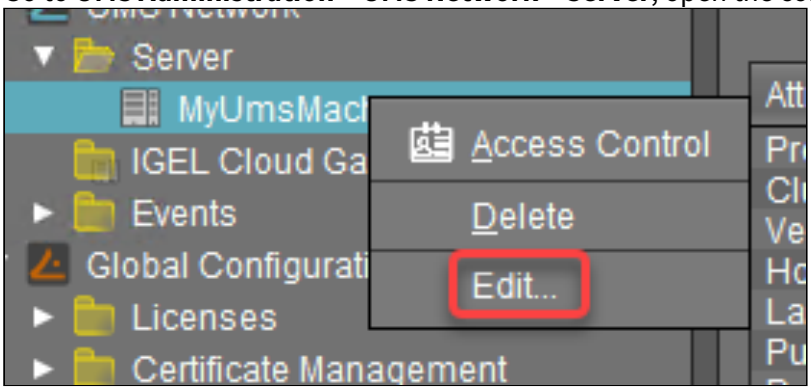
1. Ensure that your virtual machine is running.
2. Click **Connect** and then select **RDP**.



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 Server**[20] **> 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 48) 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 1073).

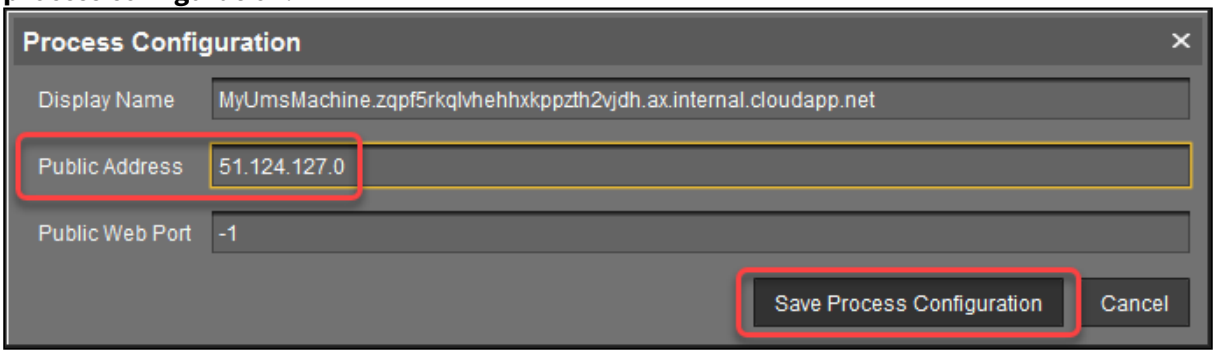
Setting the Public Address on the IGEL UMS Server

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



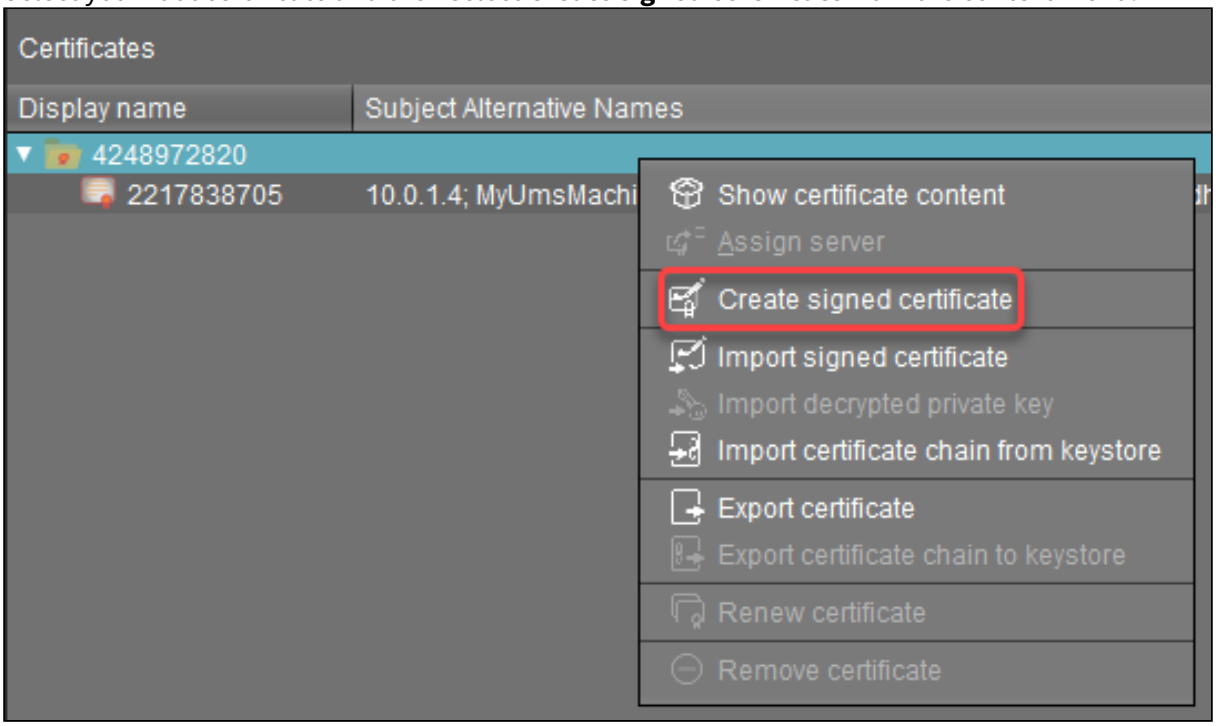
20. https://www.igel.com/software-downloads/

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

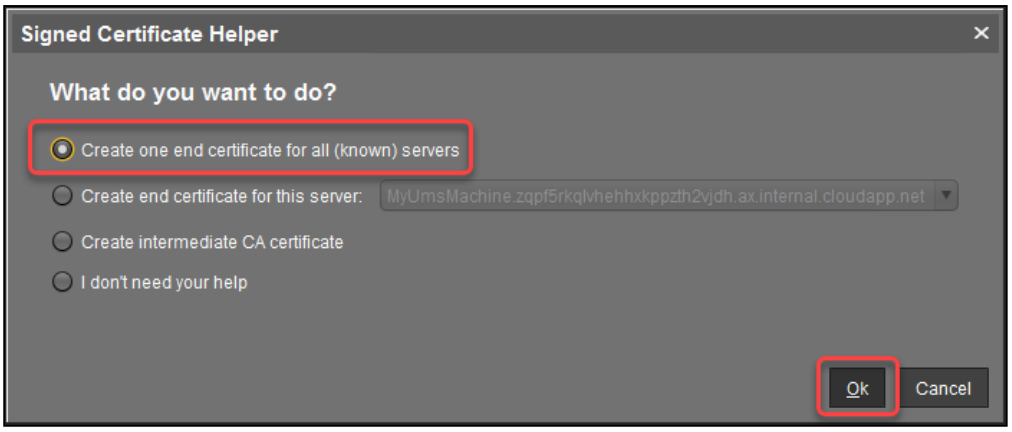


Create Web Certificates

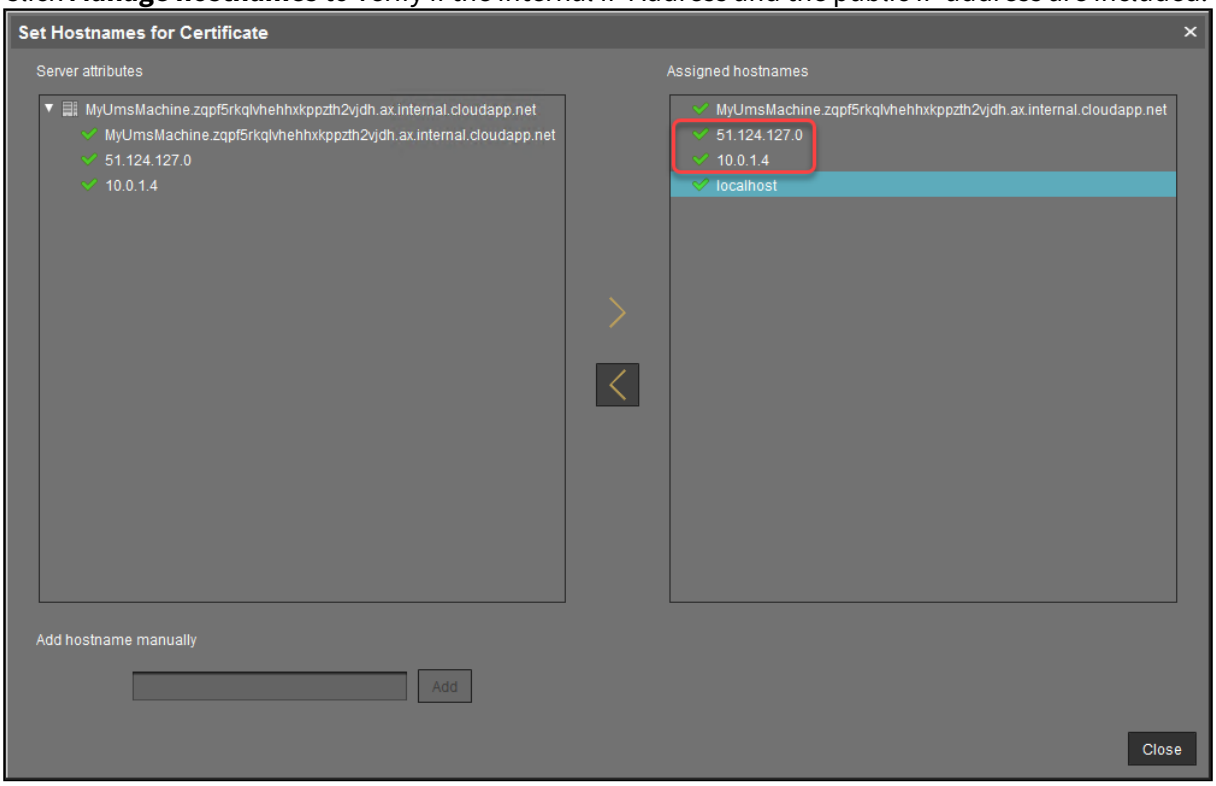
1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Select your root certificate and then select **Create signed certificate** from the context menu.



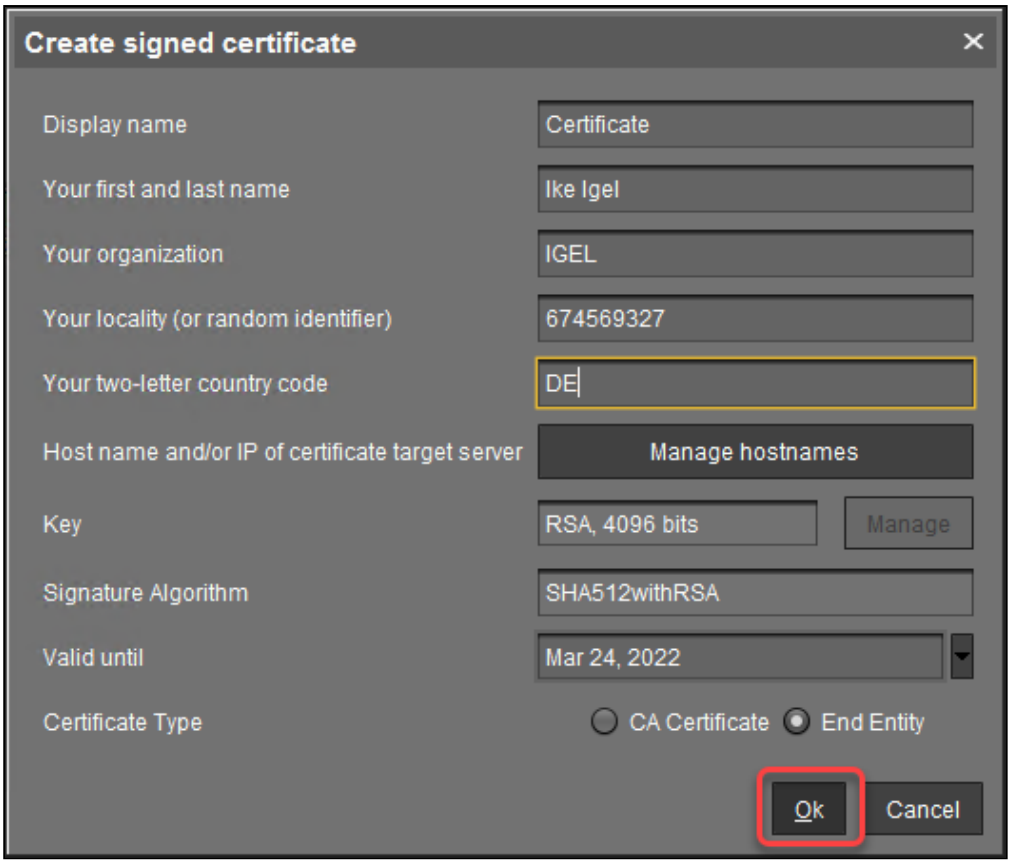
3. Select **Create one end certificate for all (known) servers** and then confirm with **Ok**.



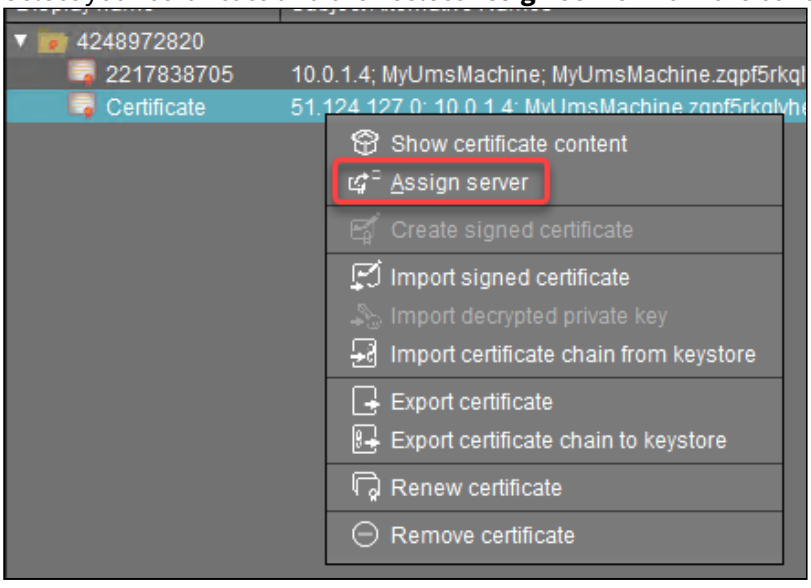
4. Fill in the details as appropriate.
5. Click **Manage hostnames** to verify if the internal IP Address and the public IP address are included.



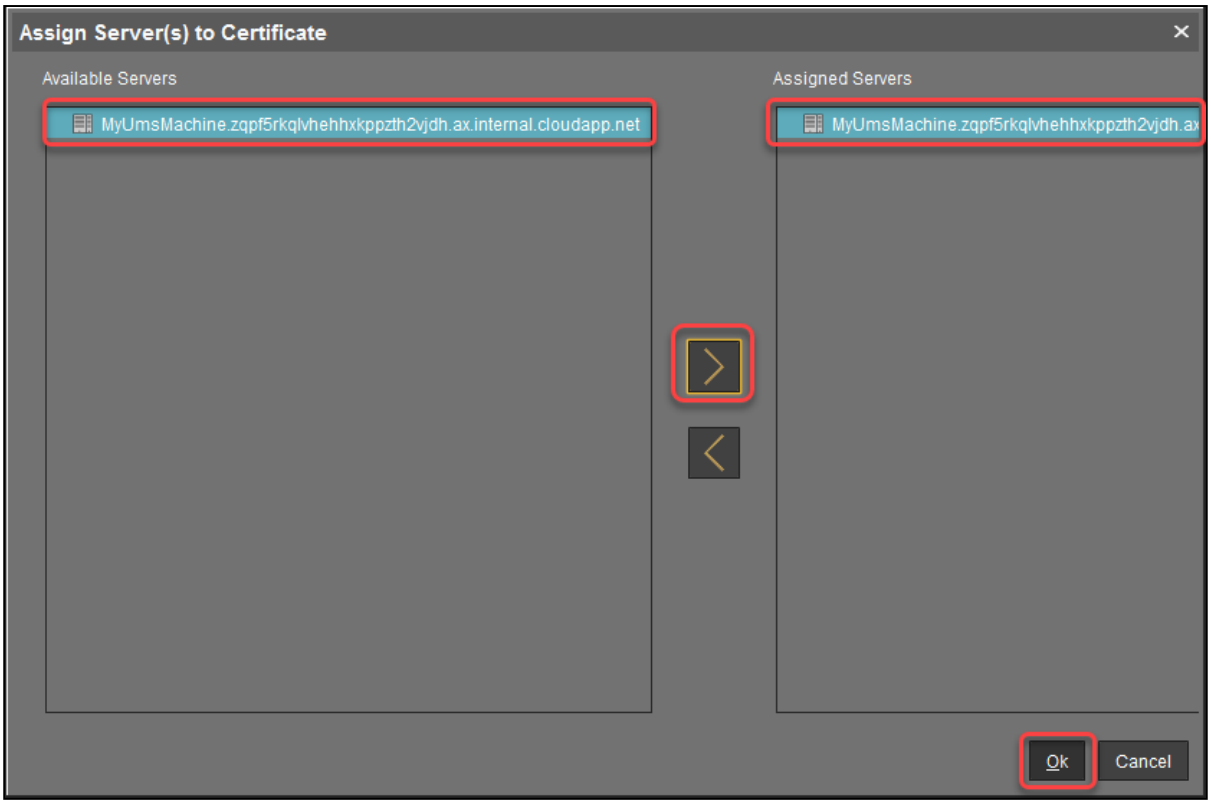
6. Review your settings and click **Ok**.



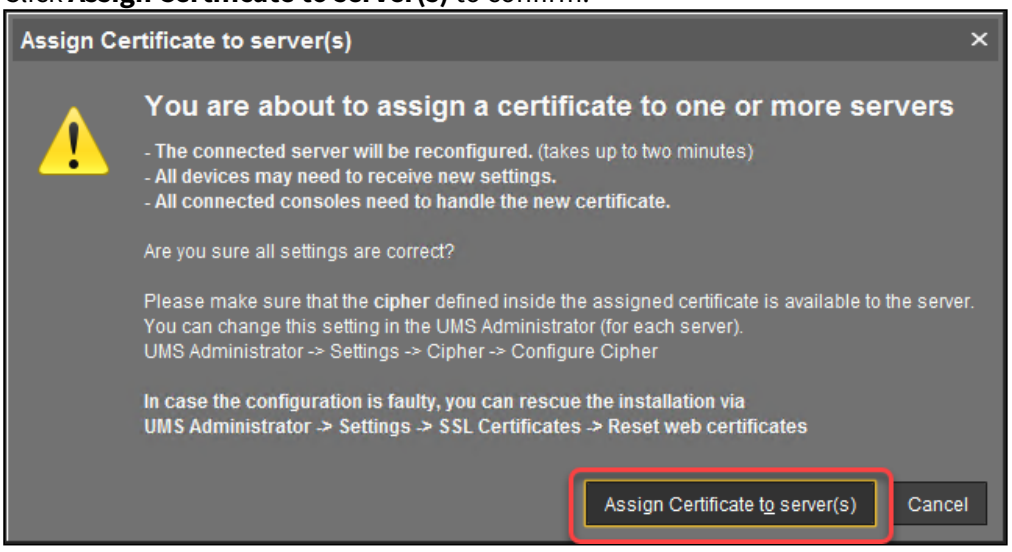
7. Select your certificate and then select **Assign server** from the context menu.



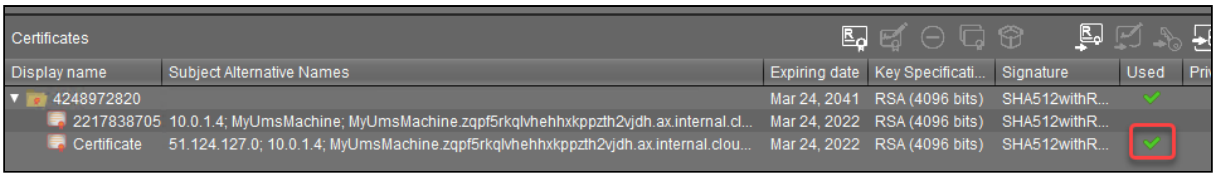
8. Assign your server to the certificate and confirm with **Ok**.



9. Click **Assign Certificate to server(s)** to confirm.



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



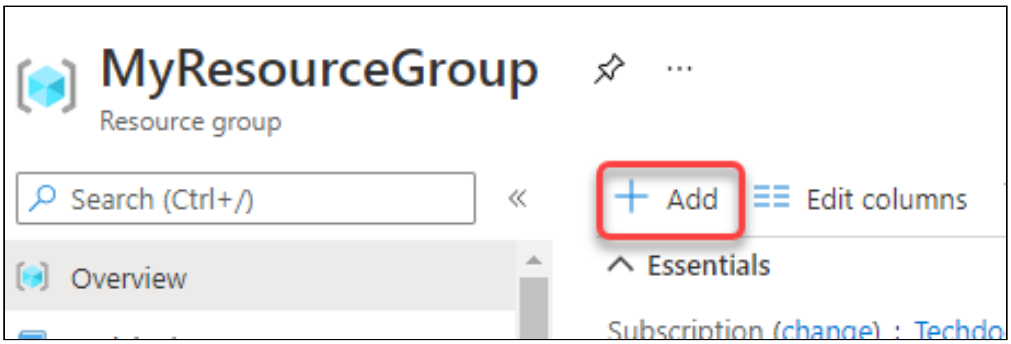
At this point, you can safely connect to your UMS from a local machine as well as from remotely installed UMS Consoles. For clarity purposes, we will still use the UMS Console on Azure.

Downloading the Installer for IGEL Cloud Gateway (ICG)

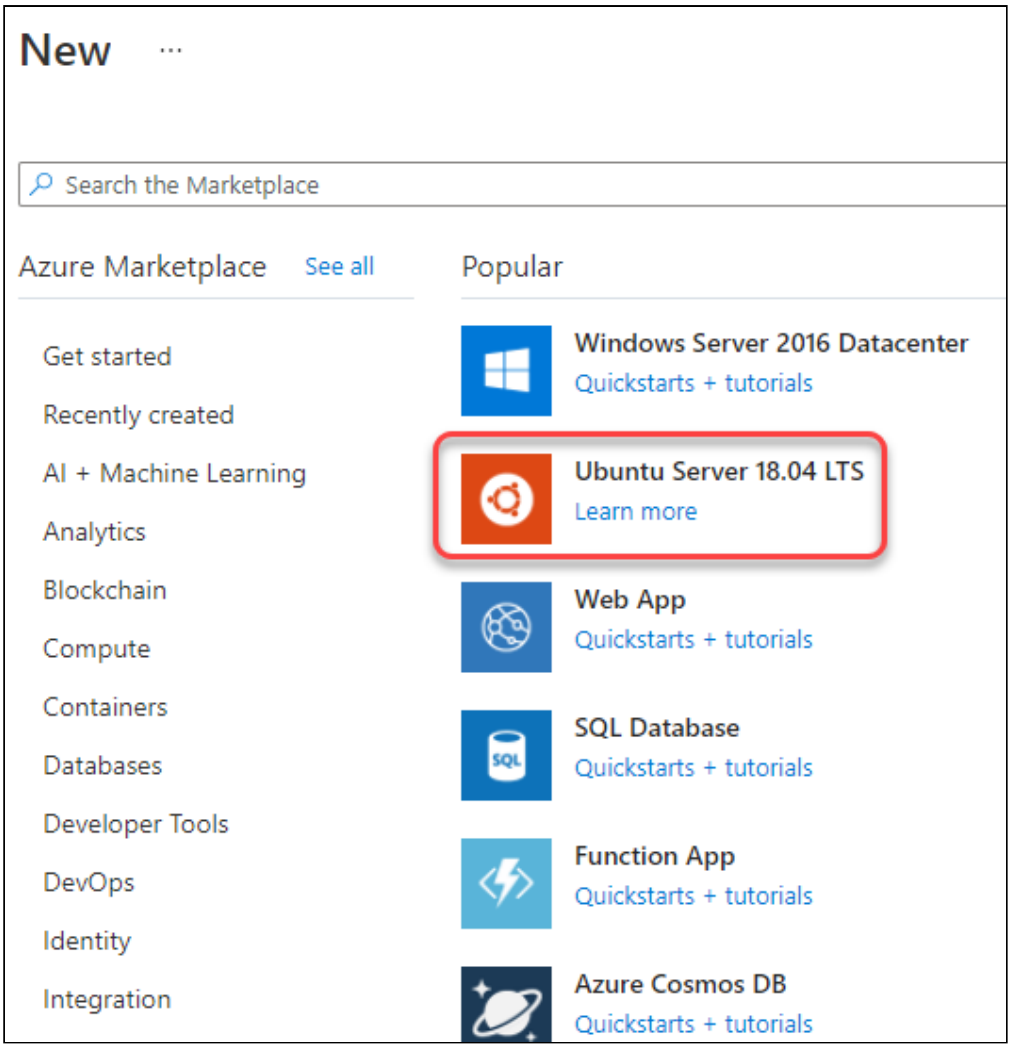
→ With a web browser, download the ICG installer from the **IGEL Download Server**[21] **> IGEL CLOUD GATEWAY (ICG)**. (Example: `installer-2.02.110.bin`) You can do this on the virtual machine or use your local machine and then copy the file to your virtual machine via RDP (clipboard).

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**.



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

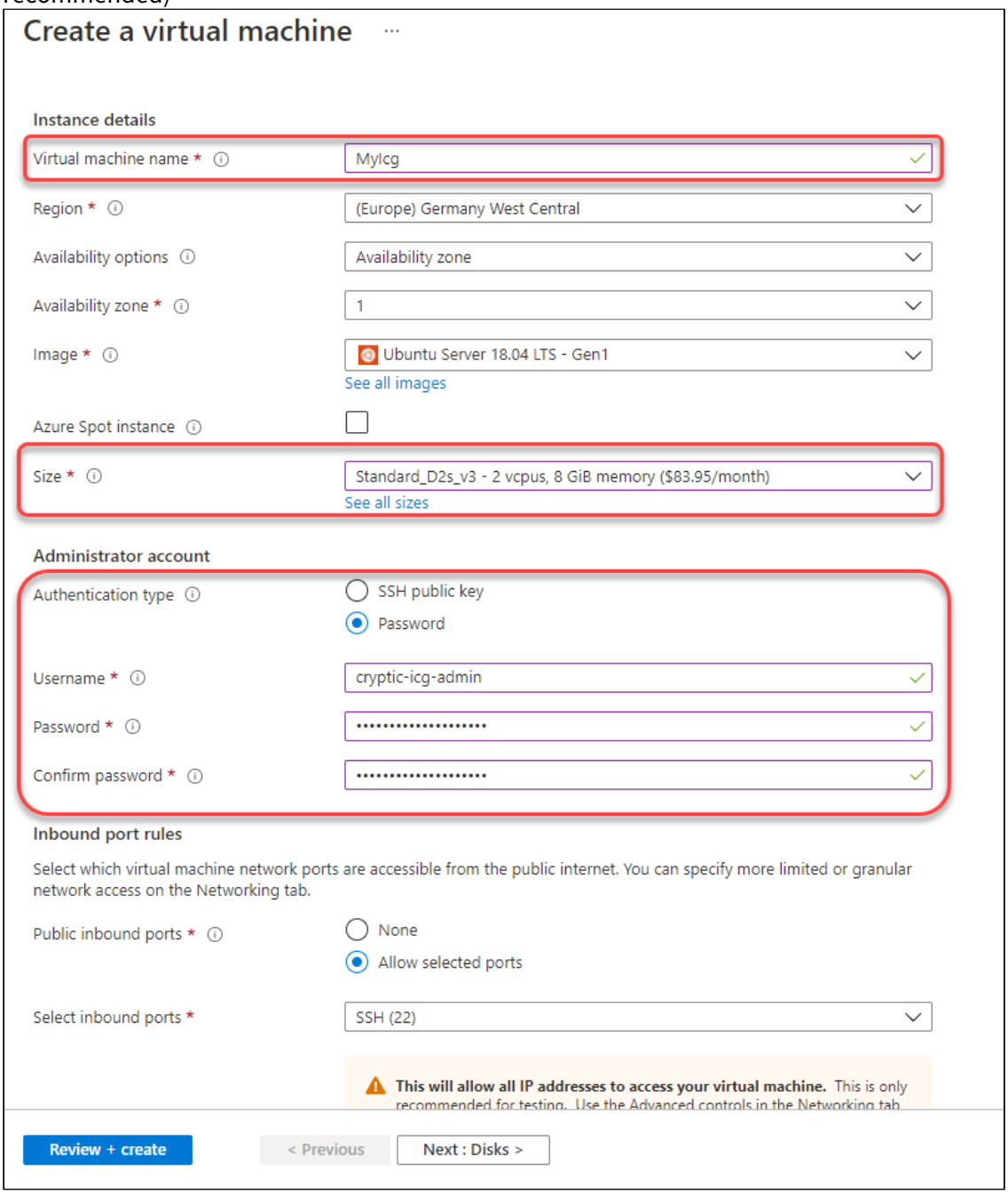


2. Edit the settings as follows:
   - **Resource group**: This must be set to the resource group we have created before (in our example: MyResourceGroup).
   - **Virtual machine name**: Enter a name for the virtual machine.
   - **Size**: “D2s v3” (2 CPUs/8 GiB RAM) or higher is recommended.
   - **Authentication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

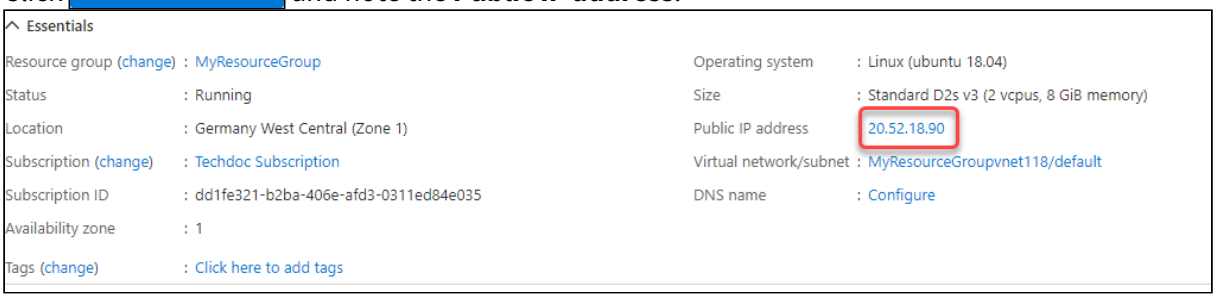
     ⚠ For security reasons, the username should be long (20 to 30 characters) and cryptic.

> **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)

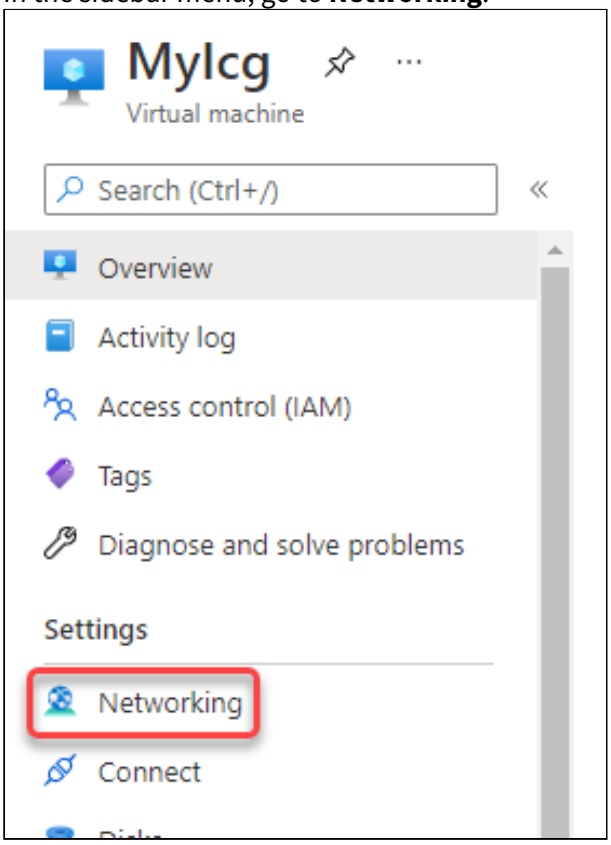


3. Click **Review + create** and review the settings.
4. Click **Create**.
5. Click **Go to resource** and note the **Public IP address**.



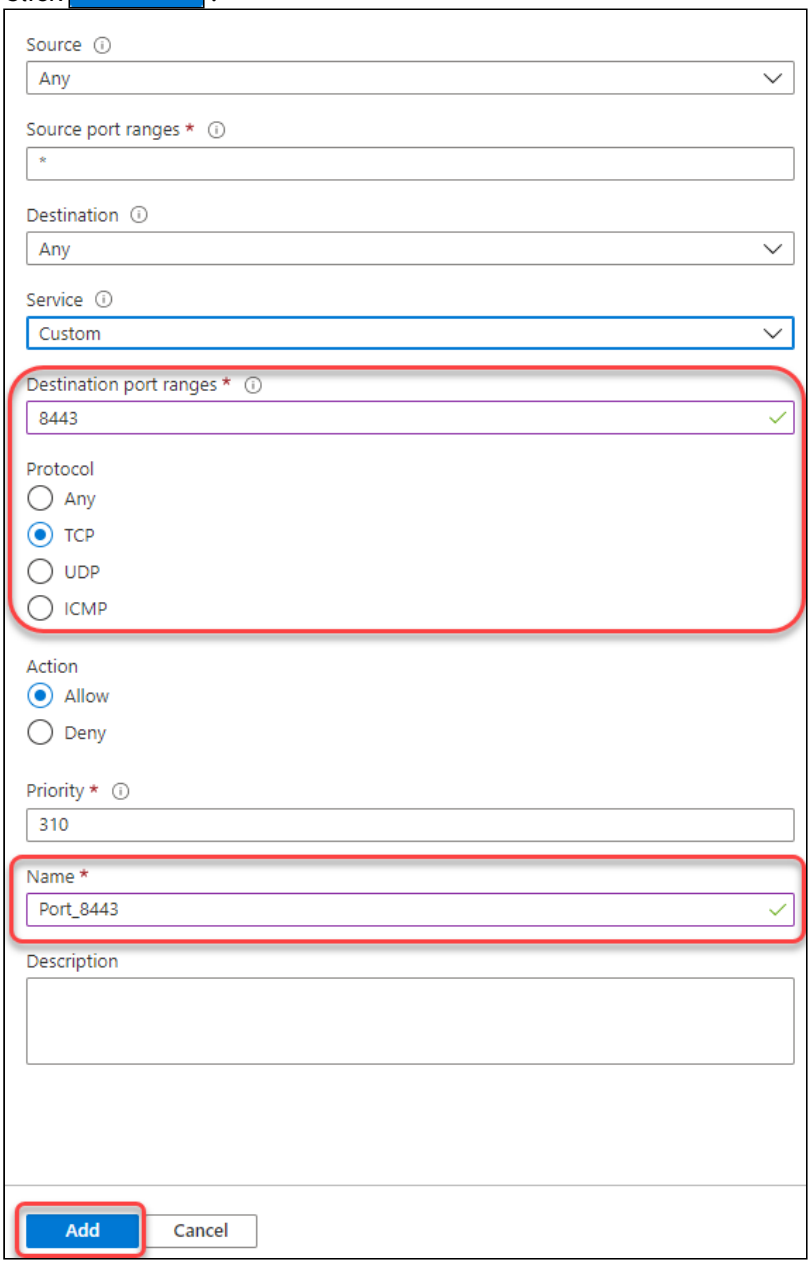
Configuring the IGEL Cloud Gateway Server

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 .



Installing the IGEL Cloud Gateway

1. Follow the instructions under Providing the Certificates[22].
2. Follow the instructions under Installing the IGEL Cloud Gateway[23].

Connecting the Devices

→ Follow the instructions under Connecting the Devices[24].

22. https://kb.igel.com/en/igel-cloud-gateway/current/providing-the-certificates
23. https://kb.igel.com/en/igel-cloud-gateway/current/installing-the-igel-cloud-gateway
24. https://kb.igel.com/en/igel-cloud-gateway/current/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.

For the supported operating systems, see the "Supported Environment" section of the release notes (see page 1440).

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

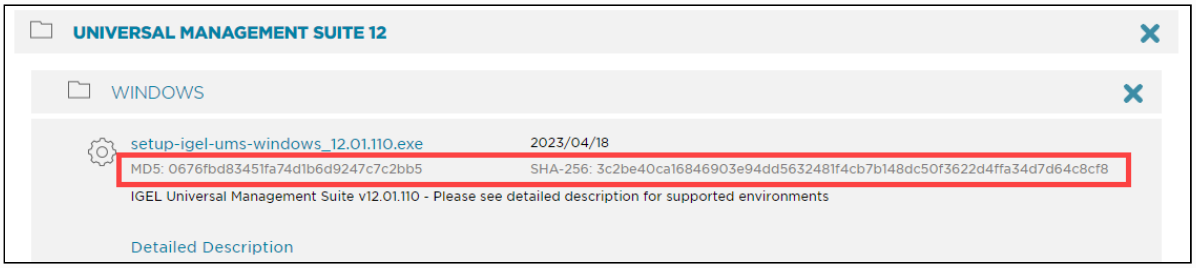
Standard Installation of the UMS

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

1. Familiarize yourself with security recommendations on user access under Best Practices for User Access to IGEL UMS Server and create the user to run the UMS Tomcat Server.

2. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server[25].

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



3. Launch the installer. You need administrator rights to install the UMS.

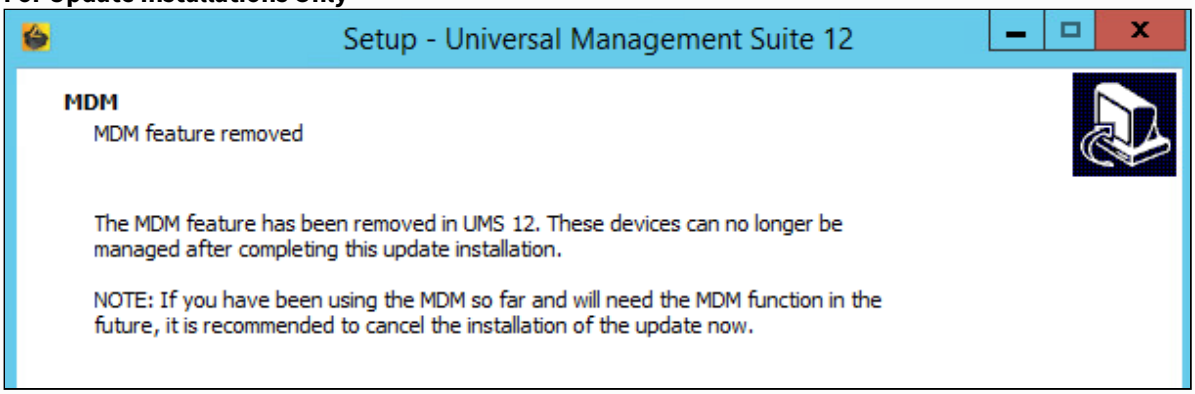
4. Read and confirm the **License Agreement**.

5. Read the **Information** regarding the installation process and click **Next**.

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

6. 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.

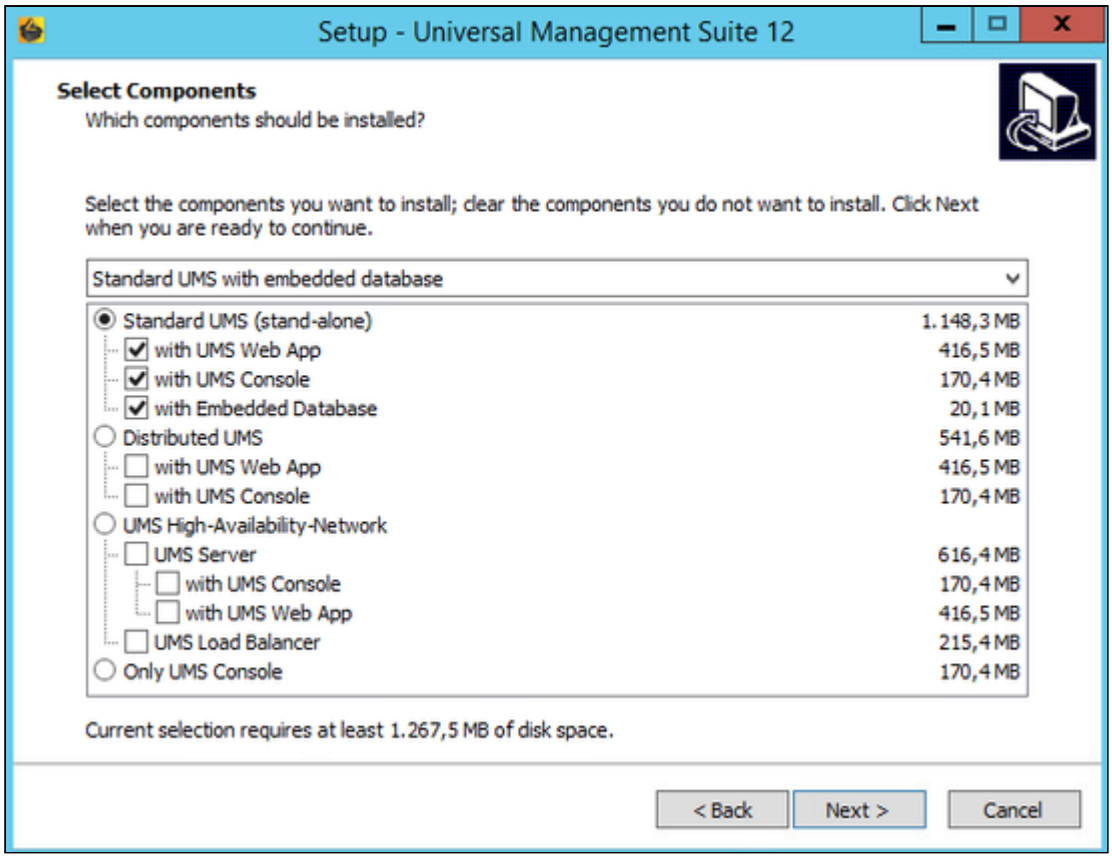
For Update Installations Only



As of UMS 12, the 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.
For standard UMS update installations, selecting the checkbox **with Embedded Database** has no effect.

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

8. Choose the components to be installed under **Select Components**. The selected components will define the installation type.
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.



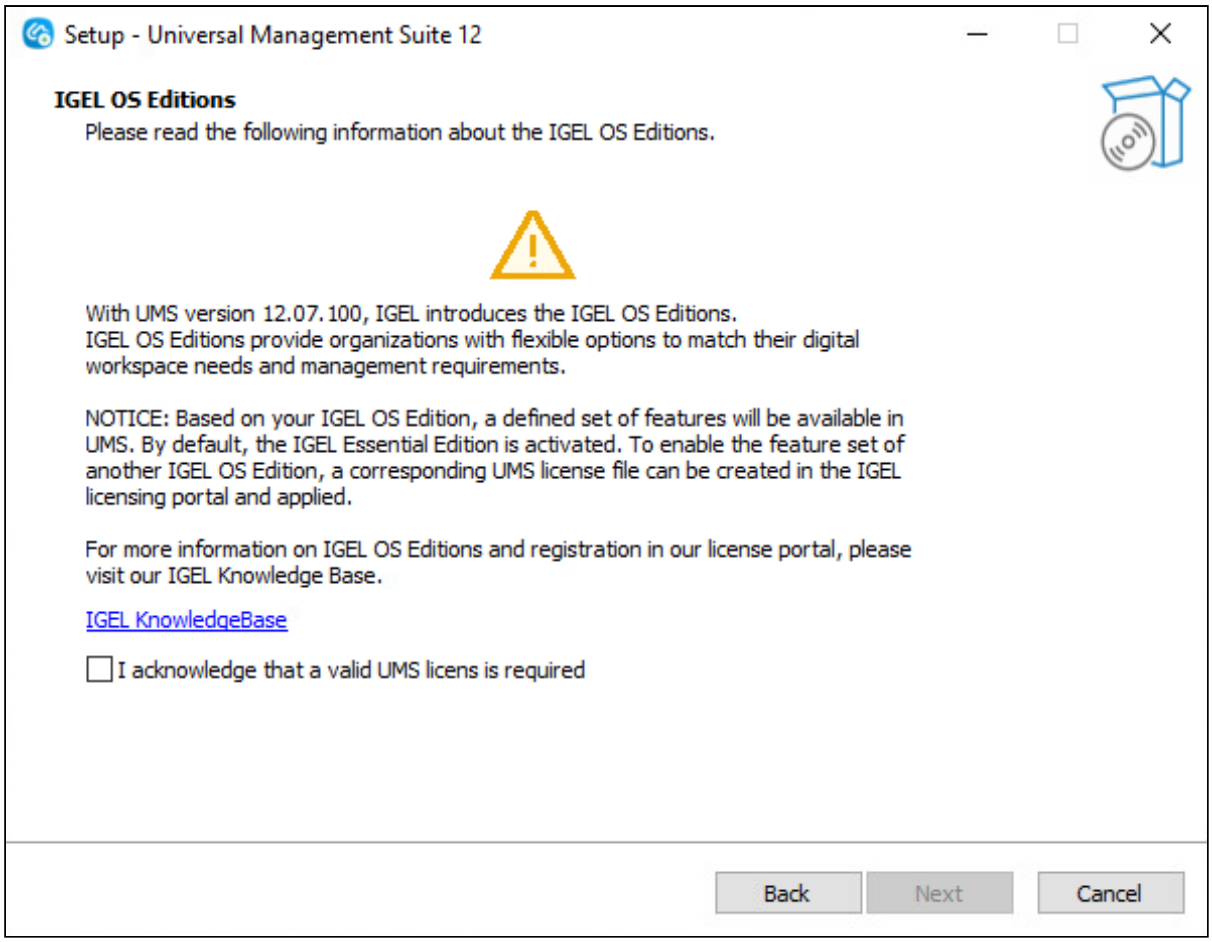
The embedded database is suitable for most purposes. If not disabled, the embedded database will automatically be installed if you select **Standard UMS**.
The use of an external database system is recommended in the following cases:

- 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.

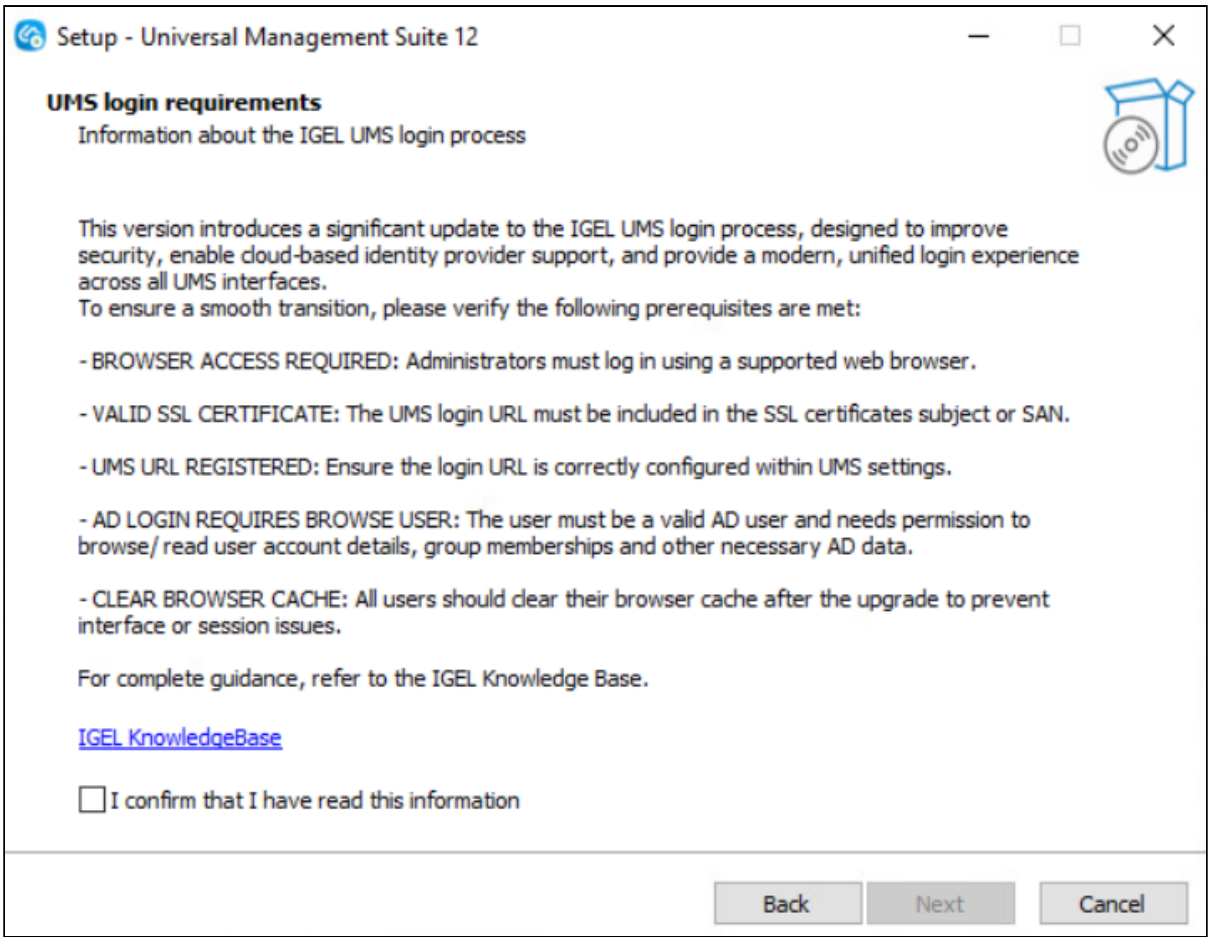
9. Read and confirm the information regarding IGEL OS Editions and UMS Licenses[26] and click **Next**.

26. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums

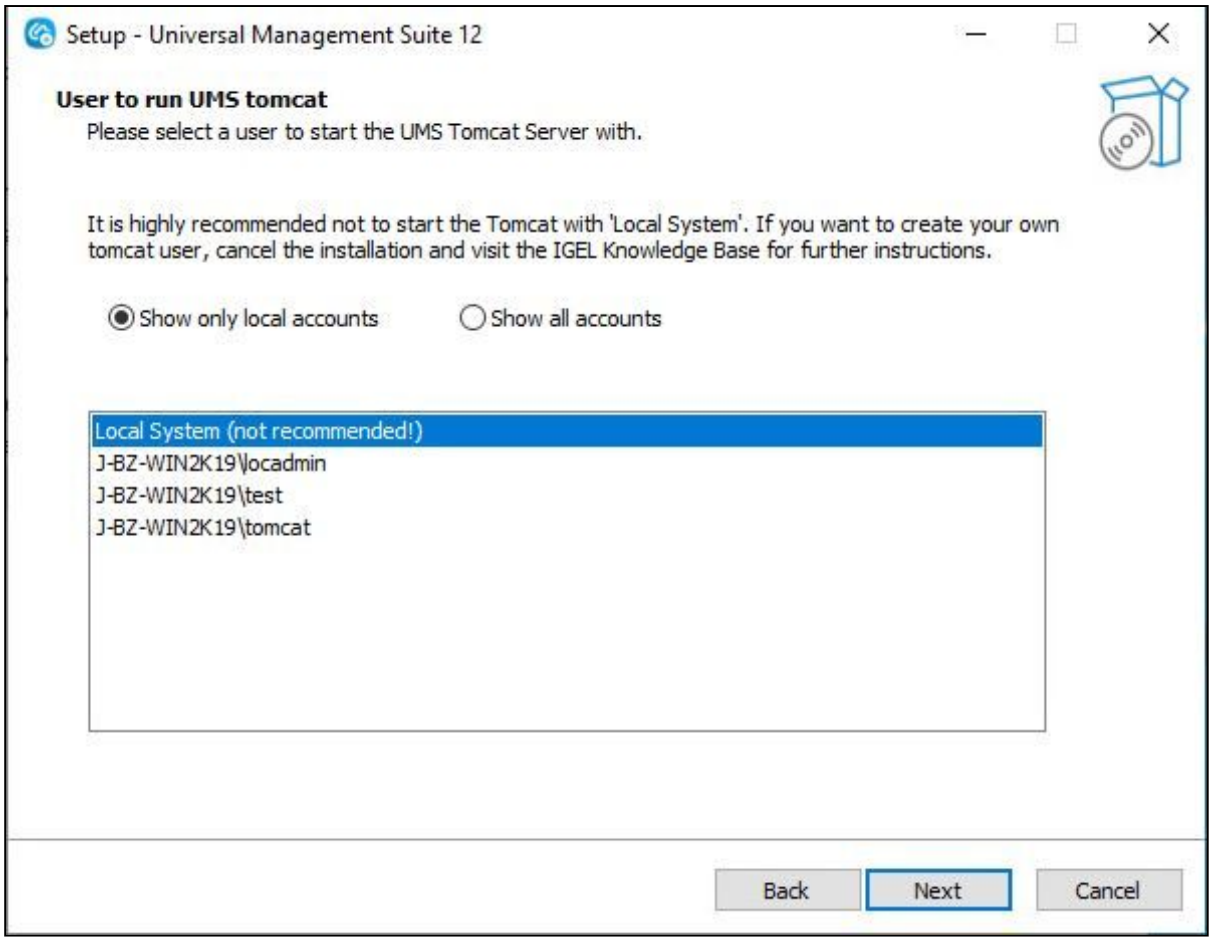


10. Read and confirm information about the **UMS login requirements**. For more information, see UMS Login Requirements[27].

27. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements



11. Select the user to run the UMS Tomcat Server. The user needs to be created before the installation, so if the user is not yet configured, cancel the installation and restart once the user is created. If **Show all accounts** is selected, you can also select users from domain-joined devices (for example, Active Directory).



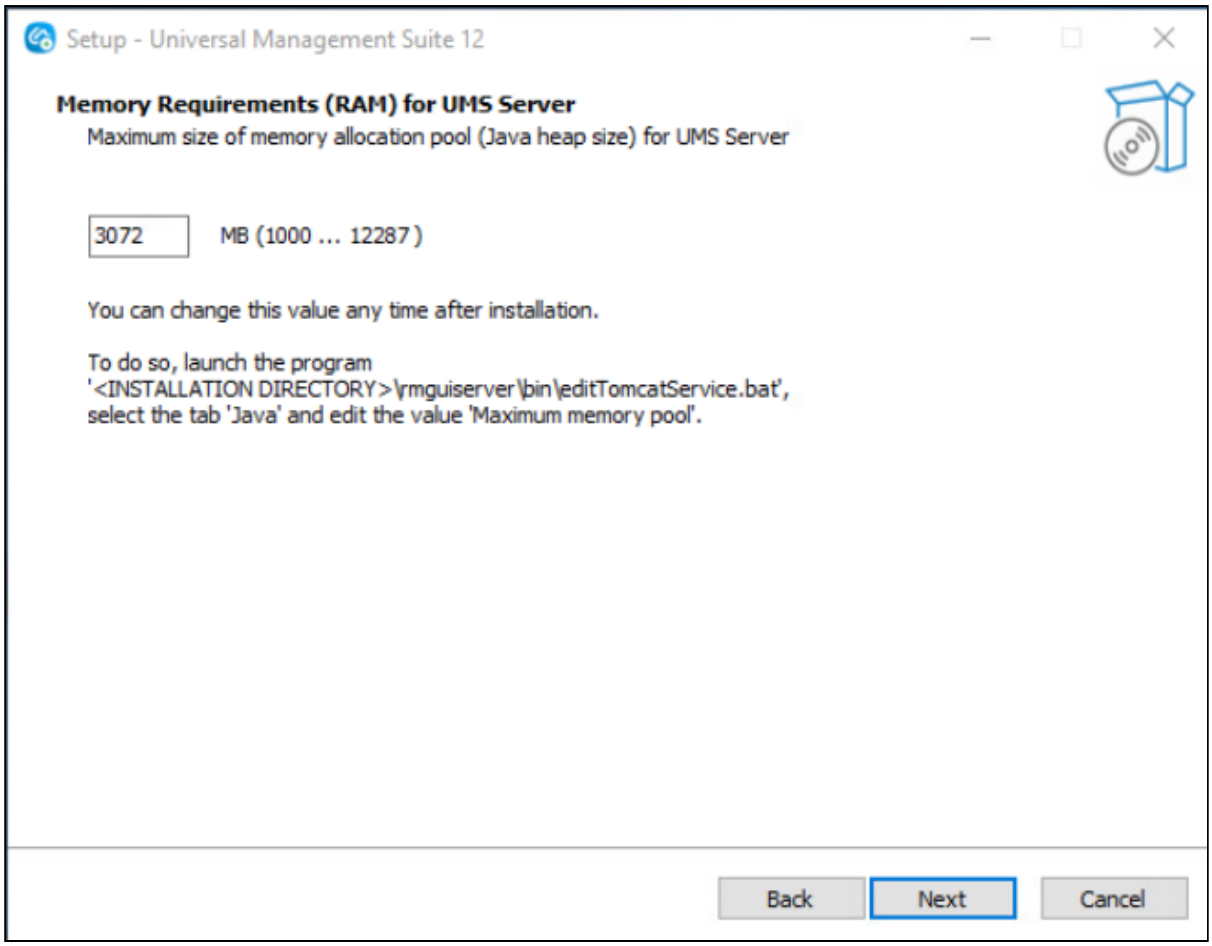
We strongly recommend using a user with minimal authorizations in order to follow the principle of least privilege and increase system security. For more information, see Best Practices for User Access to IGEL UMS Server.

Note for domain environments

The service user specified during installation is automatically added to the local security policy `Log on as a service`. In Active Directory environments, this right may be centrally managed by Group Policy Objects (GPOs), which can override local settings. Ensure that the service account is also explicitly granted the `Log on as a service` right within the applicable GPOs. Otherwise, the service will not be able to start.

12. Enter the user password and click **Next**.

13. 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.



14. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.

15. Select the **UMS data directory**. (Default: `C:\Program Files\IGEL\RemoteManager`)

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

17. 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 Universal Management Suite Network Configuration) 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.

18. Choose a folder name under **Select Start Menu Folder**.

19. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and UMS Administrator on the desktop.

20. 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.

21. 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.

22. Start the UMS Console.

23. Connect the UMS Console to the UMS Server using the access data for the database that you entered during the installation. See Connecting the UMS Console to the IGEL UMS Server[28].

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

28. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server

- 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

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.

For the management of IGEL OS 12 devices, it is necessary to register your UMS after the installation, see Registering the IGEL UMS.

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.

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 large size of your IGEL Universal Management Suite (UMS) installation, you have decided to install the UMS Console on a separate client machine, not on the UMS Server host. For more on installation sizes, see Installation and Sizing Guidelines for IGEL UMS (see page 231).

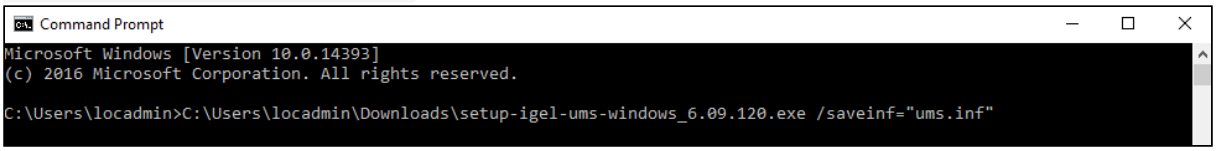
You can use the following instructions for an unattended / silent installation of the UMS Console. They are also applicable when you updated the UMS Server and, thus, need to update the UMS Console on the client machines.

> 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:

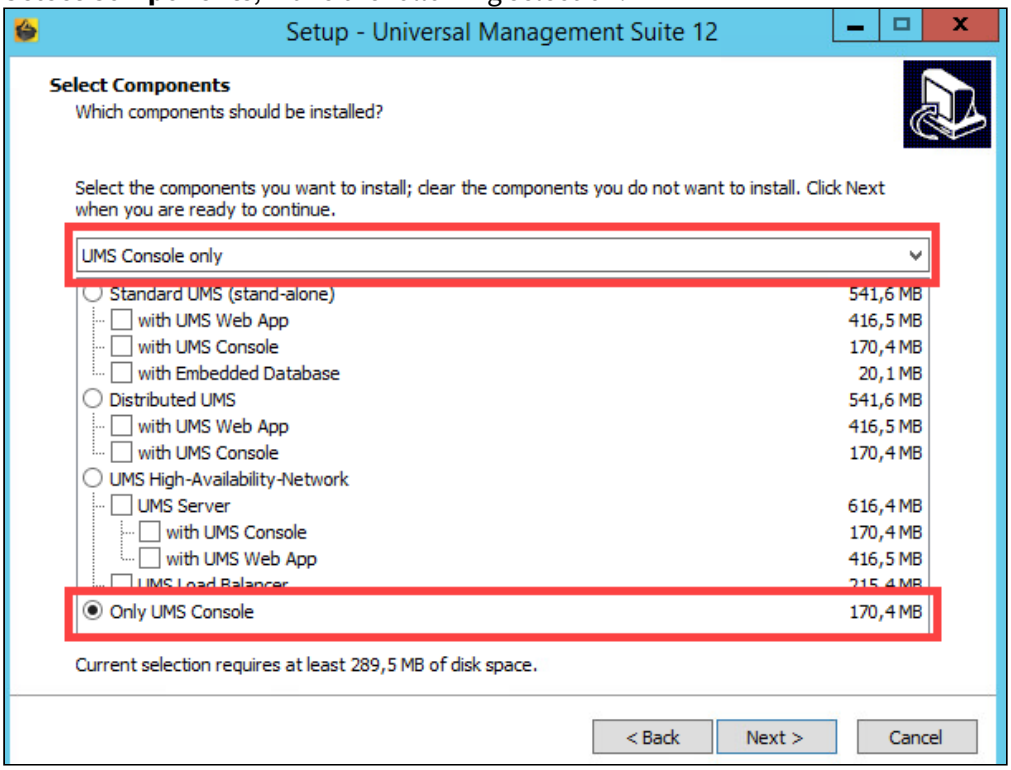
1. Download the IGEL UMS from the IGEL Download Server[29]. Select the same version you used for the installation / update of the UMS Server.
2. In `cmd` or `powershell`, create a config file using the following command:
   `C:\[download directory]\setup-igel-ums-windows_x.y.z.exe /saveinf="[config-file]"`



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

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

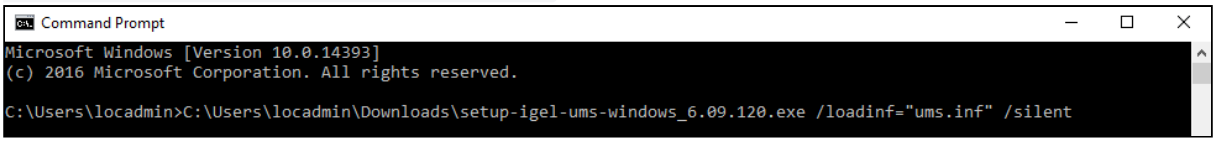
4. Use the wizard displayed to complete the installation while recording it to the config file. Under **Select Components**, make the following selection:



> 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:

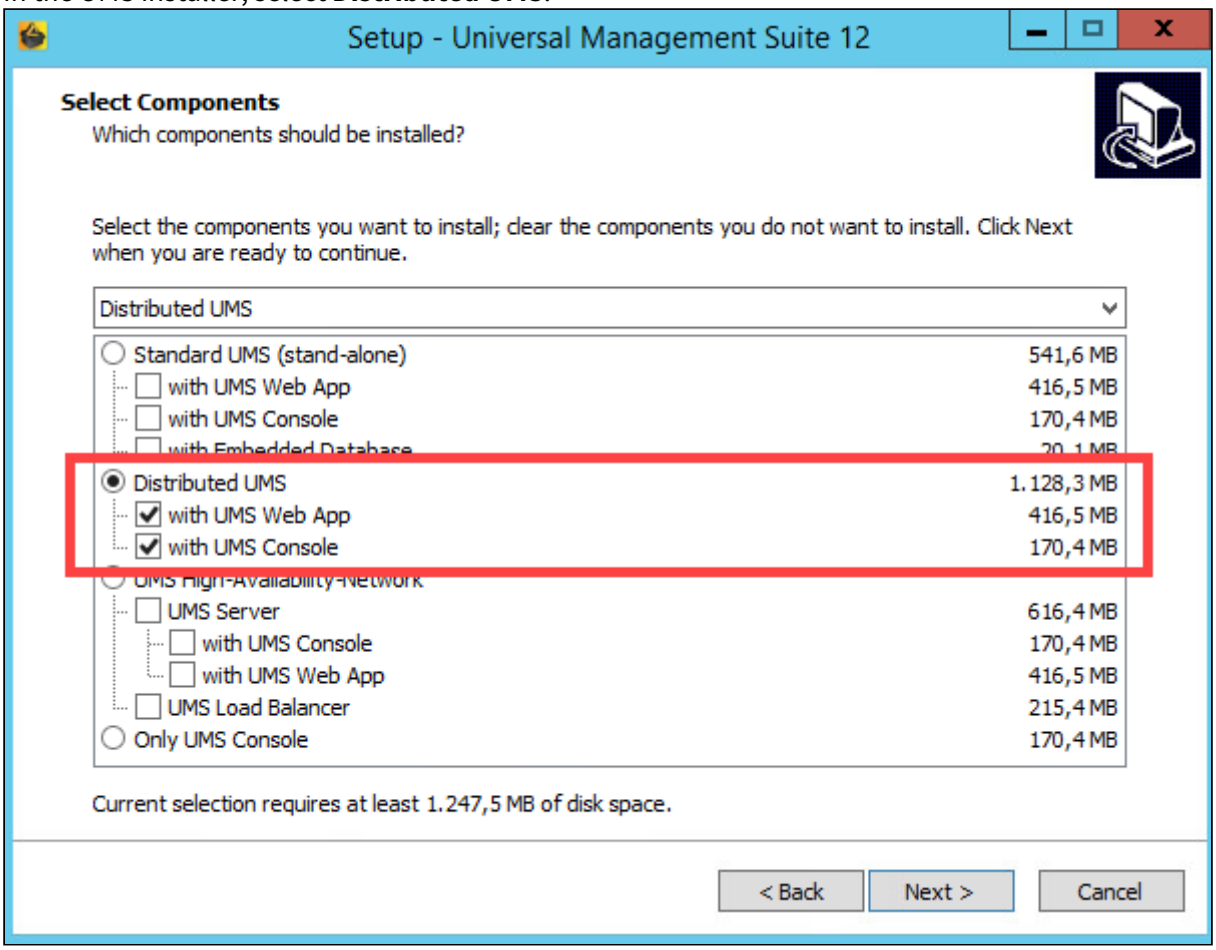
- if you plan a new installation of the Distributed UMS
- if you already have a standard UMS installation but want to switch to the Distributed UMS

> 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 48) or IGEL UMS Installation under Linux (see page 17).
   In the UMS installer, select **Distributed UMS**.



2. Configure an external database, see Connecting External Database Systems (see page 63).
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 1073).
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.

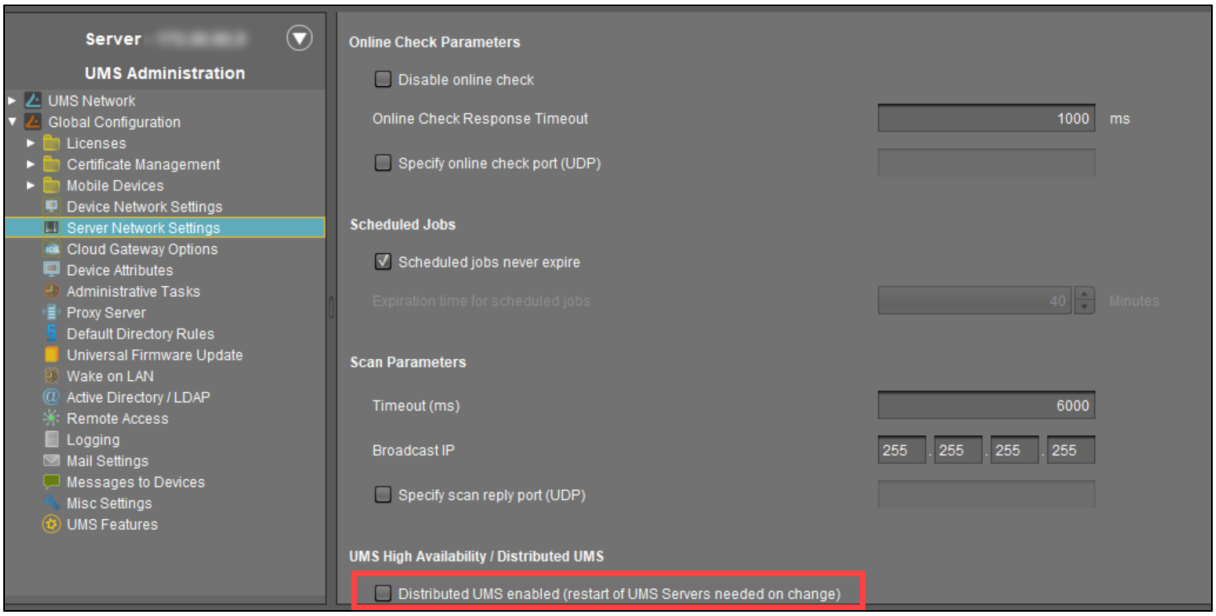
⚠ If you activated the Distributed UMS feature and have multiple UMS Servers, take care in case you decide to disable the feature. If the Distributed UMS feature is deactivated but more than one UMS Server is using the same database, no synchronization will be done between the UMS Servers.

Switching from the Standard UMS to the Distributed UMS

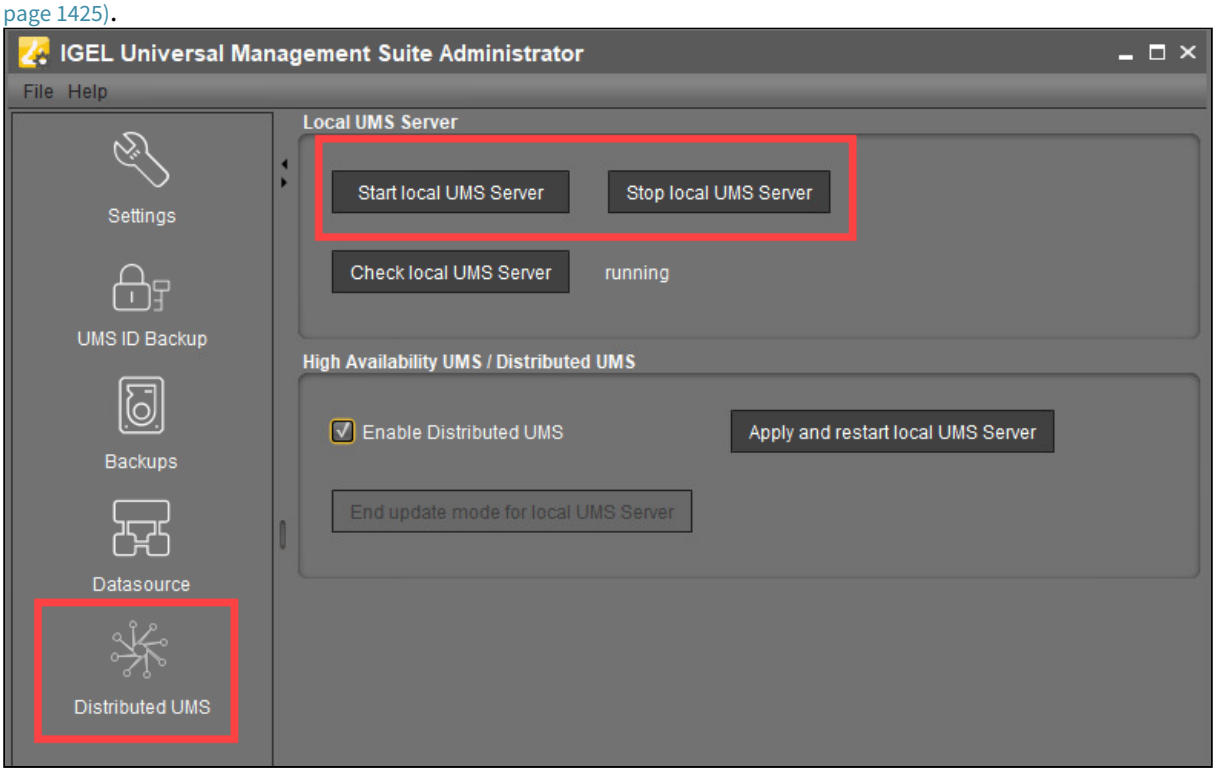
If you want to extend your existing standard UMS installation to the Distributed UMS, proceed as follows:

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 63)) 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 1073)).
2. Copy the embedded database to the new external data source, see Copying a Data Source (see page 1065), and **activate** the new data source.

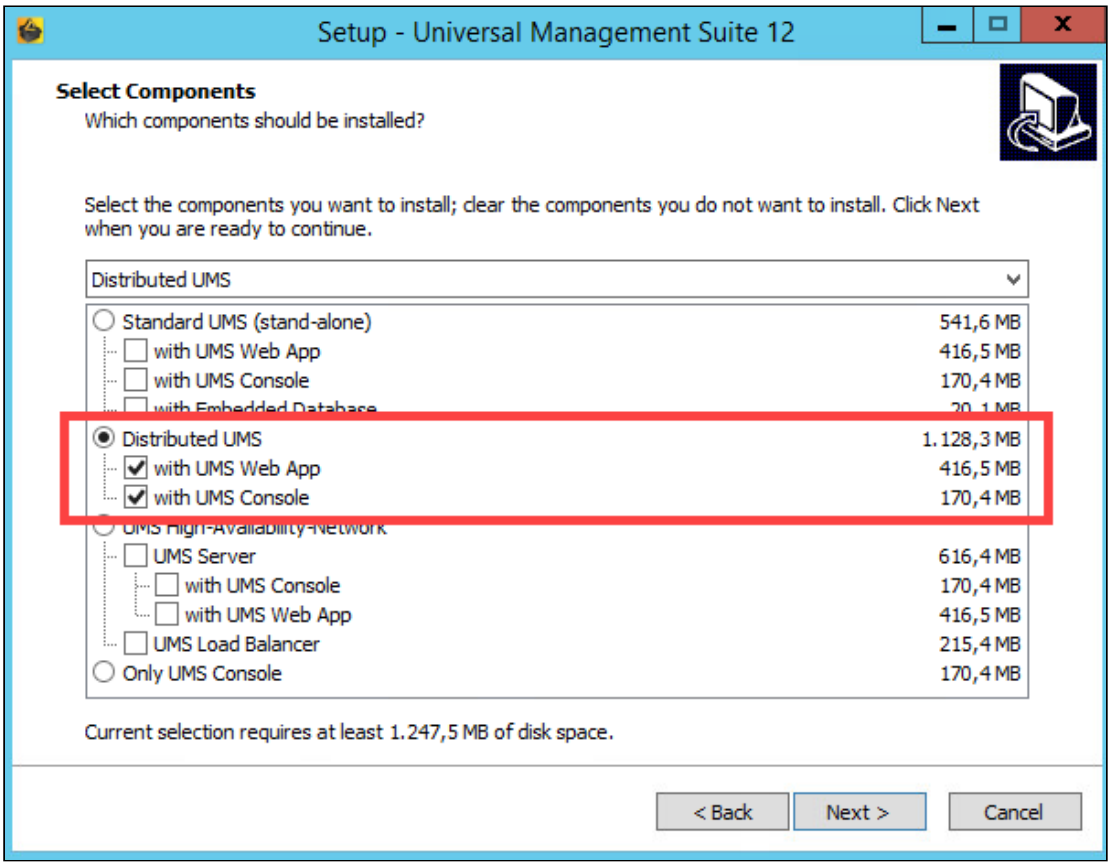
3. Open the UMS Console and go under **UMS Administration > UMS Network > Server** to check that the server is up and running.
4. Go under **UMS Administration > Global Configuration > Server Network Settings** and activate **Distributed UMS enabled**.



5. Restart the UMS Server service, e.g. via **UMS Administrator > Distributed UMS** (see page 1077). For detailed instructions on how you can restart services, see IGEL UMS HA Services and Processes (see page 1425).



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.

Connecting External Database Systems

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

- You manage a large network of devices.
- A dedicated database system is already in use in your company.
- You integrate the High Availability (see page 1387) 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 48) or IGEL UMS Installation under Linux (see page 17).

For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 1440). 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 1037) > Datasource (see page 1061).

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 1051).

See also How to Migrate a UMS Database From Embedded DB to Microsoft SQL Server (see page 446).

- Oracle (see page 64)
- Oracle RAC (see page 65)
- Microsoft SQL Server/Cluster with Native SQL Authentication (see page 66)
- Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84)
- Microsoft SQL Server/Cluster with Active Directory (AD) Authentication via Kerberos (see page 103)
- PostgreSQL (see page 125)
- Apache Derby as a Data Source for the IGEL UMS (see page 127)
- Using an AWS Aurora PostgreSQL Database with IGEL Universal Management Suite (UMS) (see page 128)
- Using an Azure SQL Managed Instance Database with IGEL UMS (see page 129)

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 * [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 1037), set up a new **Oracle** type data source.

Oracle RAC

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

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

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

2. Use the UMS Administrator (see page 1037) 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 * [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

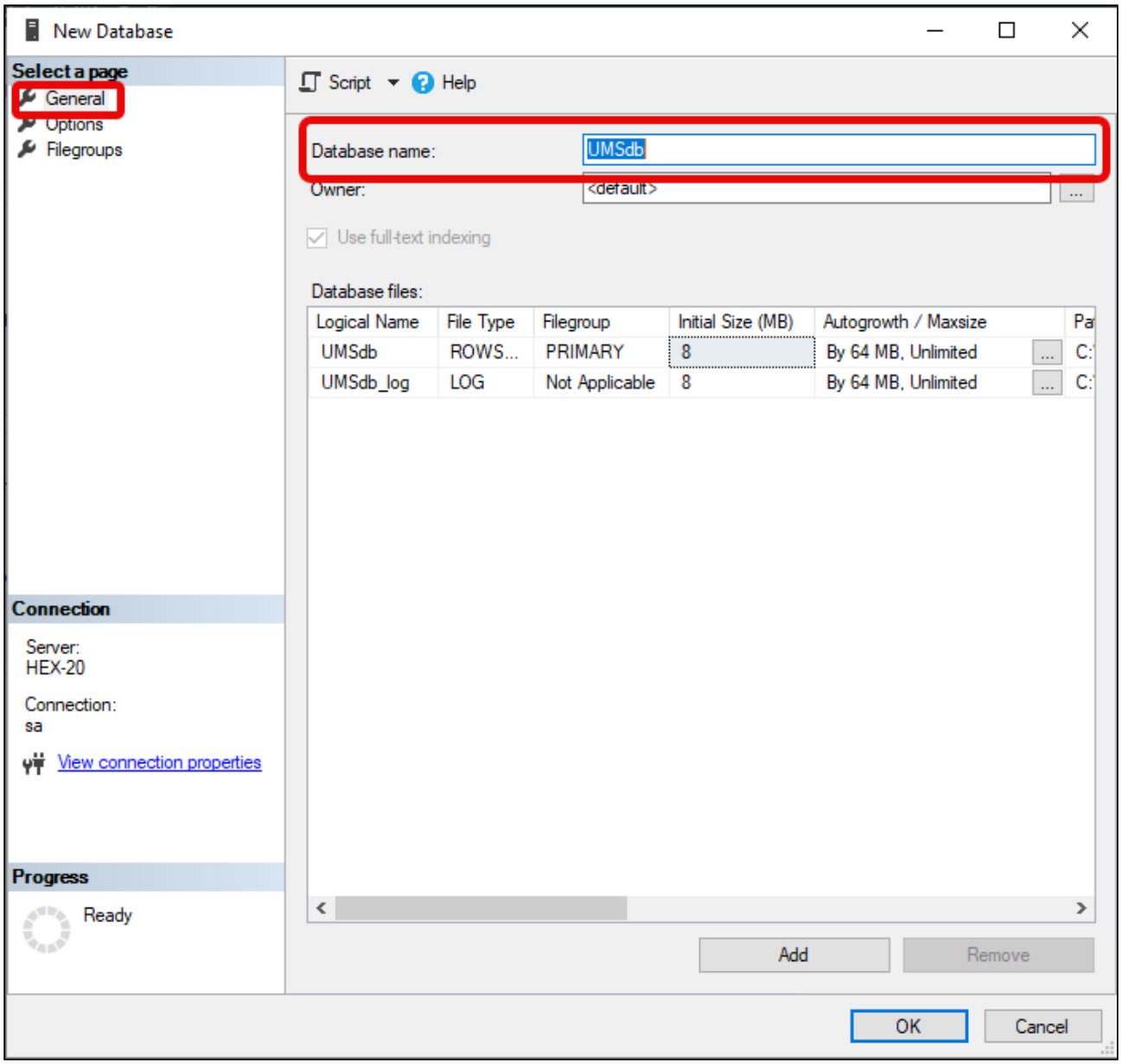
```
USE [master]
GO
CREATE DATABASE [<database_name>];
GO
USE [<database_name>];
GO
CREATE SCHEMA [<schema_name>];
GO
```

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

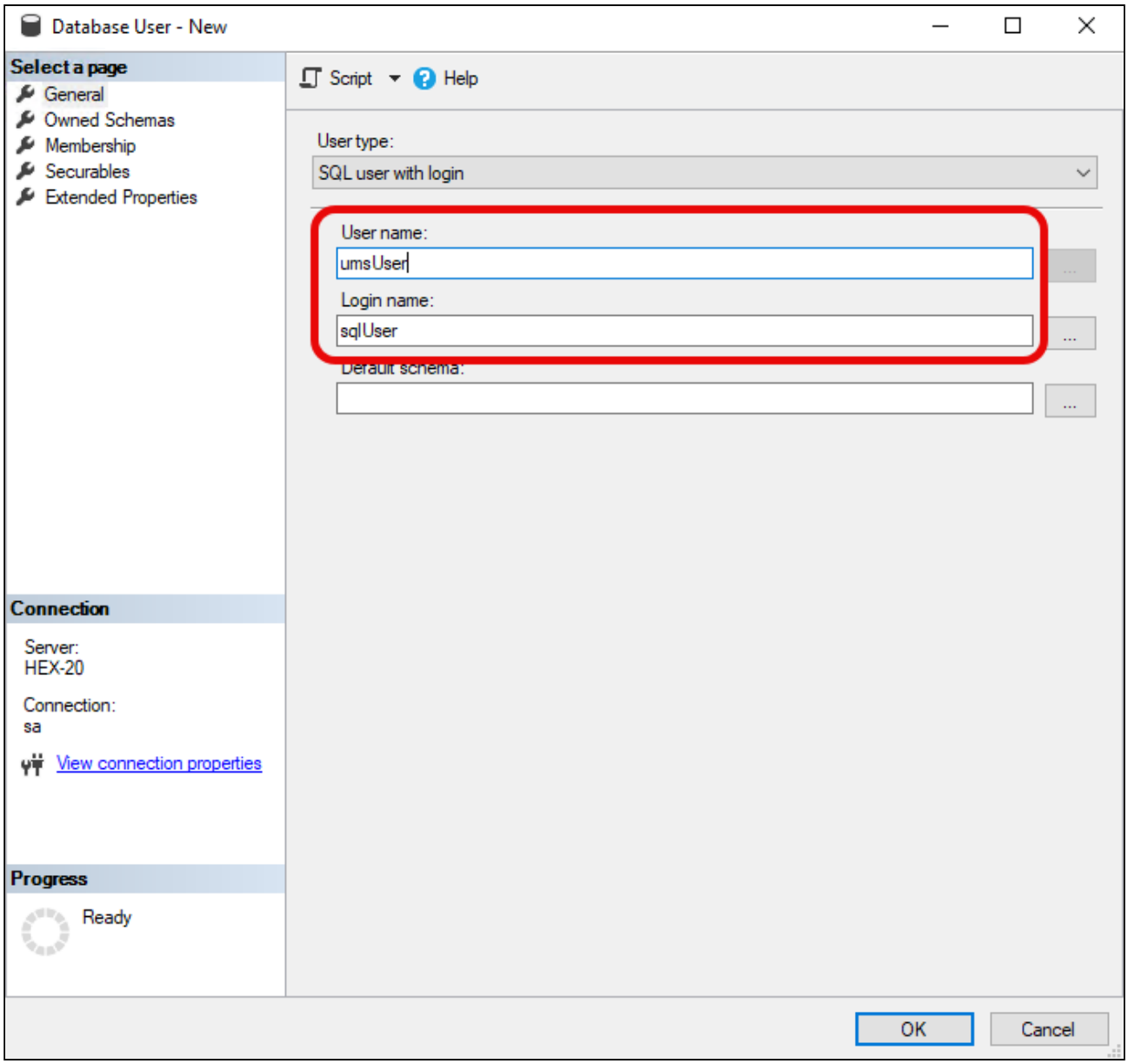
→ In the SQL Management Console, select **New Query** and enter the script below; please note the following.

- `<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.

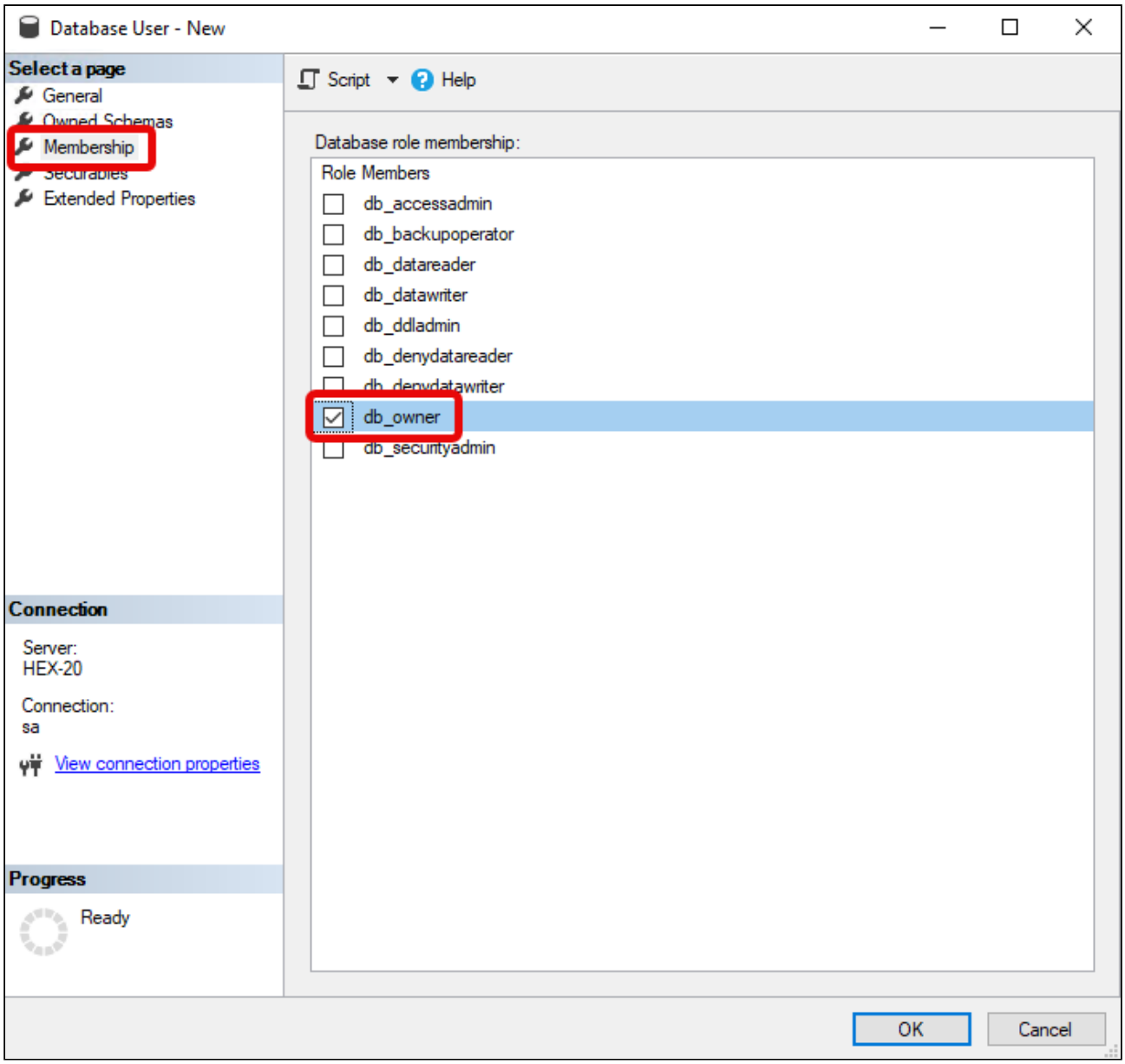
```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<sql_user];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

Using the GUI

1. In SQL Server Management Studio, open the database created in Creating the UMS Database (see page 66).
2. Under **Security > Users**, right-click **New User**.
3. Under **General**, search for your login name (`<sql_user>`) and give the user a name.

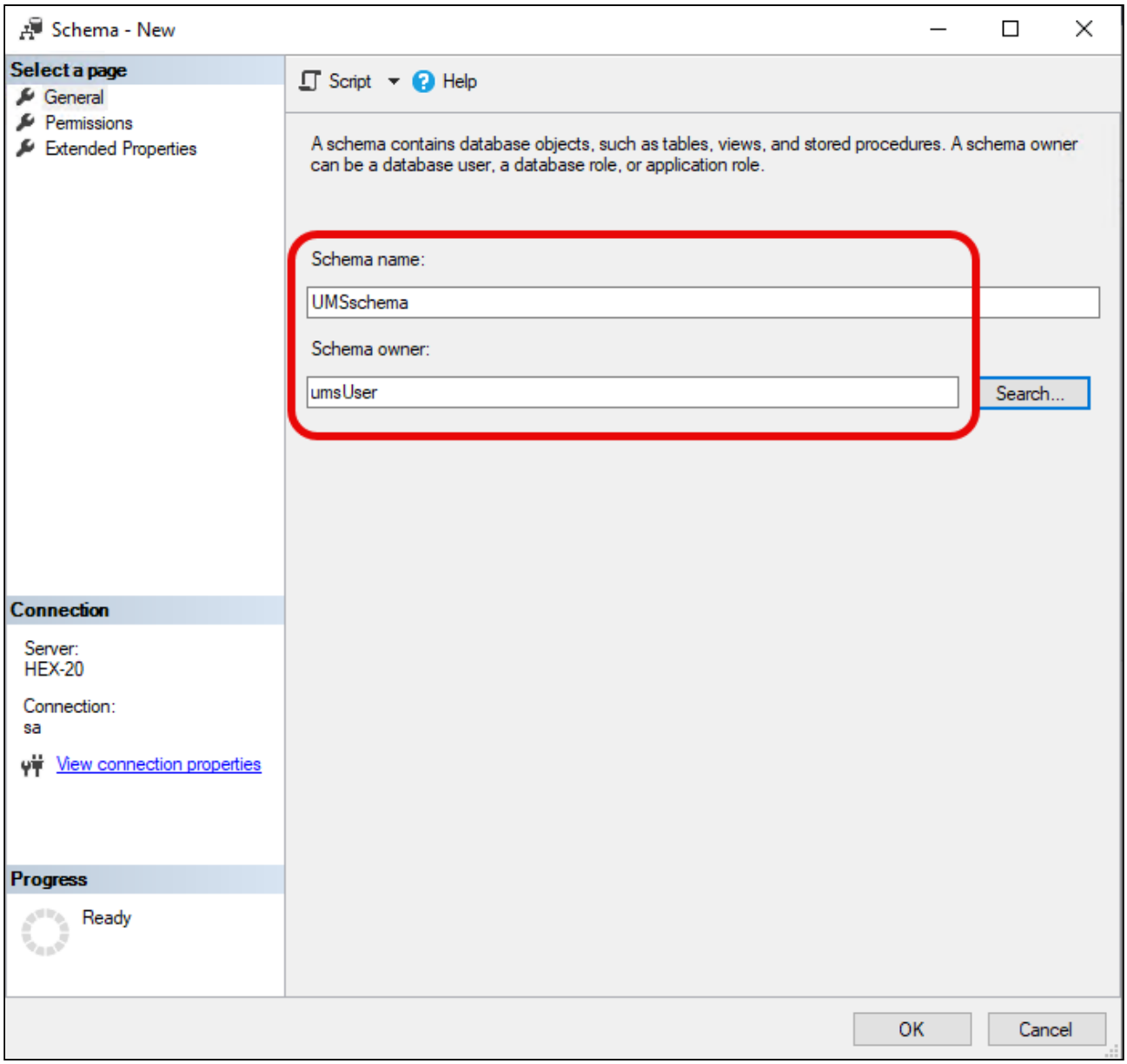


4. In the **Membership** area, give the user the **db_owner** role.



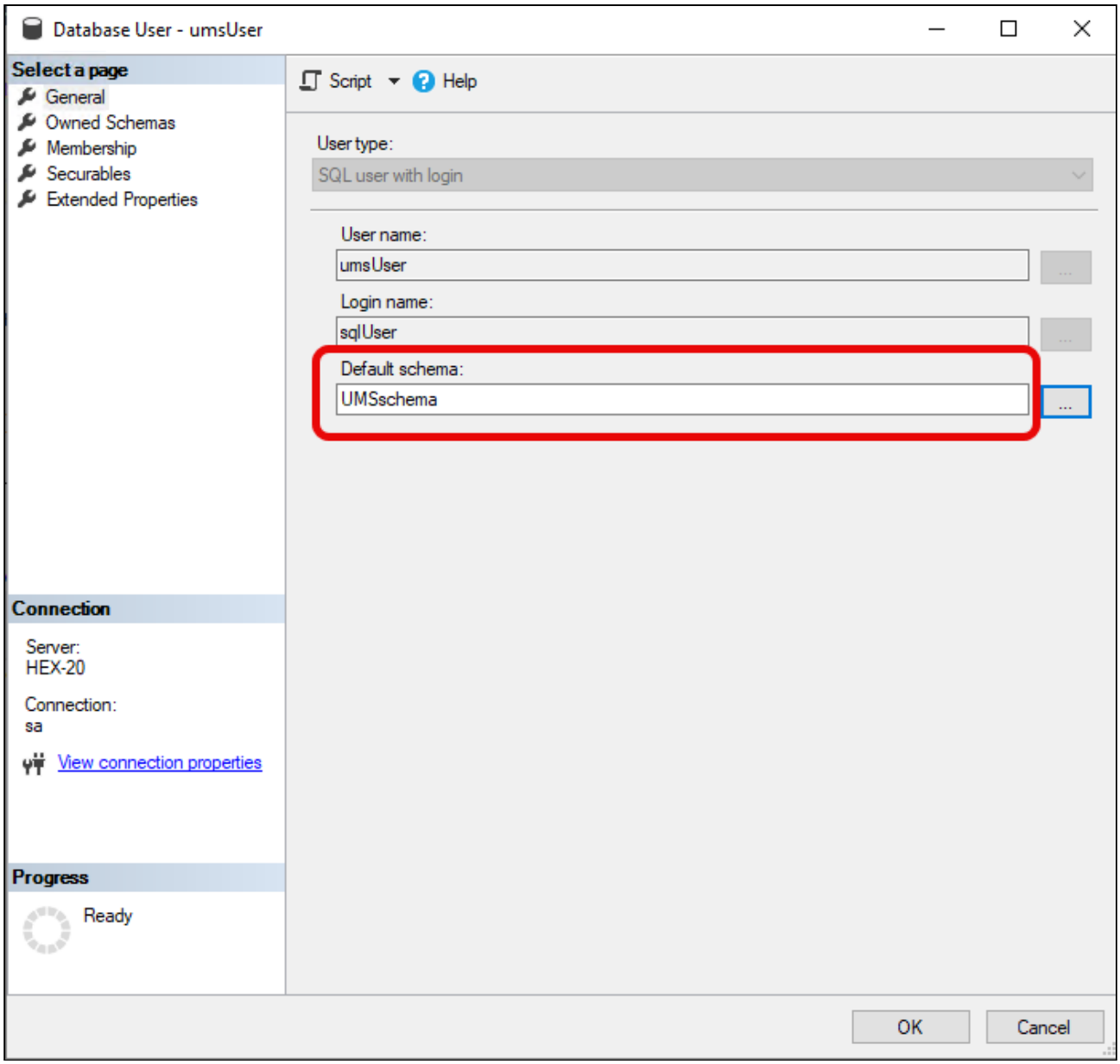
5. Go to **Security > Schemas** and right-click on **New Schema**.

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

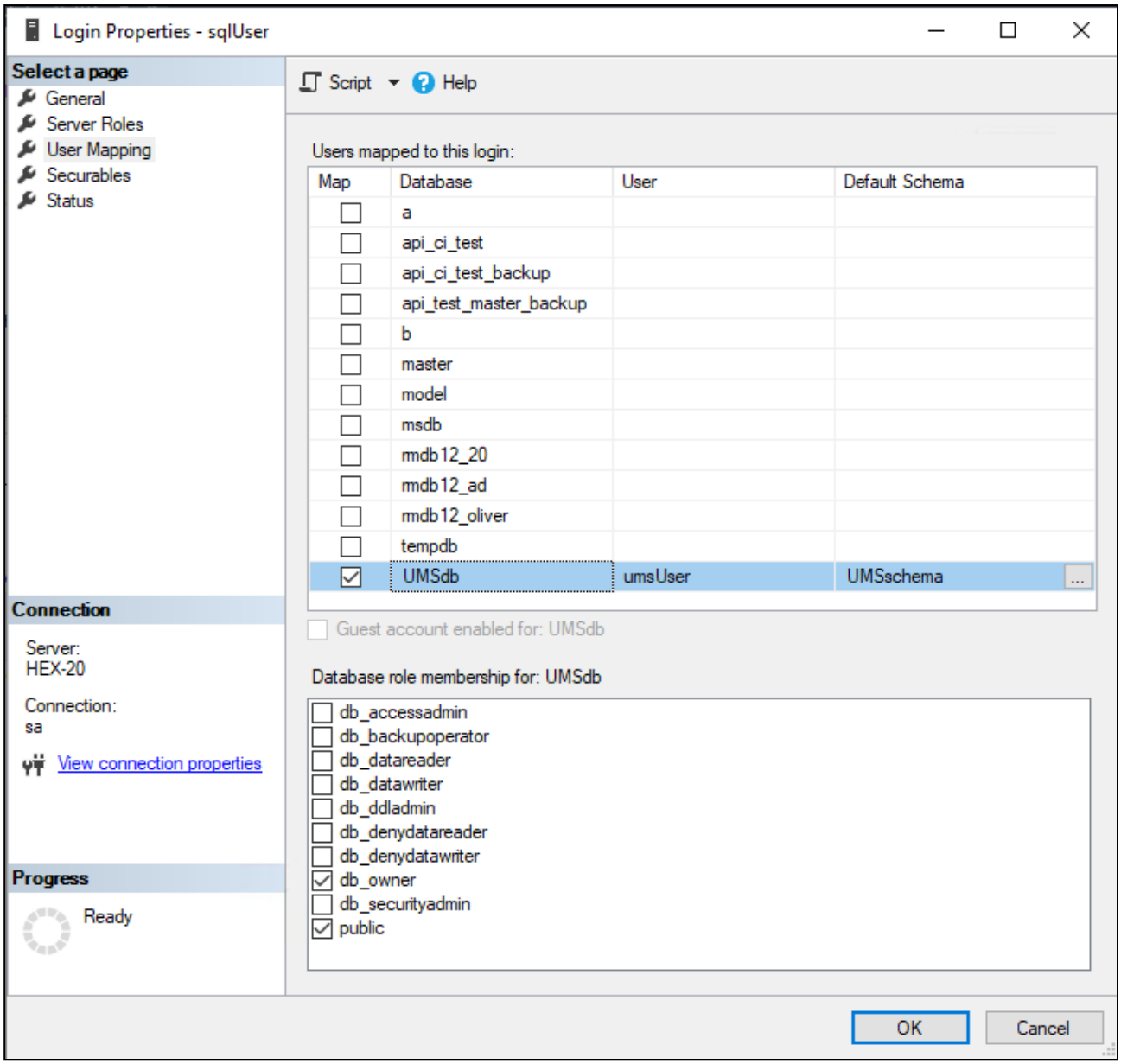


7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.

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



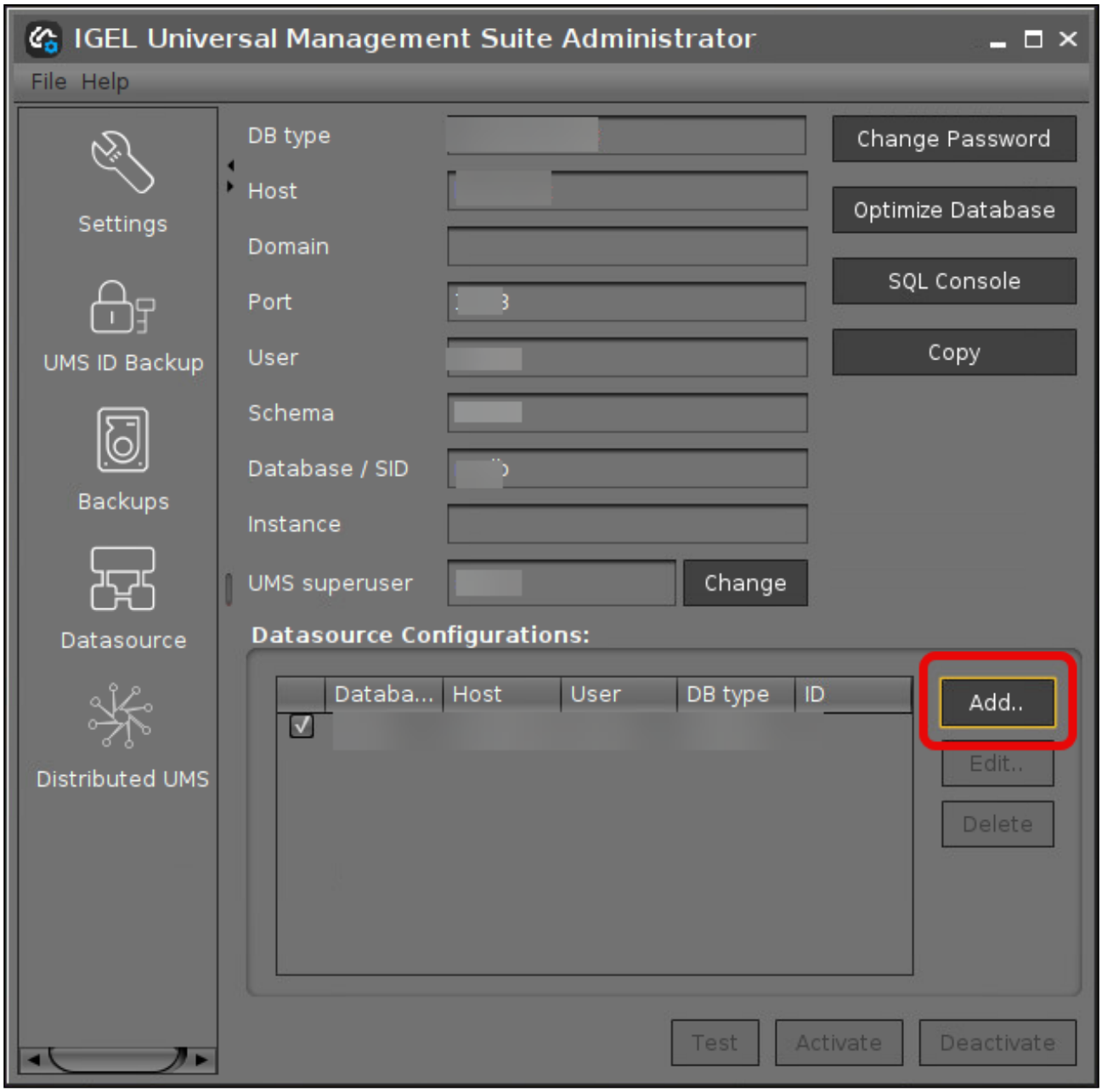
9. Under **Security > Logins > Users**, double-click on the <sql_user>.
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.

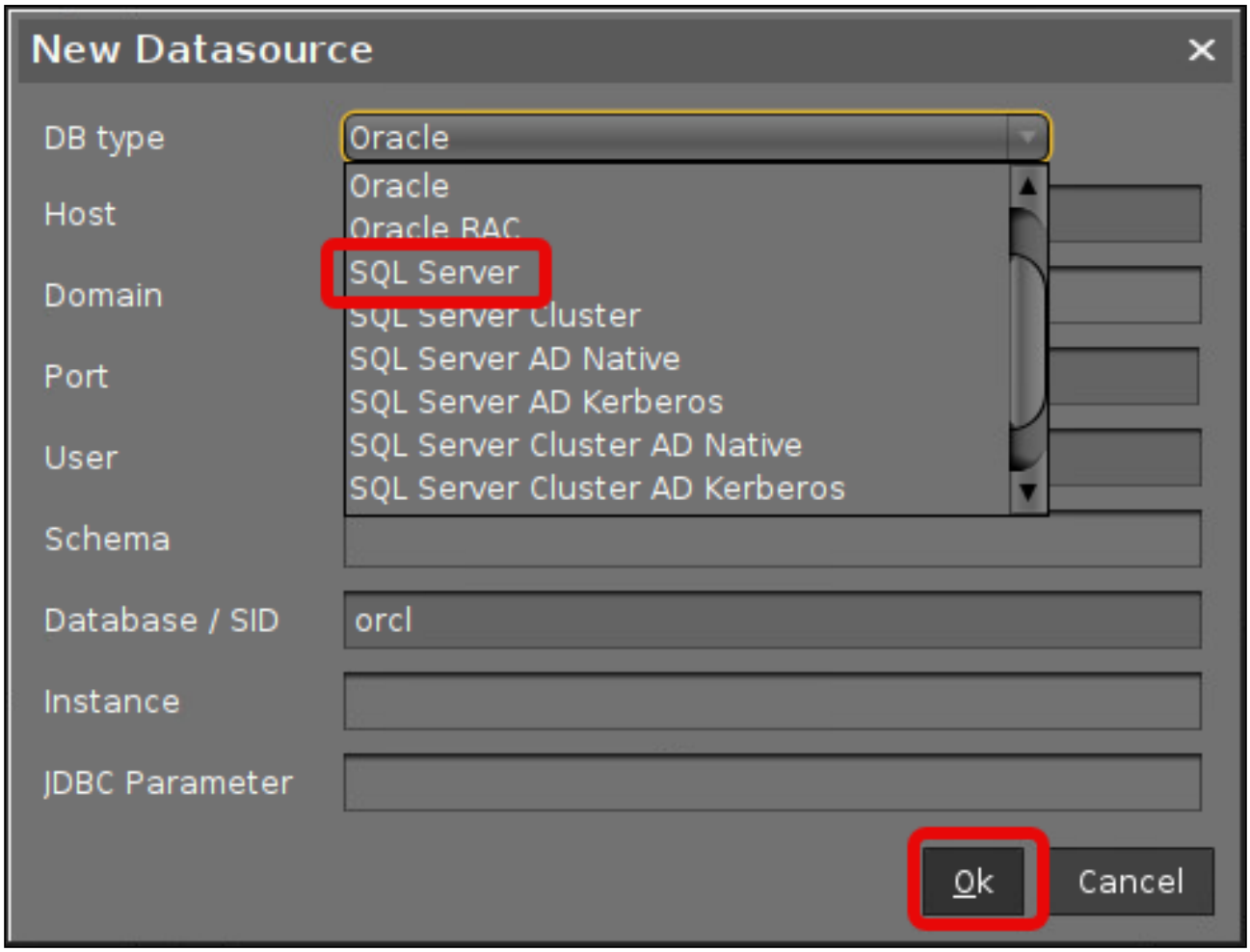


11. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with Connecting the UMS to the Database (Single Server Instance) (see page 73) or Connecting the UMS to the Database (Cluster) (see page 78),

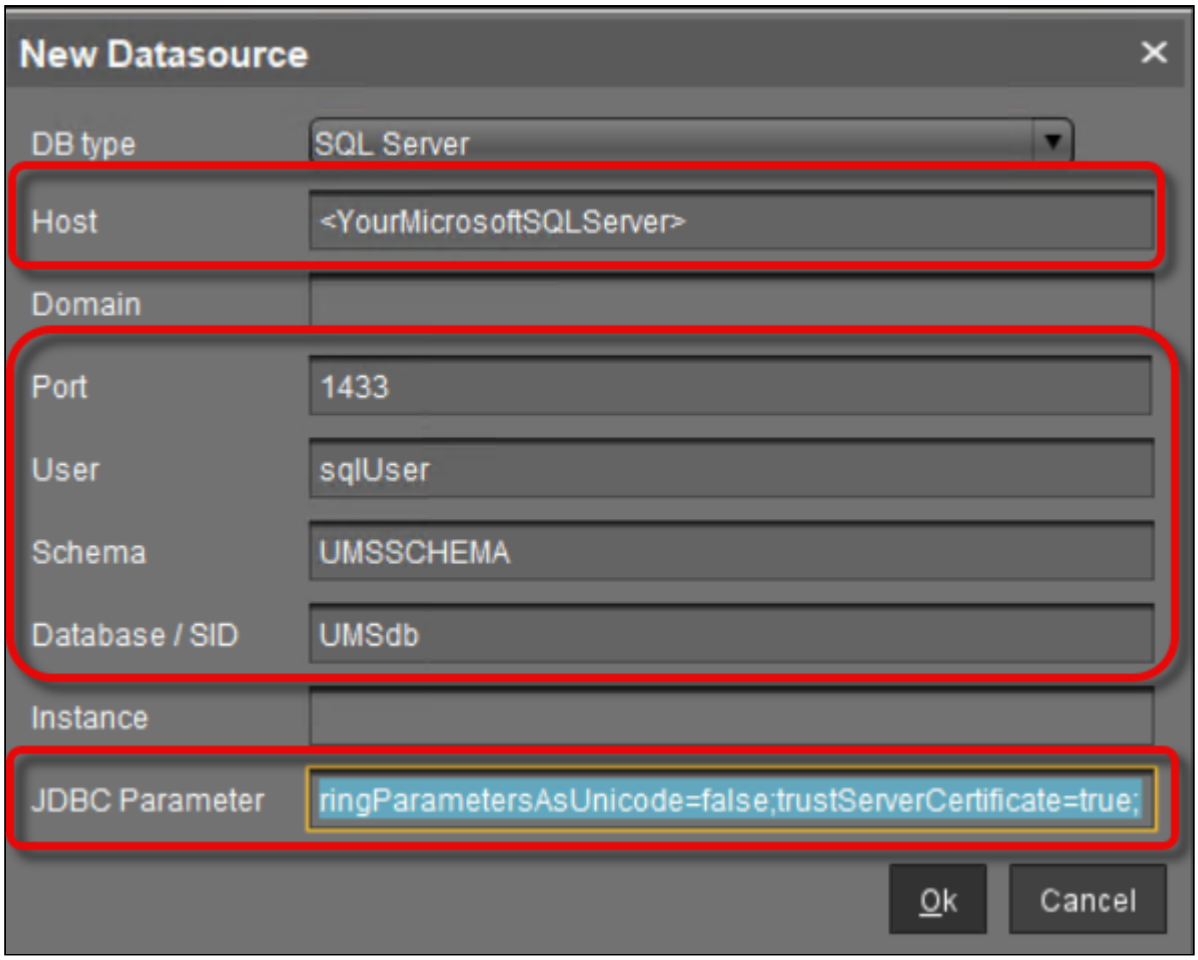
Connecting the UMS to the Database (Single Server Instance)

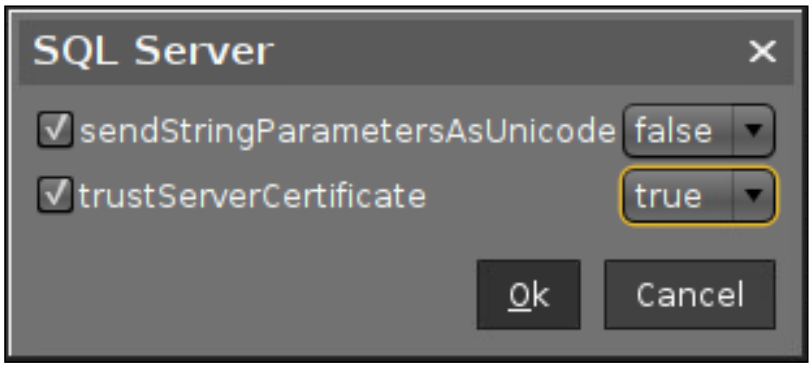
1. In the UMS Administrator (see page 1037), set up a new **SQL Server** type data source.


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
Host
Domain
Port
User
Schema
Database / SID
Instance
UMS superuser
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
Add..
Edit..
Delete
Test
Activate
Deactivate

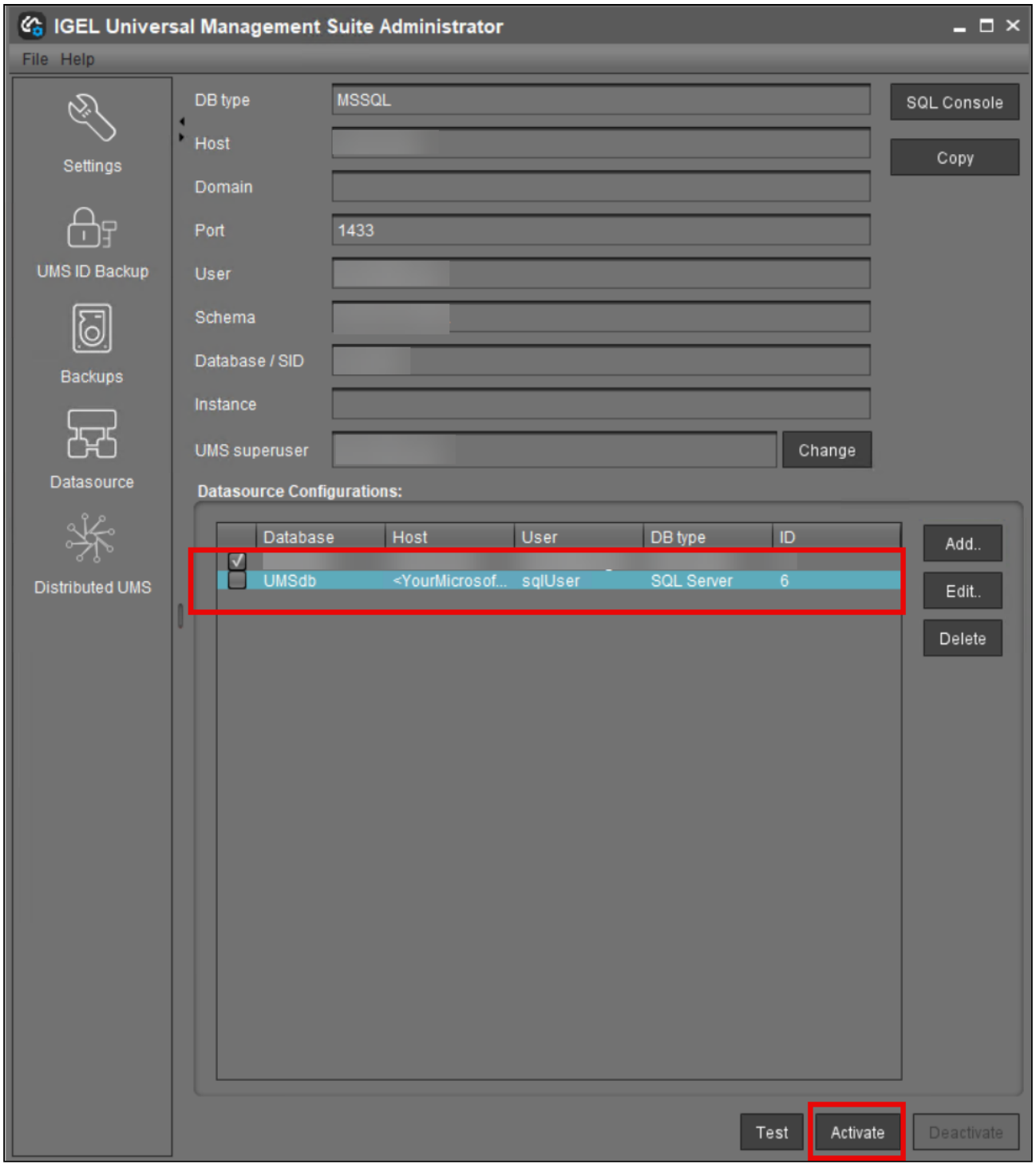


2. Edit the data as follows:
   - **Host**: The hostname or IP address of the Microsoft SQL server; if you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
   - **Port**: The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
   - **User**: The username with which the UMS connects to the UMS server; please note that this is the real login user (in our example: “sqlUser”), NOT the local alias within the database (in our example: “umsUser”)
   - **Schema**: The database schema
   - **Database / SID**: The database name
   - **JDBC Parameter** (double-click):
     - **sendStringParametersAsUnicode**: **false**
     - **trustServerCertificate**: **true**

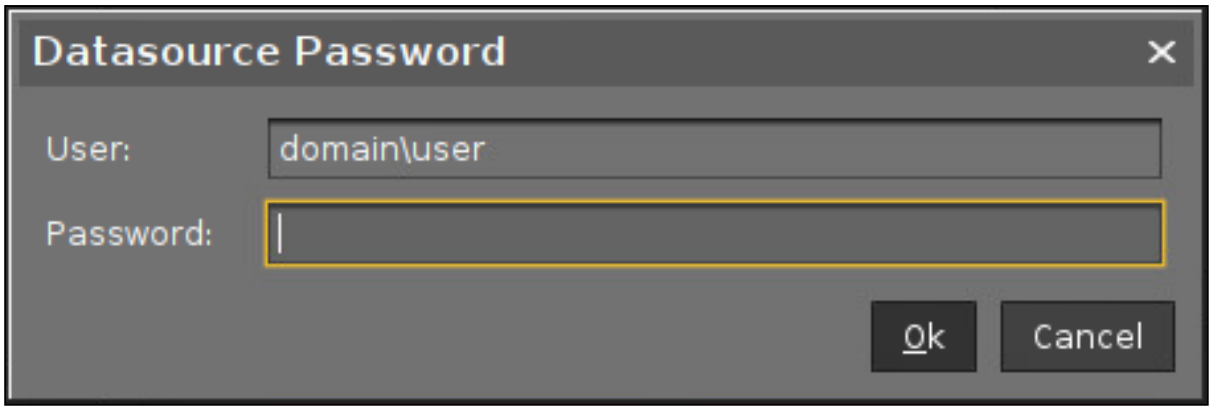




3. Select your database configuration and click **Activate**.

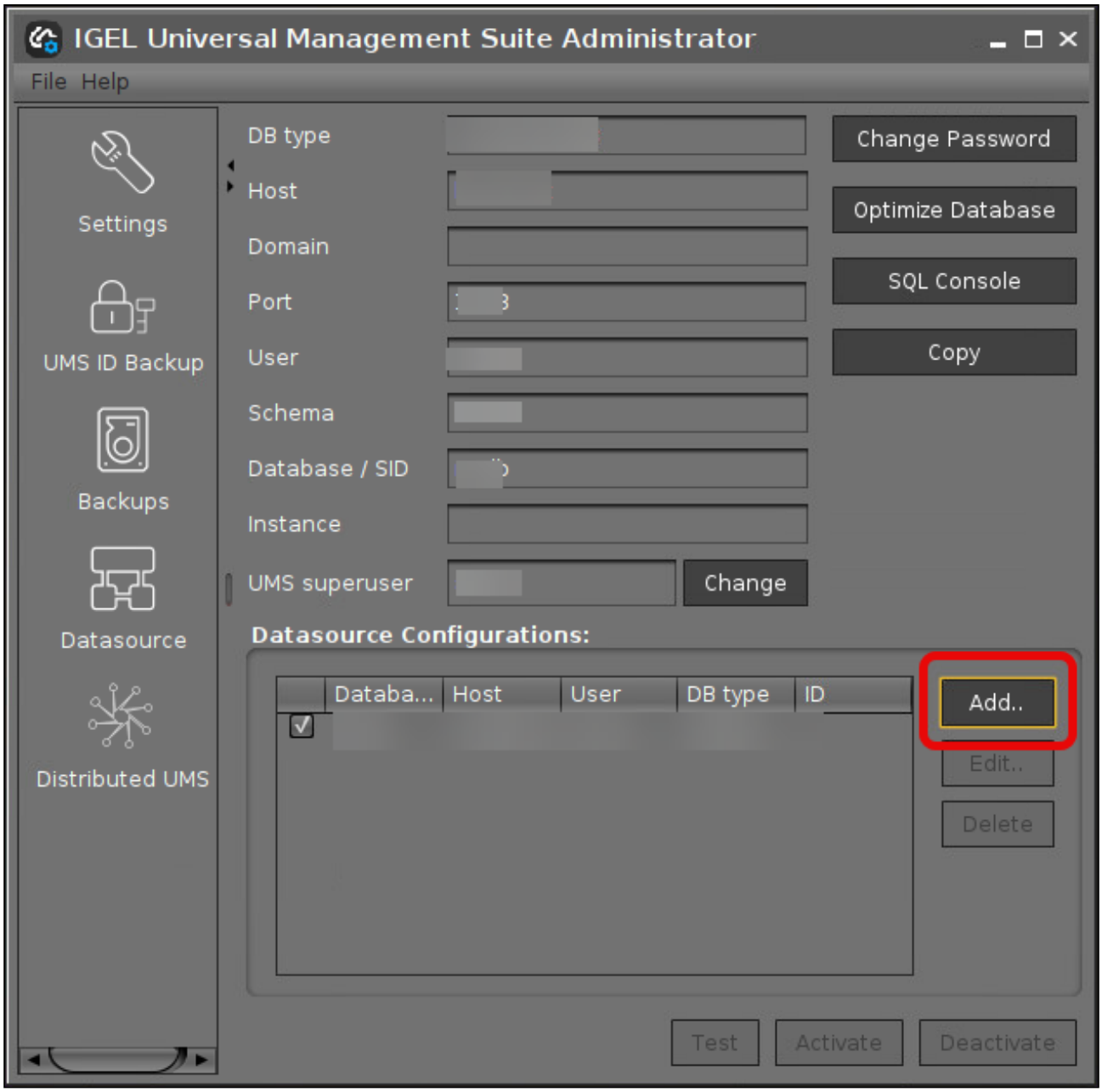


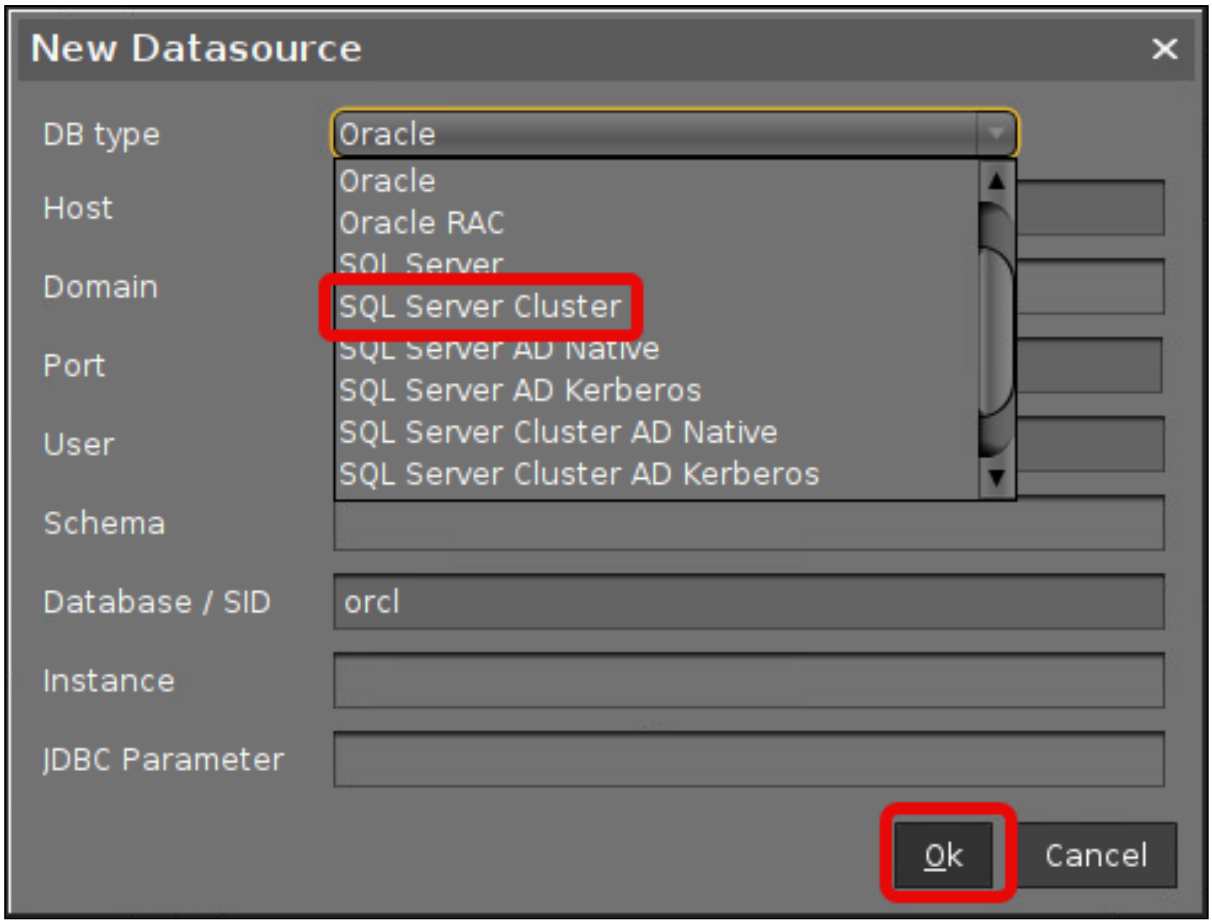
4. Enter the username and the password for the connection.



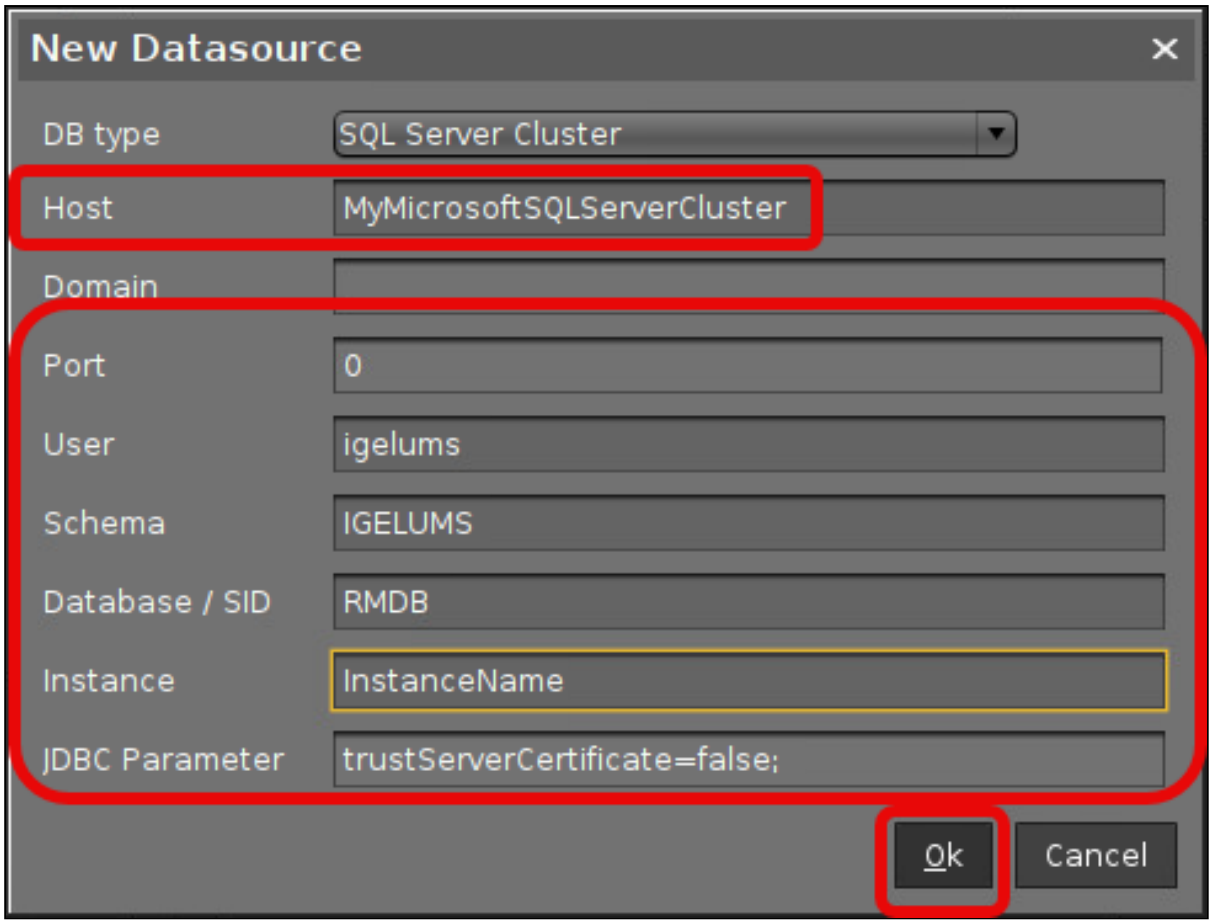
Connecting the UMS to the Database (Cluster)

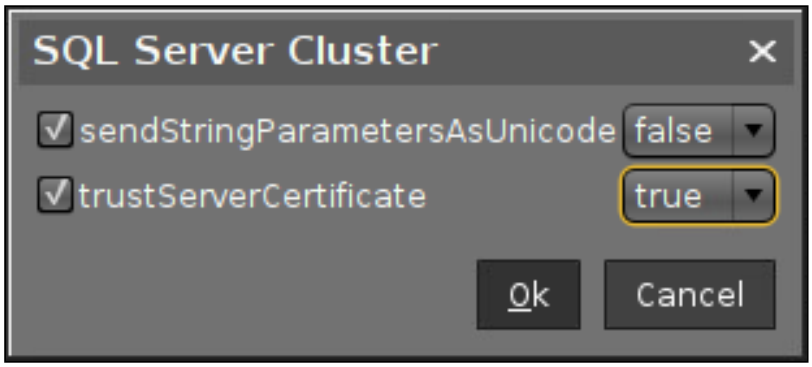
1. In the UMS Administrator (see page 1037), set up a new **SQL Server** type data source.


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
Host
Domain
Port
User
Schema
Database / SID
Instance
UMS superuser
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
Add..
Edit..
Delete
Test
Activate
Deactivate

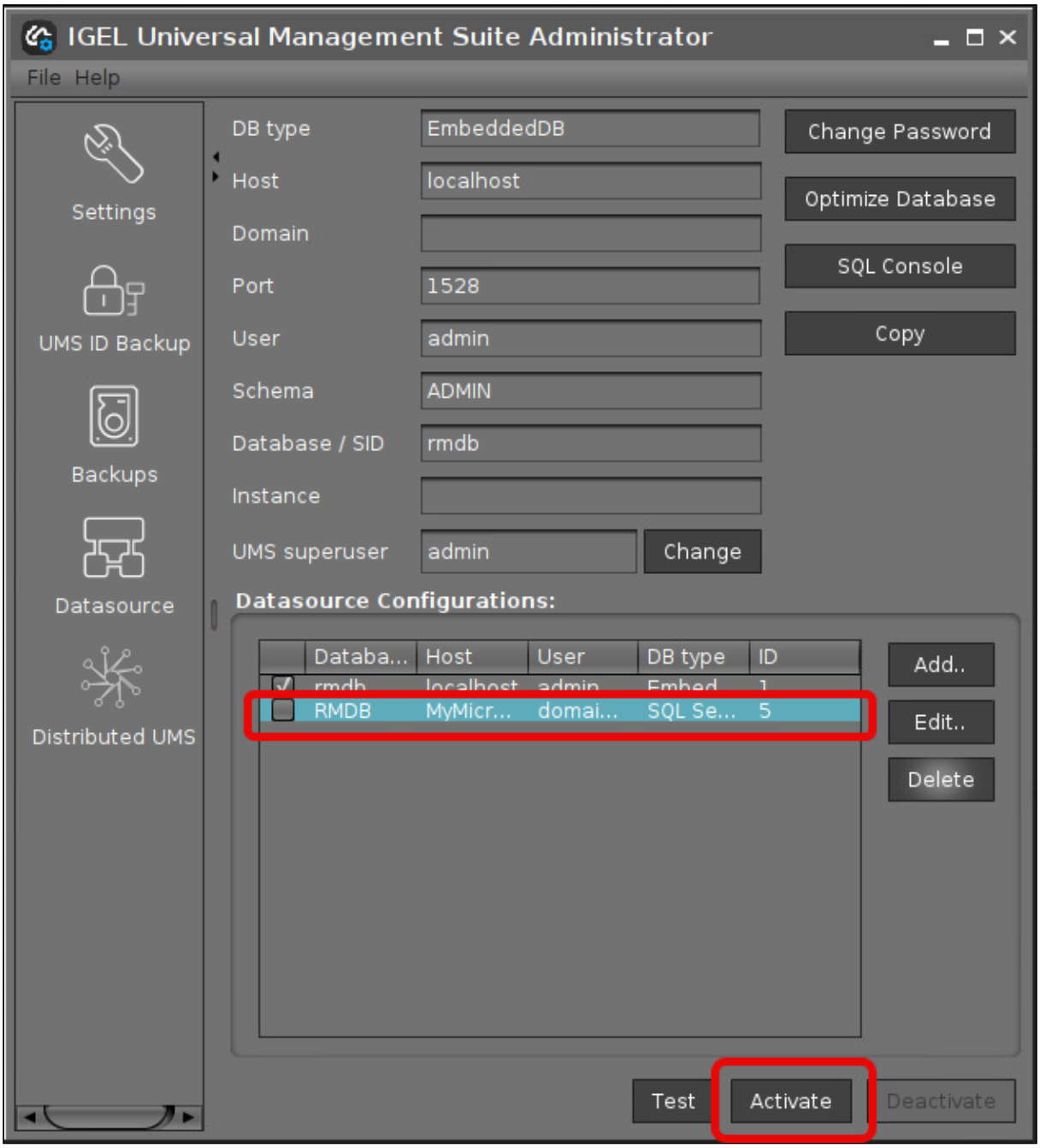


2. Edit the data as follows:
   - **Host**: The hostname or IP address of the Microsoft SQL server; if you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
   - **Port**: The port on which the Microsoft SQL Server listens for requests. (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**

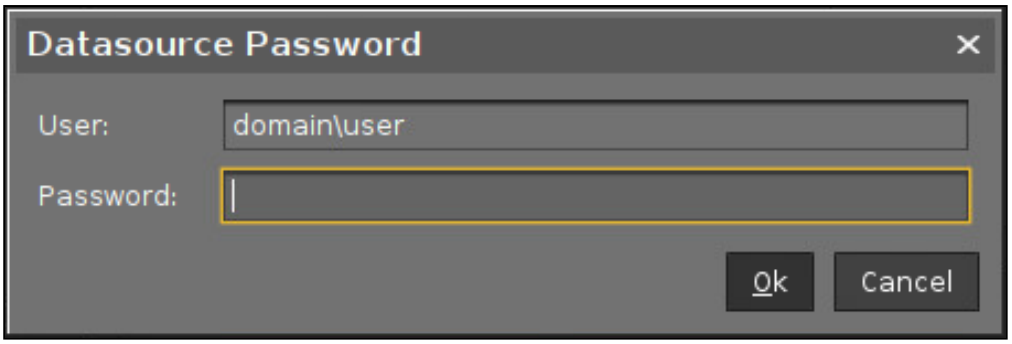




3. Select your database configuration and click **Activate**.



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


Datasource Password
User:
domain\user
Password:
Ok
Cancel

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 * [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!

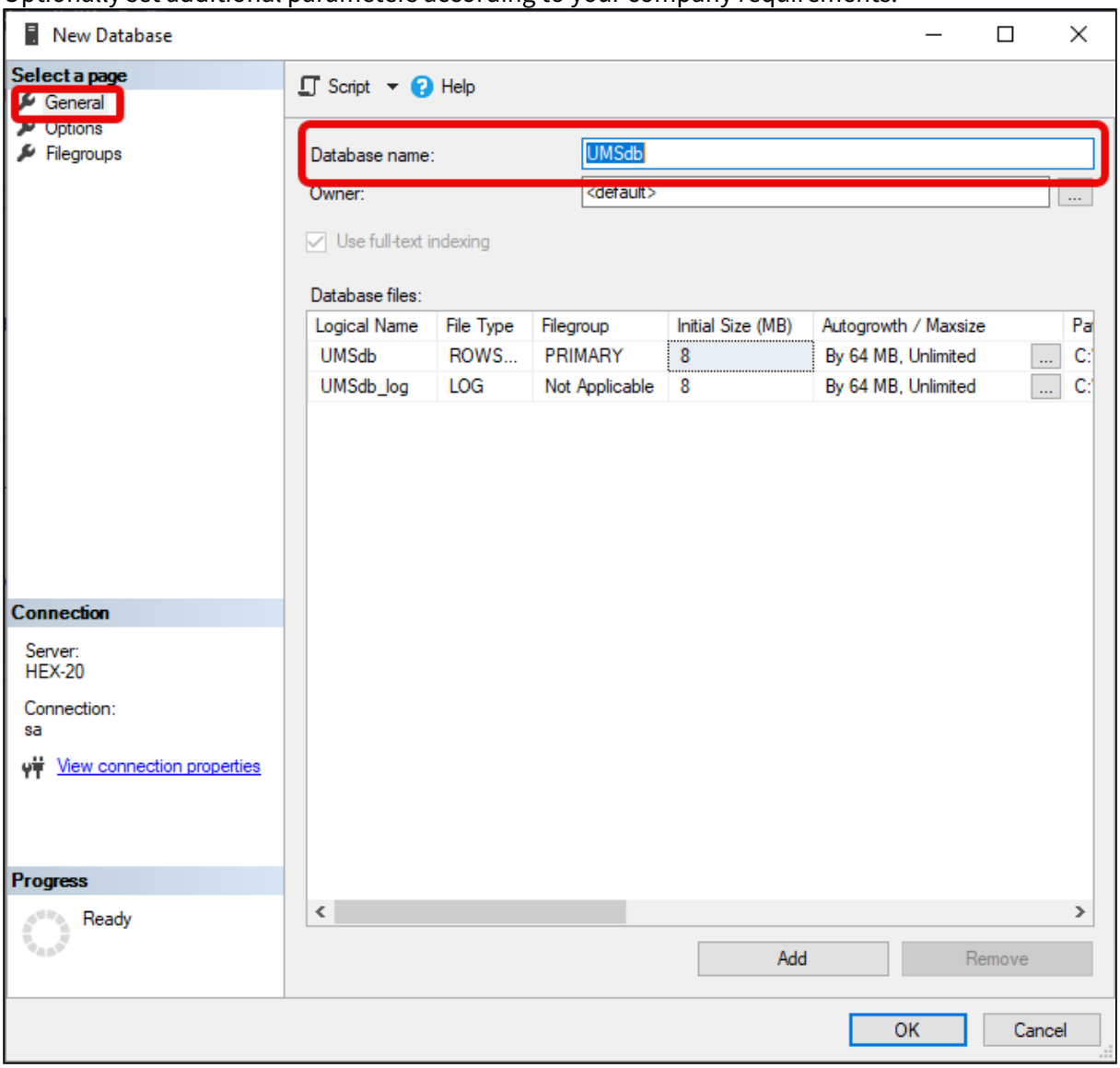
- `<database_name>` : The name for the UMS database
- `<schema_name>` : The name of the schema for the UMS database

```
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

> 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

> 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.

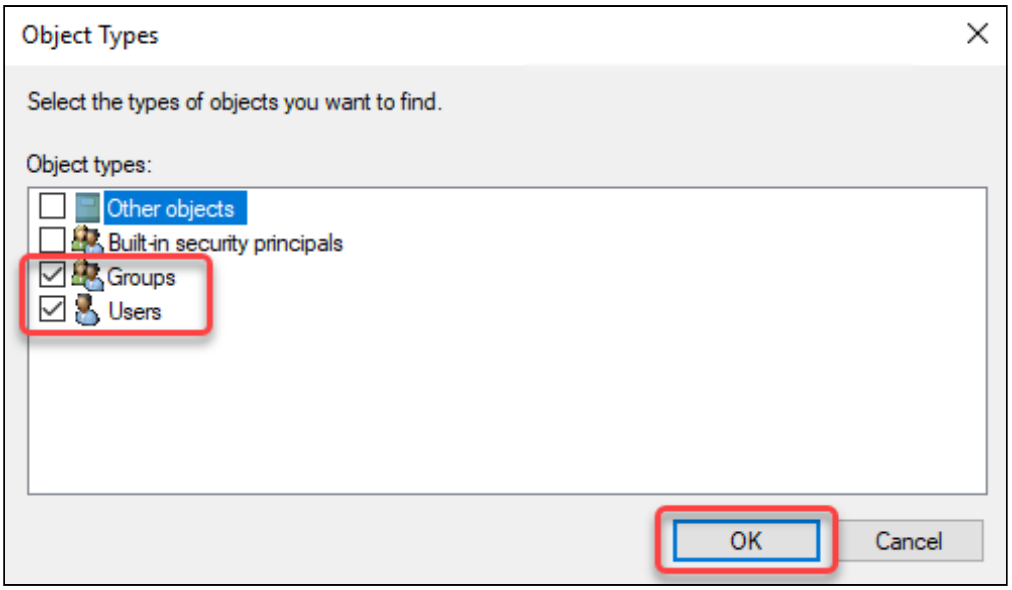
Using the SQL Management Console

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.

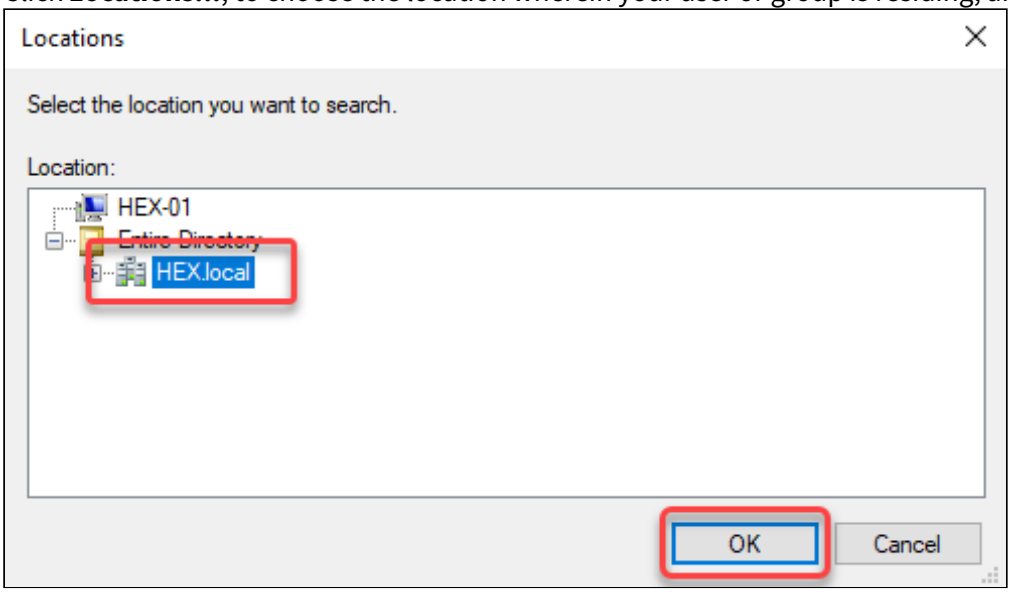
```
USE [master]
GO
CREATE LOGIN [[<ad_user>]] FROM WINDOWS;
GO
```

Using the SQL Server Management Studio (GUI Mode)

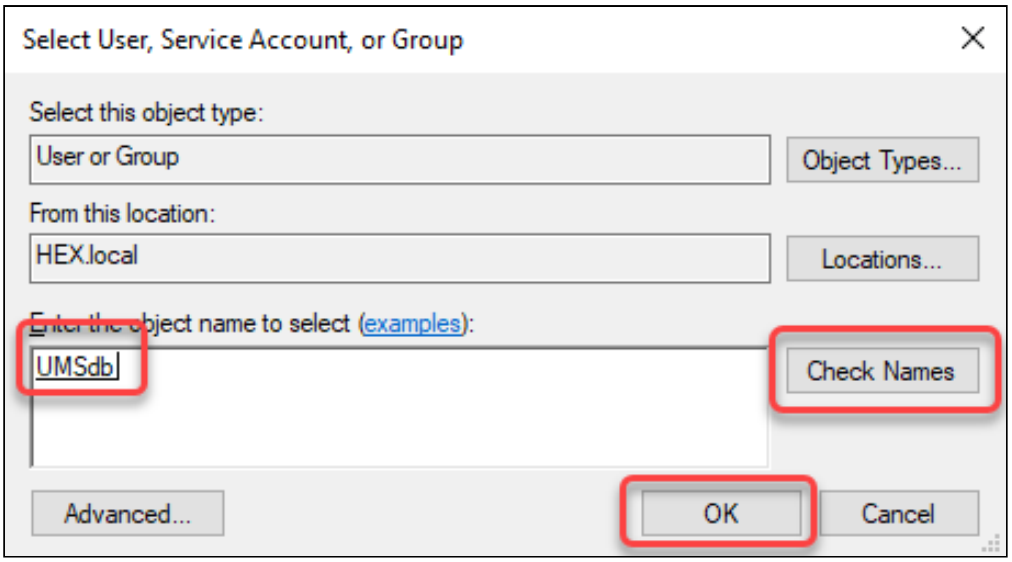
1. Connect to the database with the SQL Server Management Studio.
2. Open the **Security** branch, right-click on **Logins**, and select **New Login**.
3. Choose **Windows Authentication** for the login, and click **Search**.
4. Click **Object Types...**, select **Groups** and **Users**, and click **OK**.



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

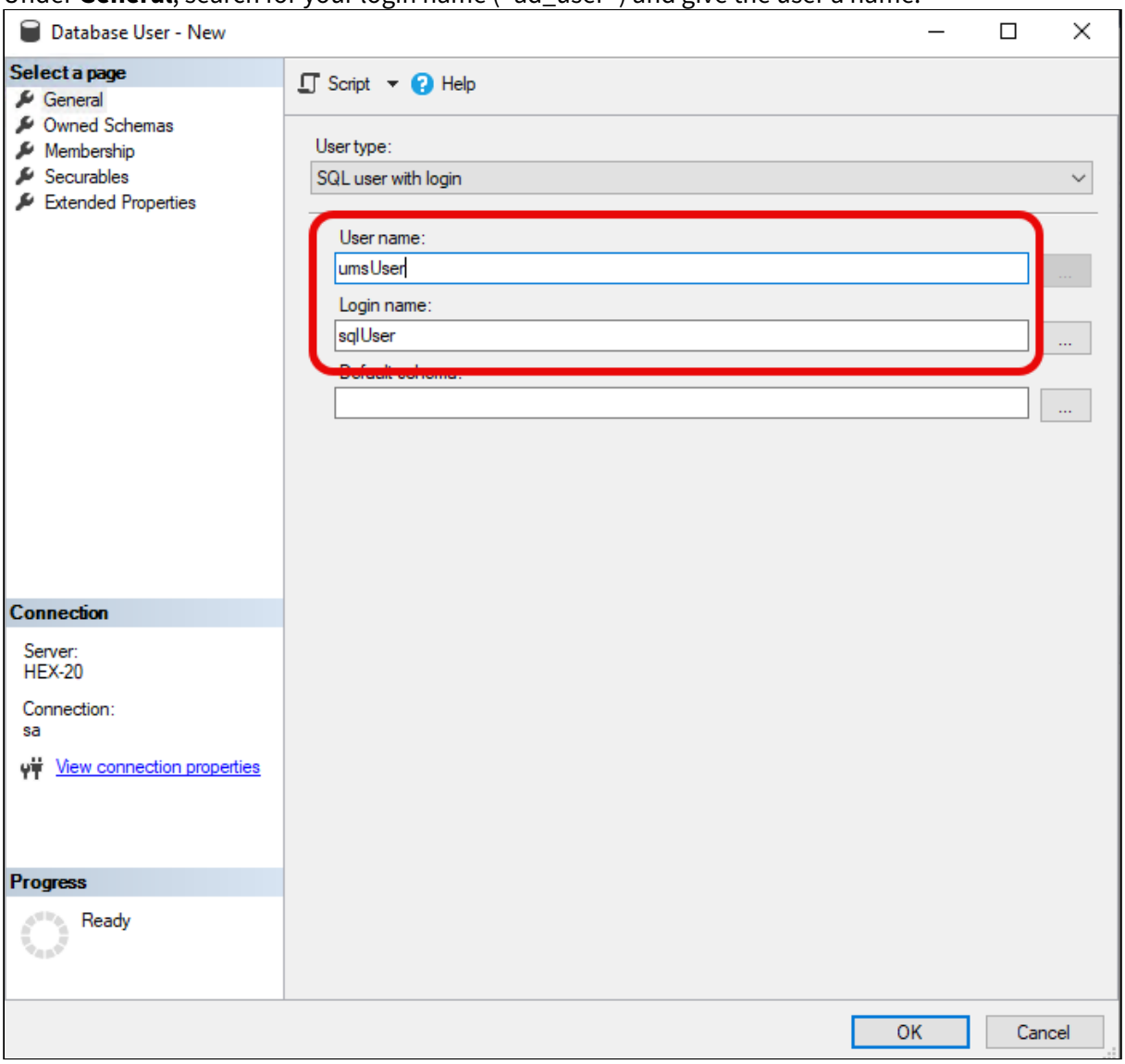
→ In the SQL Management Console, select **New Query** and enter the script below; please note the following.

- `<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.

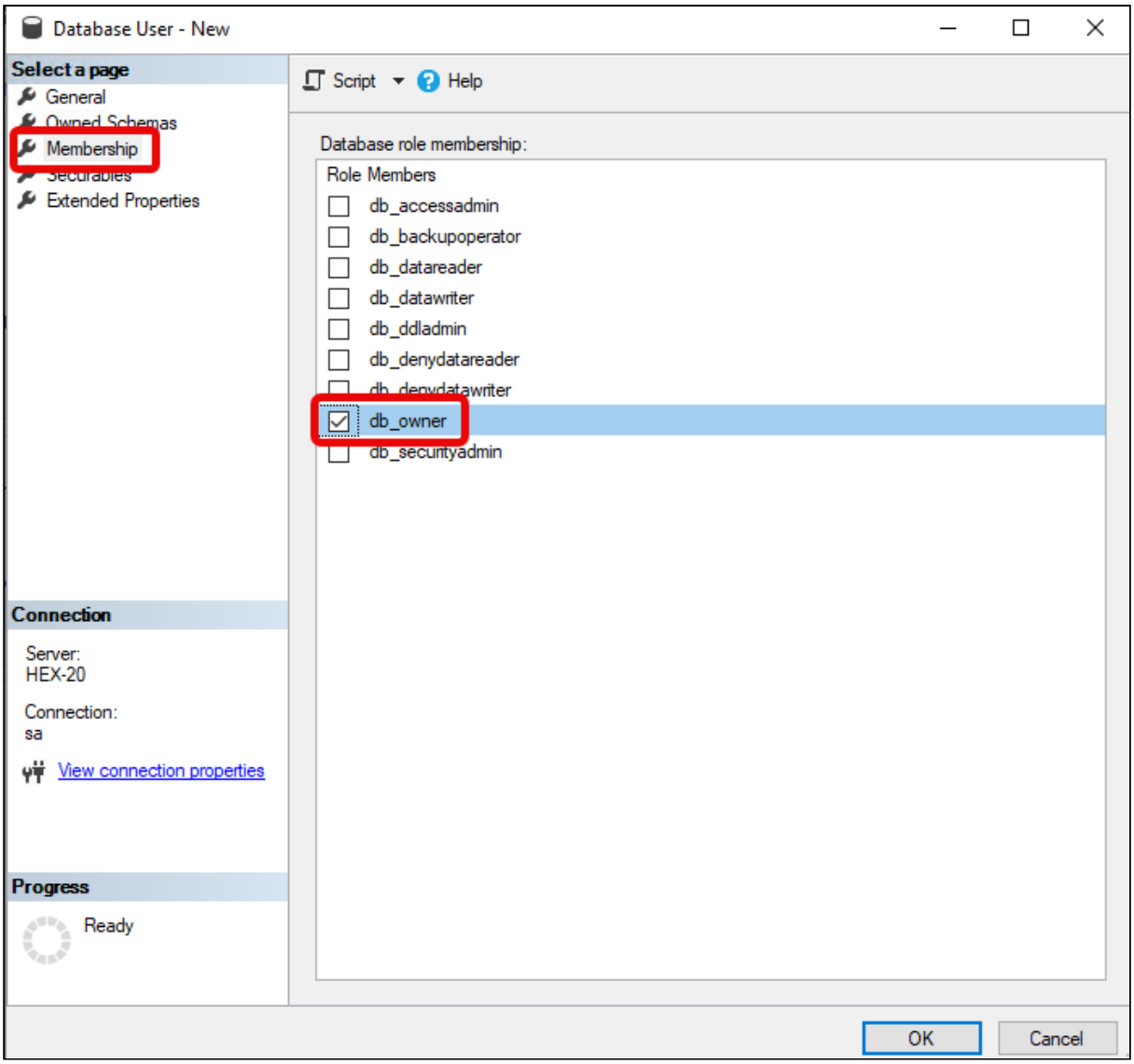
```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<ad_user];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

Using the GUI

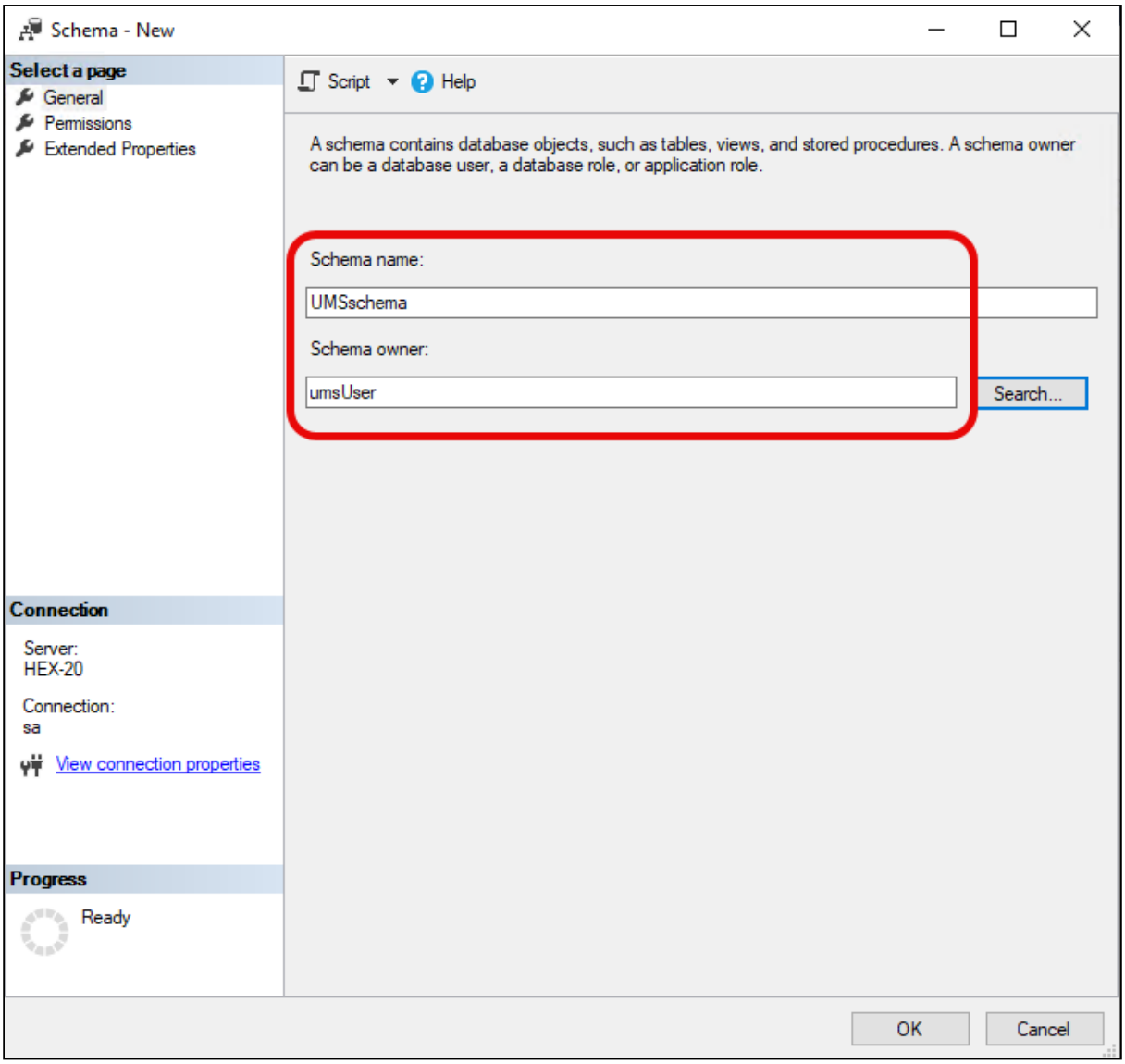
1. In SQL Server Management Studio, open the database that was created in Creating the UMS Database.
2. Under **Security > Users**, right-click **New User**.
3. Under **General**, search for your login name (<ad_user>) and give the user a name.



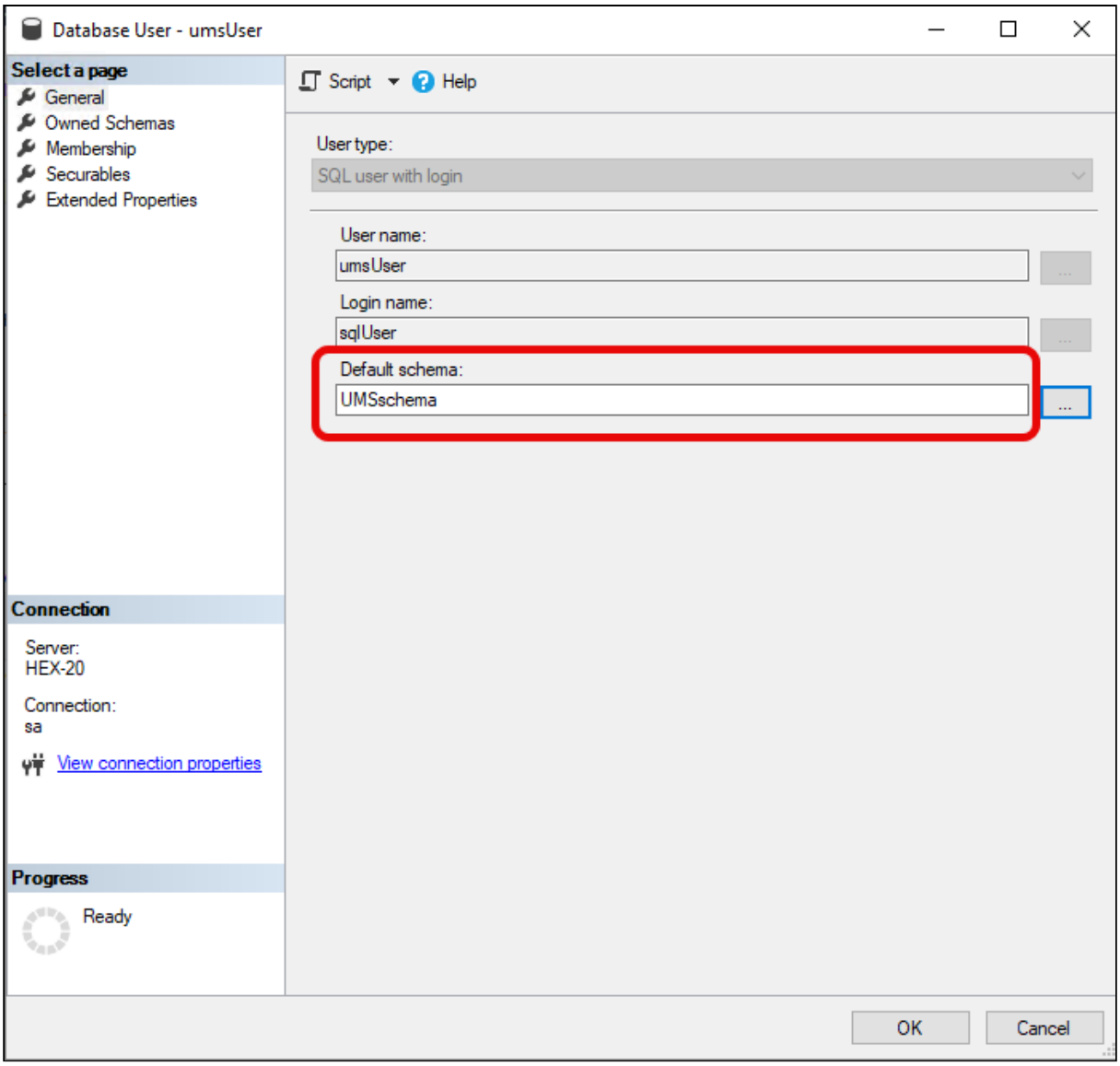
4. In the **Membership** area, give the user the **db_owner** role.



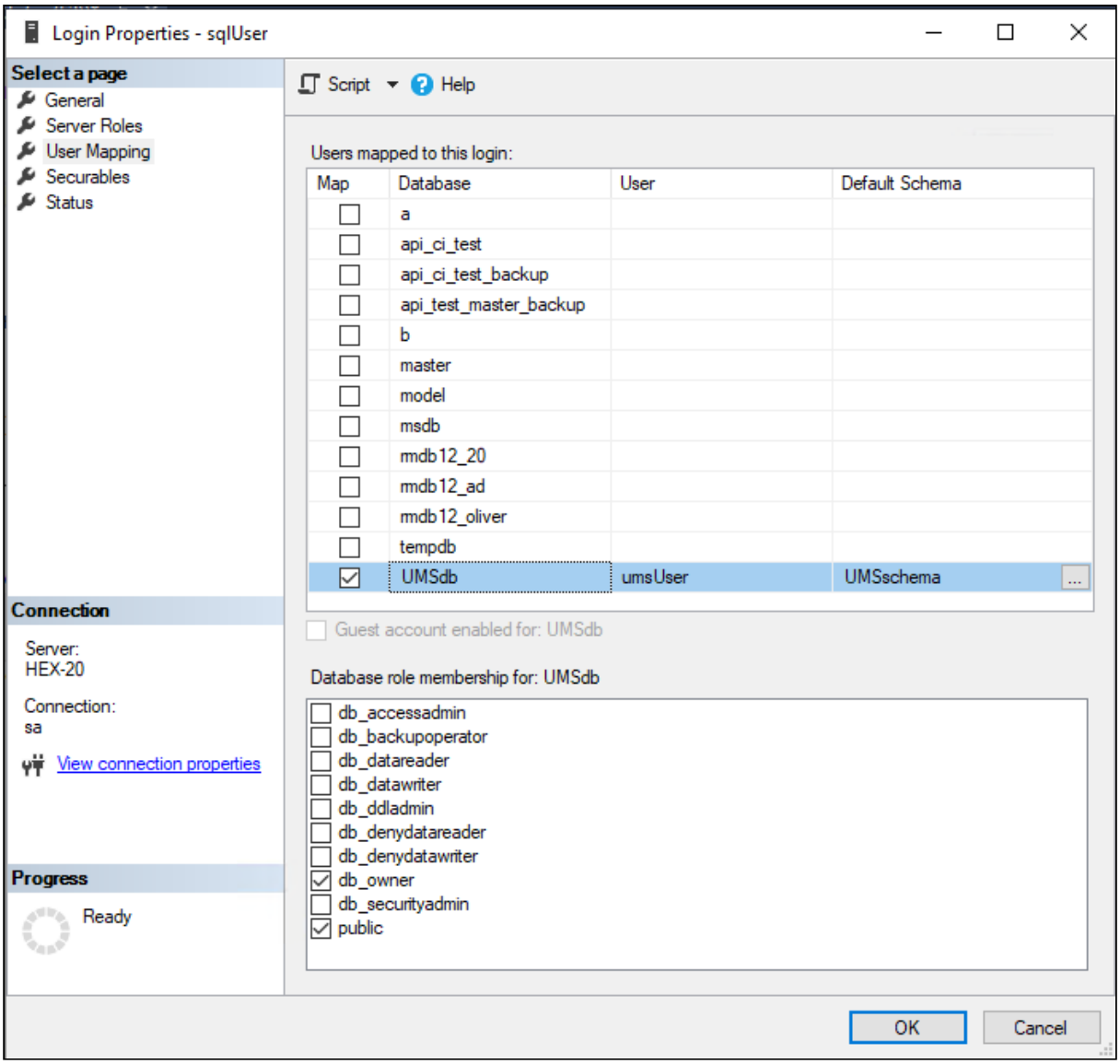
5. Go to **Security > Schemas** and right-click on **New Schema**.
6. Search for the <ums_user> as the **Schema owner** and provide a **Schema name**.



7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.
8. Under **General**, set the default schema to <schema_name>.

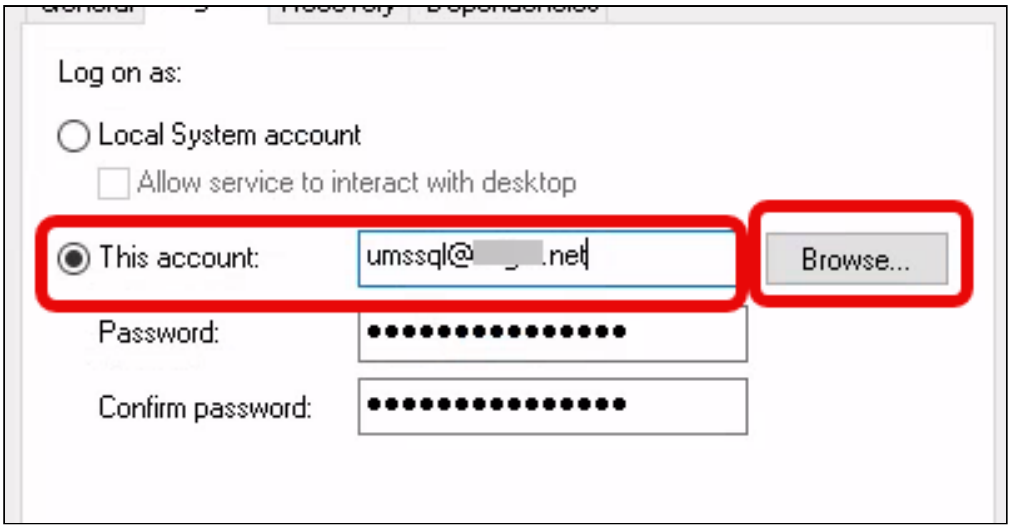


9. Under **Security > Logins > Users**, double-click on the <ad_user>.
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.



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.

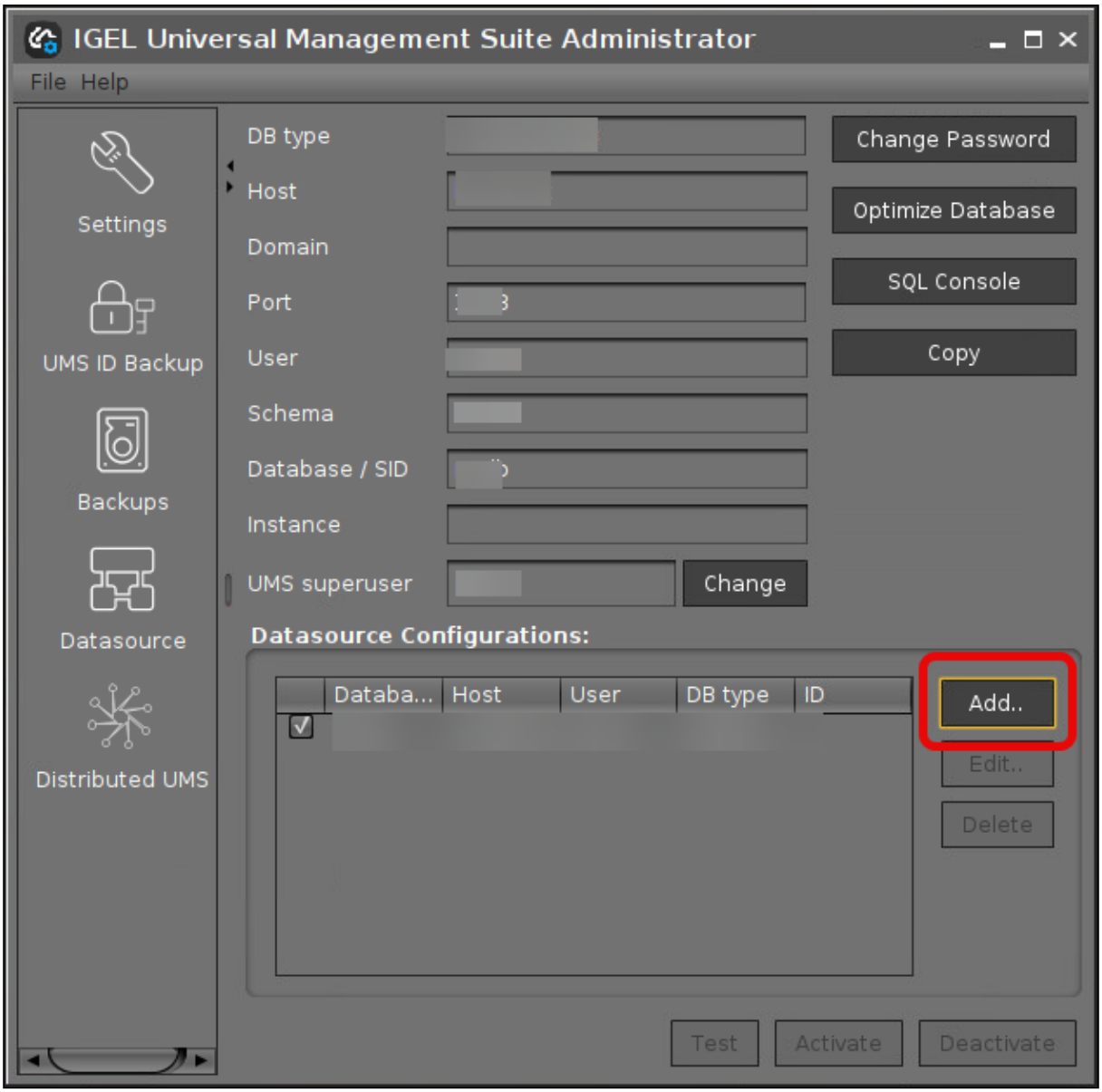


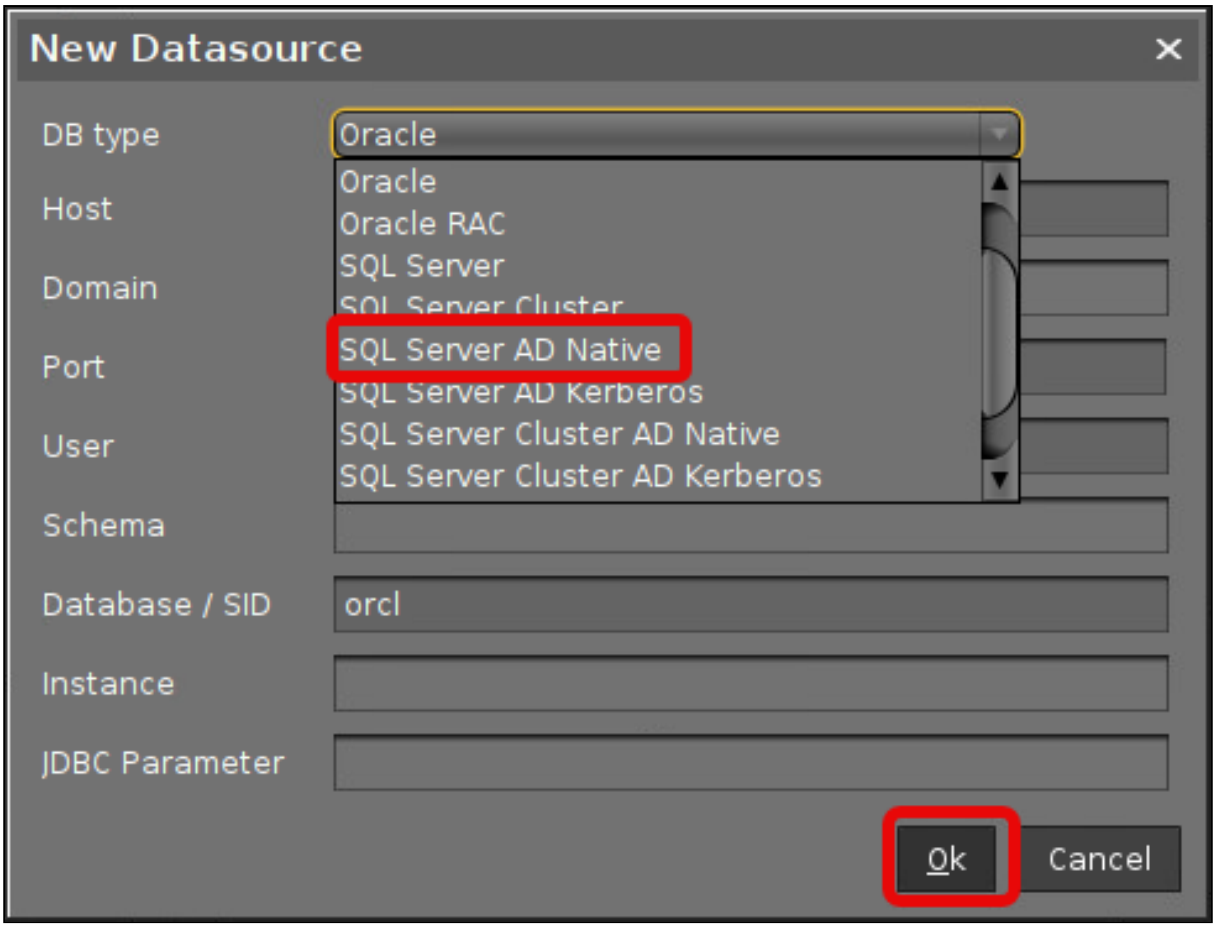
5. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with Connecting the UMS to the Database (Single Server Instance) or Connecting the UMS to the Database (Cluster),

Connecting the UMS to the Database (Single Instance)

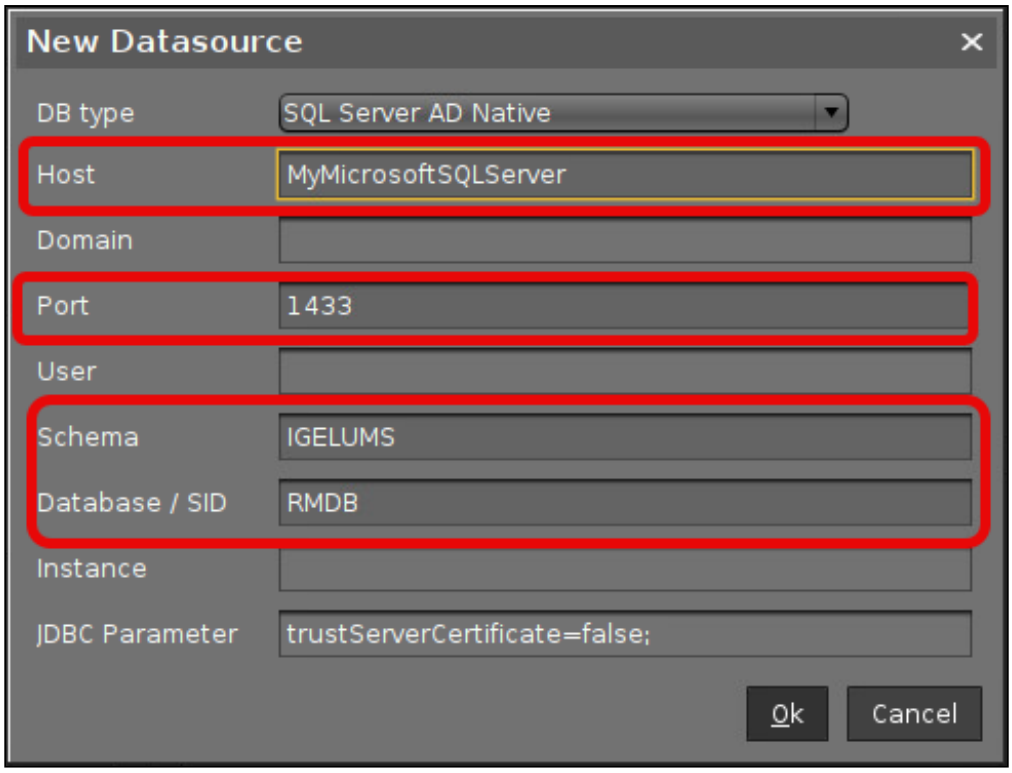
⚠ Before configuring the connection, perform the following:
1. Right-click the UMS Administrator (for example, in the start menu) and select **Run as different user** from the context menu.
2. Authenticate with the SQL AD Service Account.
3. Log into the UMS server as the SQL AD Service Account.
4. Run the UMS Administrator.

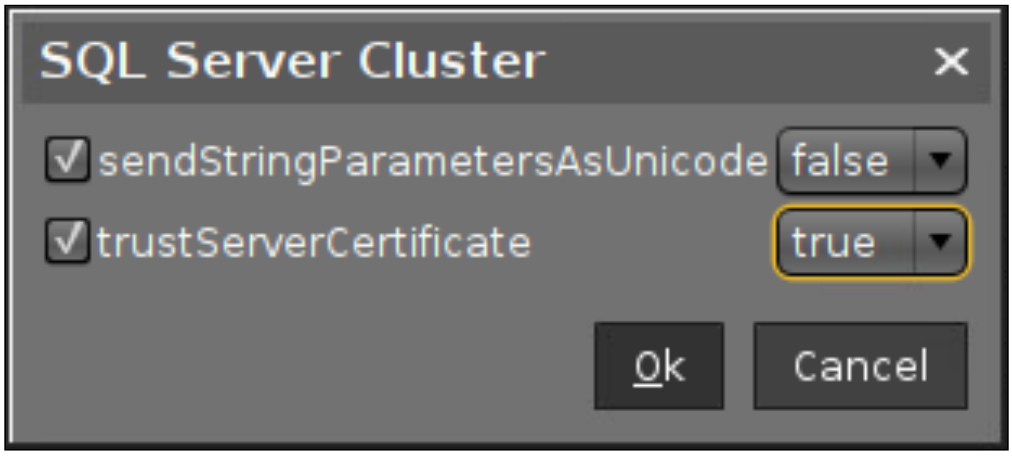
1. In the UMS Administrator (see page 1037), set up a new **SQL Server AD Native** type data source.


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
Host
Domain
Port
User
Schema
Database / SID
Instance
UMS superuser
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
Add..
Edit..
Delete
Test
Activate
Deactivate

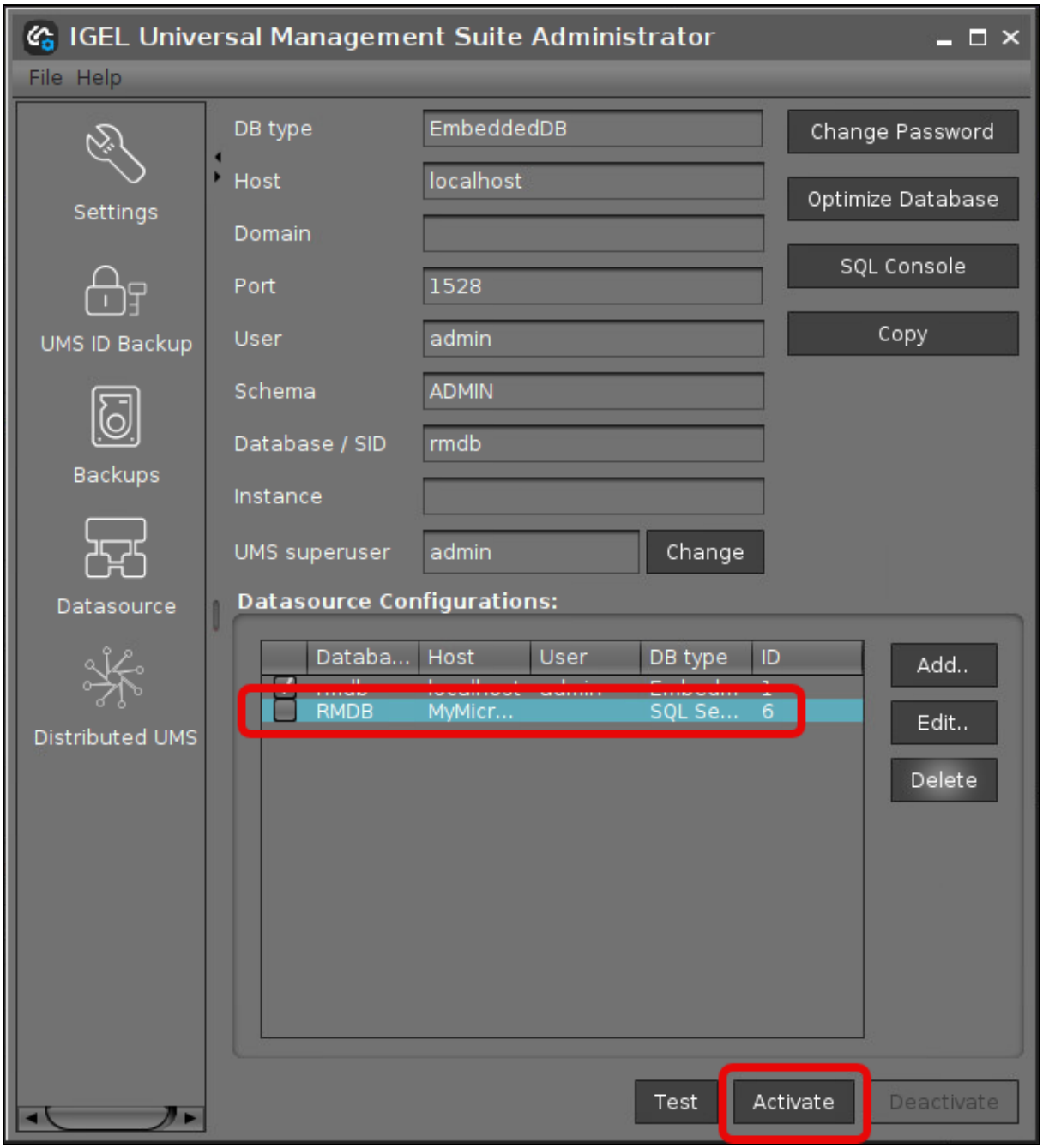


2. Edit the data as follows:
   - **Host**: The Fully Qualified Host Name (FQDN) of the Microsoft SQL server. If you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
   - **Port**: The port on which the Microsoft SQL Server listens 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**.



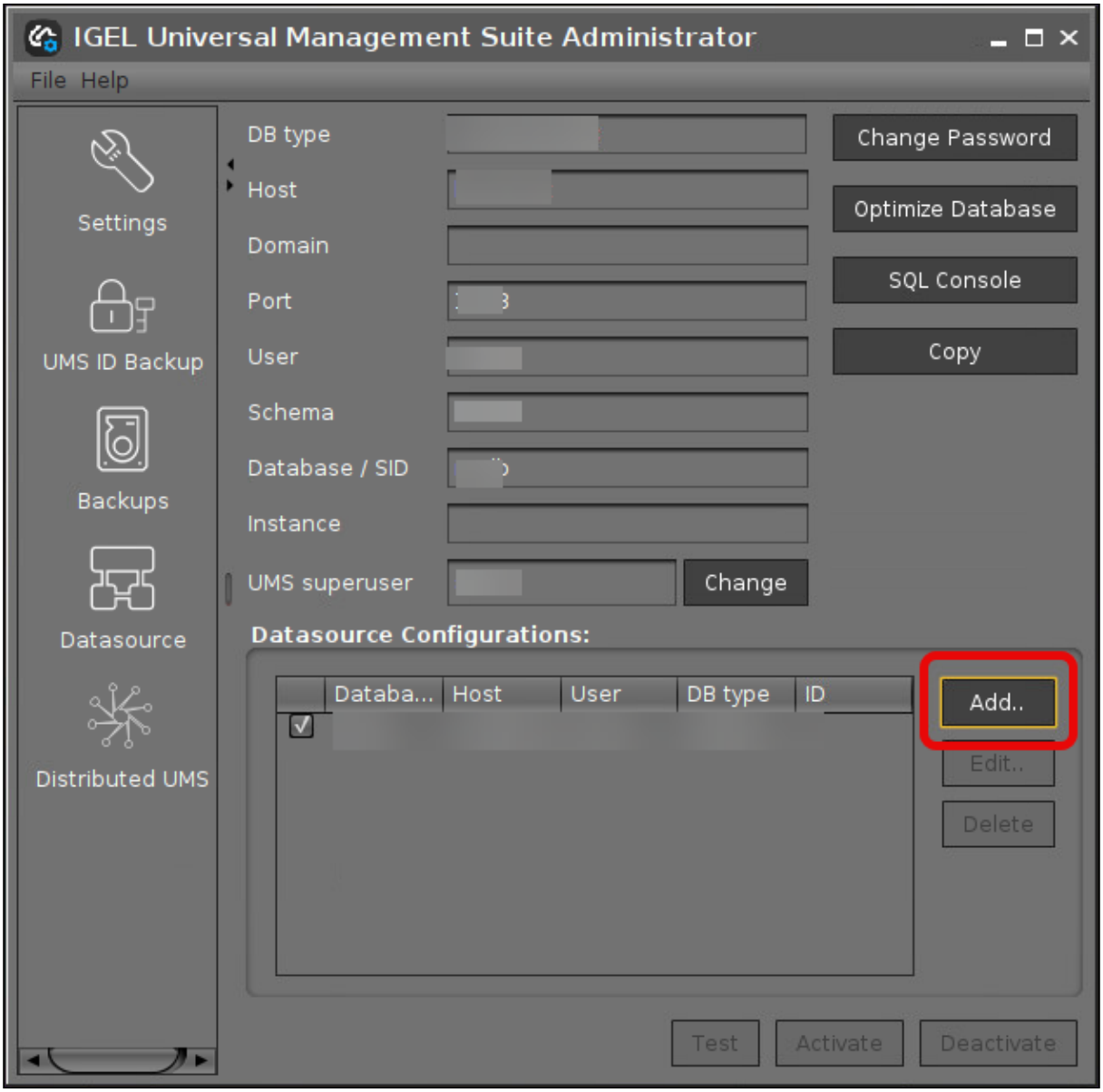
Connecting the UMS to the Database (Cluster)

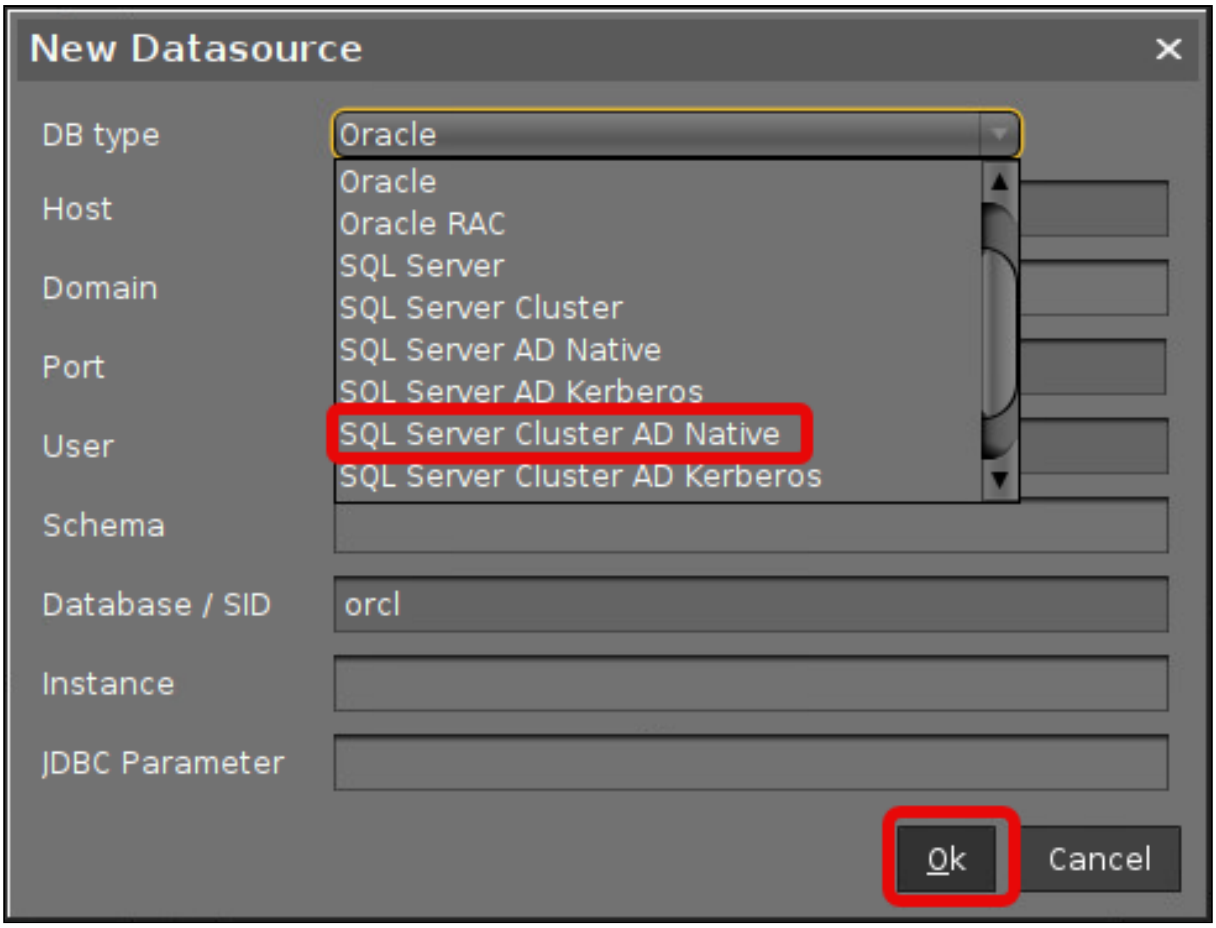
⚠ Before configuring the connection, perform the following:

1. Right-click the UMS Administrator (for example, in the start menu) and select **Run as different user** from the context menu.
2. Authenticate with the SQL AD Service Account.

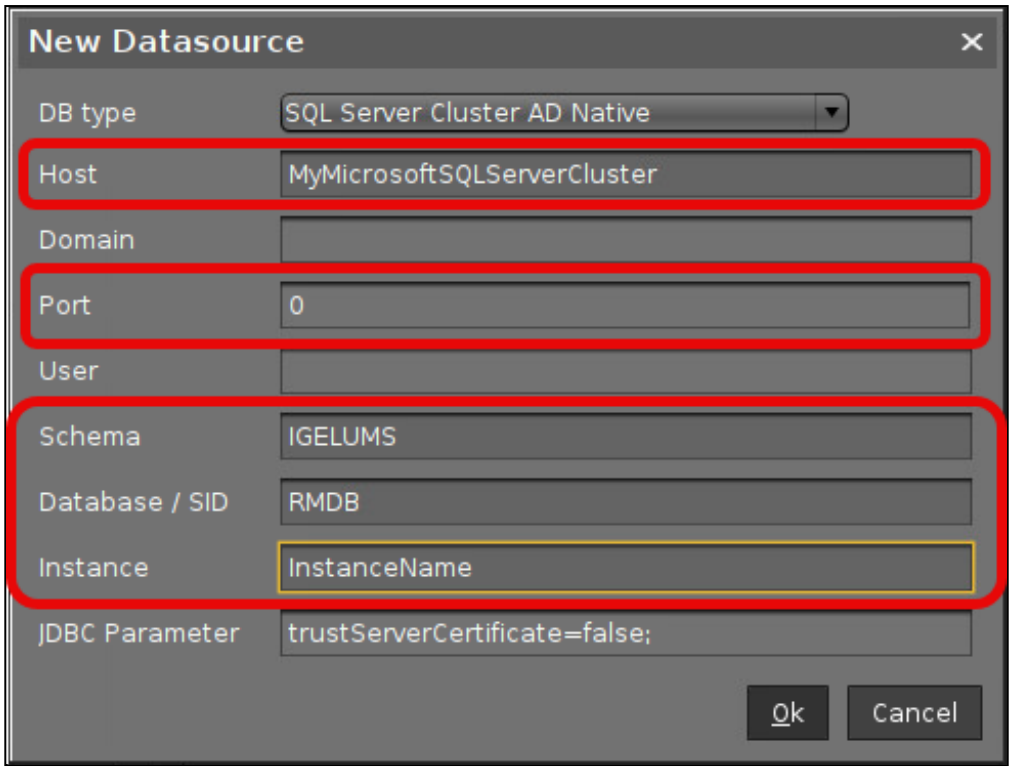
3. Log into the UMS server as the SQL AD Service Account.
4. Run the UMS Administrator.

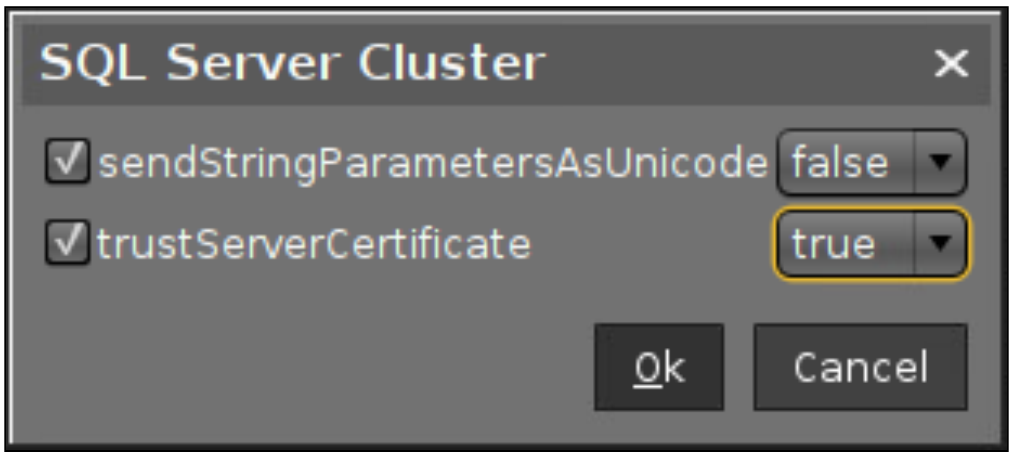
1. In the UMS Administrator (see page 1037), set up a new **SQL Server Cluster AD Native** type data source.



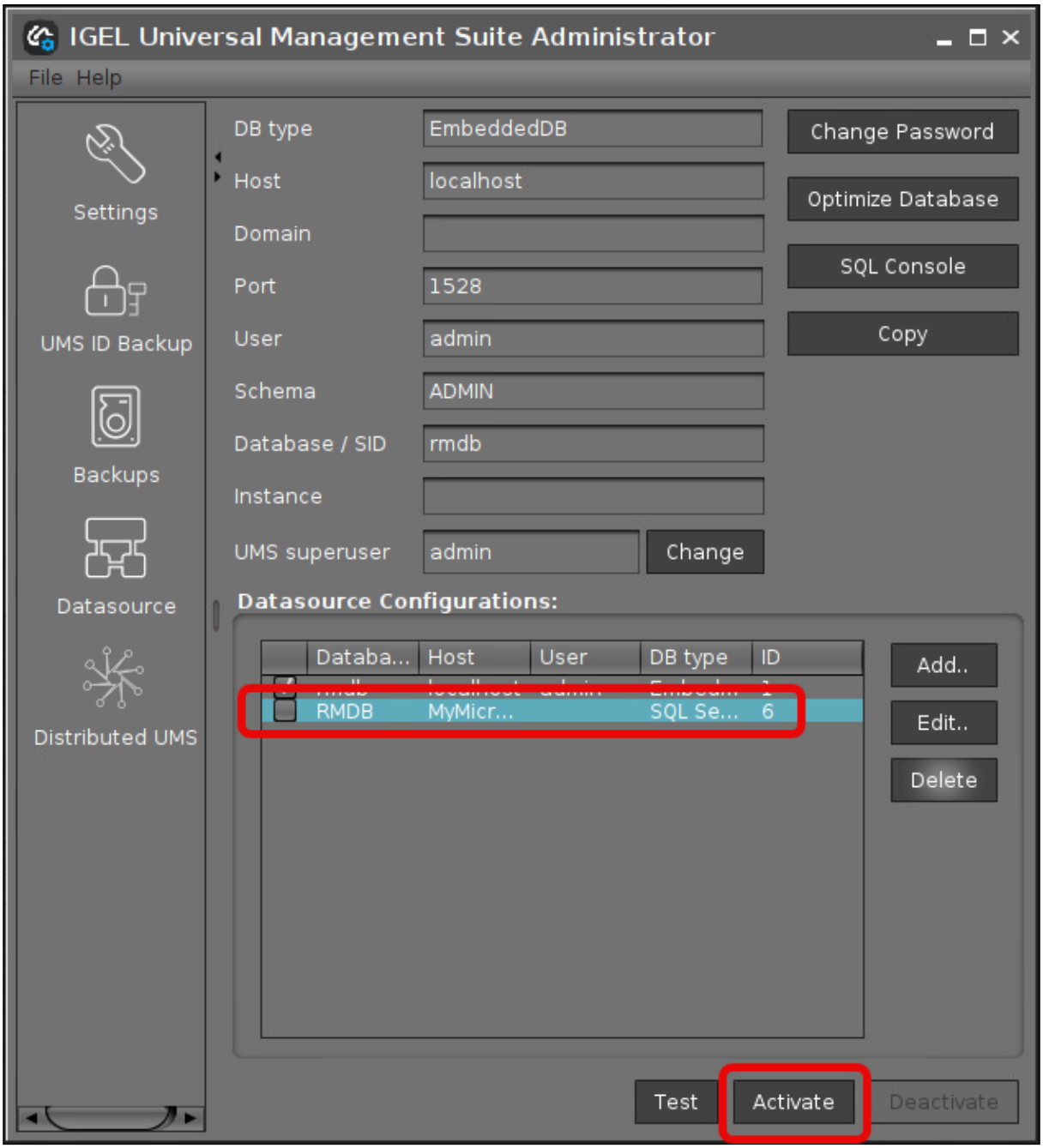


2. Edit the data as follows:
    - **Host**: The Fully Qualified Host Name (FQDN) of the Microsoft SQL server
    - **Port**: The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
    - **Schema**: The database schema
    - **Database / SID**: The database name
    - **Instance**: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





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


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
EmbeddedDB
Host
localhost
Domain
Port
1528
User
admin
Schema
ADMIN
Database / SID
rmdb
Instance
UMS superuser
admin
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
RMDB
MyMicr...
SQL Se...
6
Add..
Edit..
Delete
Test
Activate
Deactivate

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 a Kerberos Configuration File

The Kerberos configuration file contains the data the system needs to access the domain information.

To learn how a Kerberos configuration file looks, see the following example:

```
[libdefaults]
default_realm = HEX.LOCAL
ticket_lifetime = 24h
[realms]
HEX.LOCAL = { kdc = 111.111.111.111 default_domain = HEX.LOCAL }
[domain_realm]
.hex.local = HEX.LOCAL
[appdefaults]
```

For a detailed description of the content, see https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html.

ℹ The domain does not have to be identical to the domain where the UMS is installed.

Saving the Kerberos Configuration File

→ Save the Kerberos configuration file in the directory `<UMS installation directory>/rmguiserver/conf` with the name `krb5.conf`

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 * [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.

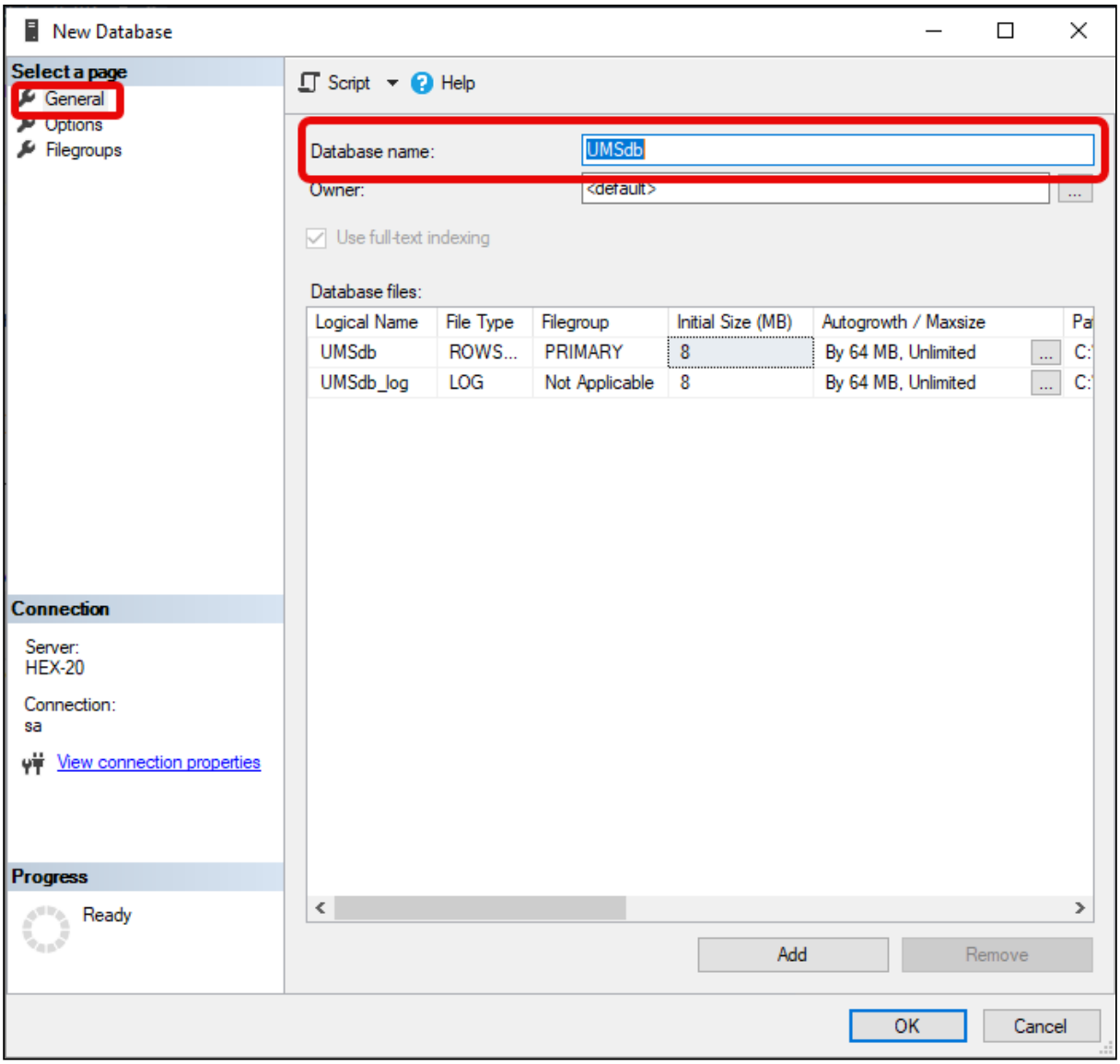
> Do NOT use the schema **dbo** for the UMS database tables!

- `<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.

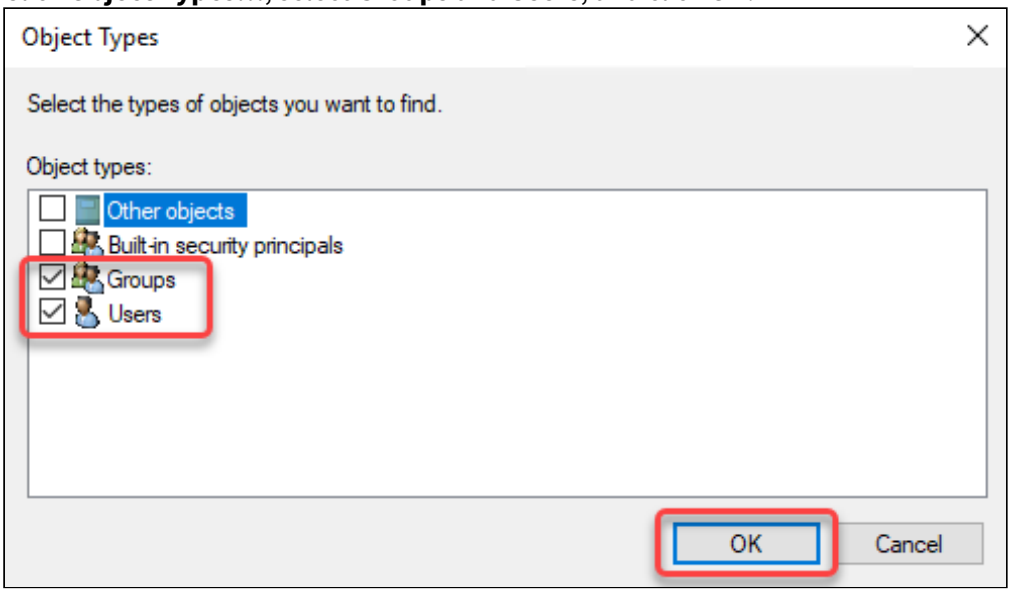
Using the SQL Management Console

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.

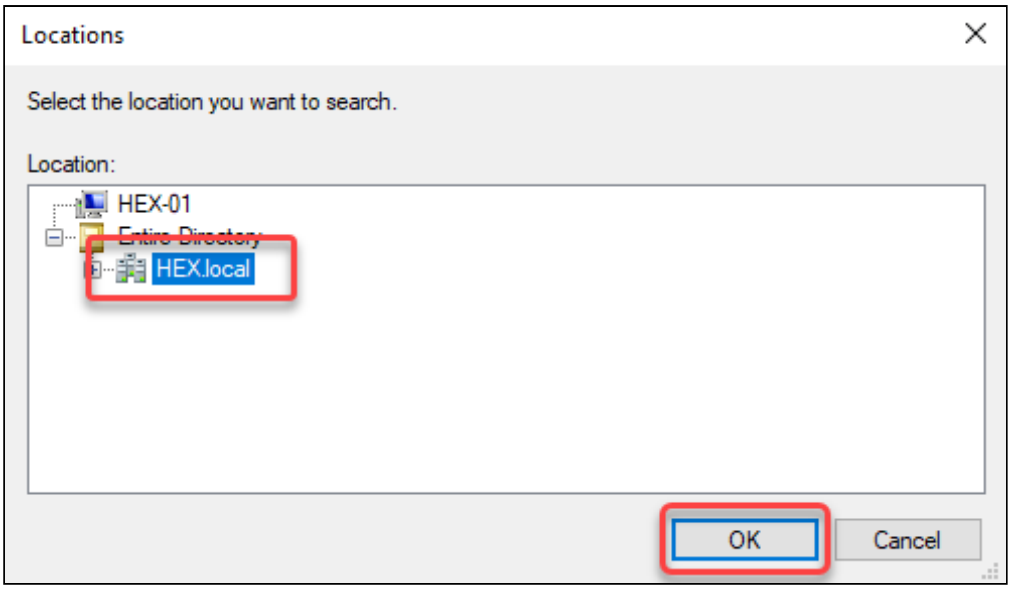
```
USE [master]
GO
CREATE LOGIN [[<ad_user>]] FROM WINDOWS;
GO
```

Using the SQL Server Management Studio (GUI Mode)

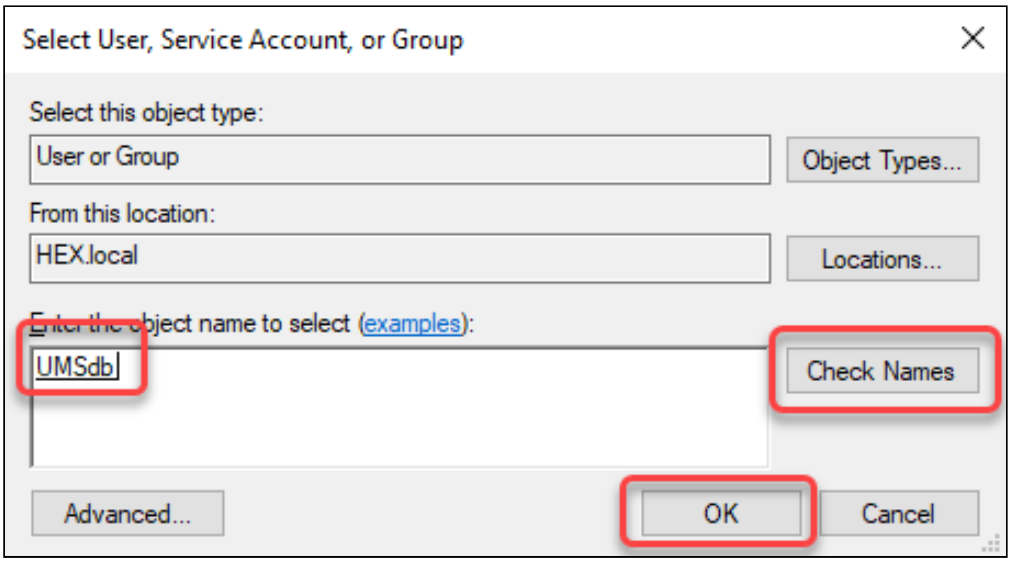
1. Connect to the database with the SQL Server Management Studio.
2. Open the **Security** branch, right-click on **Logins** and select **New Login**.
3. Choose **Windows Authentication** for the login, and click **Search**.
4. Click **Object Types...**, select **Groups** and **Users**, and click **OK**.



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

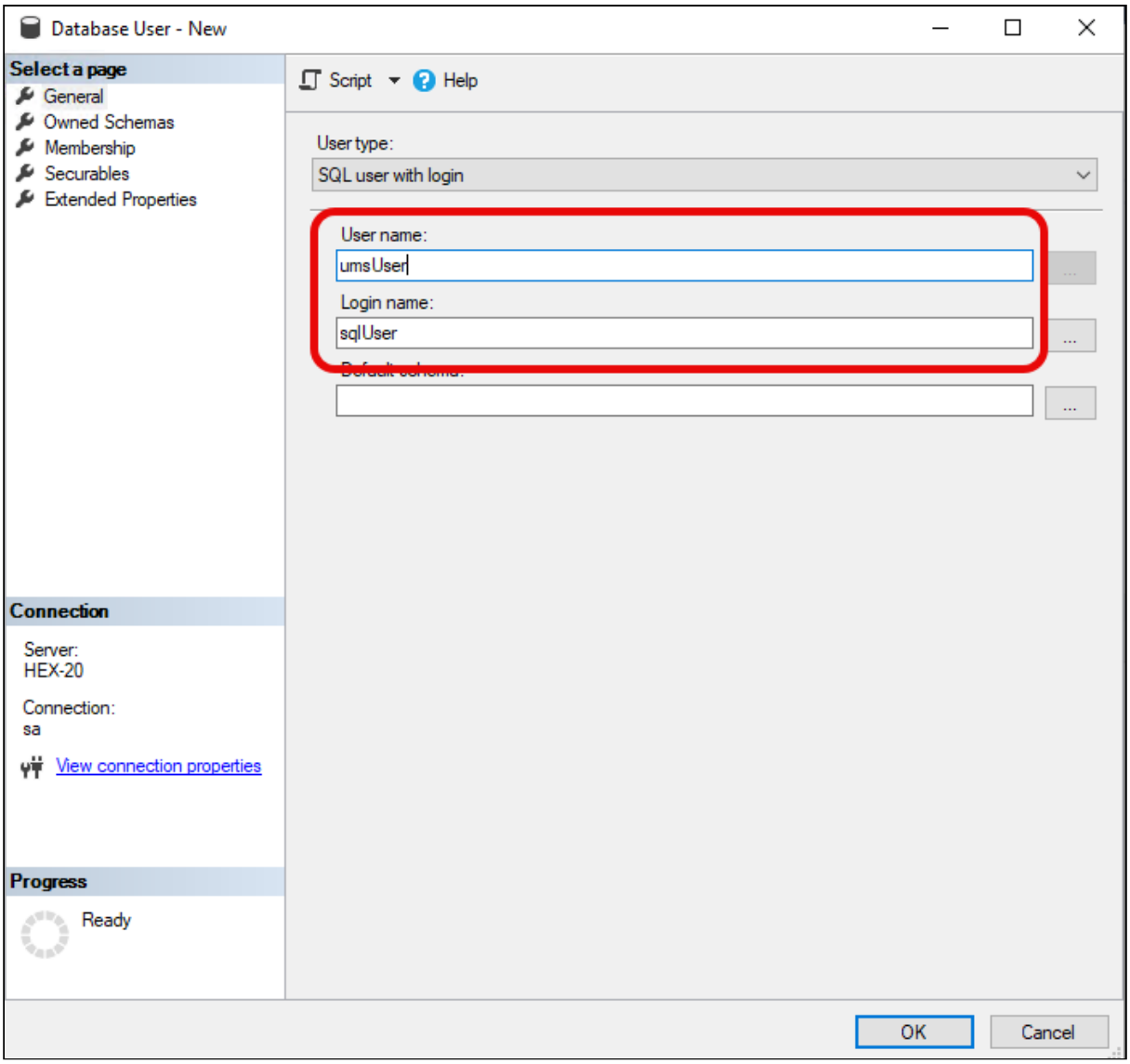
→ In the SQL Management Console, select **New Query** and enter the script below; please note the following.

- `<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.

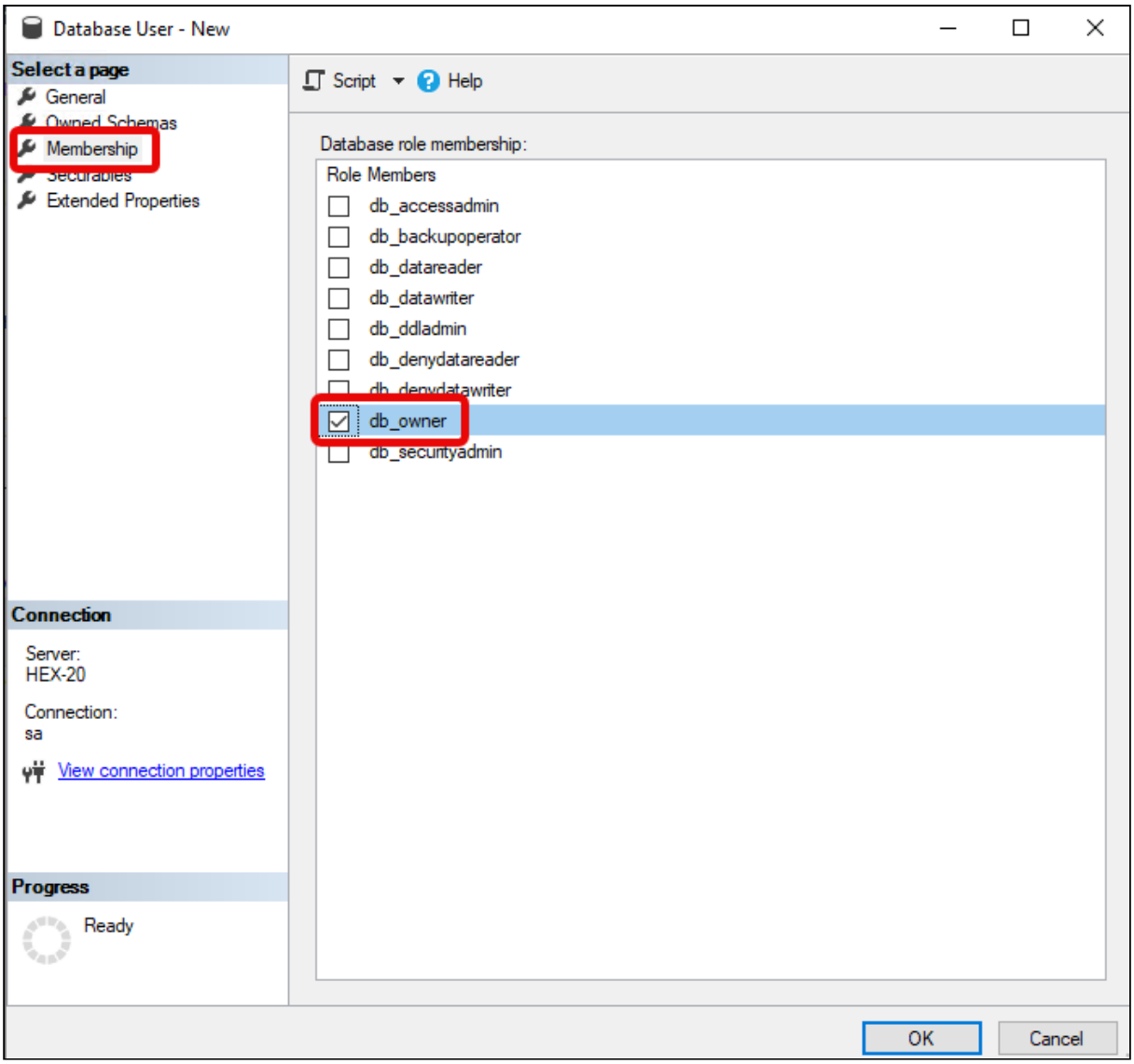
```
USE [<database_name>]
GO
CREATE USER [<ums_user>] FOR LOGIN [<ad_user];
GO
ALTER ROLE [db_owner] ADD MEMBER [<ums_user>];
GO
ALTER USER [<ums_user>] WITH DEFAULT_SCHEMA = [<schema_name>];
GO
ALTER AUTHORIZATION ON SCHEMA::[<schema_name>] TO [<ums_user>]
GO
```

Using the GUI

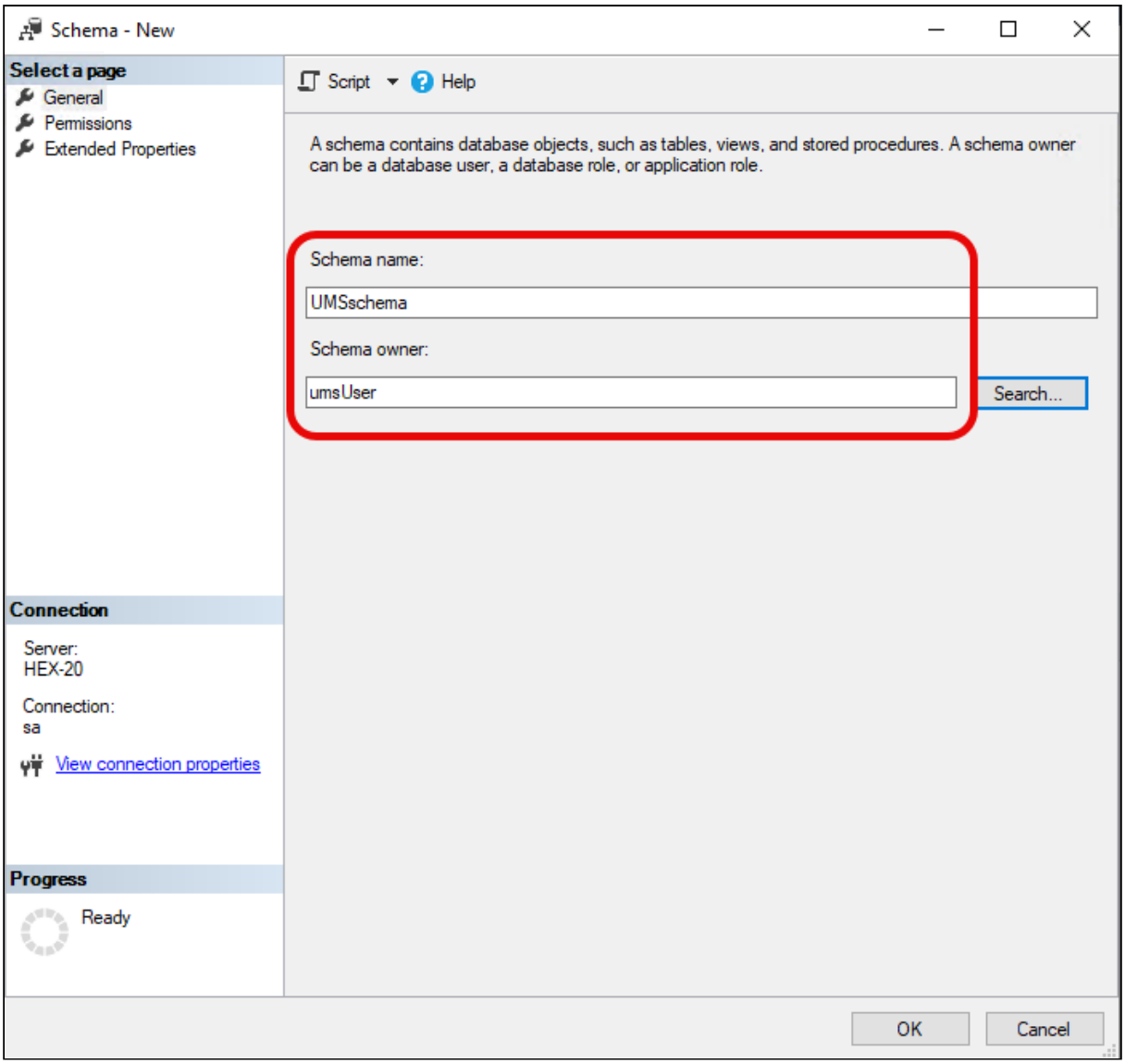
1. In SQL Server Management Studio, open the database that was created in Creating the UMS Database.
2. Under **Security > Users**, right-click **New User**.
3. Under **General**, search for your login name (<ad_user>) and give the user a name.



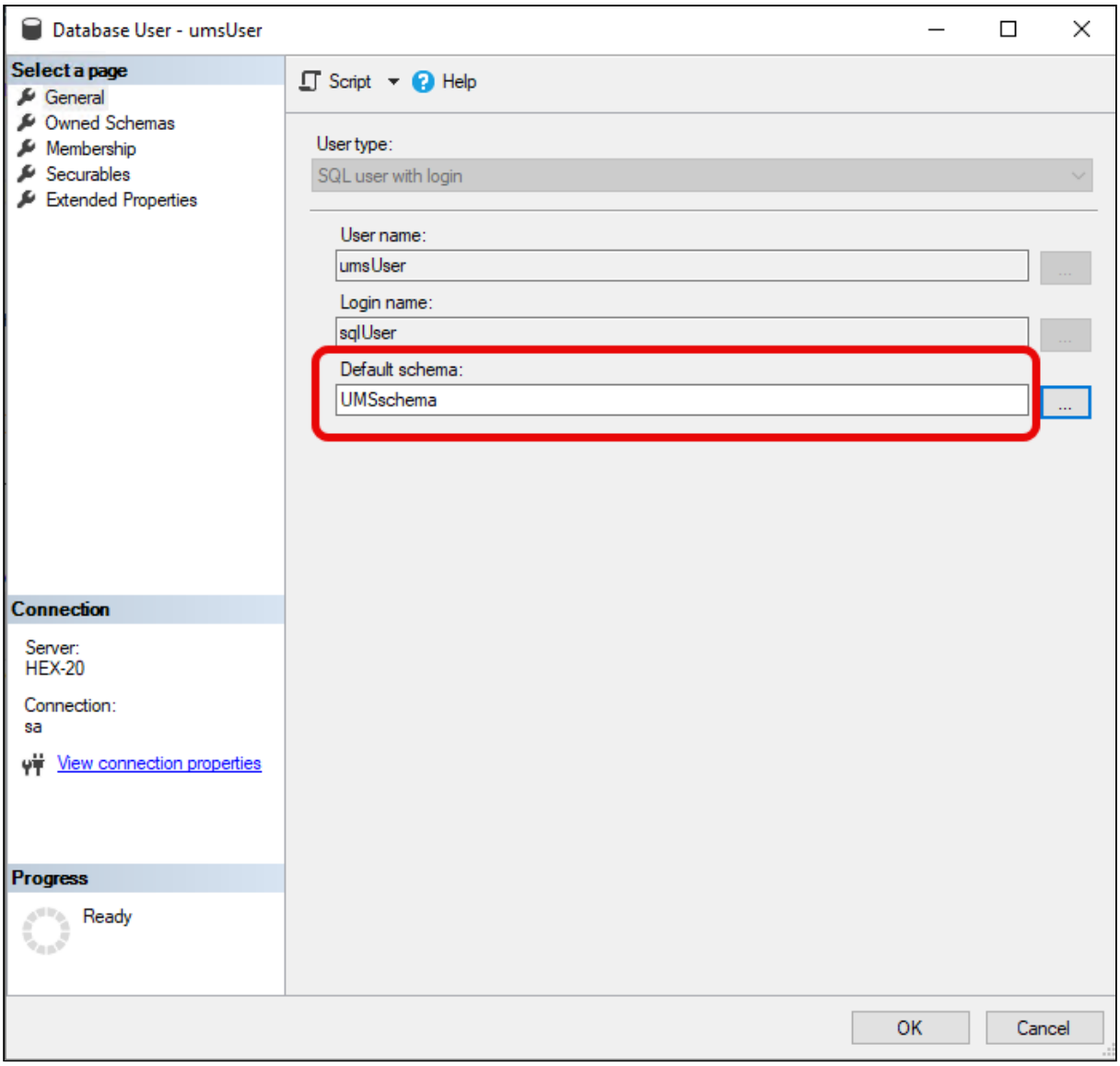
4. In the **Membership** area, give the user the **db_owner** role.



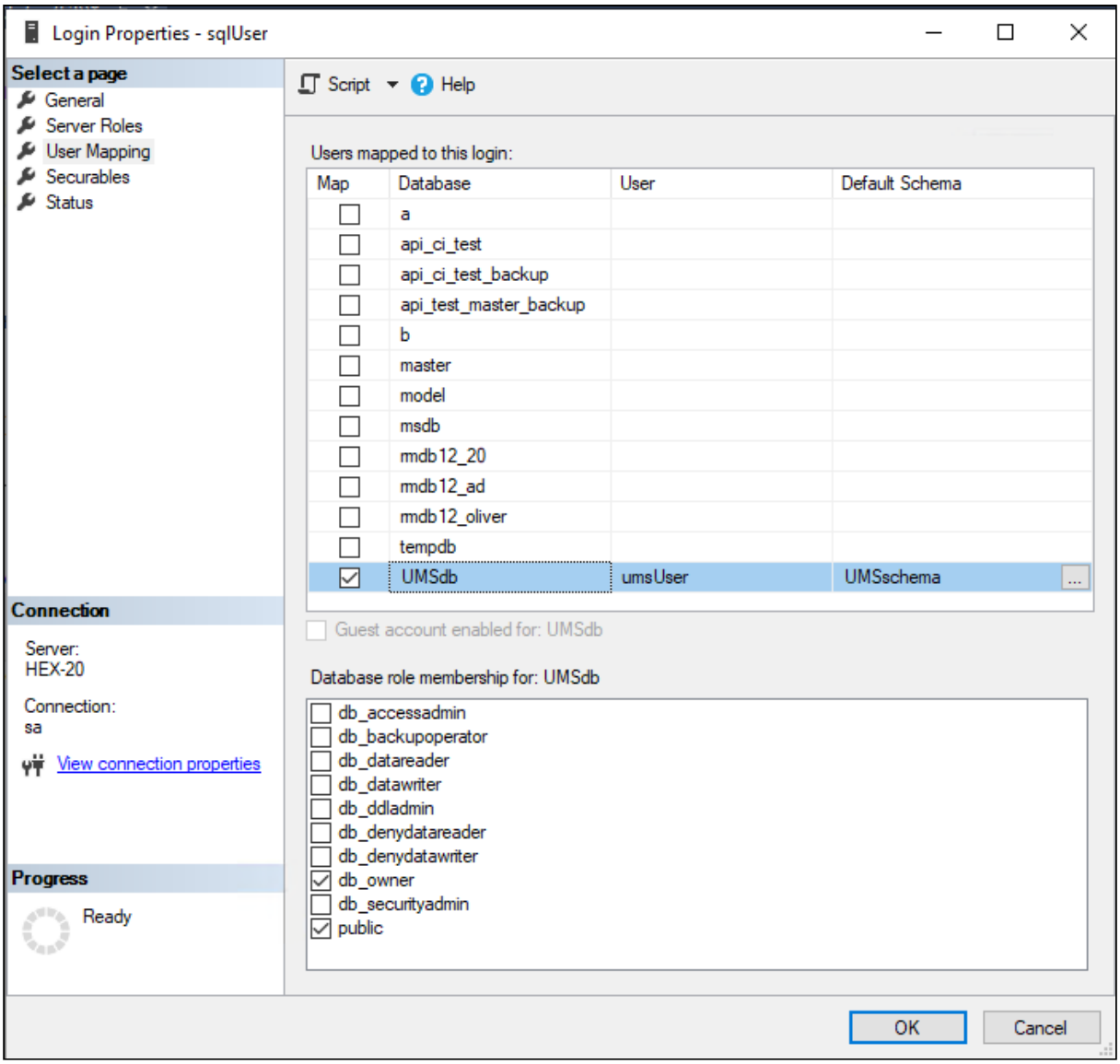
5. Go to **Security > Schemas** and right-click on **New Schema**.
6. Search for the <ums_user> as the **Schema owner** and provide a **Schema name**.



7. Under **Security > Users** in your UMS database, double-click on the <ums_user>.
8. Under **General**, set the default schema to <schema_name>.

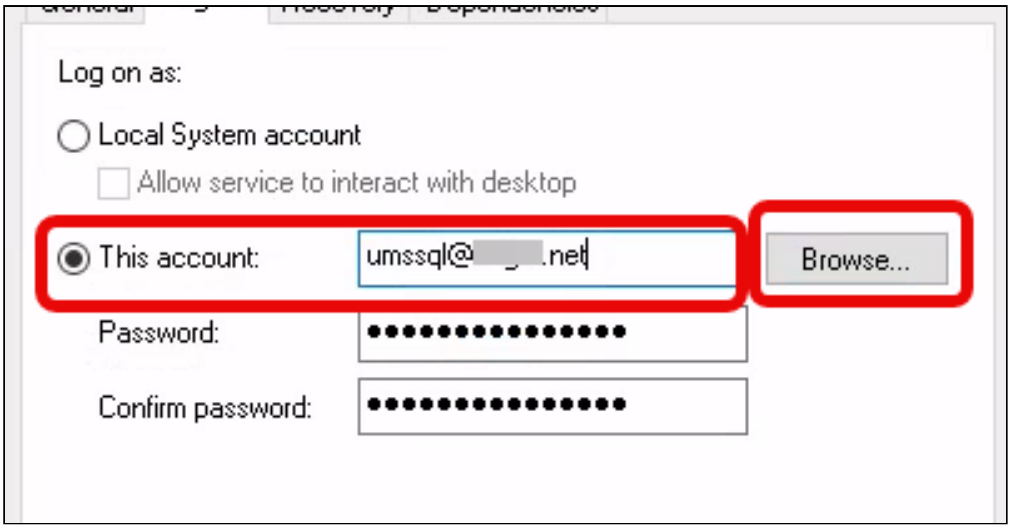


9. Under **Security > Logins > Users**, double-click on the <ad_user>.
10. In the **User Mapping** area, check the mapping of the UMS database, the user, and the default schema.



Configuring the UMS Services

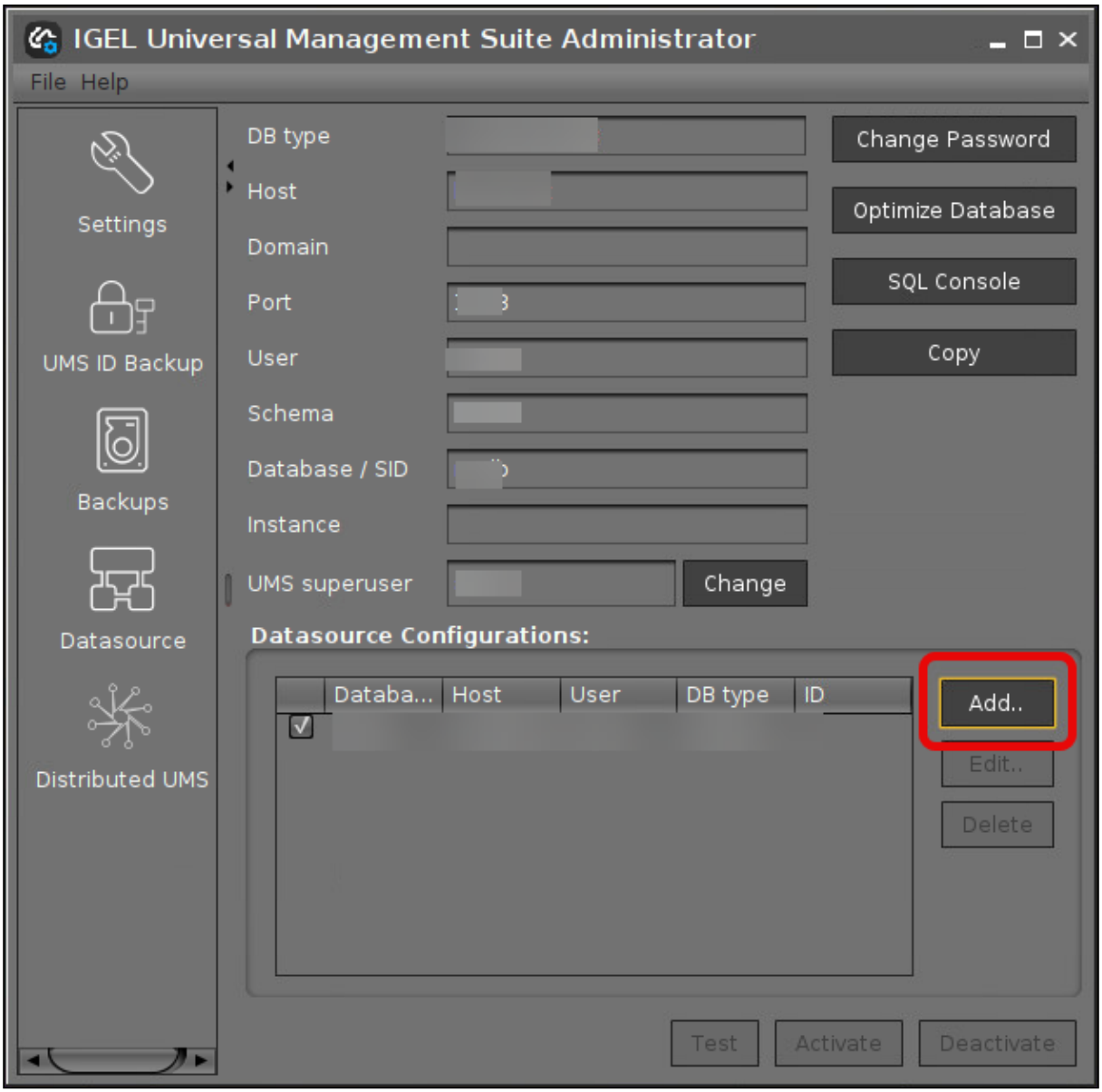
1. Log into the UMS Server with the credentials configured for connecting to the UMS database on the Microsoft SQL Server.
2. Open **services.msc** and right-click the **IGEL Remote Manager Server** service.
3. Select **Properties** and navigate to the **Log On** tab.
4. Select **This Account** and use the **Browse** button to find the one that owns the SQL database.

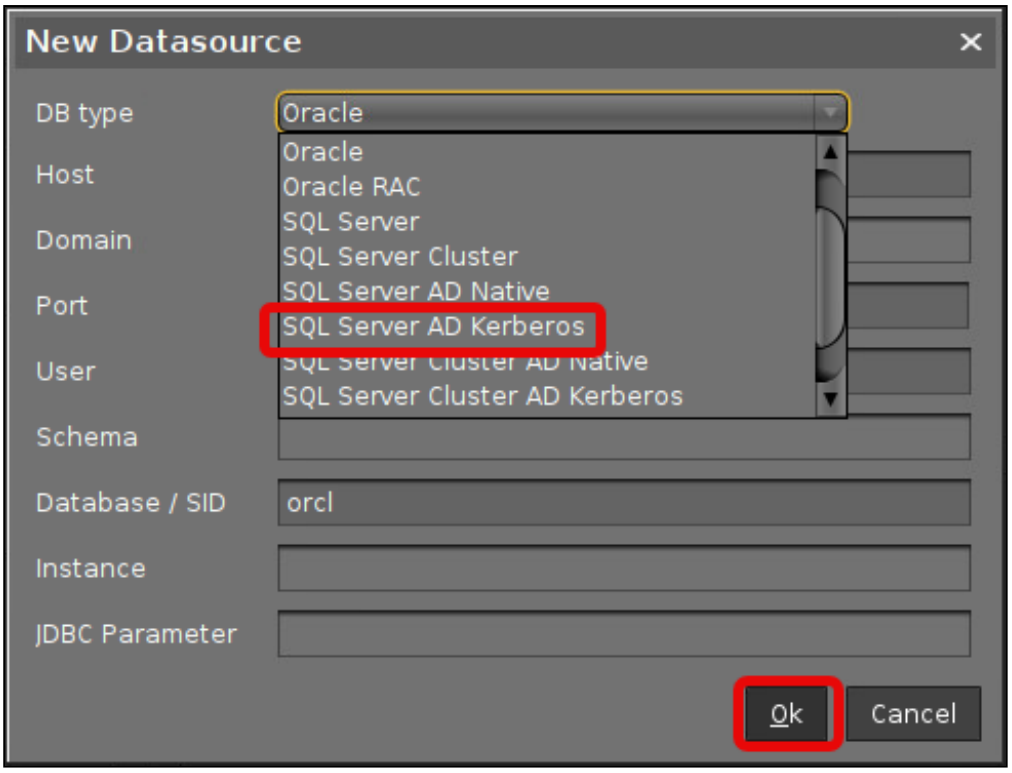


5. Depending on whether you are using a single server or a cluster for your Microsoft SQL database, continue with Connecting the UMS to the Database (Single Server Instance) or Connecting the UMS to the Database (Cluster),

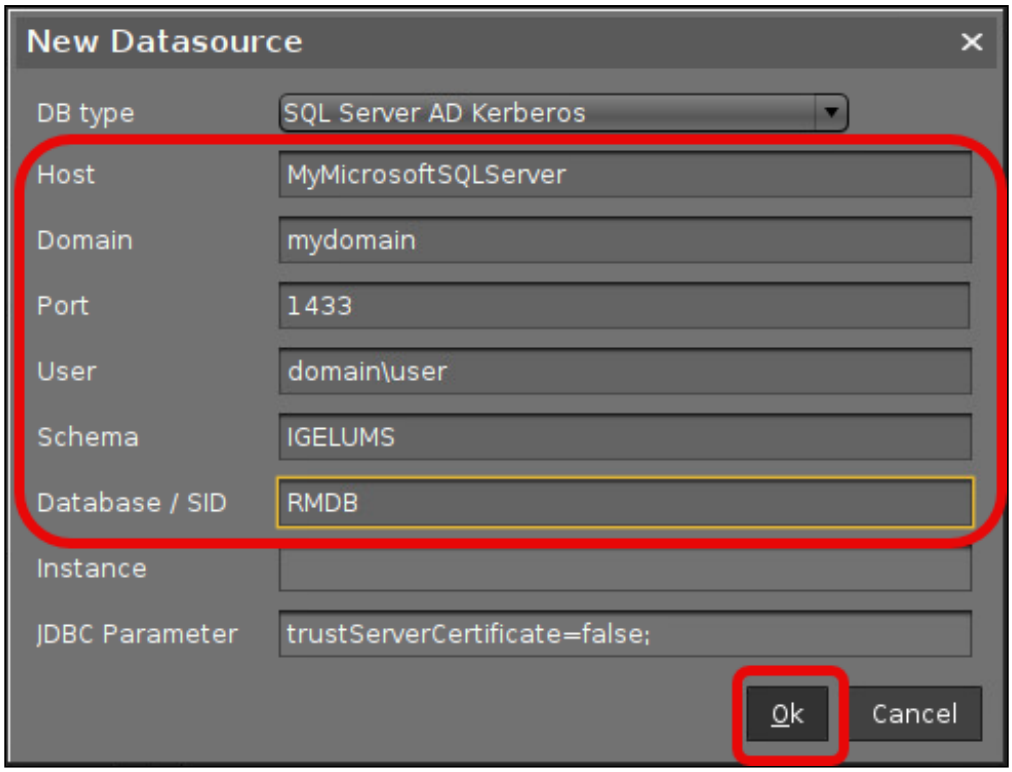
Connecting the UMS to the Database (Single Instance)

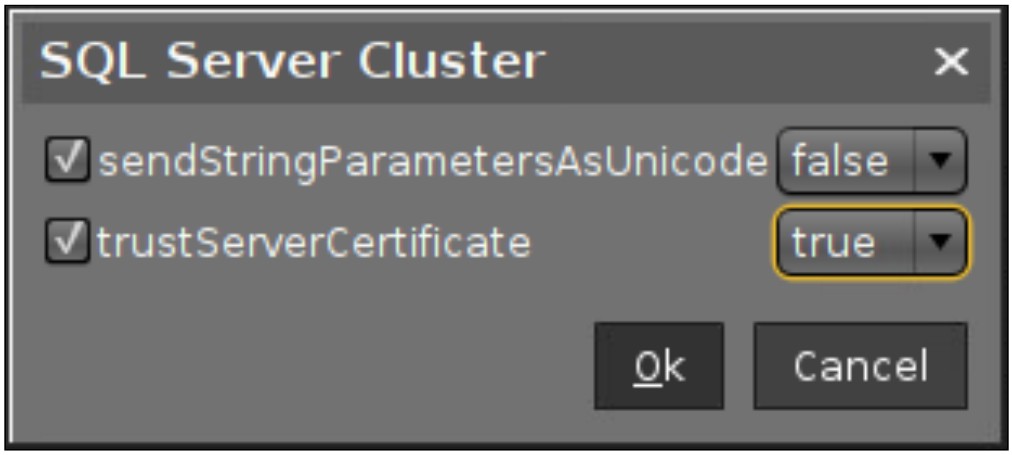
1. Set up a new **SQL Server AD Kerberos** type data source.


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
Host
Domain
Port
User
Schema
Database / SID
Instance
UMS superuser
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
Add..
Edit..
Delete
Test
Activate
Deactivate

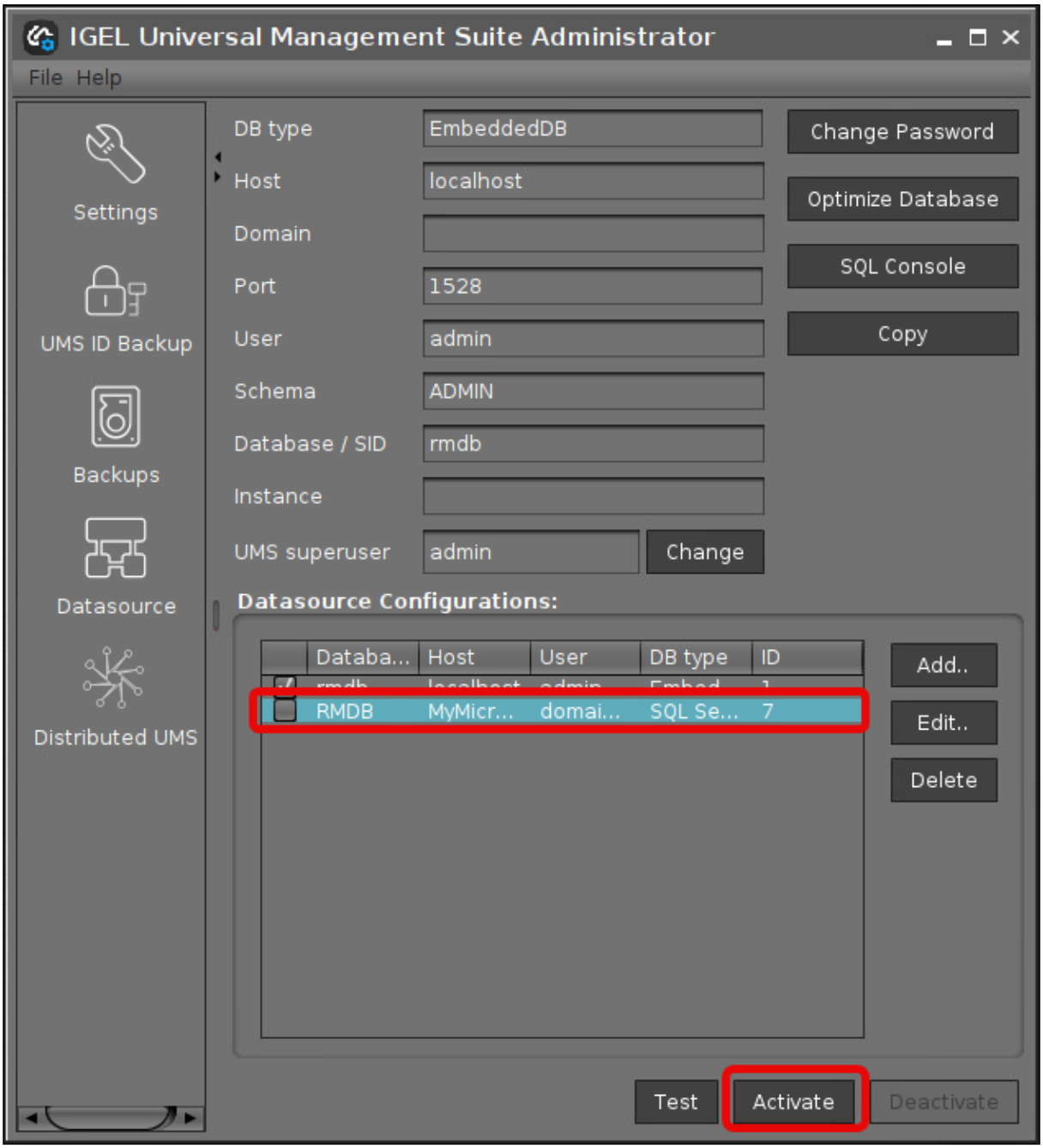


2. Edit the data as follows:
    - **Host**: The Fully Qualified Host Name (FQDN) of the Microsoft SQL server. If you deploy MS SQL Server Always On Availability Groups, enter the domain name of the Always On Availability Group listener.
    - **Domain**: The domain in which the <ad_user> is residing
    - **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**

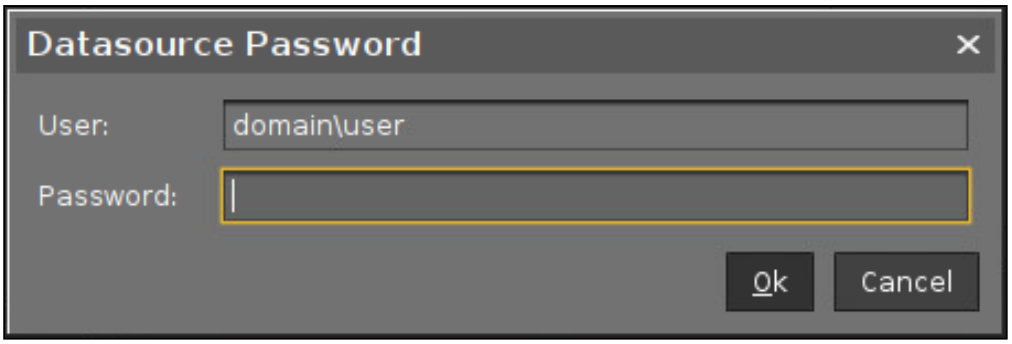




3. Select your database configuration and click **Activate**.

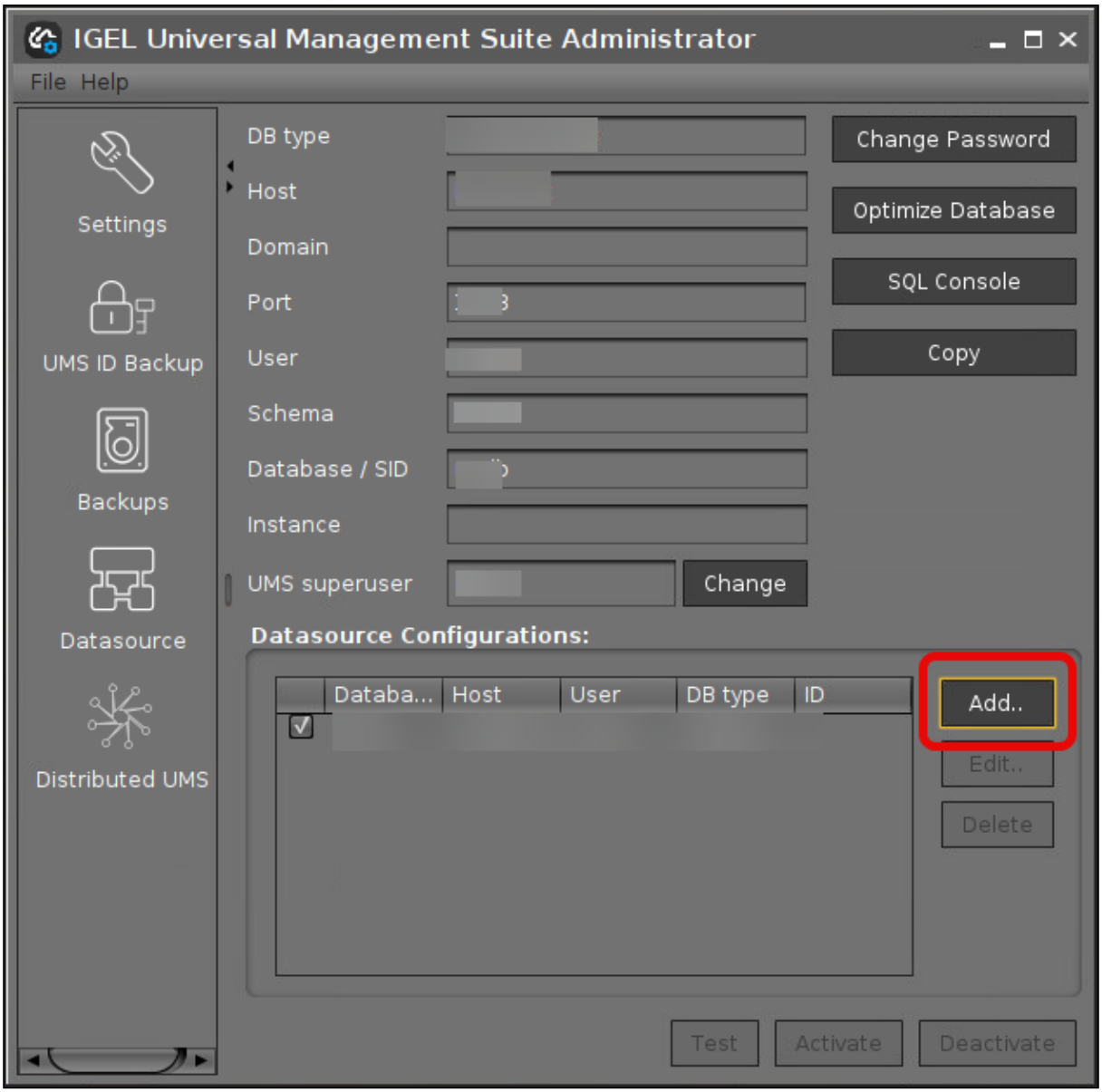


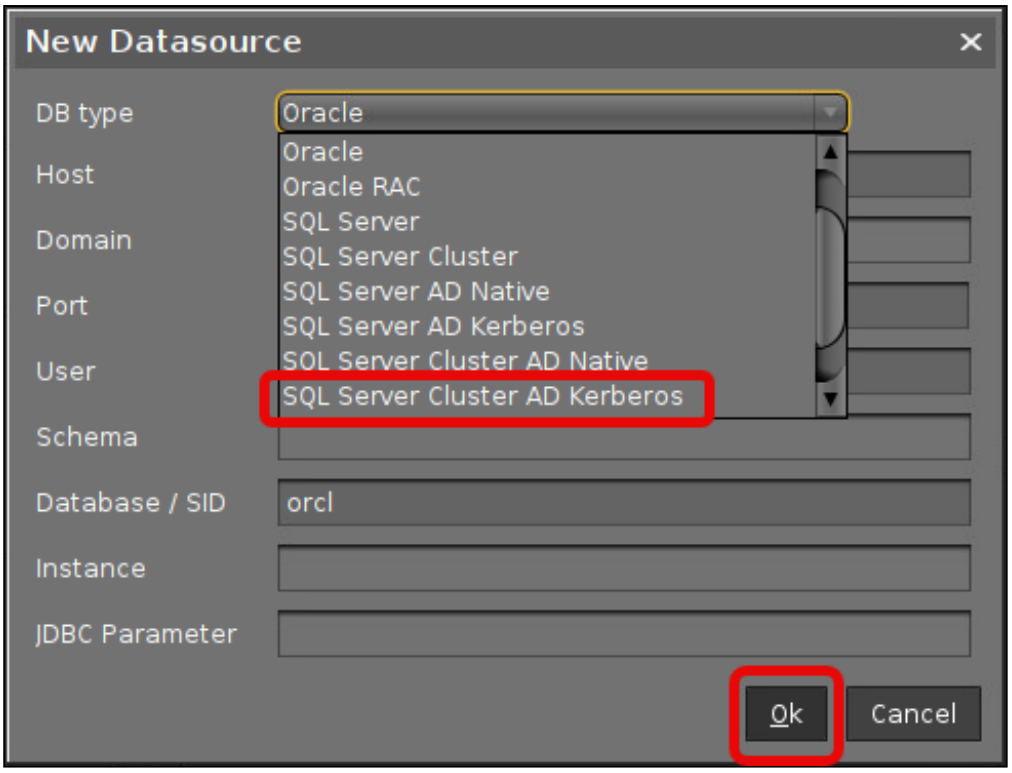
4. Enter the username and the password for the connection.



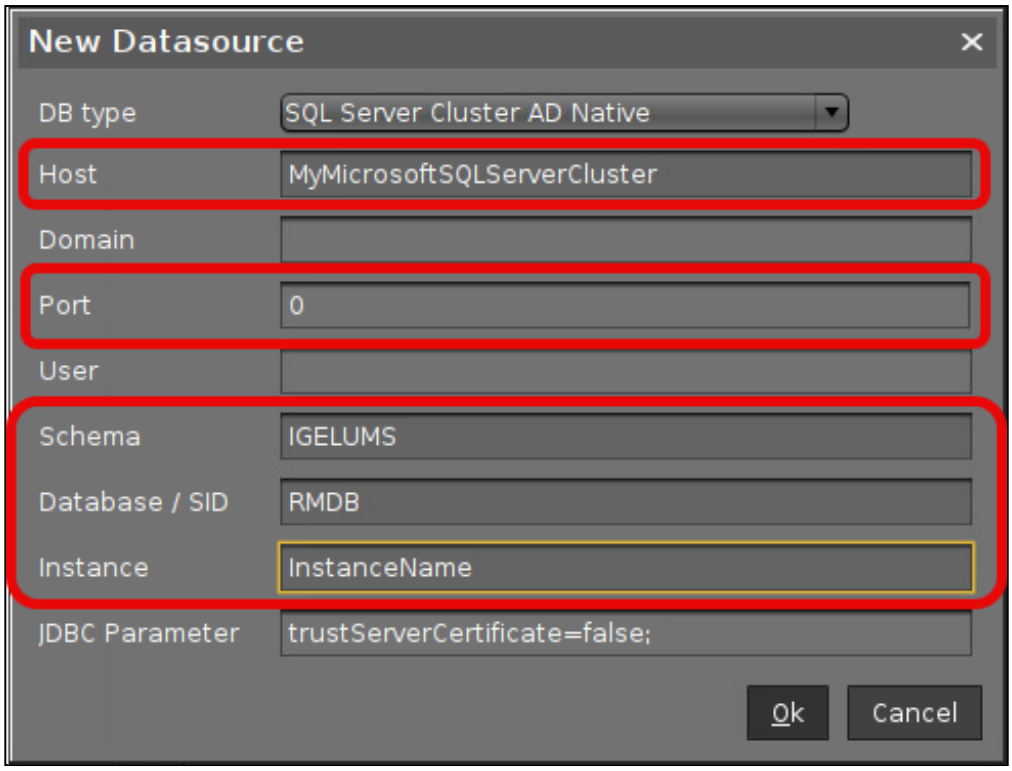
Connecting the UMS to the Database (Cluster)

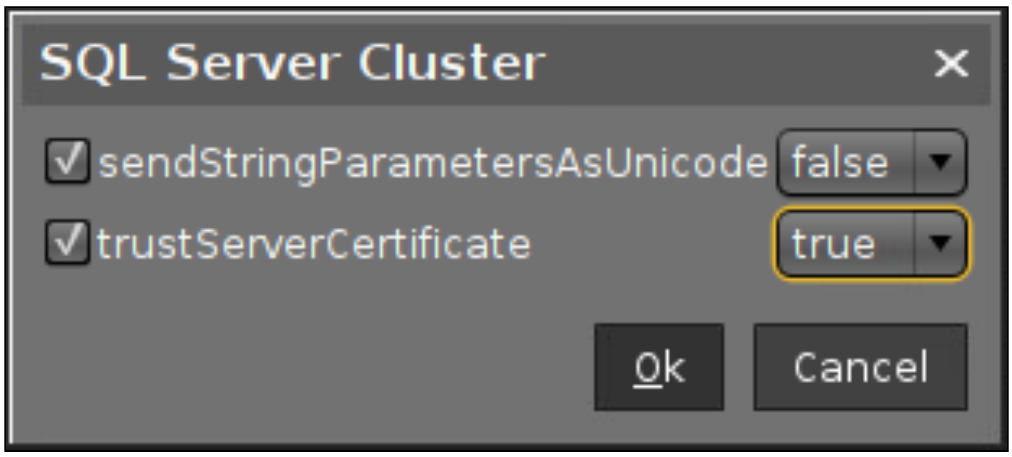
1. In the UMS Administrator (see page 1037), set up a new **SQL Server Cluster AD Kerberos** type data source.


IGEL Universal Management Suite Administrator
File Help
Settings
UMS ID Backup
Backups
Datasource
Distributed UMS
DB type
Host
Domain
Port
User
Schema
Database / SID
Instance
UMS superuser
Change
Change Password
Optimize Database
SQL Console
Copy
Datasource Configurations:
Databa...
Host
User
DB type
ID
Add..
Edit..
Delete
Test
Activate
Deactivate

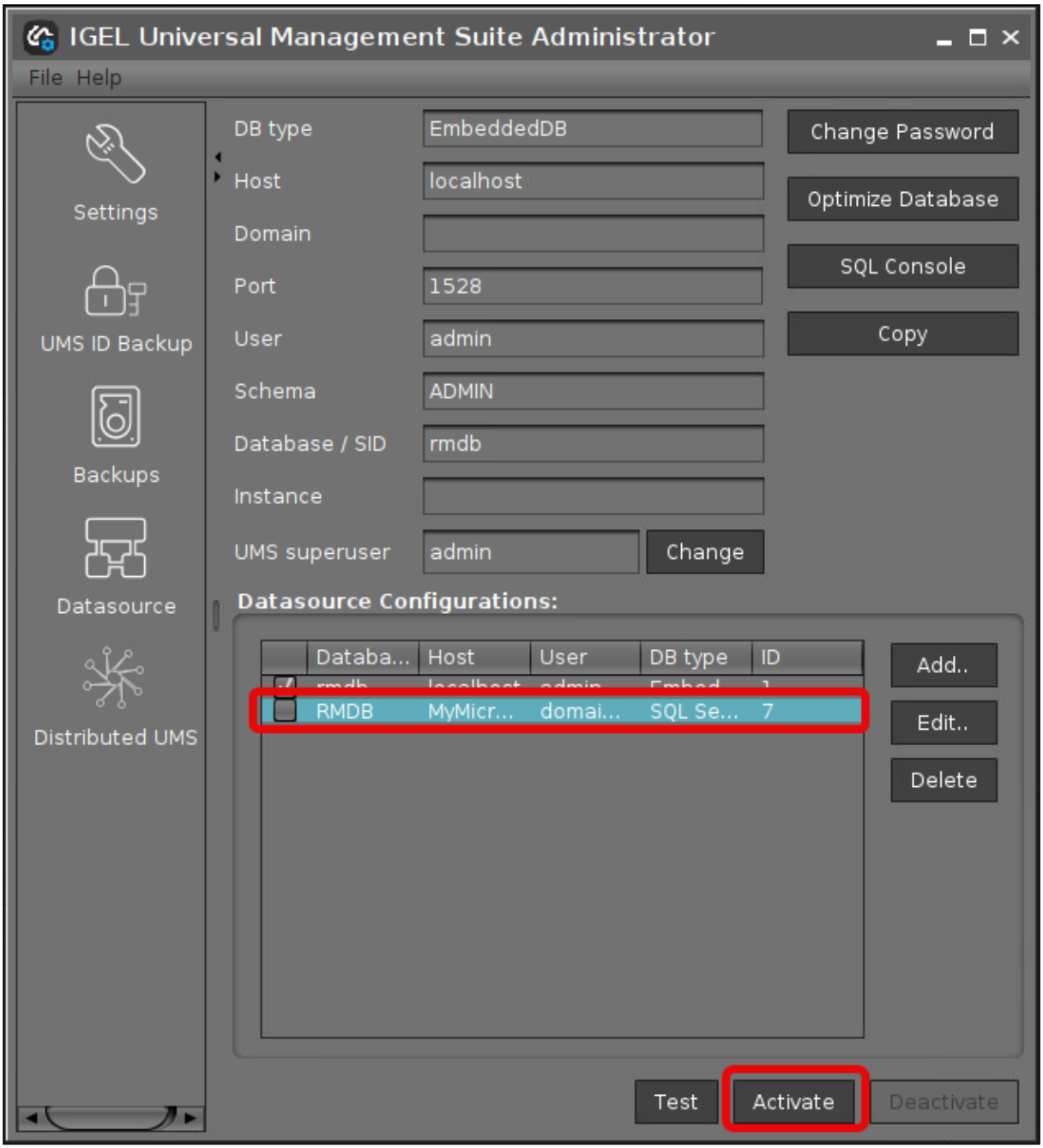


2. Edit the data as follows:
    - **Host**: The Fully Qualified Host Name (FQDN) of the Microsoft SQL server
    - **Port**: The port on which the Microsoft SQL Server listens for requests. (Default: 1433)
    - **Schema**: The database schema
    - **Database / SID**: The database name
    - **Instance**: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

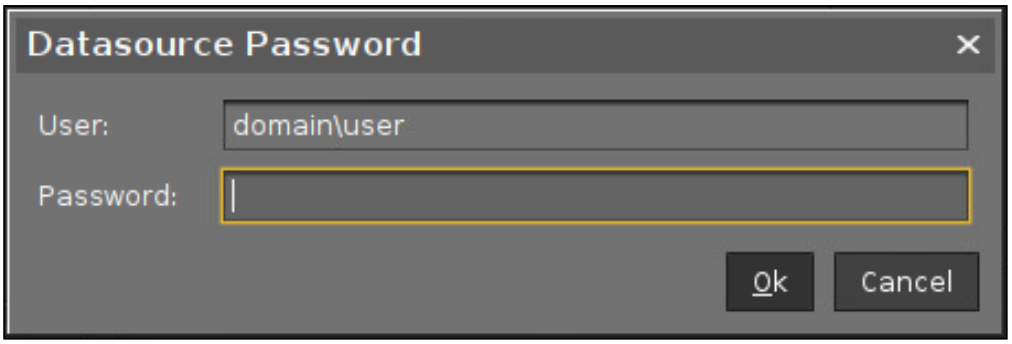




3. Select your database configuration and click **Activate**.



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


Datasource Password
User:
domain\user
Password:
Ok
Cancel

PostgreSQL

For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 1440). 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[30].

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

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

If the IGEL UMS Server is installed on the same machine as the PostgreSQL Server, no changes to these files are needed.

3. Launch the administration tool pgAdmin.

30. http://www.postgresql.org/

4. Create a new login role with the name `rmlogin.`
5. Create a new database with
   name = `rmdb`
   owner = `rmlogin`
   encoding = `UTF-8`
6. Set up a new schema within the rmdb database with
   name = `rmlogin`
7. Check whether the language plpgsql is available in the rmdb database.
   If not, set it up.
8. In the UMS Administrator (see page 1037), 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 (see page 1440). 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 1073).

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 (see page 1440). 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 cluster[31]. 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 1037), 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 document[32], 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 document[33], 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 document[34], 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**.

31. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
32. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
33. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
34. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

Using an Azure SQL Managed Instance Database with IGEL UMS

This article describes how to connect an Azure SQL Managed Instance database to the IGEL Universal Management Suite (UMS).

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 1440). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

Creating Your Azure SQL Managed Instance

→ Follow the steps described in the document Getting started with Azure SQL Managed Instance[35].

Connecting Your Azure SQL Managed Instance Database to Your UMS

→ In the UMS Administrator > Data Source (see page 1061), create a new data source with the following parameters:

- **DB type**: Microsoft SQL Server
- **Host**: The hostname or IP address of the Managed Instance
- **Port**: The port on which the Managed Instance listens for requests. (Default: 1433)
- **User**: The login name for connecting to the database
- **Database / SID**: The database name
- **Schema**: The database schema
- **JDBC Parameter** (double-click):
  - `sendStringParametersAsUnicode: false`
  - `trustServerCertificate: true`

Configuring Entra ID Authentication

→ Follow the steps described in the document Microsoft Entra authentication - Azure SQL Database & Azure SQL Managed Instance & Azure Synapse Analytics[36].

35. https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/quickstart-content-reference-guide?view=azuresql
36. https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-overview?view=azuresql

Login to the IGEL UMS

Here, you can find information about the login process and requirements for the IGEL Universal Management Suite (UMS).

UMS Login Requirements

With UMS 12.08.100, the login process has changed, which entails new requirements for your environments.

Overview

The main benefits of the new login process are:

- Increased security
- Support of Cloud IdPs, like Microsoft Entra ID, Okta, or PingIdentity
- Modernized and centralized login process for the UMS Web App and the UMS Console
  For the login process, see Connecting the UMS Console to the IGEL UMS Server[37].

The UMS login process uses the following protocols:

- oAuth2
- OpenID Connect
- JWT

Browser Requirements

The login procedure requires a modern browser on the system. For a list of supported browsers, see the Supported Environment section of the corresponding Release Notes[38].

UMS Web Certificate

The UMS Web Certificate must contain all possible address formats that will be used for login in the UMS Console or UMS Web App. The following formats are possible:

- FQDN
- ShortName (hostname only)
- IP address used to connect to the UMS Web App or the UMS Console

Reason: The login process executes a full SSL Handshake and verifies if the certificate presented is issued for the requested FQDN or IP Address.

UMS Server Public Address / Cluster Address

The public address of the UMS Server must be set correctly, in line with the UMS web certificate. For details, see Set the Correct Public Address and Public Web Port for each UMS server[39].

37. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server
38. https://kb.igel.com/en/universal-management-suite/current/ums-release-notes
39. https://kb.igel.com/en/universal-management-suite/current/post-installation-configuration-of-the-igel-ums-se#id-(12.07.110-en)Post-InstallationConfigurationoftheIGELUMSServer-SettheCorrectPublicAddressandPublicWebPortforeachUMSserver

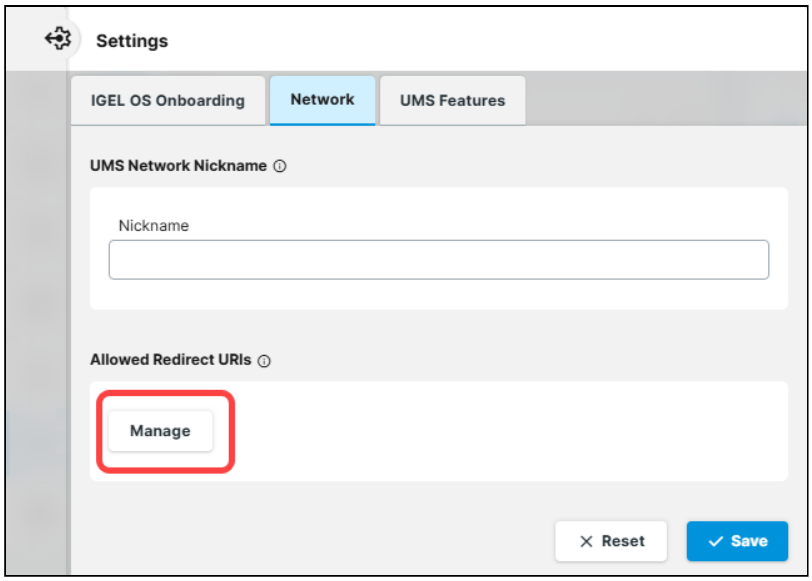
Reason: The authentication service of the UMS validates the redirect URI provided by the client (UMS Web App or UMS Console) against the registered values. From UMS 12.08.100 onward, the redirect URIs are derived from the UMS Server public address resp. the cluster address.

Logging in to the local machine as the UMS superuser (with “localhost” as the server address) is always possible. This can help fix login issues.

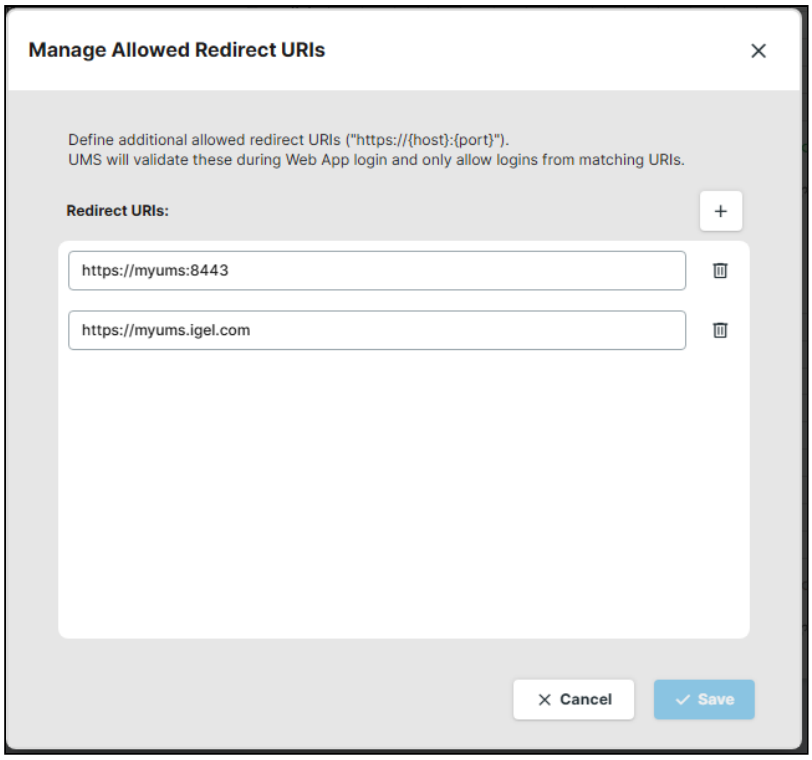
Redirect URIs for UMS Web App Login

If you use a URL to login to your UMS, which is not detected automatically (see above) you can add additional redirect URIs:

1. Log in to the UMS by logging in to the server itself with localhost.
2. Open the UMS Web App and go to **Network > Settings**.
3. Click **Manage** under **Allowed Redirect URIs**.



4. Add additional redirect URIs in the format `https://{host}:{port}`



After saving, you will be able to login with these configured URIs.

⚠ The redirect URIs configured here must be contained in the UMS Web Certificate.

Active Directory (AD) Users

An AD user must have a configured user name and password in the AD configuration to log in.

Reason: With the previous UMS version, the password of the login user was cached and used for refreshing the user data. Now, for security reasons, a valid AD user is required to refresh the user data. This user must have read access to user account details, group memberships, and other necessary AD data.

Connecting the UMS Console to the IGEL UMS Server

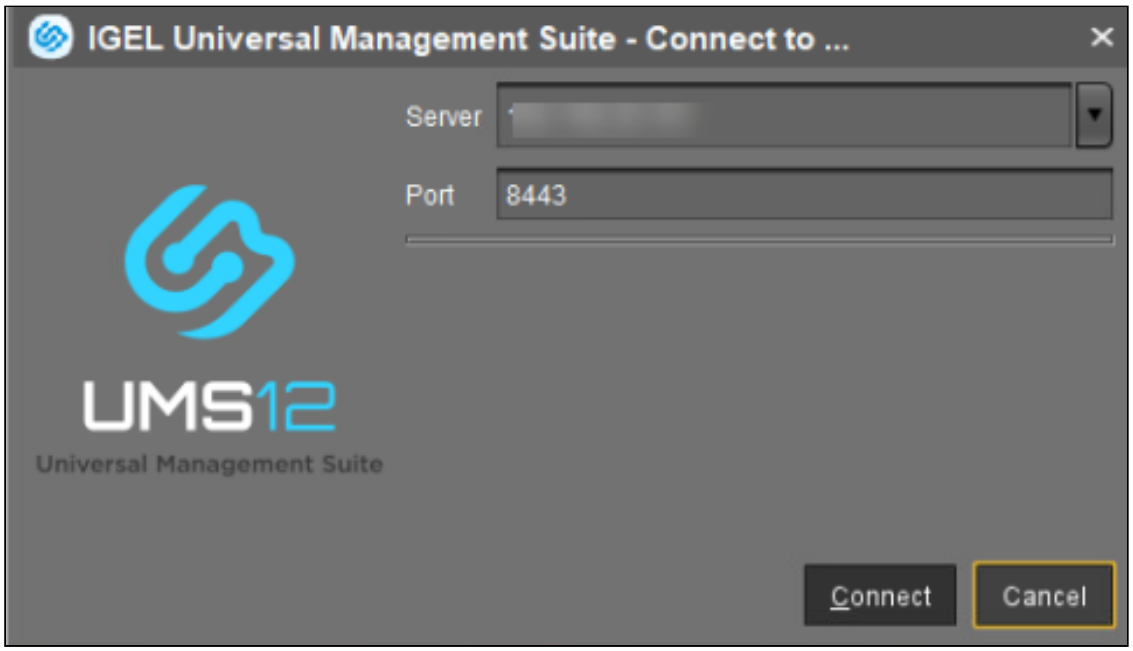
The following article describes the procedure for connecting the IGEL Universal Management Suite (UMS) Console to the UMS Server.

> 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`.

Login to the UMS Console as of UMS 12.08.100

If you are using IGEL UMS version 12.08.100 or higher, you can establish a connection to the UMS Server 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[40].



40. https://kb.igel.com/en/universal-management-suite/12.04.120/settings-change-server-settings-in-the-igel-ums-ad

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

3. Click **Connect**.
   You get redirected to the UMS login page. For the supported browsers, see the "Supported Environment" section in the corresponding release notes[41].

Error Message
You get the `Server is not fully running` error message when the `auth-service` of the UMS server is not yet running at the specified address. The browser is only opened if the `auth-service` is confirmed to be available and responsive.
Wait some time and try to connect again.

4. Provide the login data.

   User name: User name for the connection between the UMS Console / UMS Web App and the 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.
   For users imported via LDAP enter <username>@<domain>. For example:
   `username@domainname.com`

   Password: Password for the connection between the UMS Console / UMS Web App and the 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.

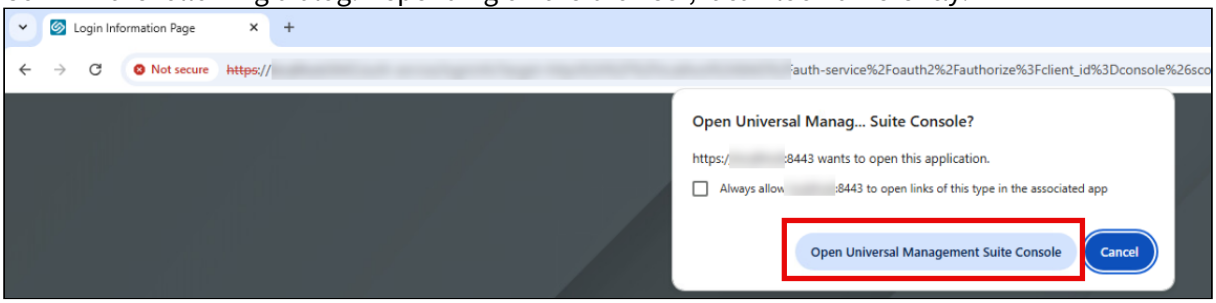
To ensure that all UMS users can log in to the UMS without any issues, please check the UMS Login Requirements[42].

41. https://kb.igel.com/en/universal-management-suite/current/ums-release-notes
42. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

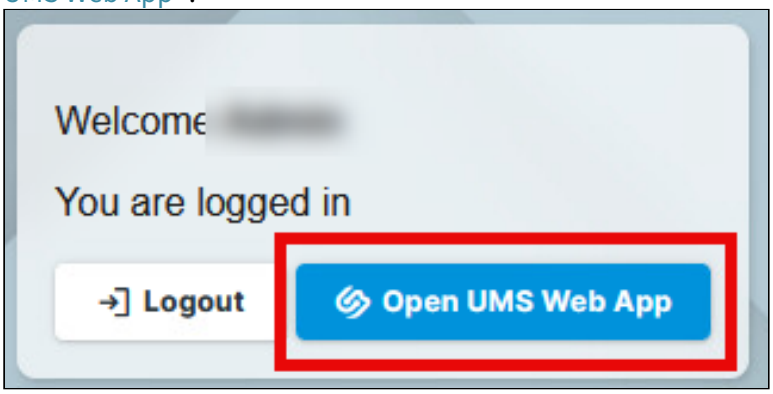
5. Click **Login**.

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 login dialog will show a corresponding message when the user account is locked.

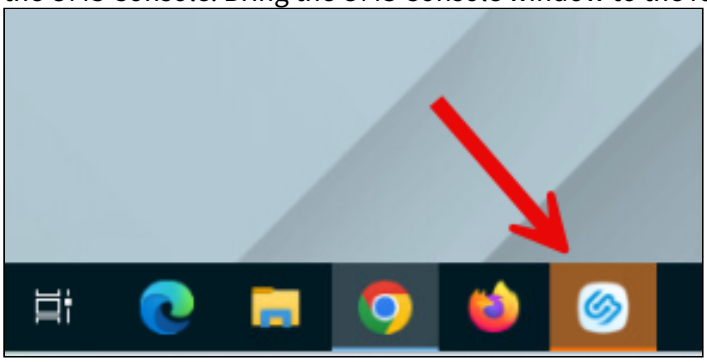
6. Confirm the following dialog. Depending on the browser, it can look differently.



7. Now you are logged in and can continue with
   - the UMS Web App: Click **Open UMS Web App** in the login dialog.
     For additional information on logging in to the UMS Web App, see How to Log In to the IGEL UMS Web App[43].



   - the UMS Console: Bring the UMS Console window to the foreground.



Troubleshooting

With UMS 12.08.100, a new login process is introduced with a new set of requirements for your environment. If you experience any issue during the login, see the related troubleshooting articles under Start of the UMS Console / Web App[44].

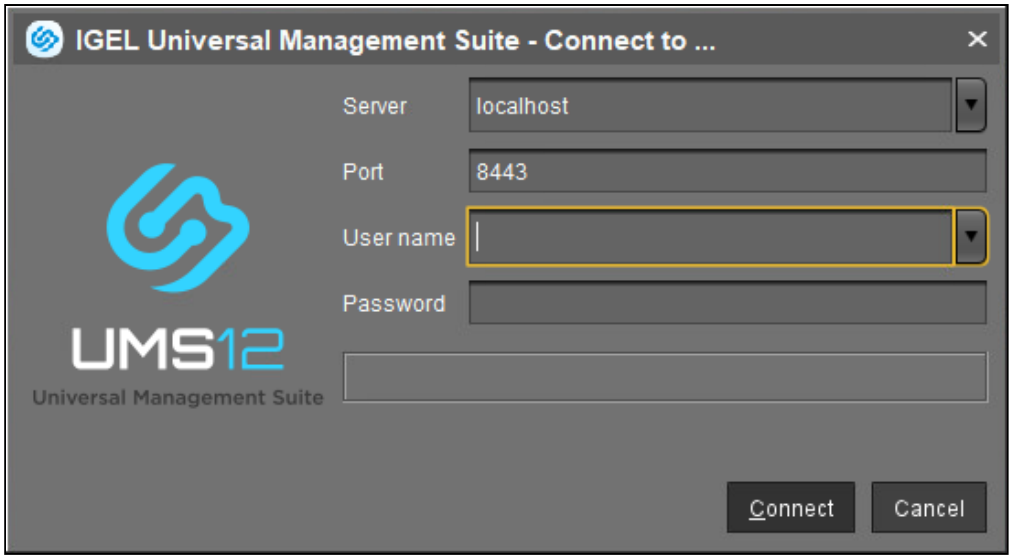
Login to the IGEL UMS Console before UMS 12.08.100

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

1. Start the UMS Console.
2. Enter the access data:

43. https://kb.igel.com/en/universal-management-suite/current/how-to-log-in-to-the-igel-ums-web-app
44. https://kb.igel.com/en/universal-management-suite/current/start-of-the-ums-console-web-app

- **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[45].
- **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.
  For users imported via LDAP enter <username>@<domain>. For example: `username@domainname.com`
- **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**.

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.

45. https://kb.igel.com/en/universal-management-suite/12.04.120/settings-change-server-settings-in-the-igel-ums-ad

How to Set Up UMS Login with SSO

You can use the following Identity Providers (IdPs) to access the Unified Management Suite (UMS):

- Microsoft Entra ID (see page 139)
- Okta (see page 168)
- Ping Identity (see page 186)

Each IdP requires specific configurations and role mappings to facilitate seamless user authentication and authorization within the UMS.

Basically, setting up an IdP for the UMS involves 4 steps:

1. Create an application in your Cloud IDP
2. Set up users and groups resp. app roles in your Cloud IDP
3. Configure your IDP connection in the UMS Console
4. Map IDP roles to UMS groups

The steps are described in general terms below; your mileage, including the exact wording of concepts like “client id”, may vary depending on the IdP you are using.

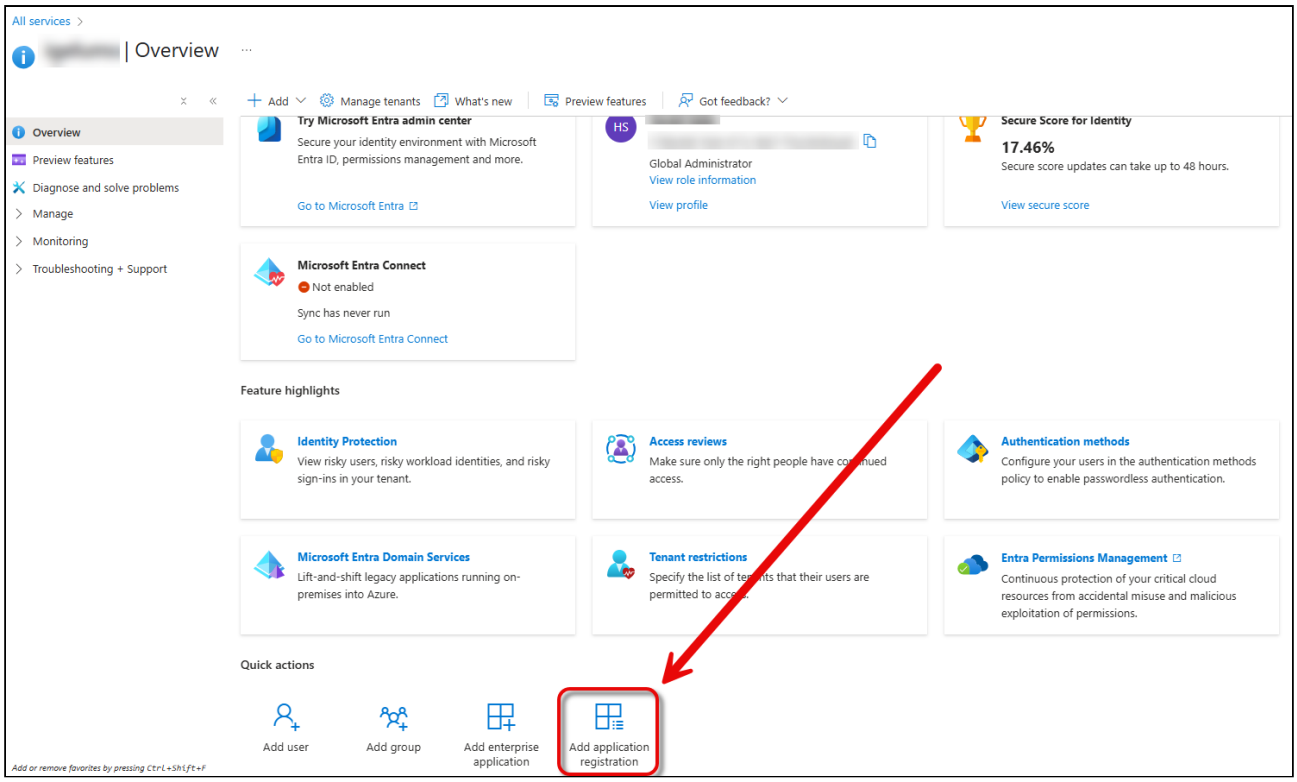
Prerequisites

- Users and groups with the appropriate permissions are already configured in your UMS

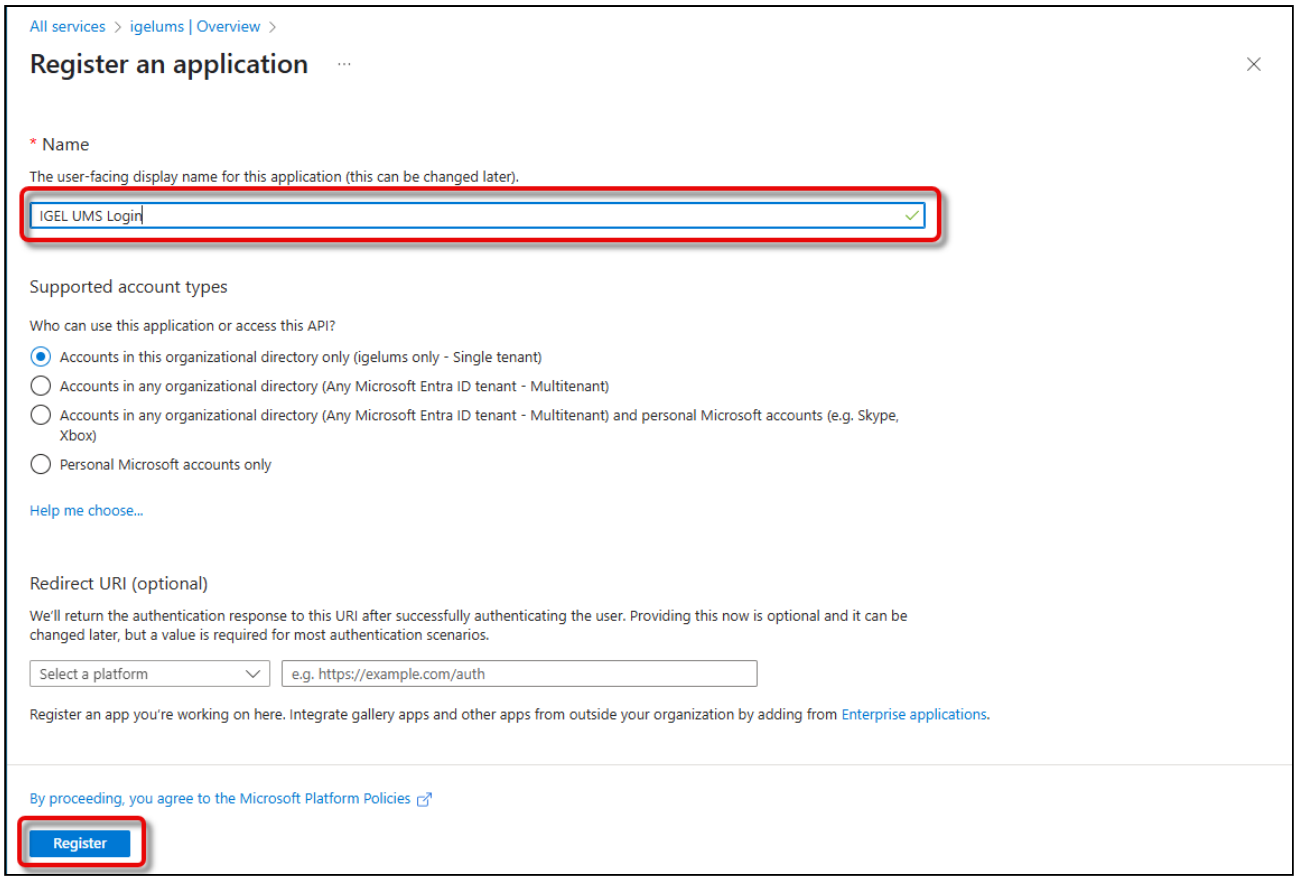
UMS Login with Microsoft Entra ID

Creating an Application in Microsoft Entra ID

1. Log in to the Microsoft Entra ID portal and click **Add application registration**.

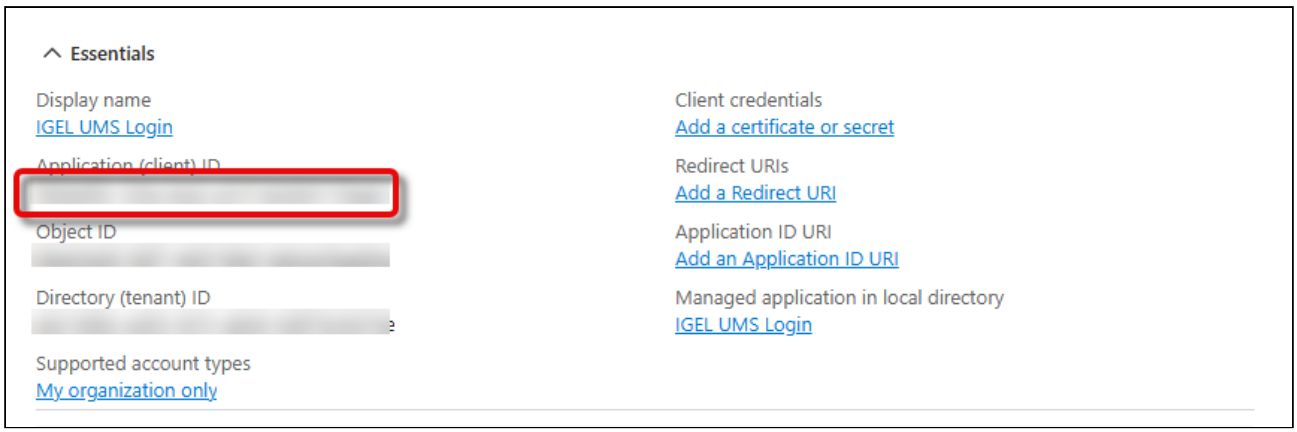


2. Enter a **Name** for this application. It is recommended to use a descriptive name, as this name is user-facing. Afterward, click **Register**.

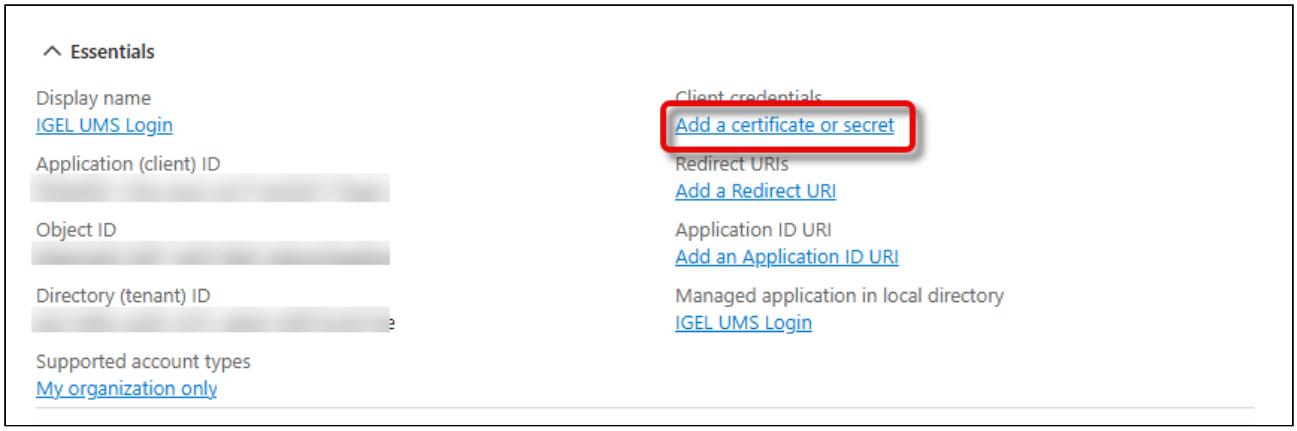


The essential data for your application is displayed.

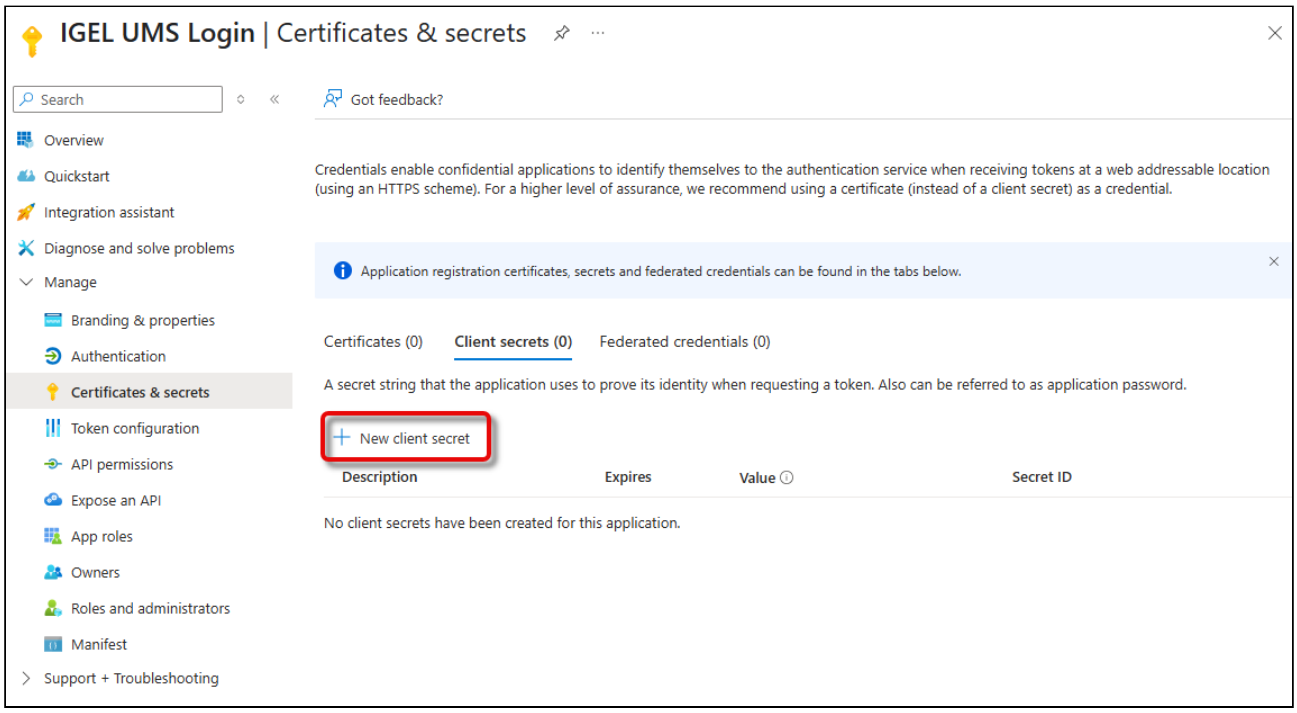
3. From the field **Application (client) ID**, copy the application ID, also referred to as the client ID.



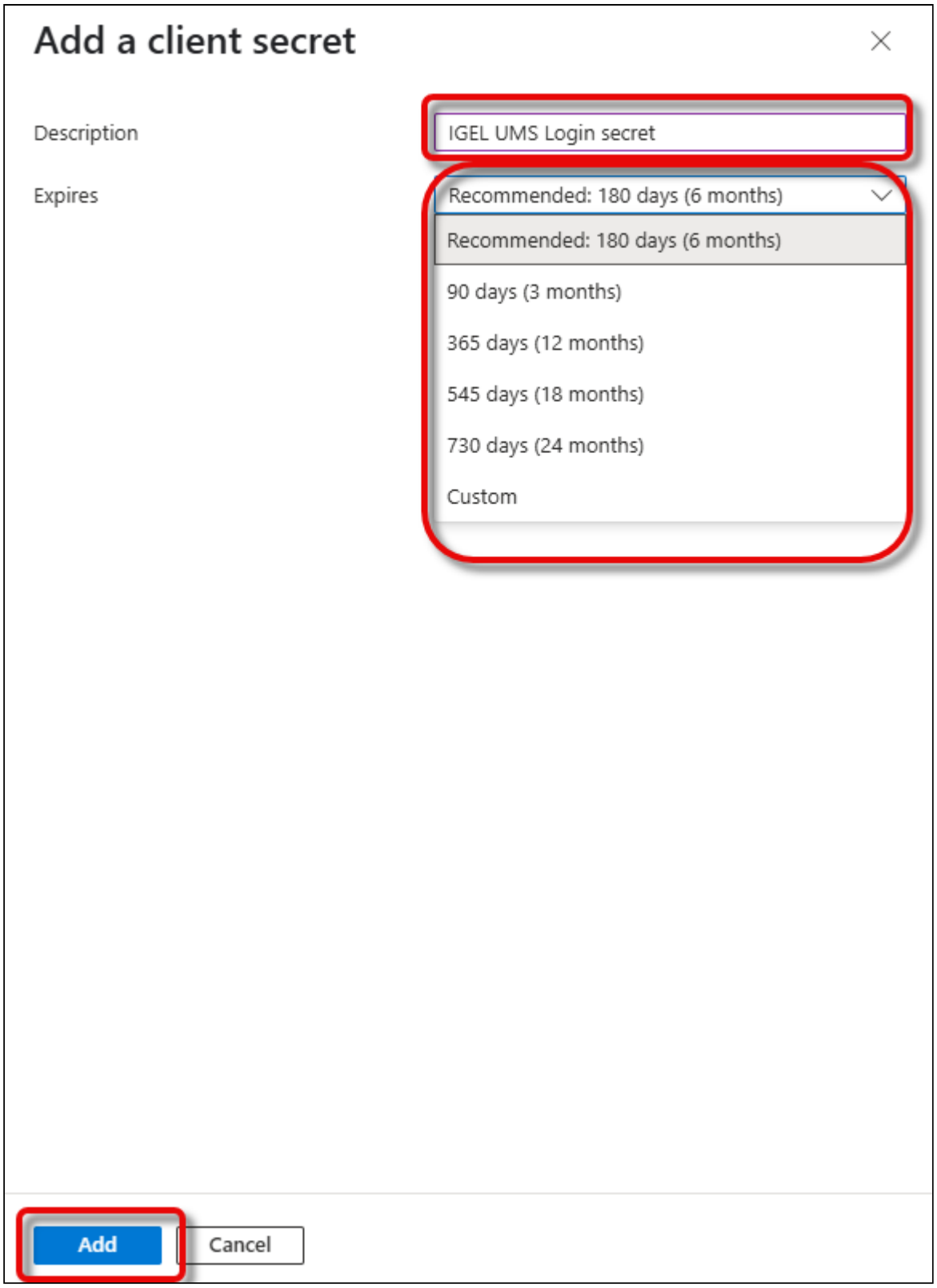
4. To open the menu for secret creation, click **Add a certificate or secret**.



5. Click **New client secret**.

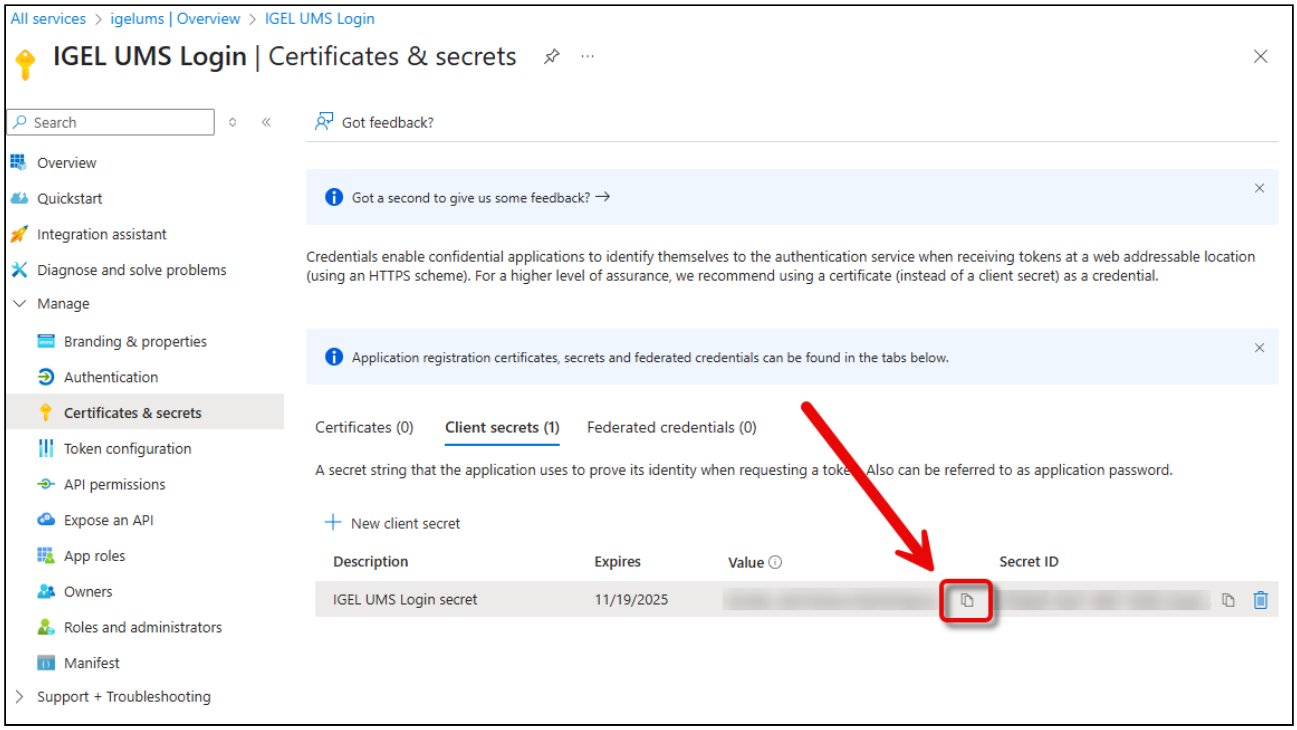


6. Add a description and an expiry date for your secret and click **Add**.

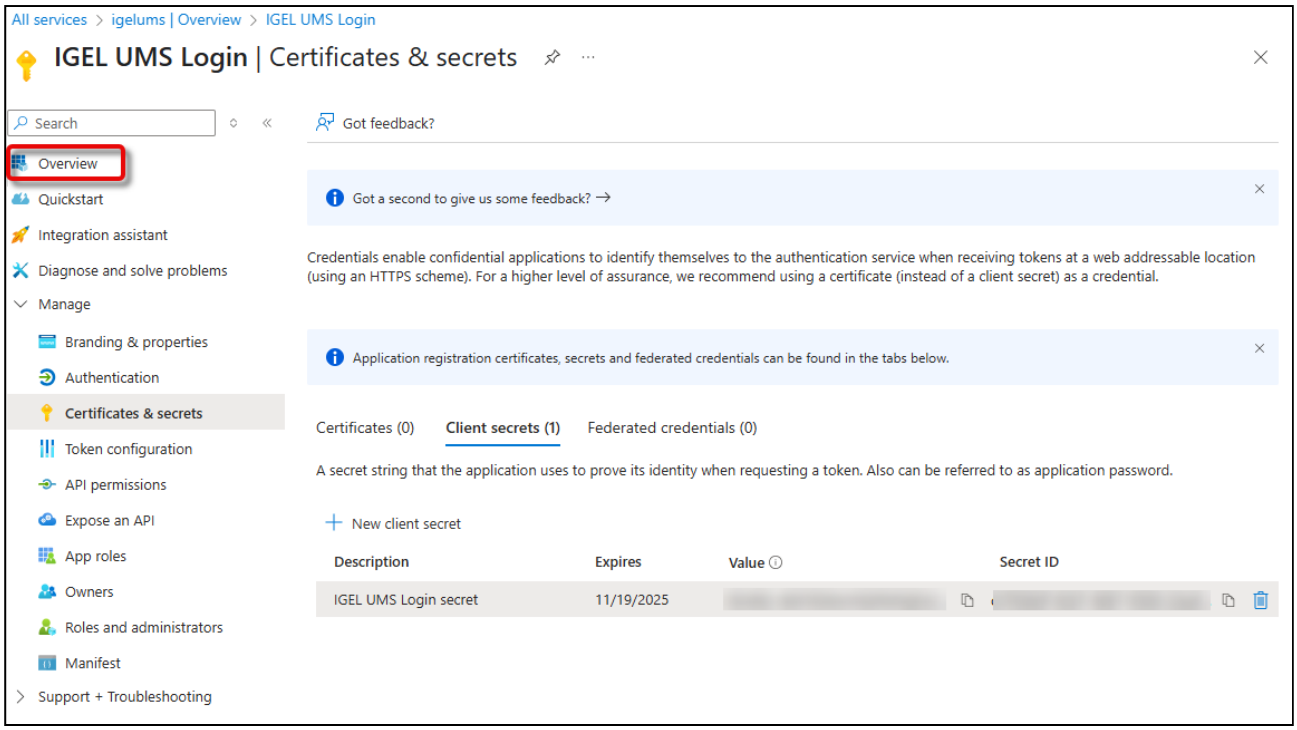

Add a client secret
Description
IGEL UMS Login secret
Expires
Recommended: 180 days (6 months)
Recommended: 180 days (6 months)
90 days (3 months)
365 days (12 months)
545 days (18 months)
730 days (24 months)
Custom
Add
Cancel

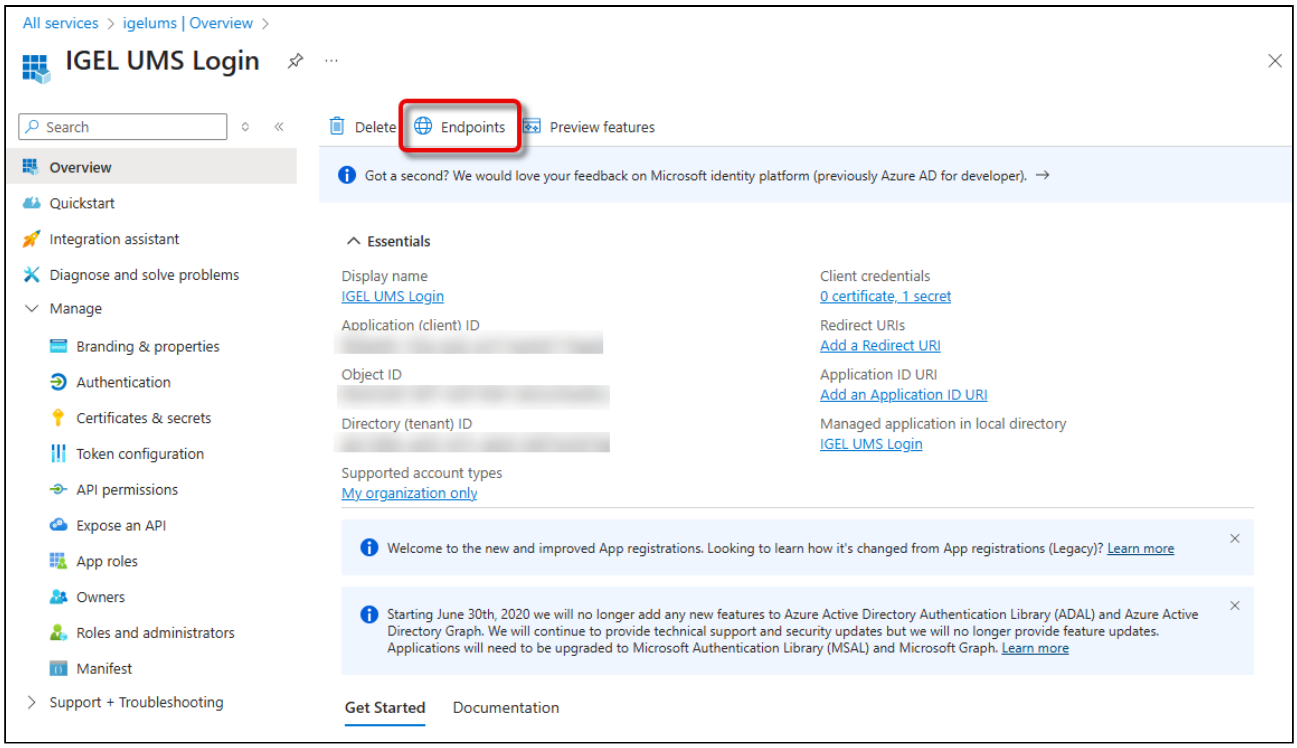
7. Copy the secret's **Value** immediately before you leave the current page.

You must copy the secret immediately because it will not be visible after leaving this page.



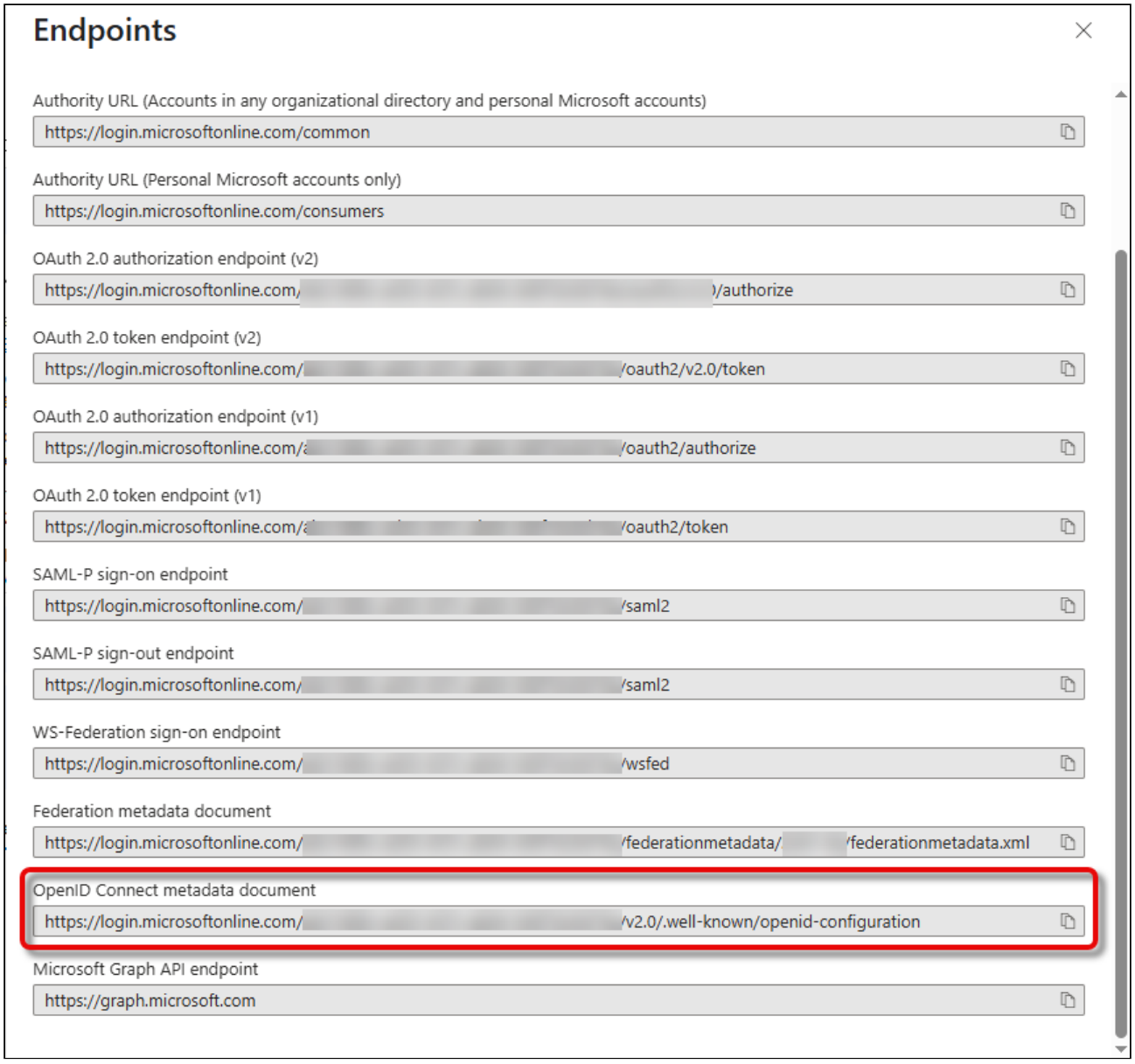
8. Go back to the **Overview** and click **Endpoints**.





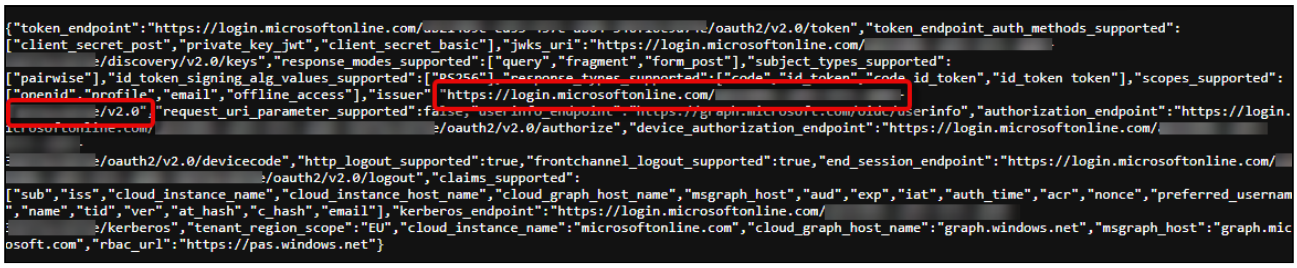
The window **Endpoints** opens.

9. Open the URL of the **OpenID Connect metadata document** in a new browser tab.



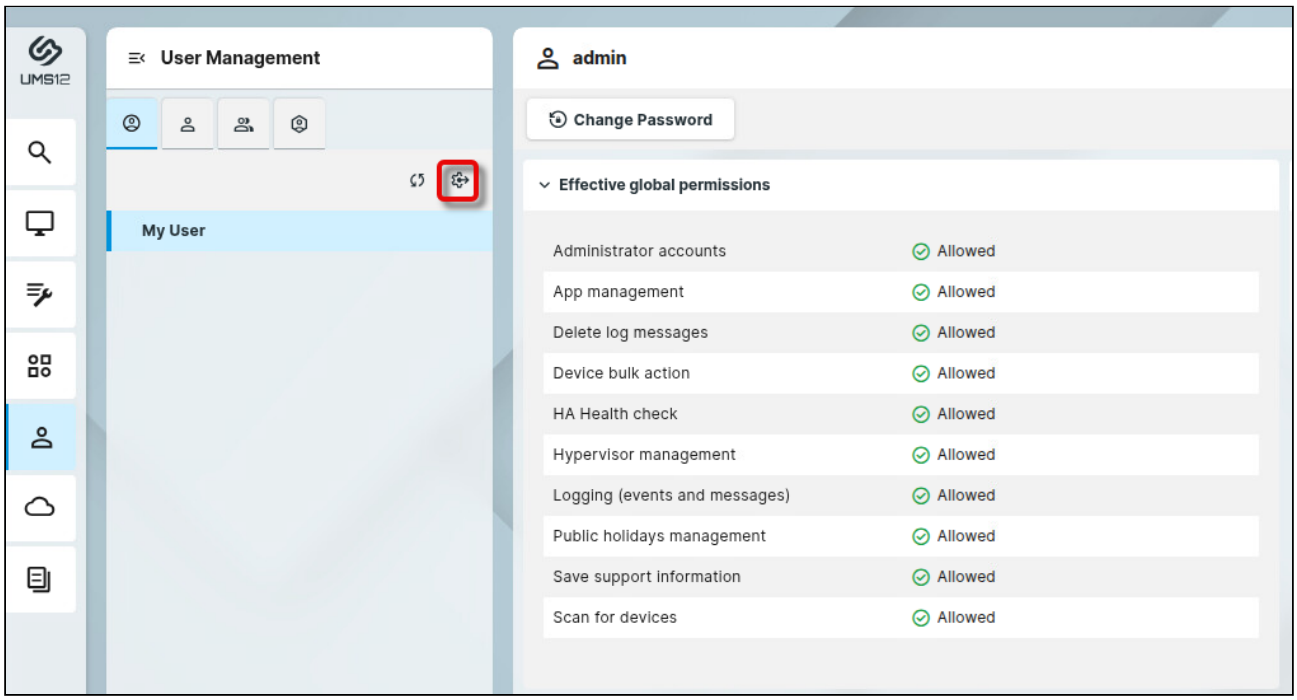
The JSON document is displayed in the new browser tab.

10. Copy the URL for the key `“issuer”` from the document.

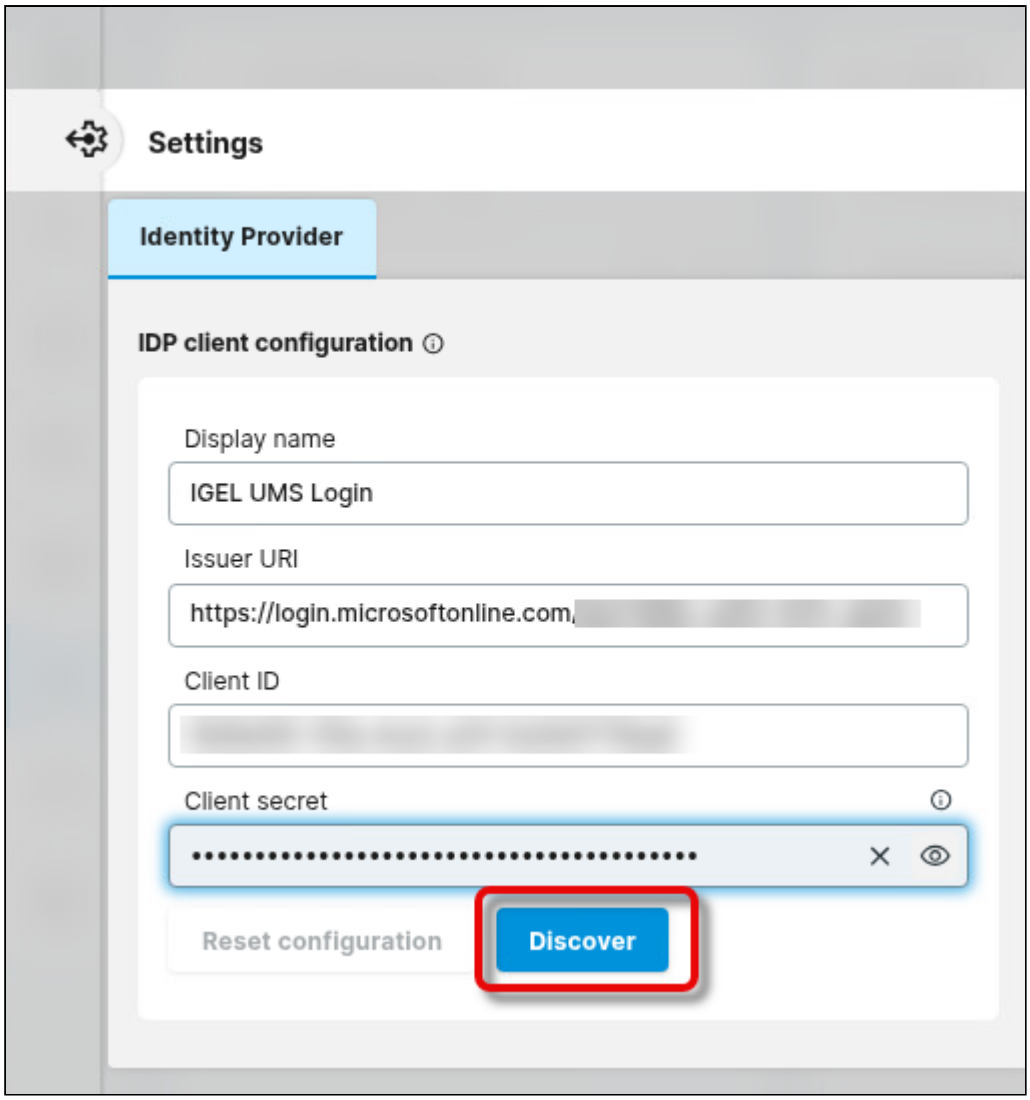


Configuring Your Connection to Microsoft Entra ID in the UMS Web App

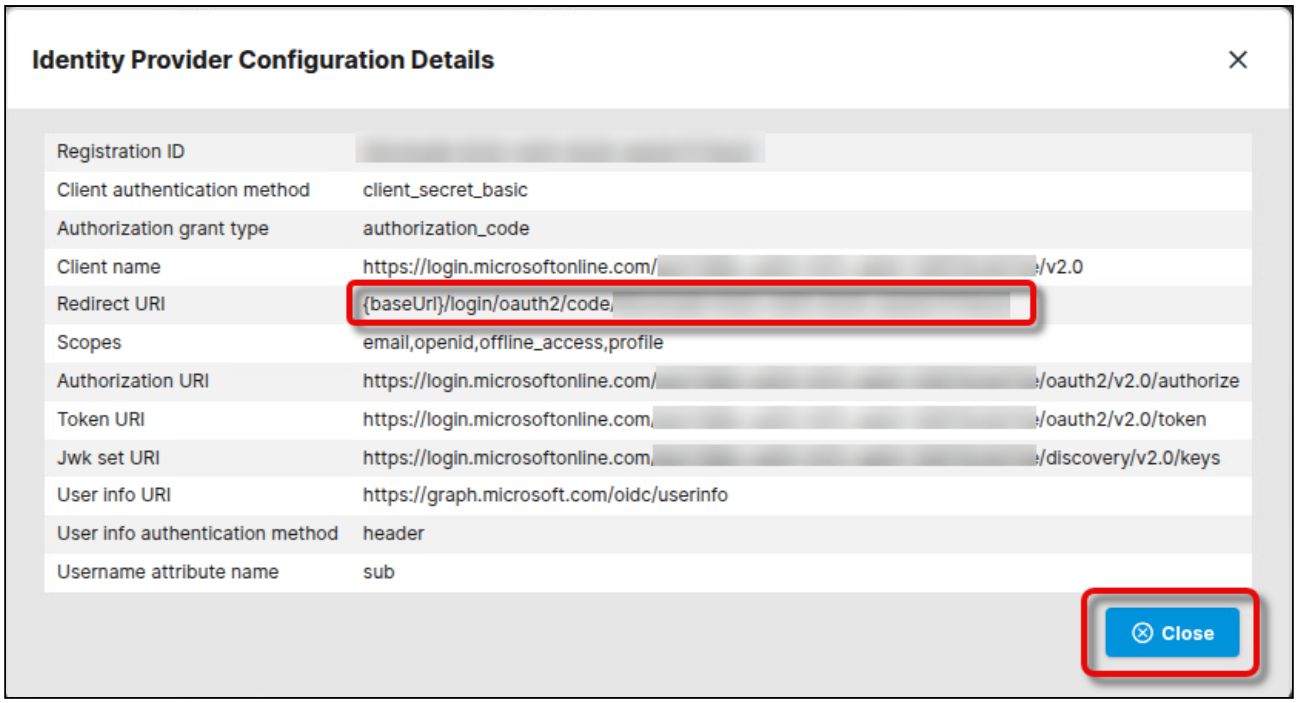
1. Open the UMS Web App, go to **User Management**, and click ⚙.



2. Enter the following data from the application you have created in Microsoft Entra ID and click **Discover**.
   - **Display name**: The name of your application
   - **Issuer URI**: The value of “issuer” you have copied from the OpenID Connect metadata document.
   - **Client ID**: The application ID or client ID for your application
   - **Client secret**: The secret you have created for your application



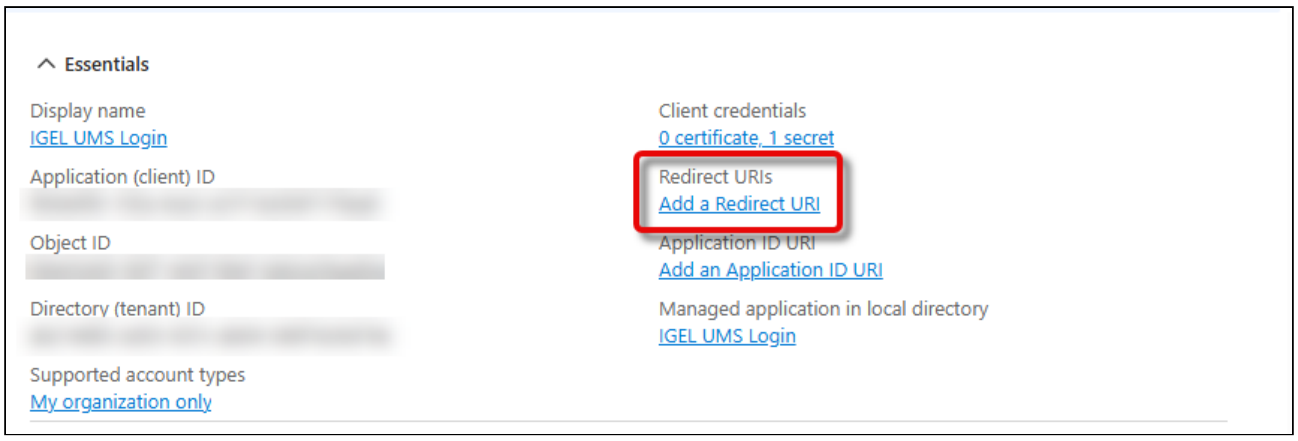
3. In the **Identify Provider Configuration Details** window, copy the **Redirect URI** and close the window.



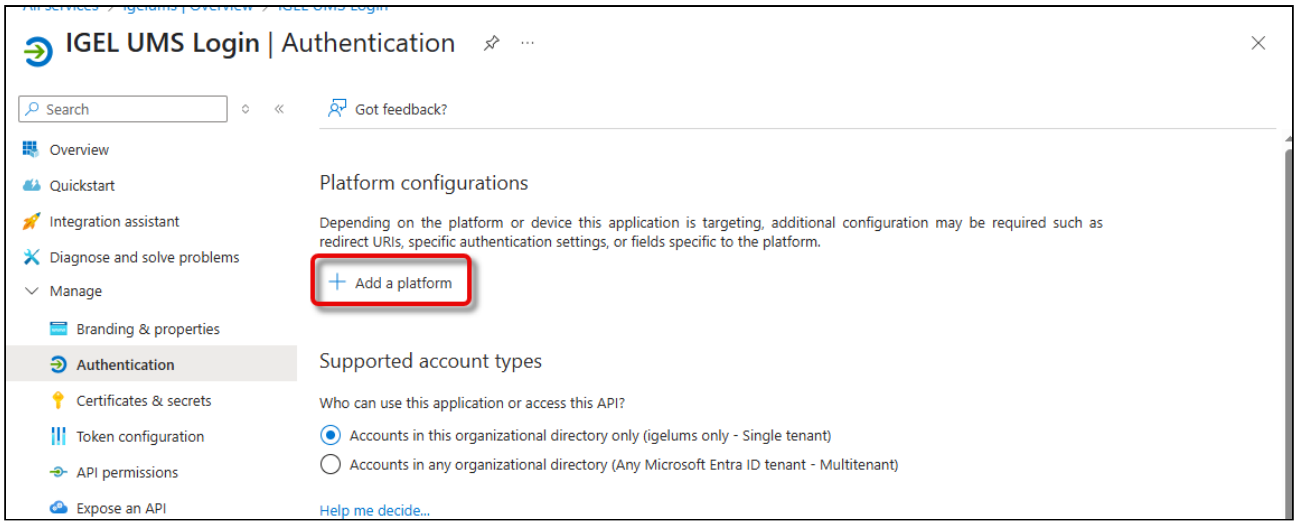
Configuring the Redirect URIs of the UMS in Microsoft Entra ID

We must configure the redirect URI for every base URL the end user will use.

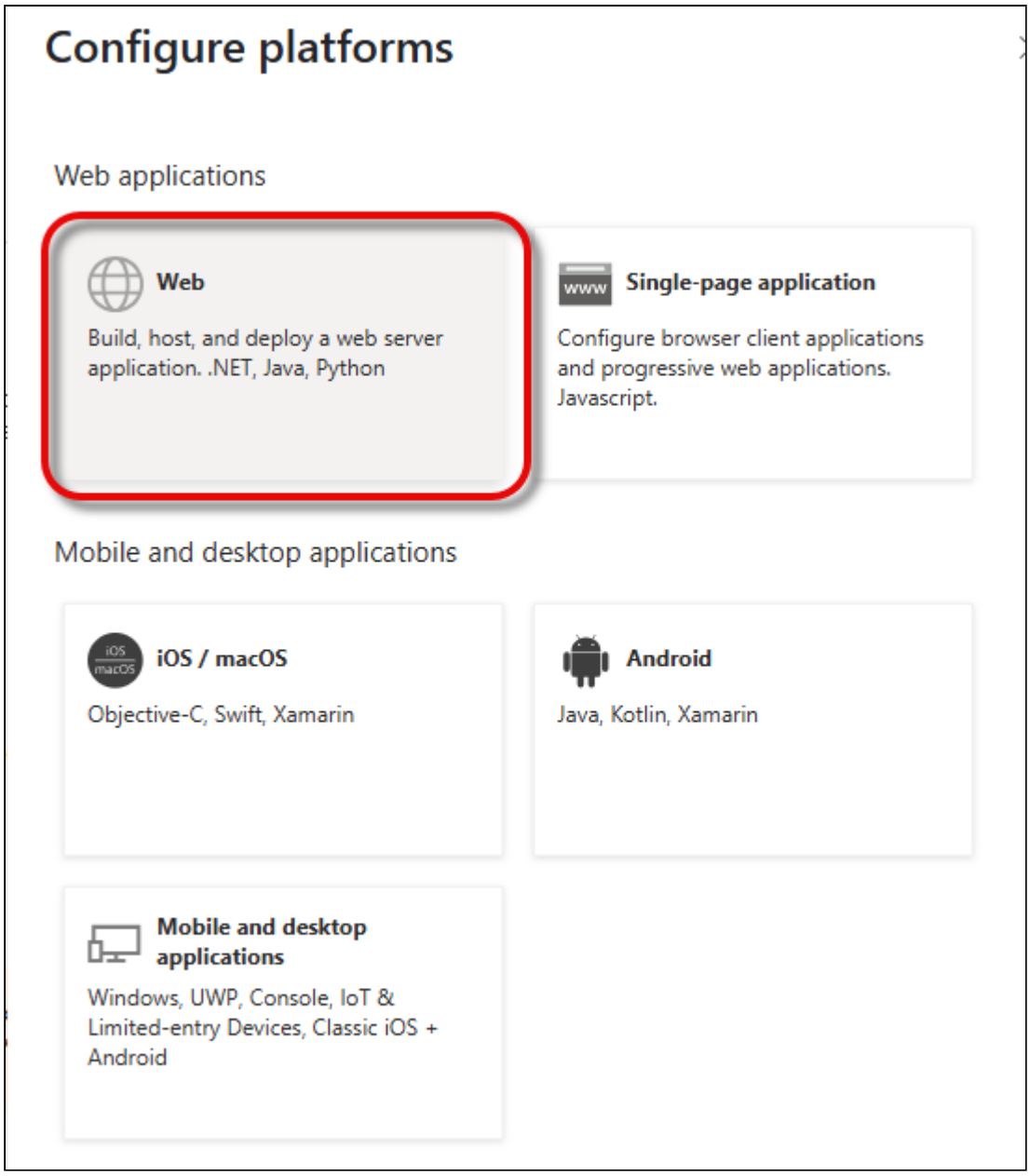
1. In Microsoft Entra, go to the **Overview** page and click **Add a Redirect URI**.



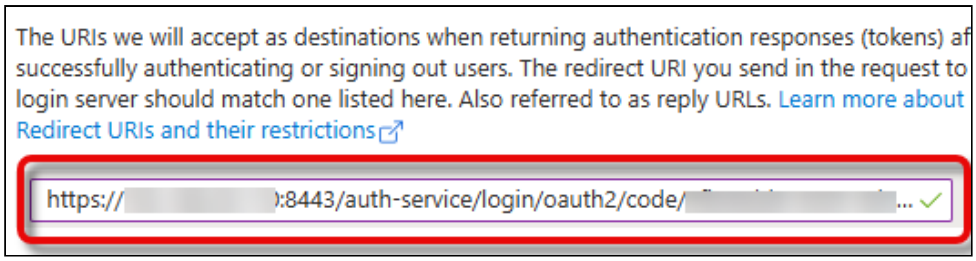
2. Click **Add a platform**.


IGEL UMS Login | Authentication
Search
Got feedback?
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Platform configurations
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.
Add a platform
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (igelums only - Single tenant)
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
Help me decide...

3. Select **Web**.



4. In the **Redirect URI** you have copied from your UMS, replace `{baseUrl}` with the actual IP address and port of your UMS, and enter it. Example: `https://123.123.123.111:8443/auth-service/login/oauth2/code/9ad85dd8-9372-5d11-1966-abe5f1365e58`. Afterward, click **Configure**.

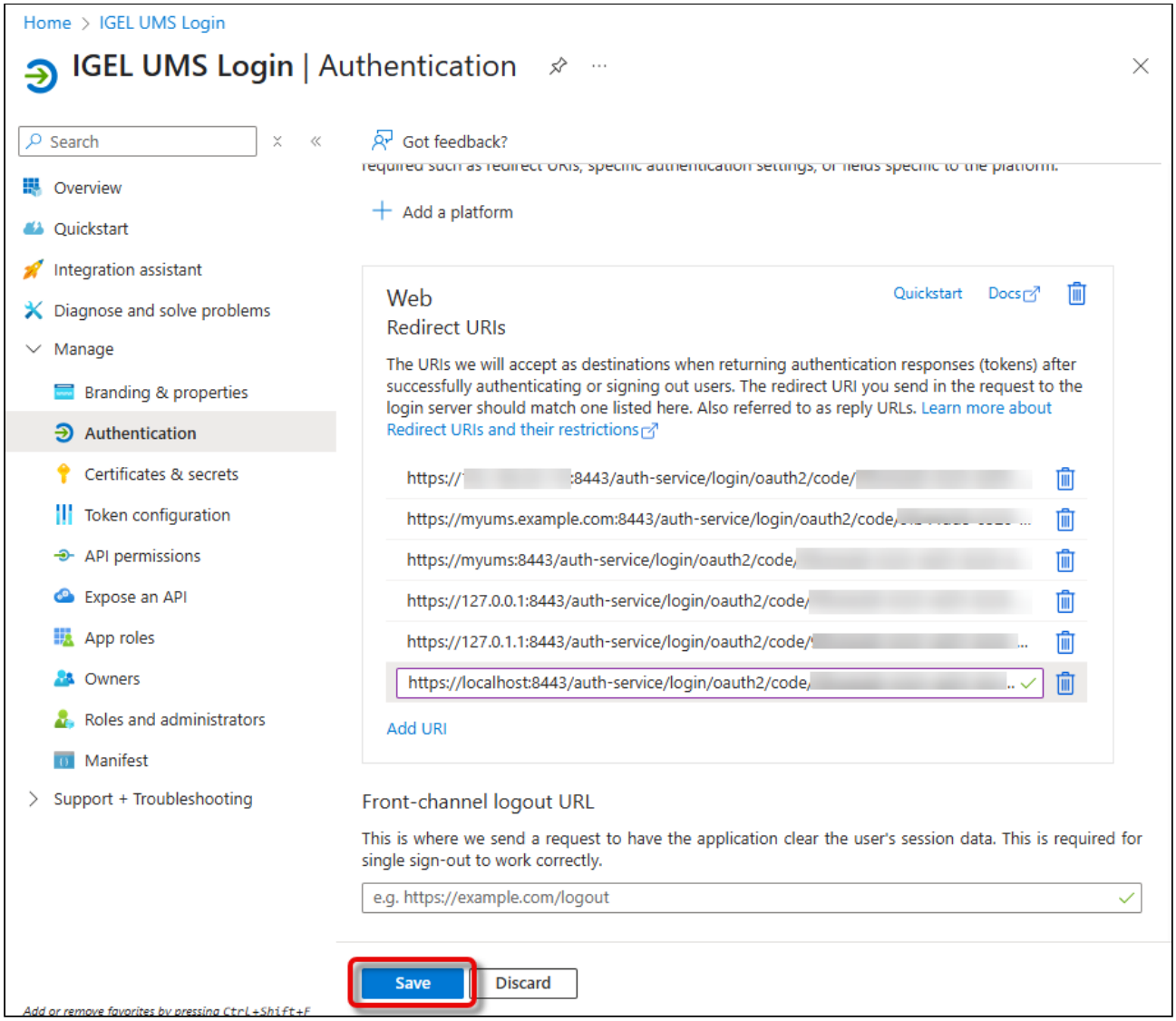


The configured redirect URI is shown.

5. Click **Add URI** to enter the other redirect URI for your UMS. All URIs that can be used for login must be added here, according to the following patterns:
   - IP address of the UMS Server: `https://<IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://123.123.123.123:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - FQDN of the UMS Server: `https://<FQDN>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums.example.com:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - Short name of the UMS Server: `https://<SHORT NAME>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - Local IP address: `https://<LOCAL IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://127.0.0.1:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - Local IP address (alternative): `https://<LOCAL IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://127.0.1.1:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - “localhost” (used when the **Server** field in the login dialog of the UMS Console is empty): `https://localhost:8443/auth-service/login/oauth2/code/`

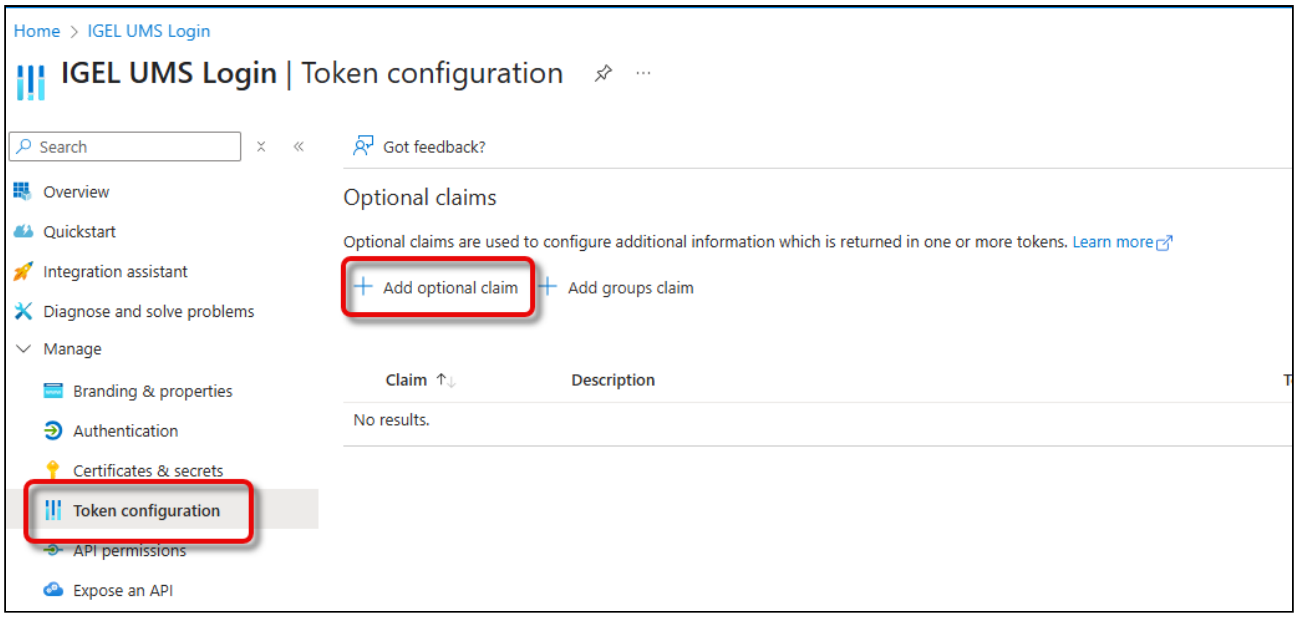
`<REGISTRATION ID>` - example: `https://localhost:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`

7. Click **Save** to save your redirect URIs.

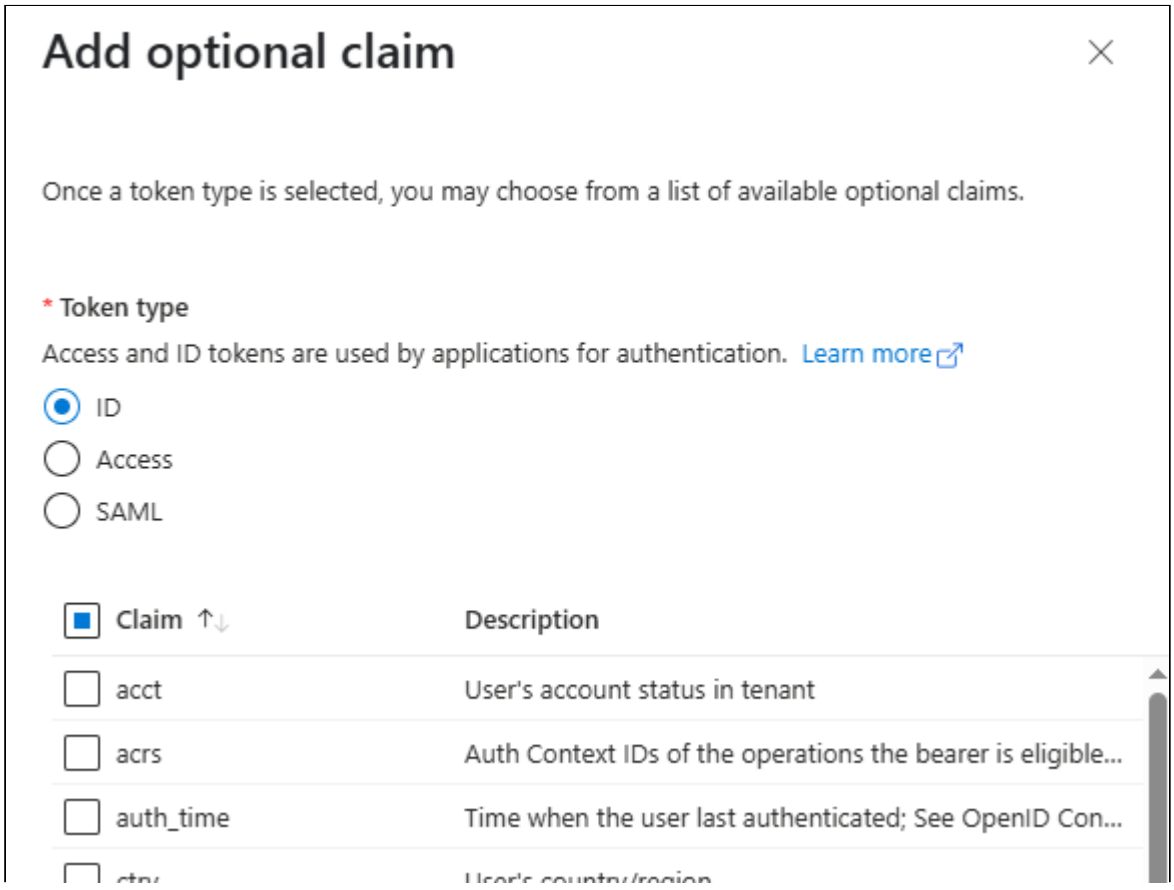


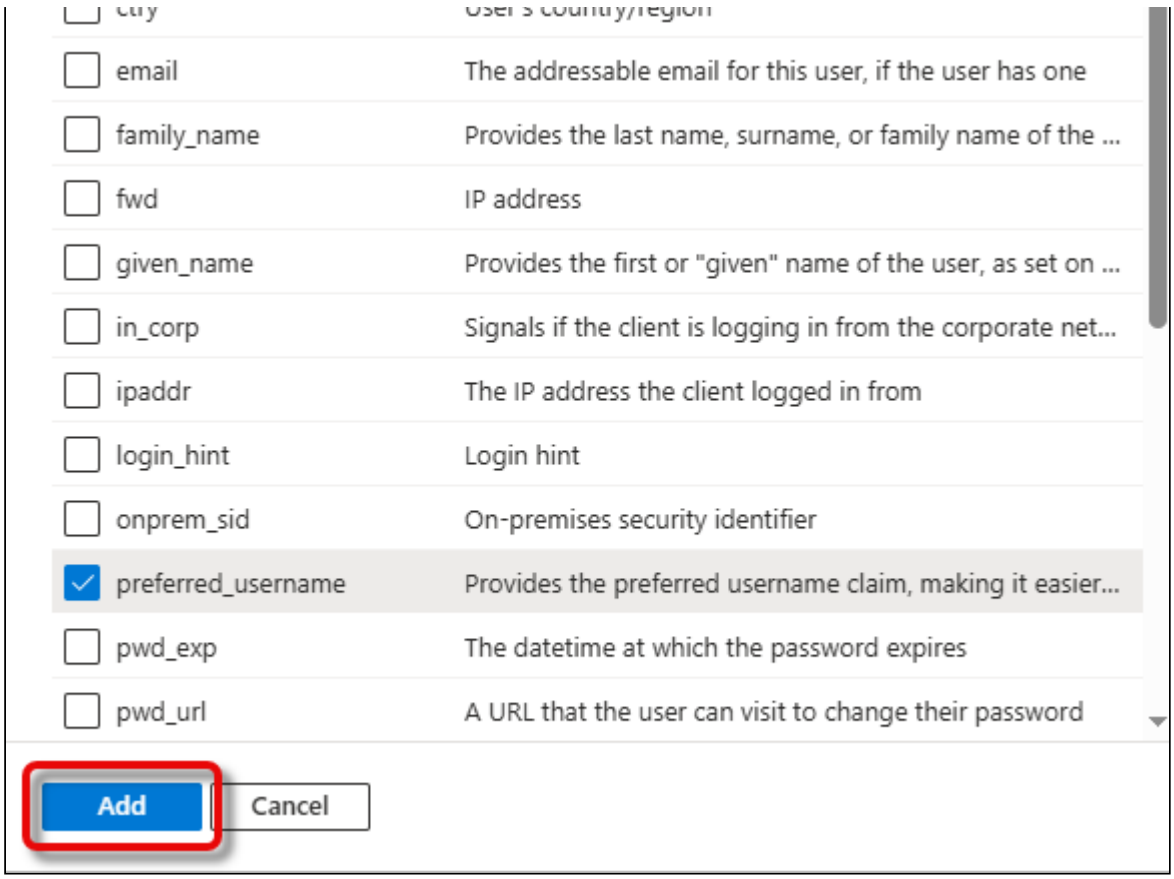
Configuring the Token

1. In Microsoft Entra ID, go to **Token configuration** and click **Add optional claim**.

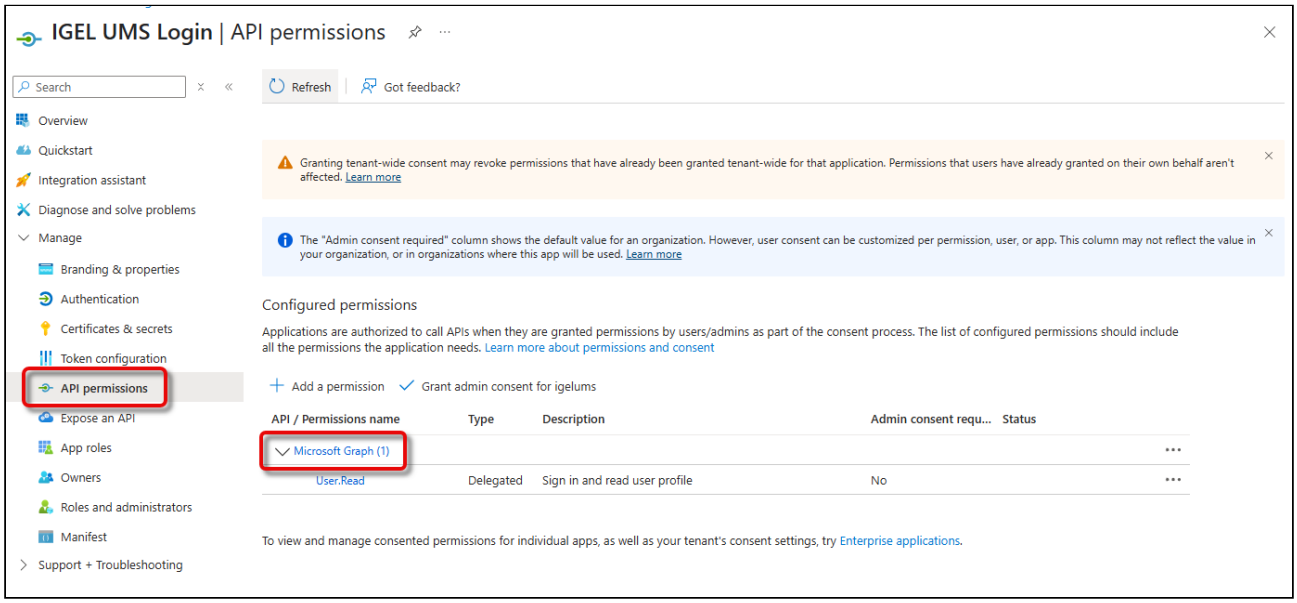


2. Select **ID** as the **Token type** and **preferred_username** as the **Claim**, and click **Add**.

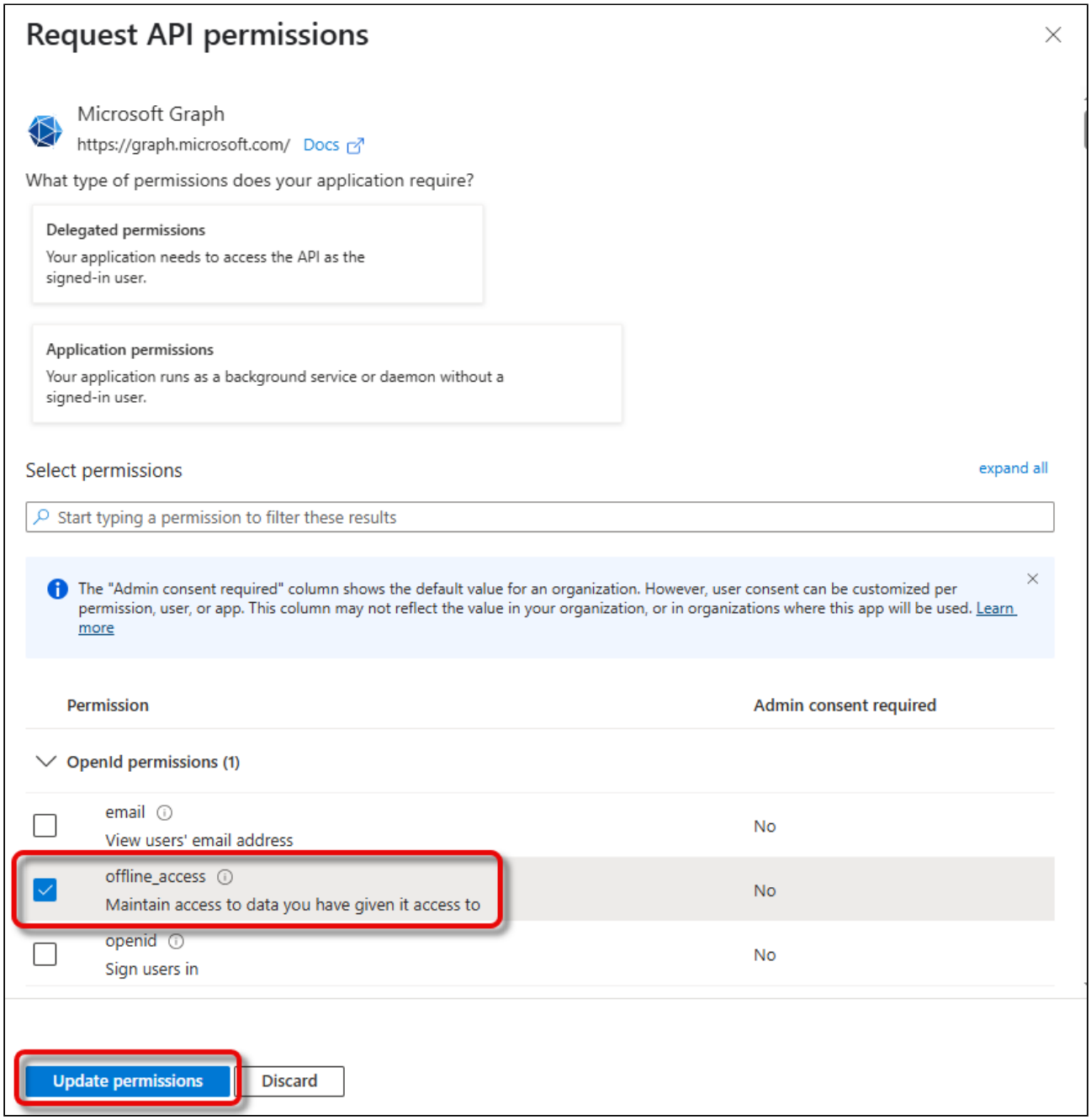




3. Go to **API permissions** and click **Microsoft Graph**.

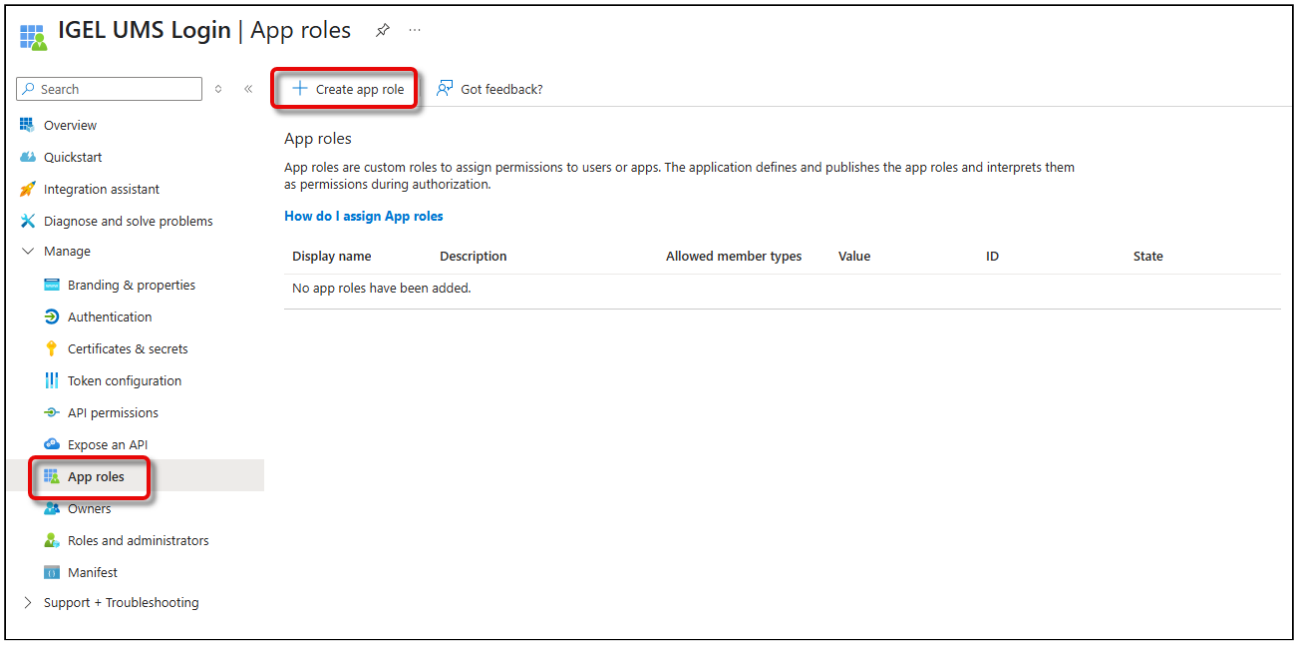


4. Select **offline_access** and click **Update permissions**. This permission is needed for refreshing the tokens.

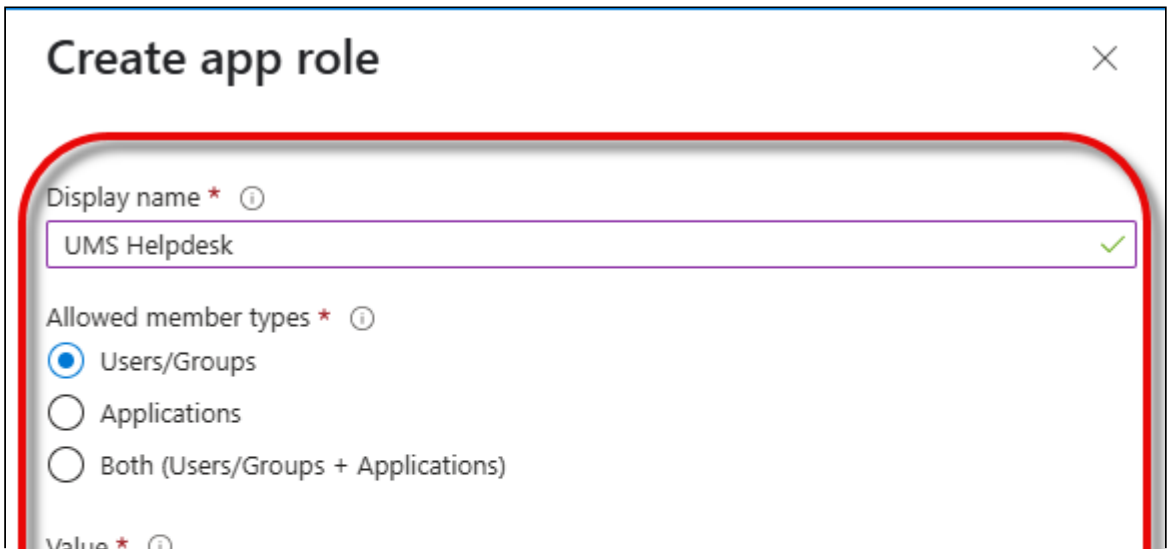


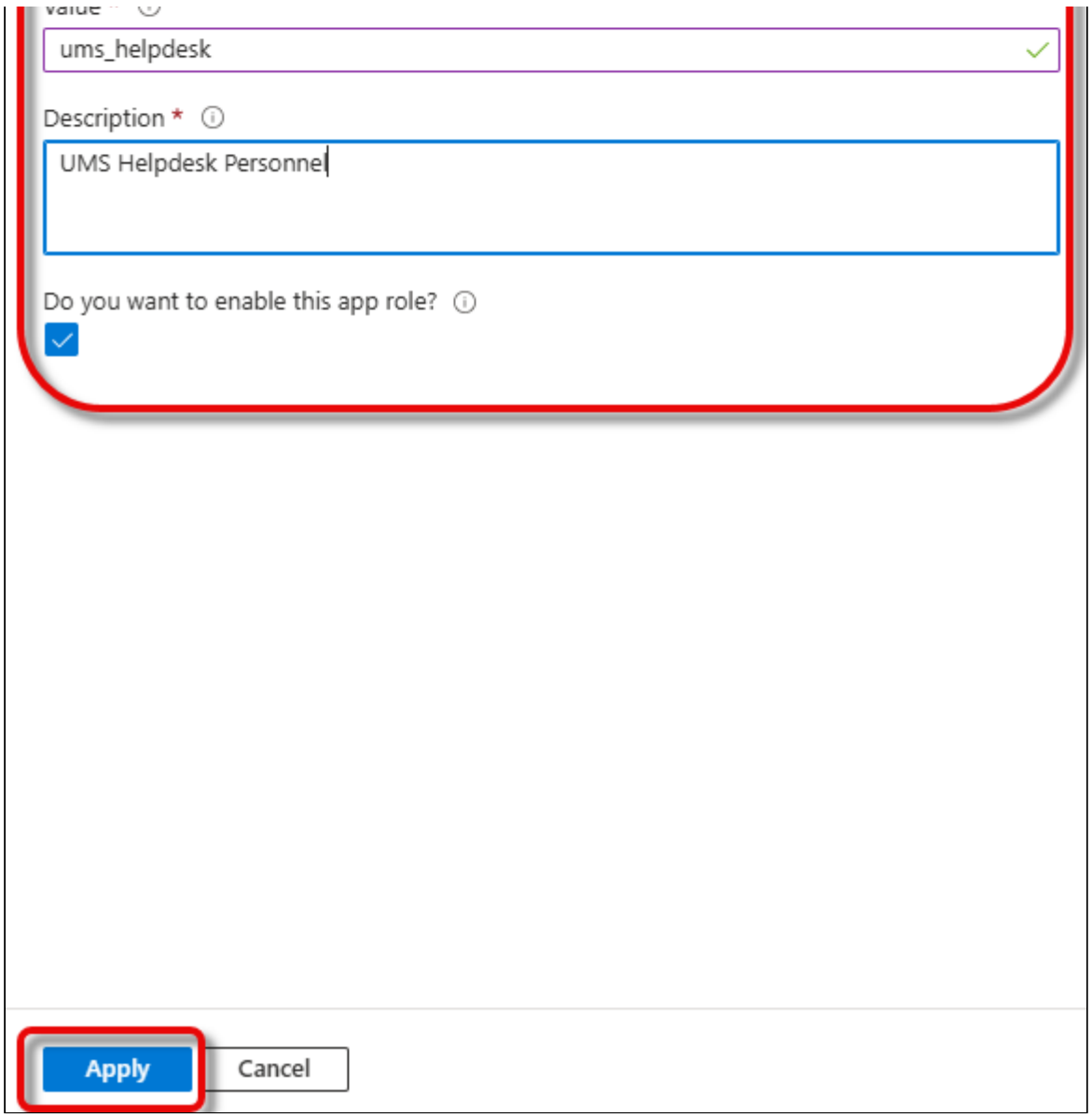
Configuring User Role Mapping in Microsoft Entra ID

1. Go to **App roles** and click **Create app role**.

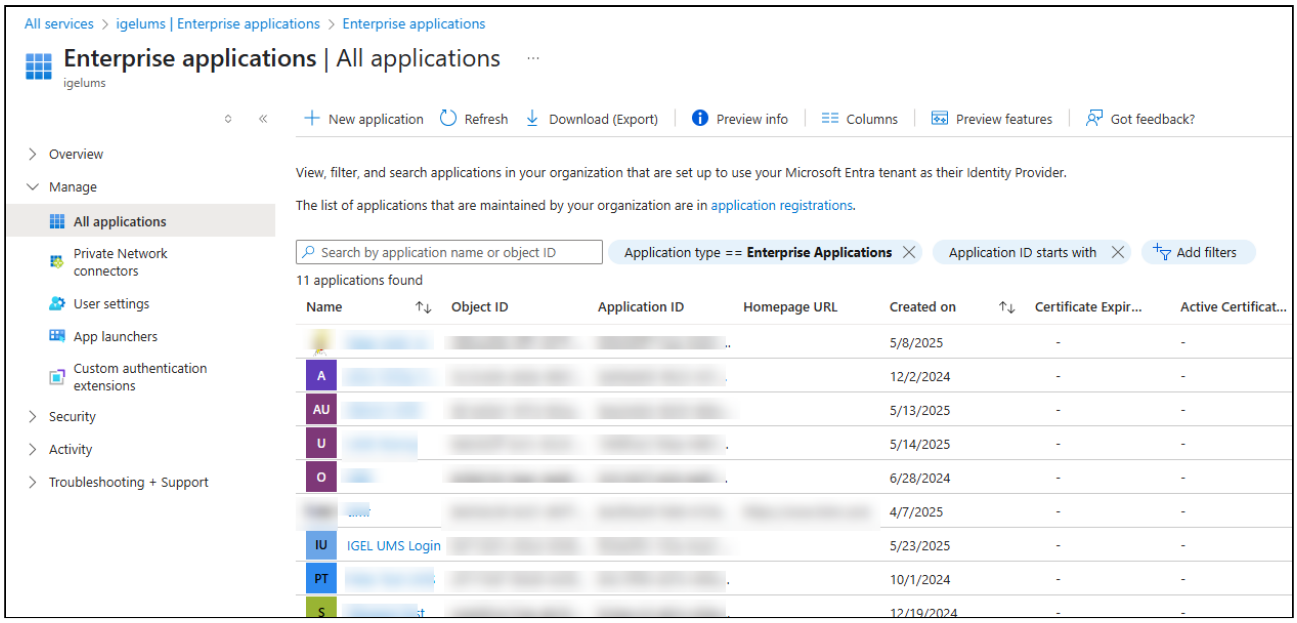


2. Provide the following data and click **Apply**.
   - **Display name**: Descriptive name for the app role
   - **Allowed member types**: Select **Users/Groups**.
   - **Value**: Name that will be included in the “roles” claim of the token that will identify a user
   - **Description**: Describes the app role
   - **Do you want to enable this app role**: Leave this enabled

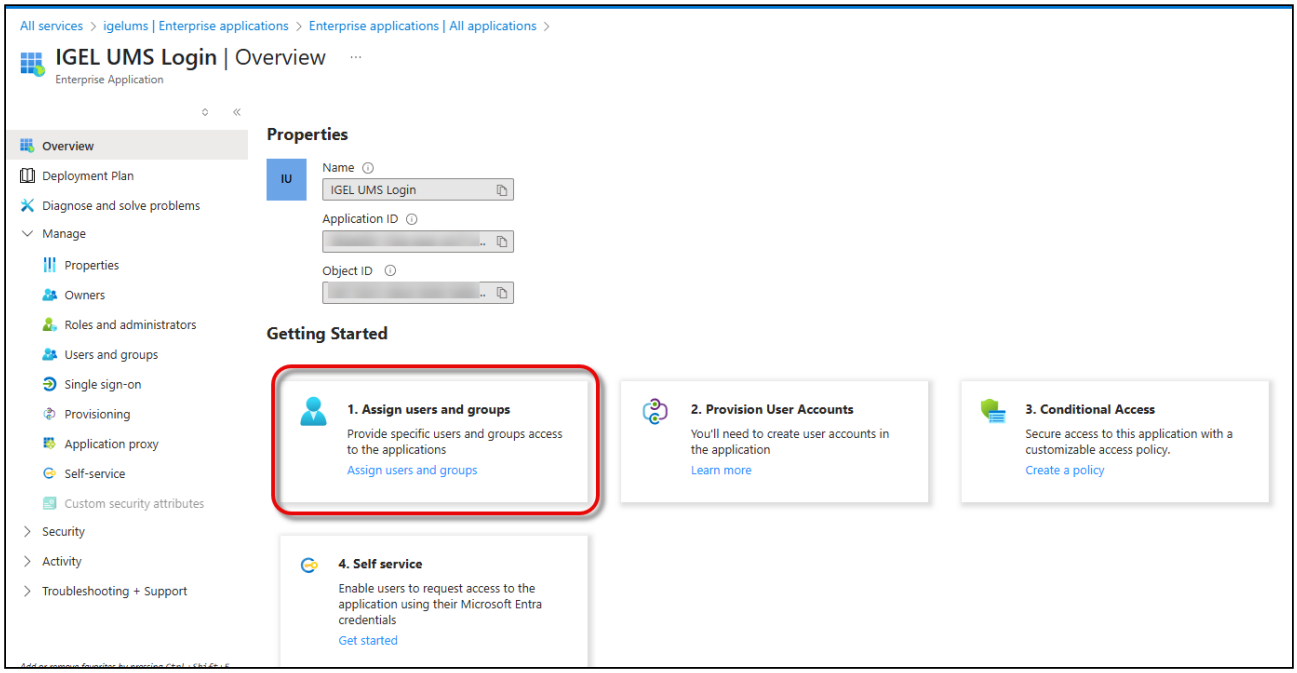




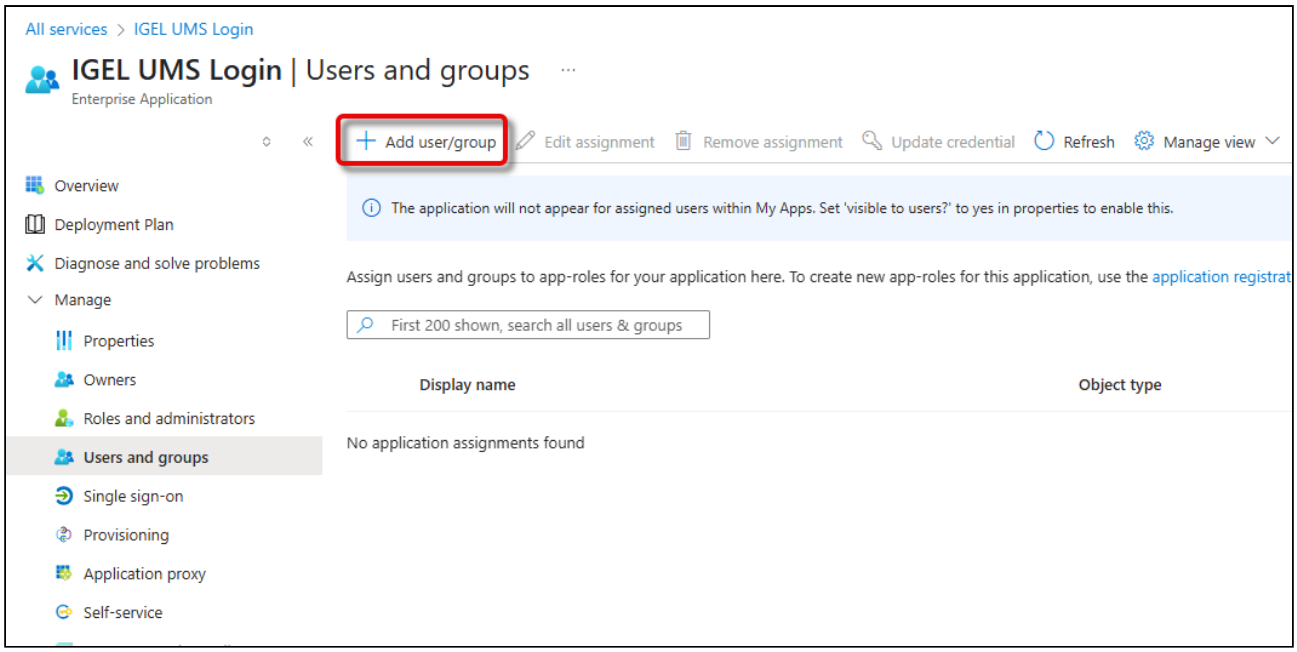
3. From your tenant's main page, go to **Enterprise applications** and select your application.



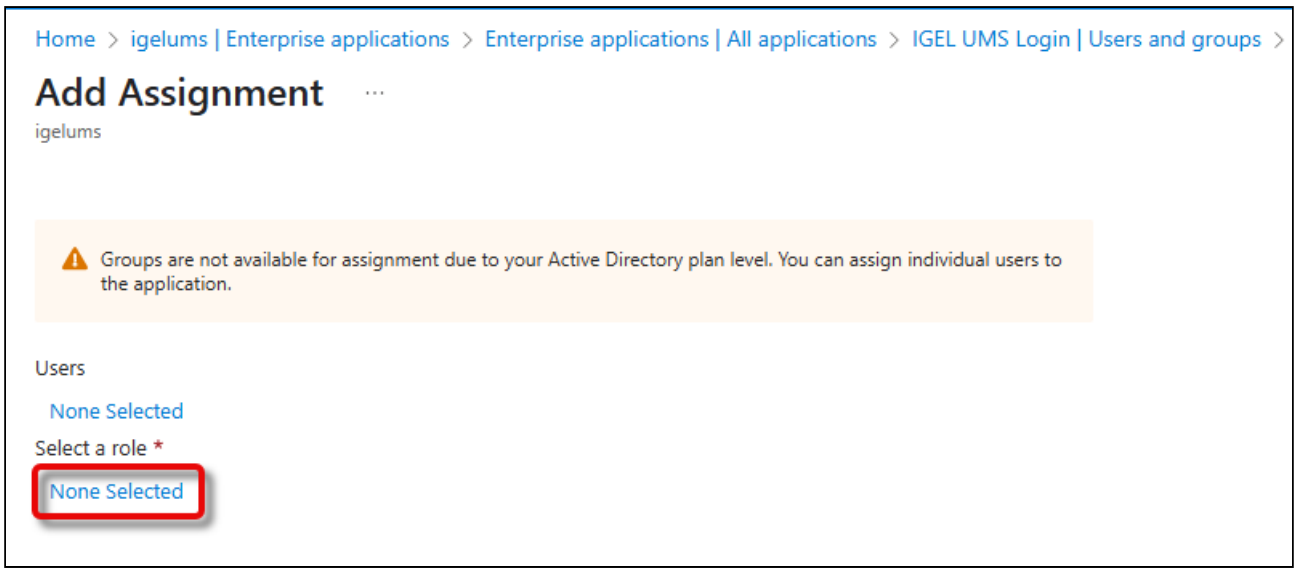
4. Click **Assign users and groups**.

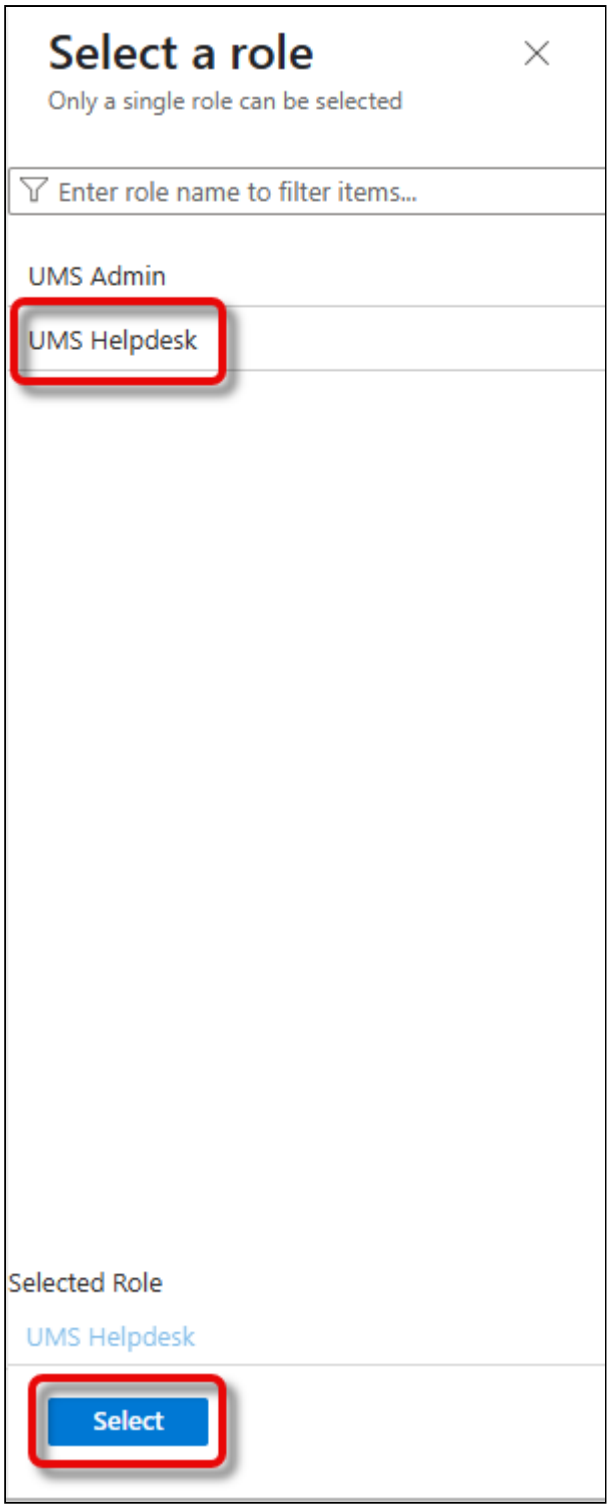


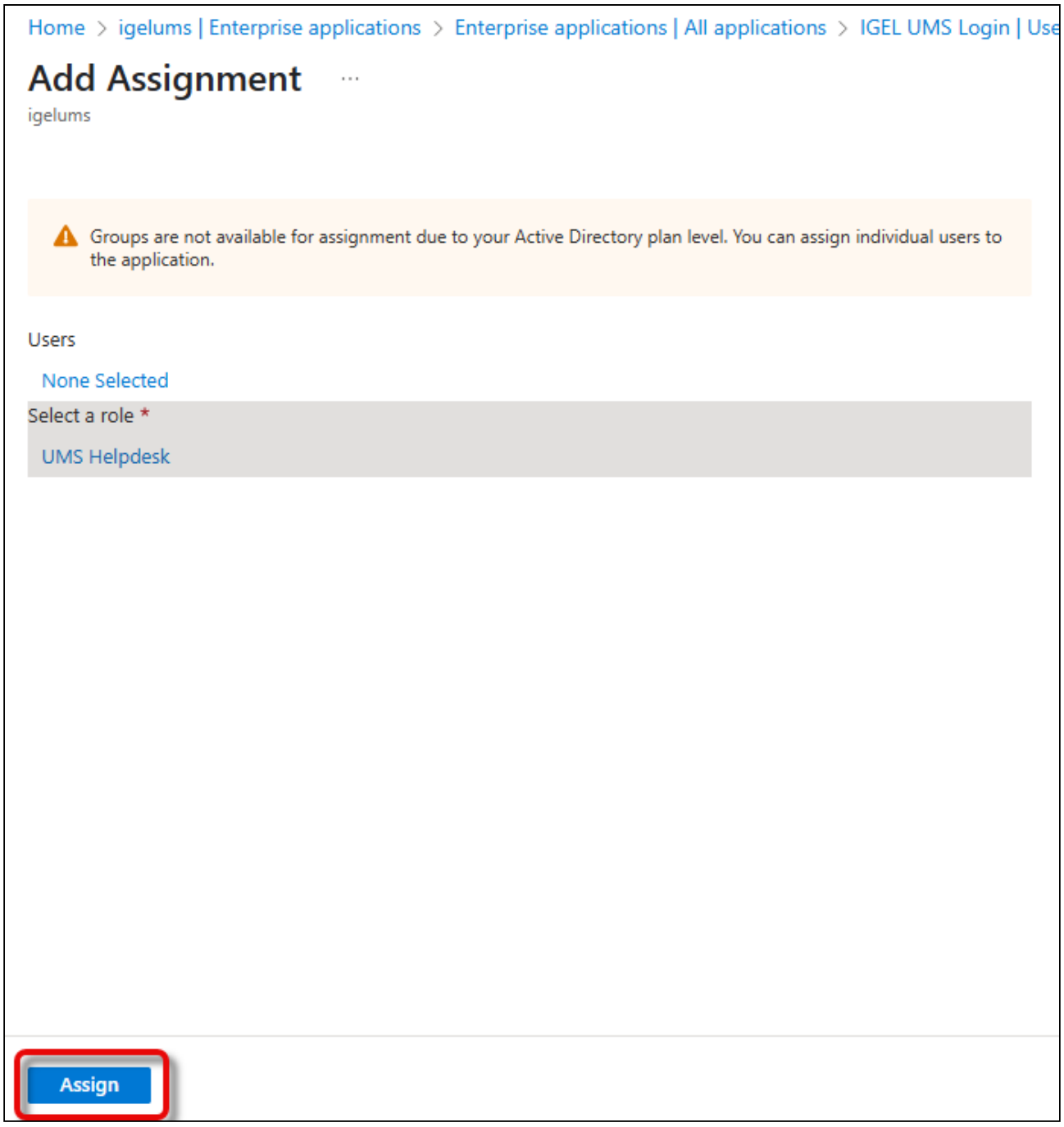
5. Click **Add user/group**.



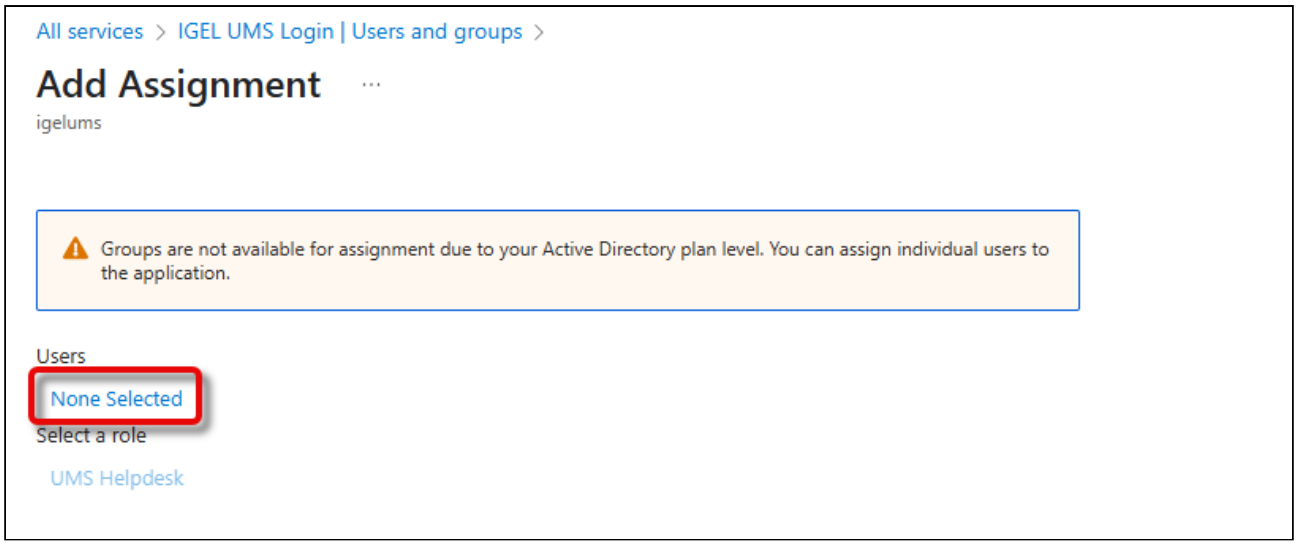
6. If an app role already exists, you must first select the role you want to add the user to: Under **Select a role**, click **None Selected**, select the appropriate role, click **Select**, and then **Assign**.

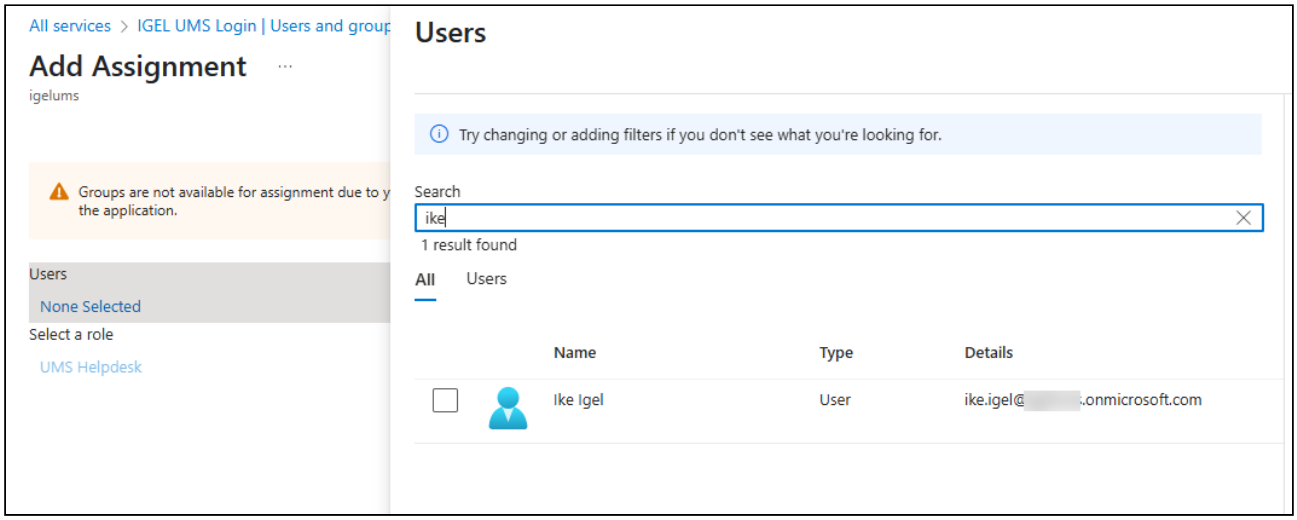


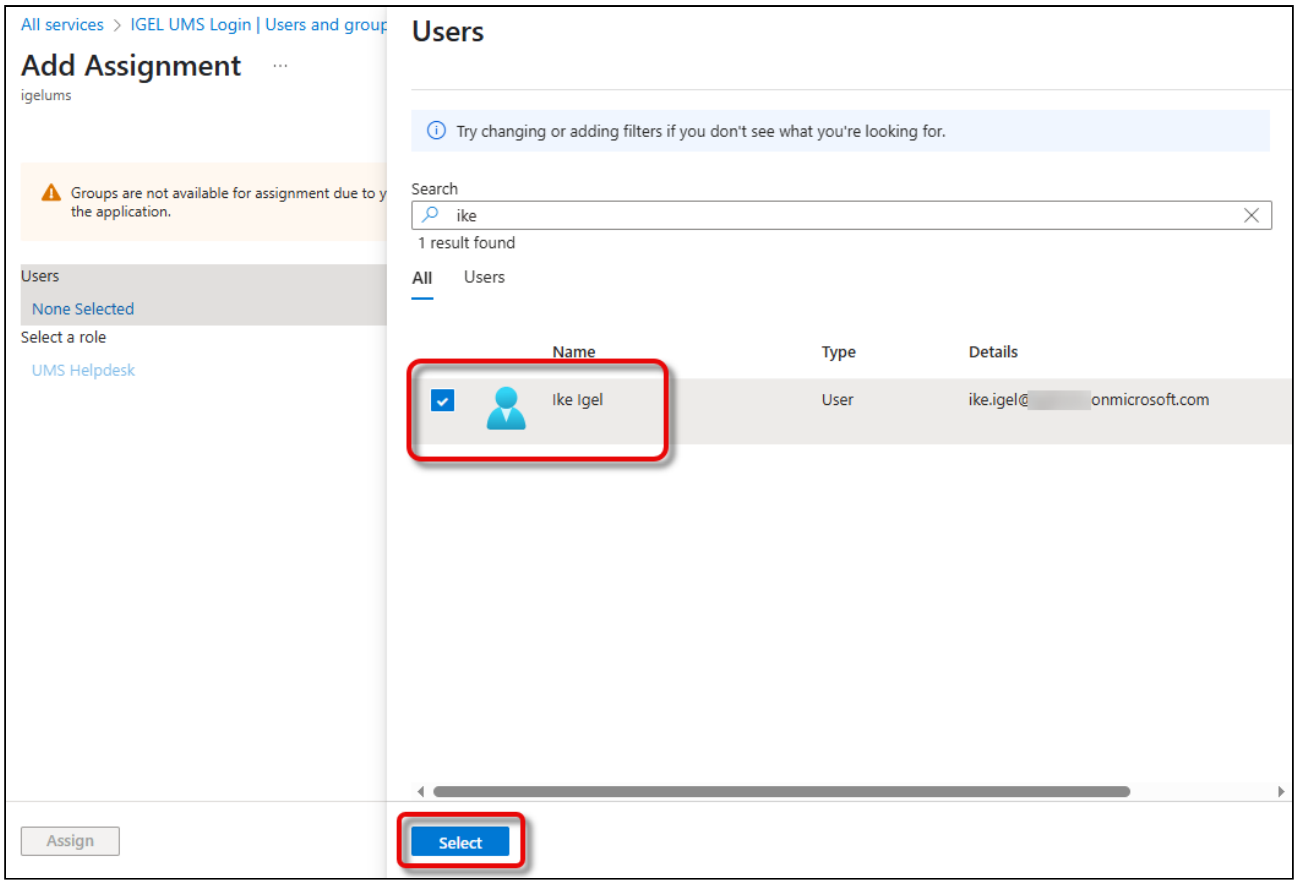

Select a role
Only a single role can be selected
Enter role name to filter items...
UMS Admin
UMS Helpdesk
Selected Role
UMS Helpdesk
Select



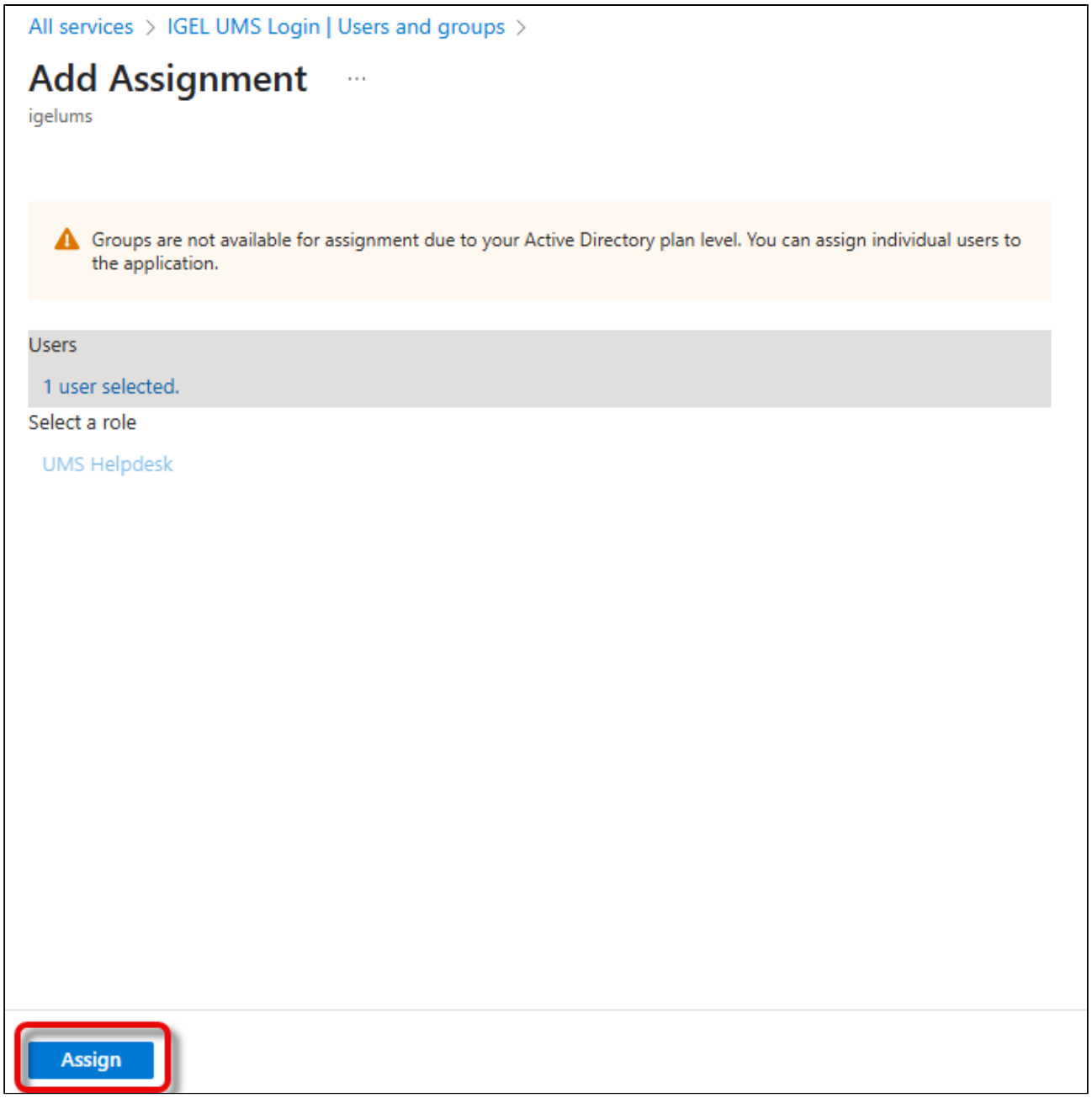
7. Under **Users**, click **None Selected**, search for the desired user, and then select the user.


All services > IGEL UMS Login | Users and groups >
Add Assignment
igelums
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
None Selected
Select a role
UMS Helpdesk


All services > IGEL UMS Login | Users and group
Add Assignment
igelums
Groups are not available for assignment due to y
the application.
Users
None Selected
Select a role
UMS Helpdesk
Users
Try changing or adding filters if you don't see what you're looking for.
Search
ike
1 result found
All
Users
Name
Type
Details
Ike Igel
User
ike.igel@ .onmicrosoft.com

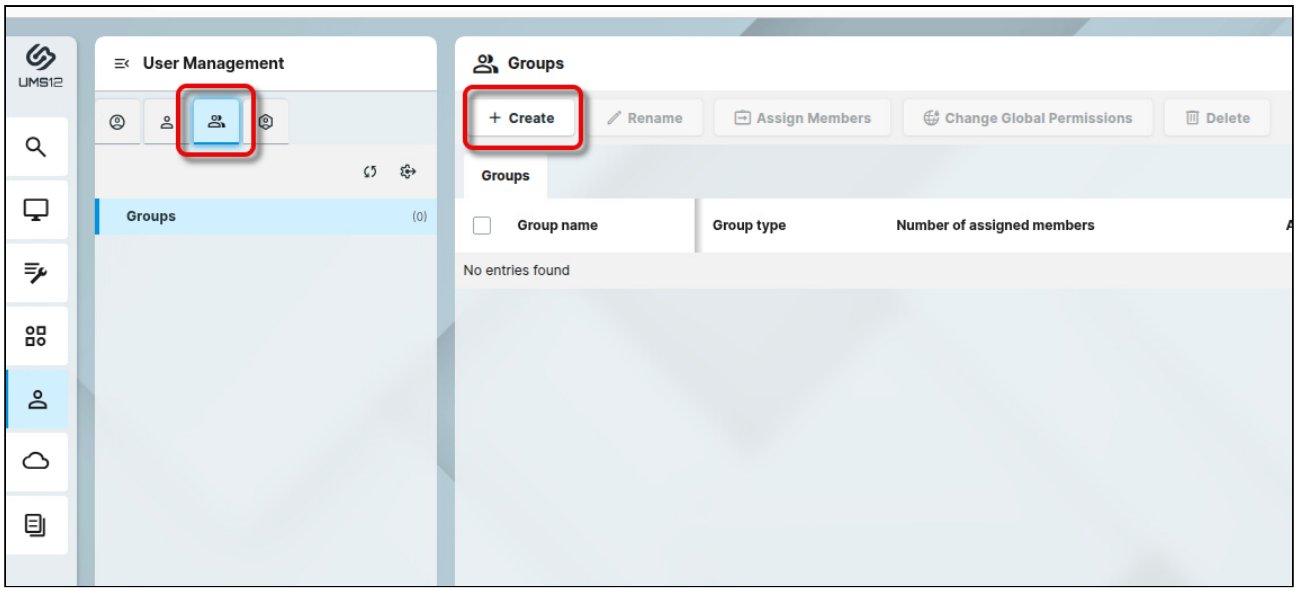


7. Confirm the assignment with **Assign**.



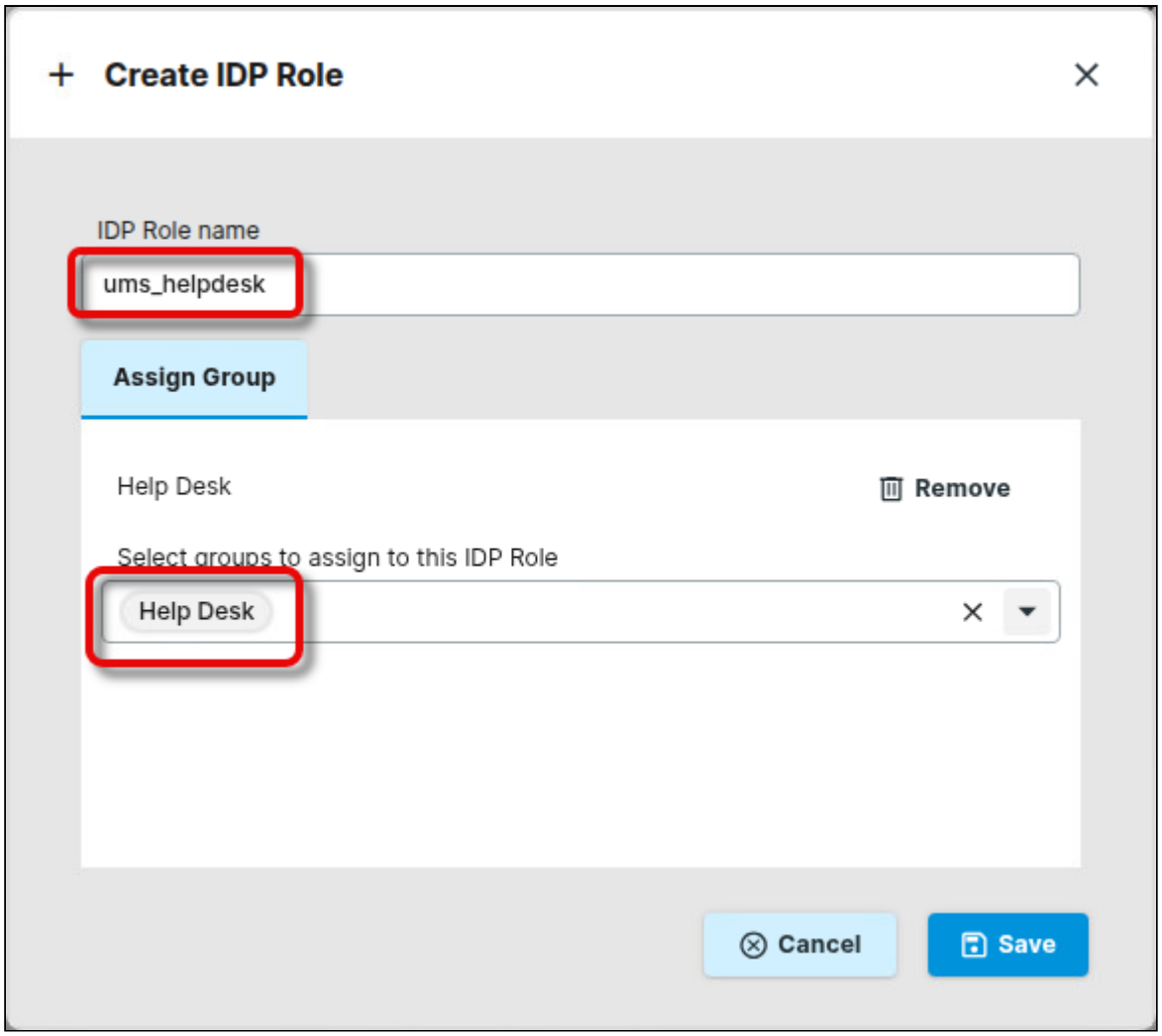
Mapping the Roles in Microsoft Entra to UMS Groups

1. Open the UMS Web App, go to **User Management**, select , and click **+ Create**.



2. Edit the settings as follows:

- **IDP Role name**: The **Value** of the app role you have configured in Microsoft Entra ID. Please note that this value is case-sensitive.
- **Assign Group**: The UMS group you want to map to the app role



3. Continue with Adapting the Mapped Role Claim for Microsoft Entra ID (see page 167).

Adapting the Mapped Role Claim for Microsoft Entra ID

The roles/groups defined within the IdP must be mapped to the IdP roles within the UMS. This is done via the token that is exchanged during the login process. By default, the UMS maps the roles/groups contained in the token claim `ums_roles` to IdP roles in the UMS.

Since Microsoft Entra does not support custom claims, we must edit the claim, which is done in the configuration file.

1. Open `<INSTALLLATION PATH>/rmguiserver/conf/appconfig/application.yml` (example for Windows: `C:\Program`

`Files\IGEL\RemoteManager\rmguiserver\conf\appconfig\application.yml`; example for Linux: `/opt/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml`) and edit it as follows:

```
igel:
  auth-service:
    idp:
      claimNameRoles: roles
  client-cert-forwarding:
    enabled: false
    client-cert-forwarded-header: X-SSL-CERT
```

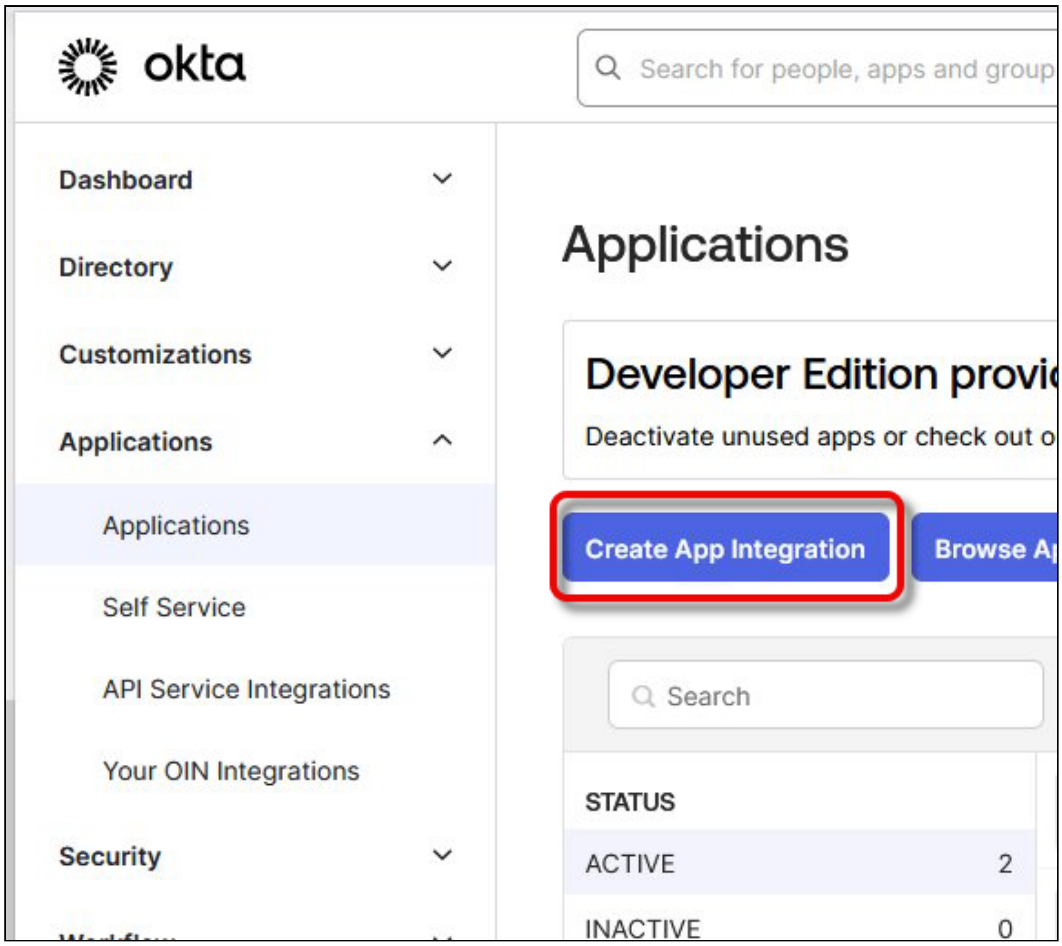
2. Restart the UMS Server.
   - On Windows: **Services > IGEL RMGUIServer**
   - On Linux: `sudo systemctl restart igel-ums-server`

UMS Login with Okta

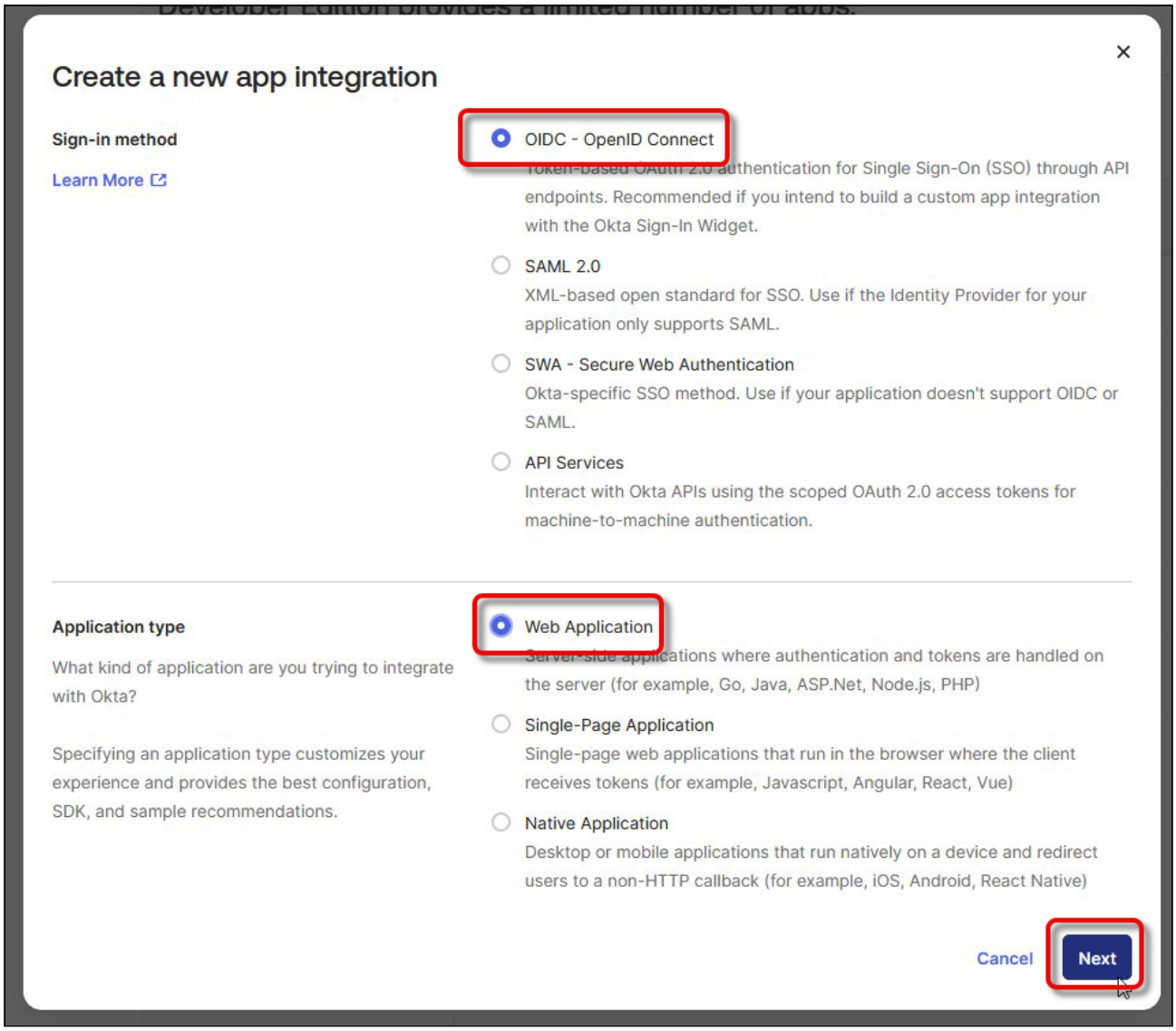
Creating an Application in Okta

1. Log in to your Okta portal and navigate to **Applications > Applications**.

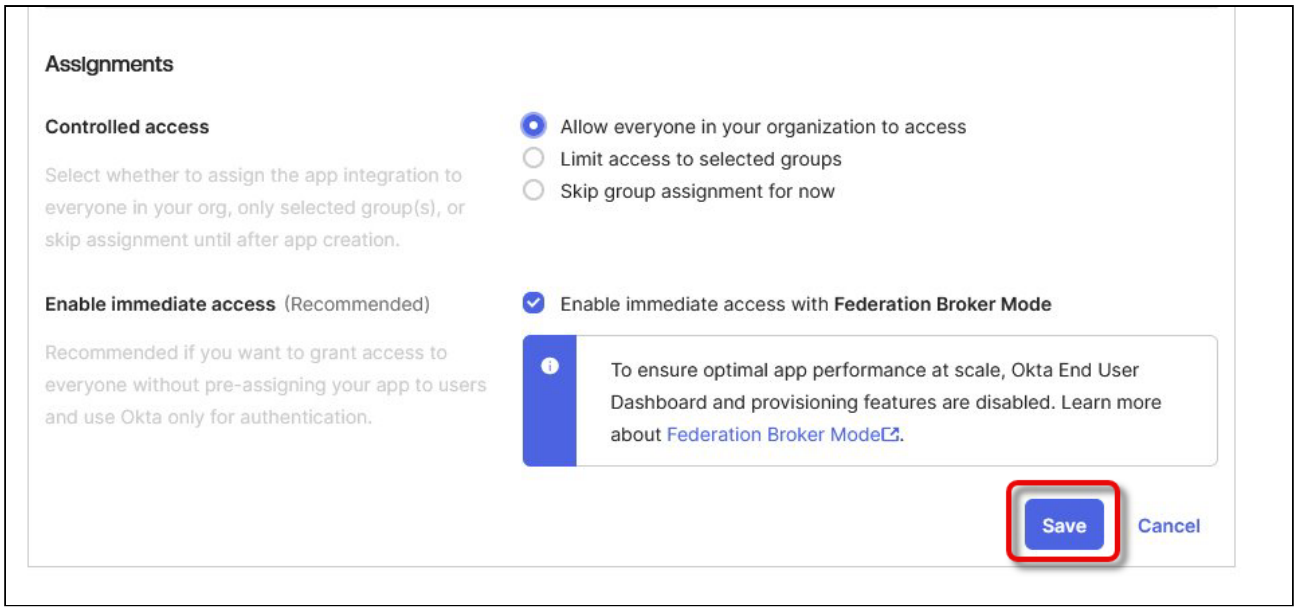
2. Click **Create App Integration**.



3. Edit the settings as follows and click **Next**.
    - Set **Sign-in method** to **OIDC - OpenID Connect**.
    - Set the **Application type** to **Web Application**.

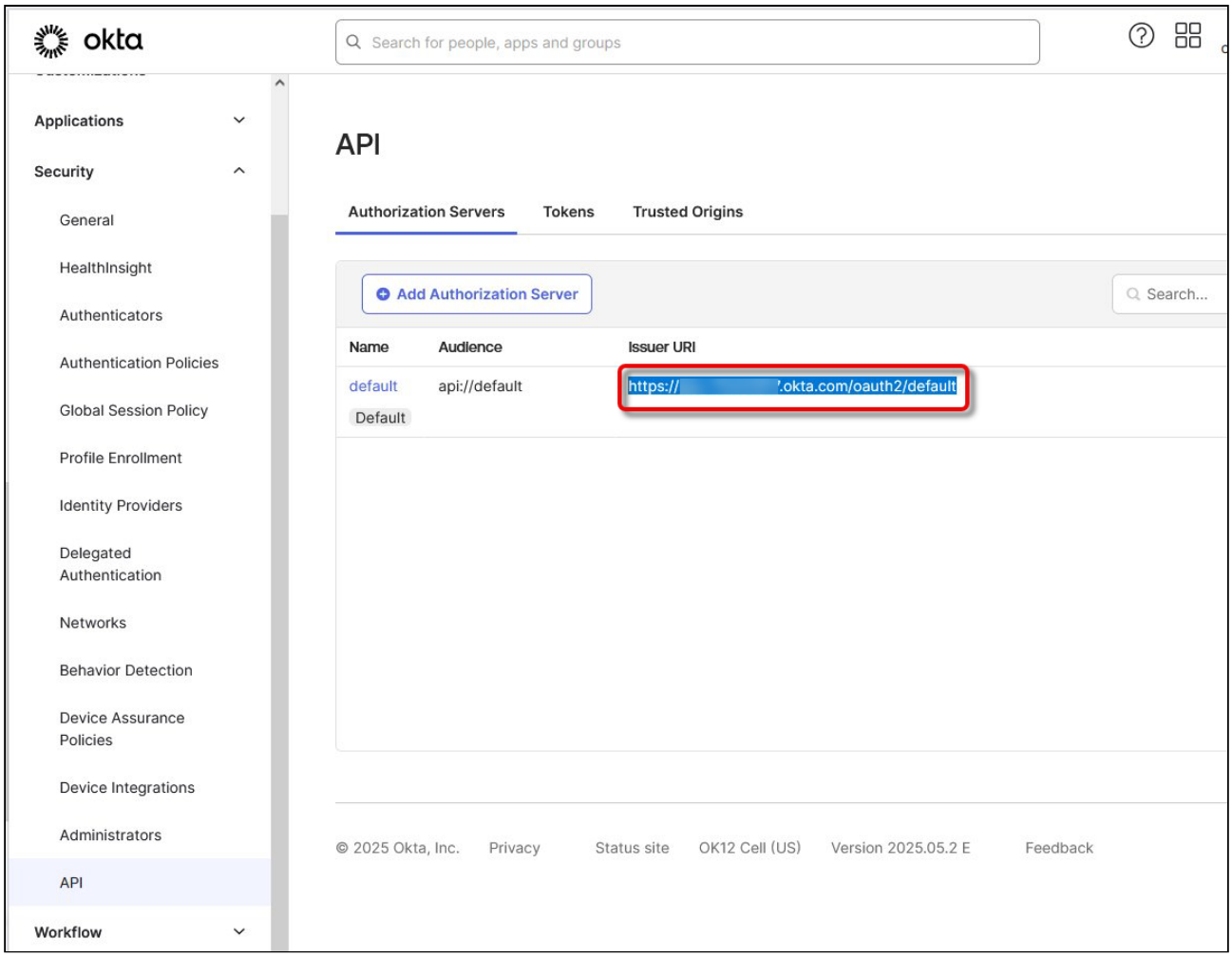


4. Under **Assignments**, select which users are allowed to access the application and save your application.

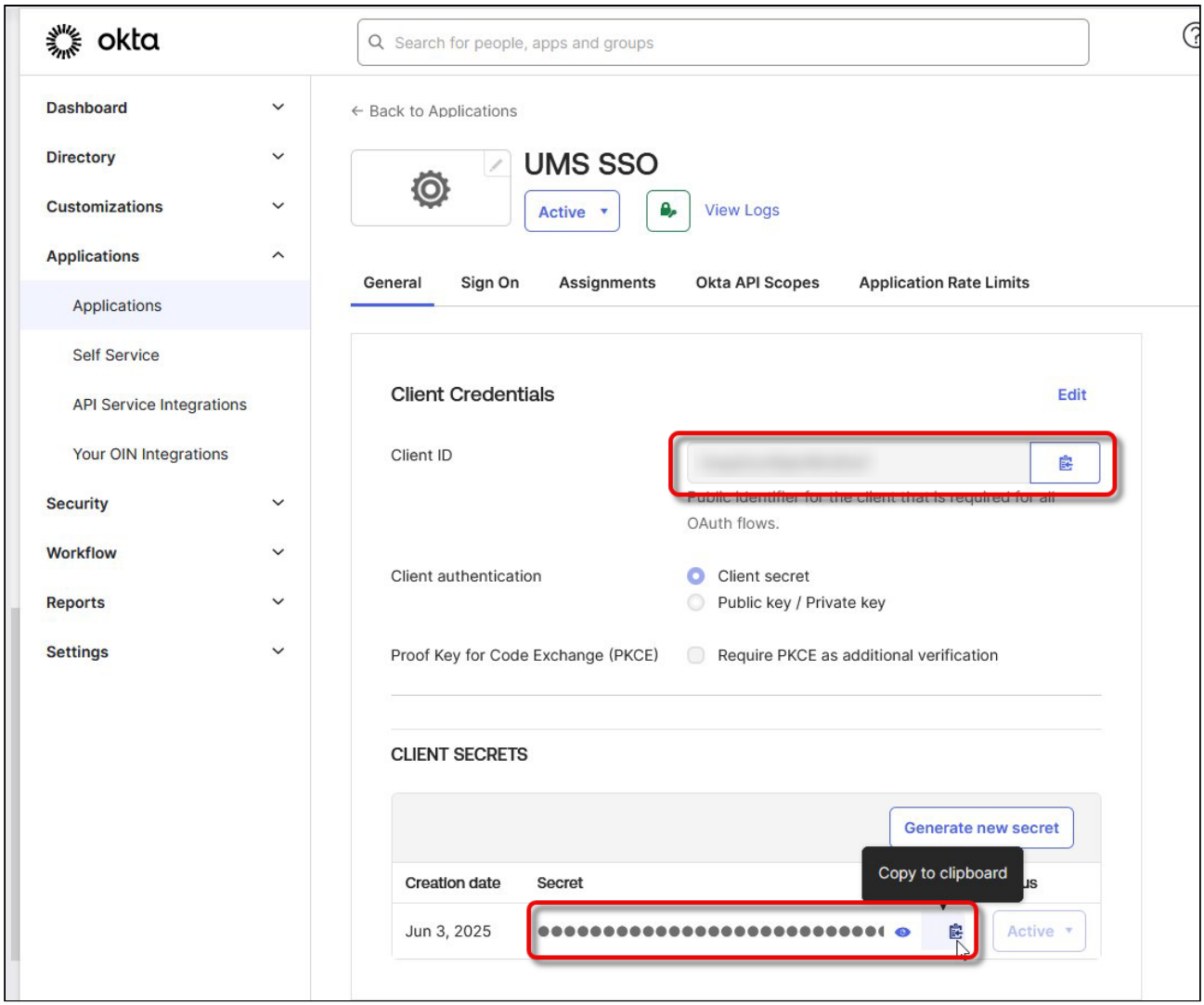


5. Save your application.

6. Go to **Security > API** and copy the **Issuer URI** of your authorization server (typically **default**).



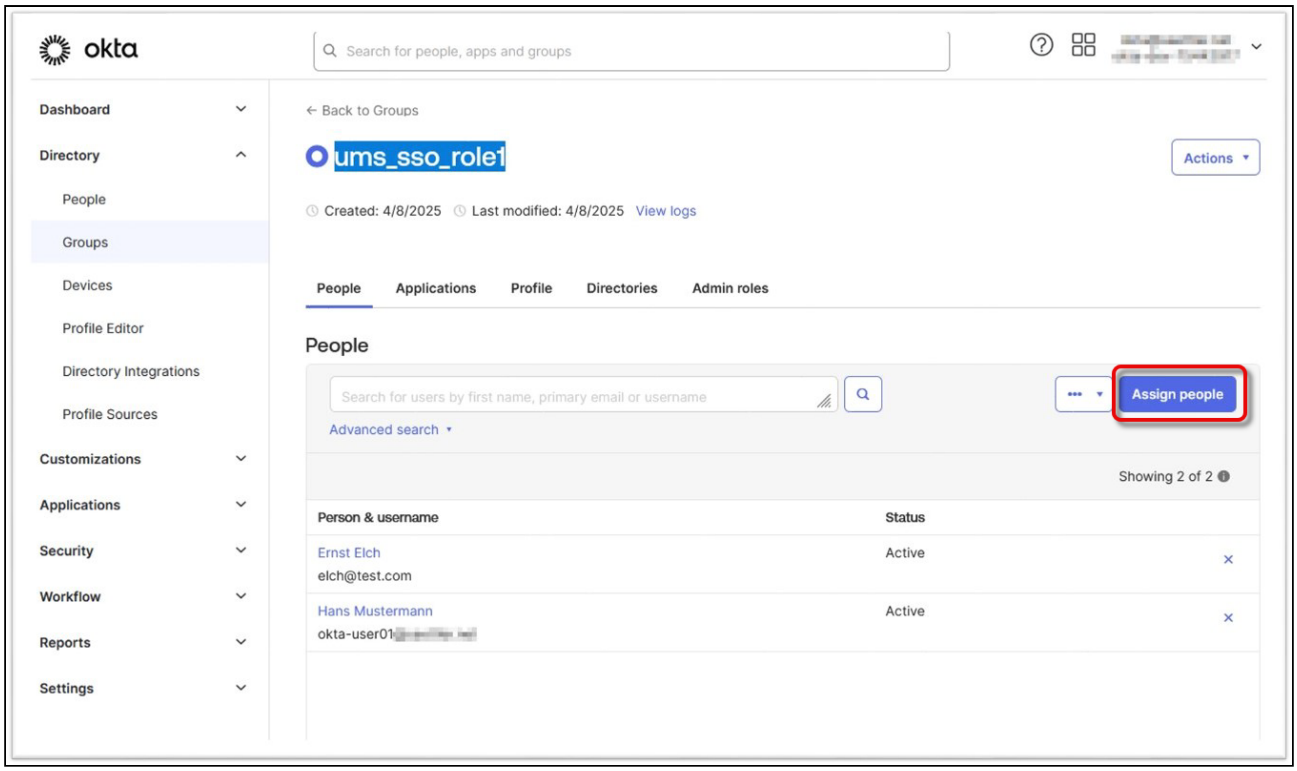
7. Open the **General** tab and copy the following data for your application:
    - **Client ID**
    - **Client Secret**



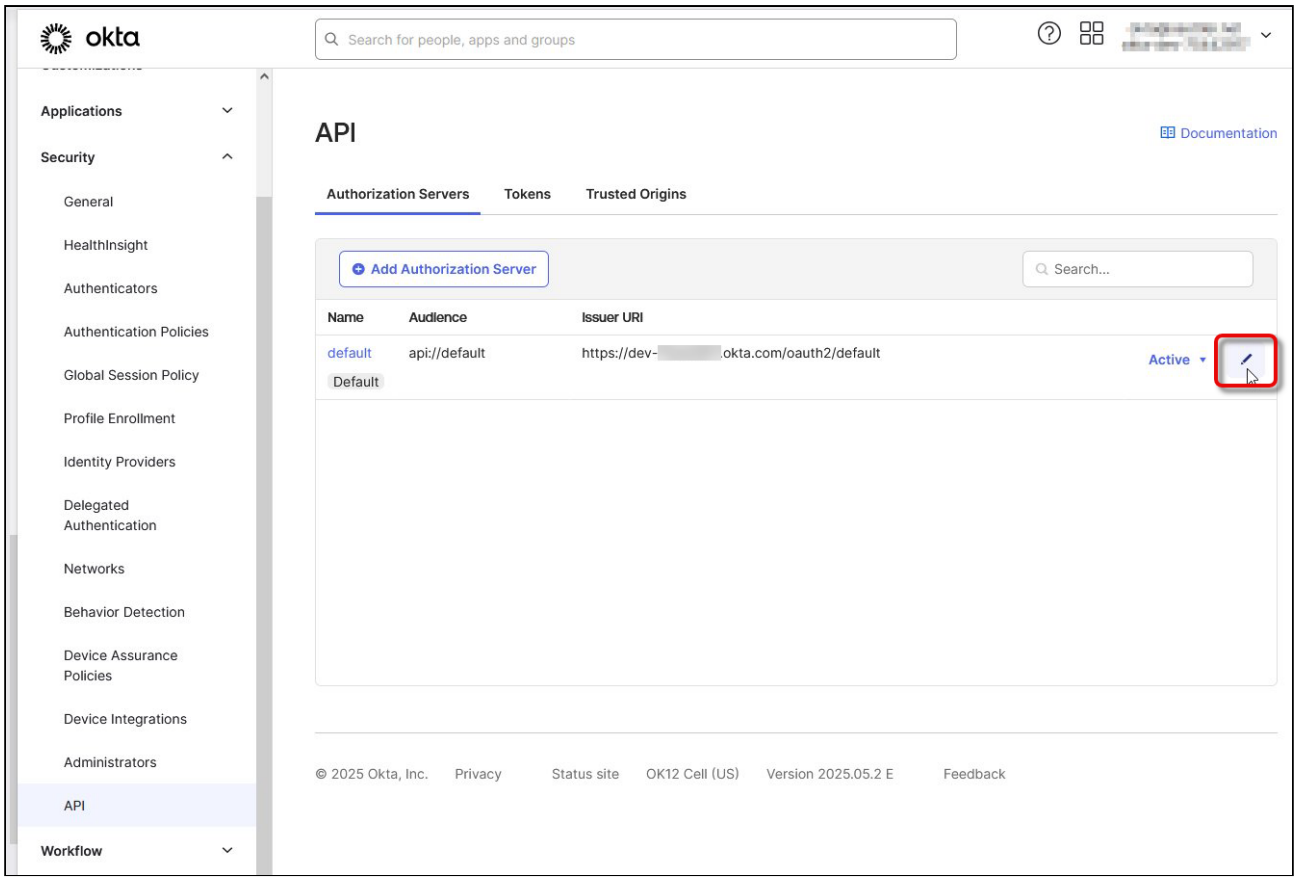
Configuring User Role Mapping in Okta

For the following procedure, we assume that a group is already defined in Okta.

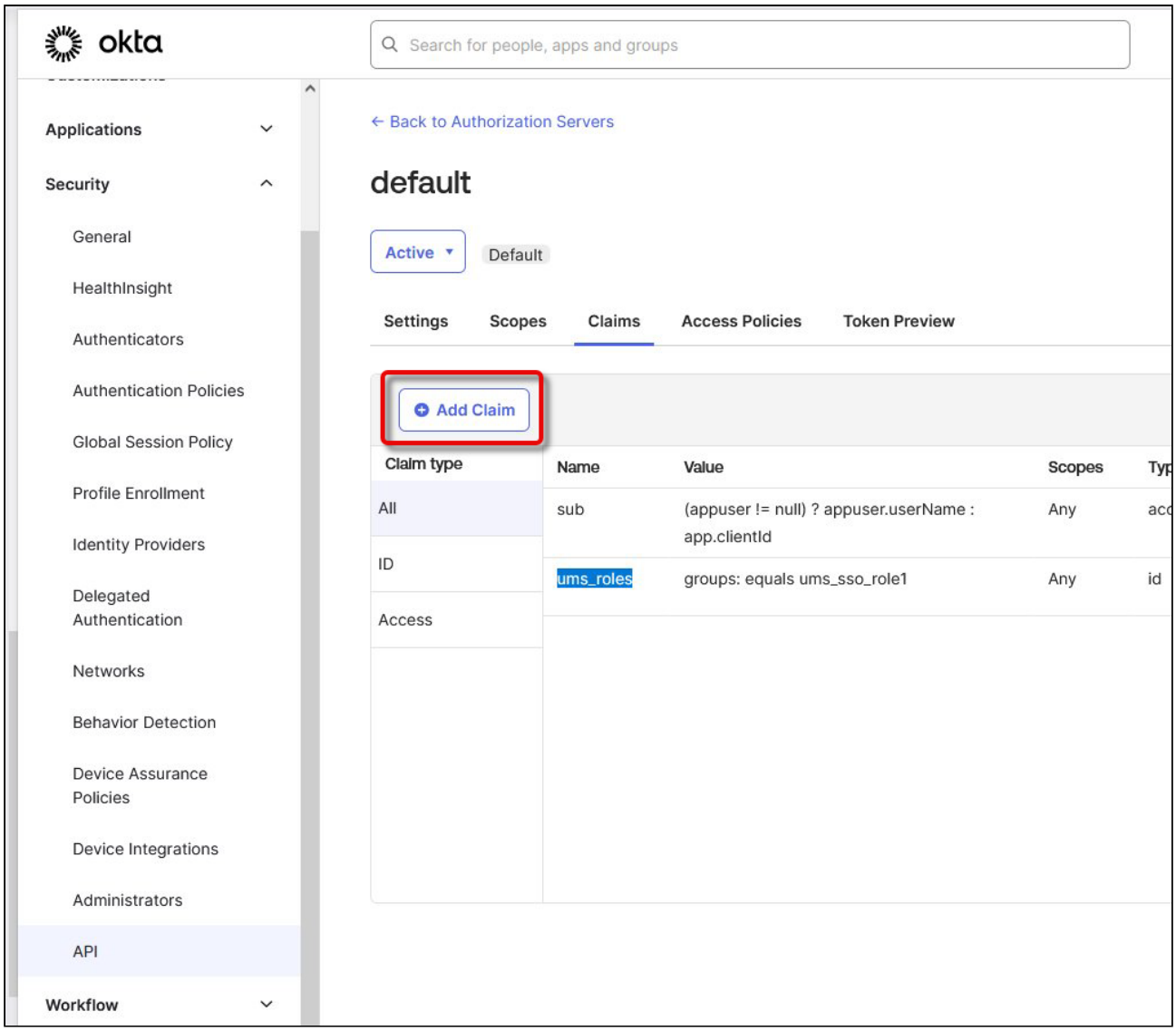
1. In the Okta portal, go to **Directory > Groups** and add the relevant users to your group.

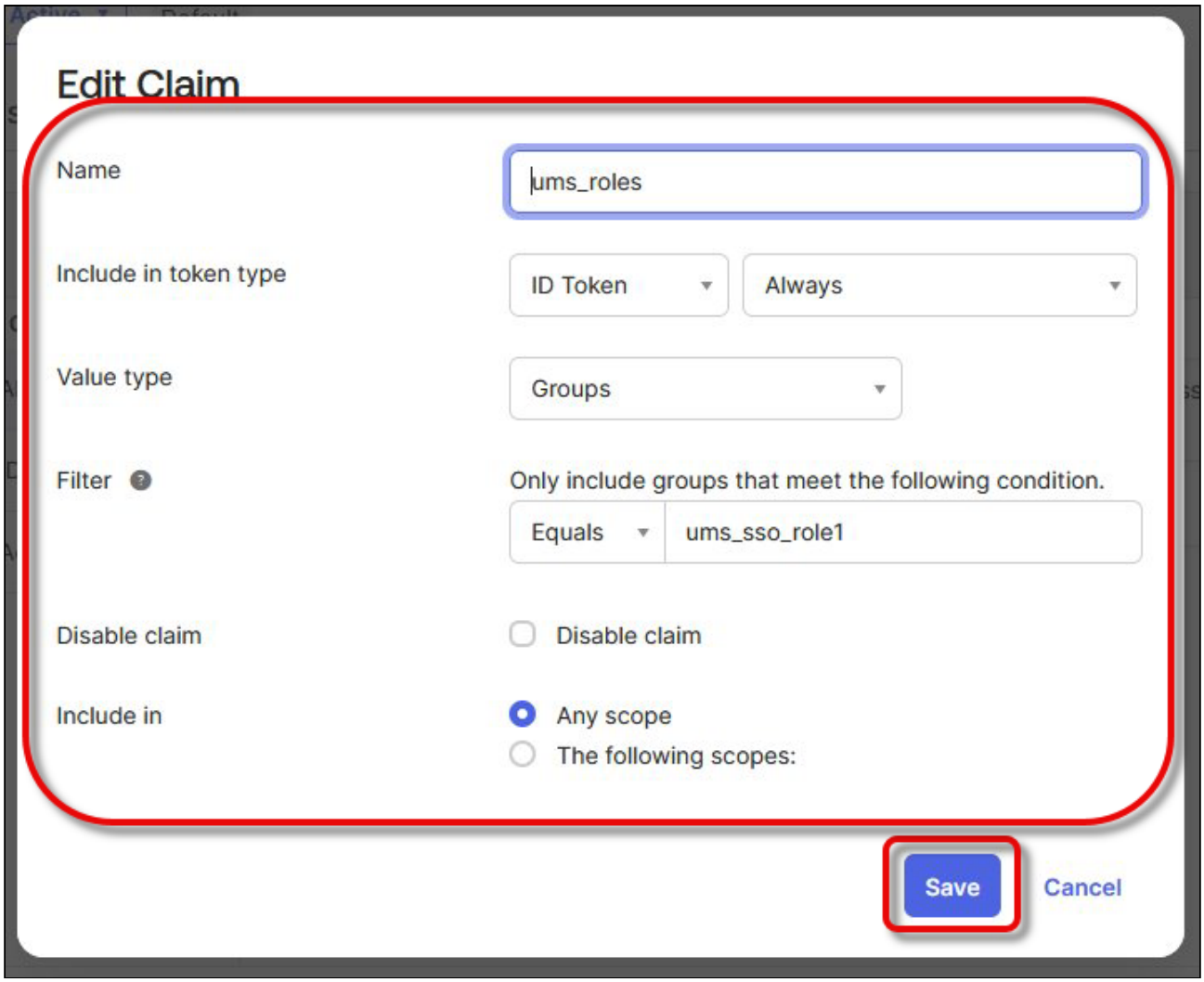


2. Switch to **Security > API** and edit your authorization server (typically **default**).



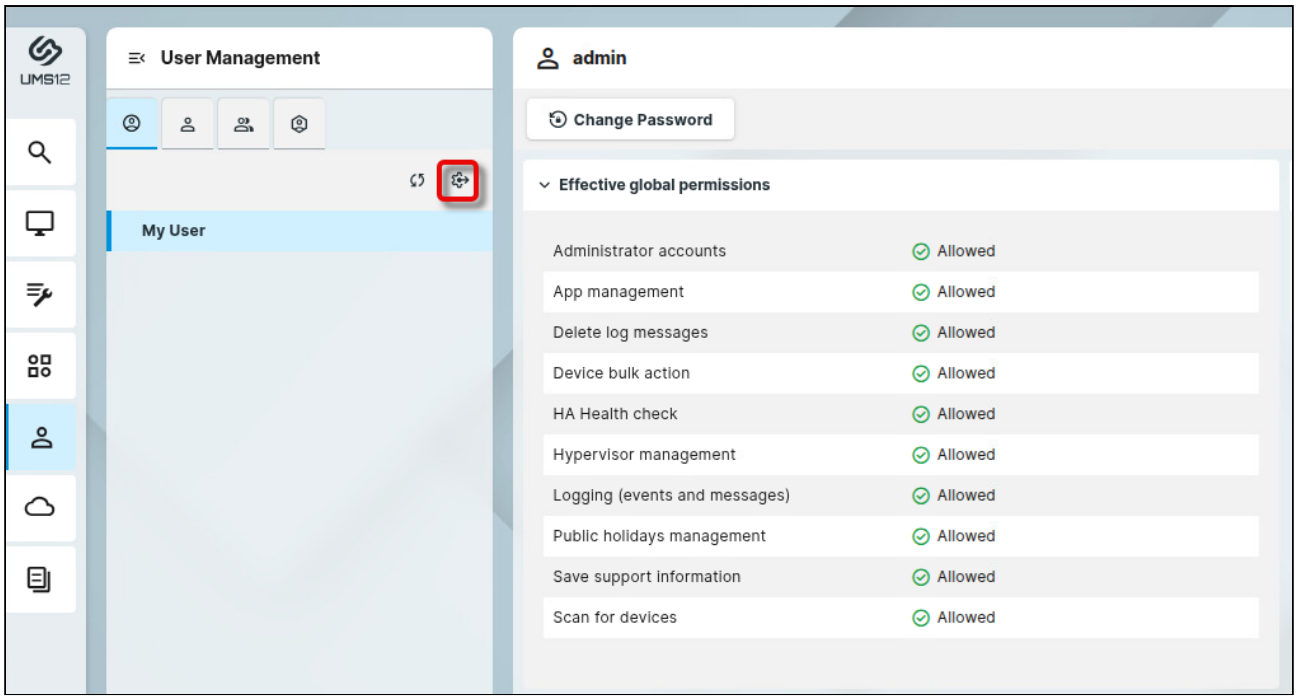
3. Open the tab **Claims** and add a new claim with the following settings:
    - Set the **Name** to “ums_roles”.
    - Set **Include in token type** to **ID Token** and **Always**.
    - Set **Value type** to **Groups**.
    - To assign your group to the claim, set **Filter > Equals** to the name of the group.
    - Use **Include in** to define the scopes. At least “openid” and “profile” should be selected.


okta
Search for people, apps and groups
Applications
Security
General
HealthInsight
Authenticators
Authentication Policies
Global Session Policy
Profile Enrollment
Identity Providers
Delegated Authentication
Networks
Behavior Detection
Device Assurance Policies
Device Integrations
Administrators
API
Workflow
← Back to Authorization Servers
default
Active
Default
Settings
Scopes
Claims
Access Policies
Token Preview
Add Claim
Claim type
All
ID
Access
Name
Value
Scopes
sub
(appuser != null) ? appuser.userName : app.clientId
Any
ums_roles
groups: equals ums_sso_role1
Any
id

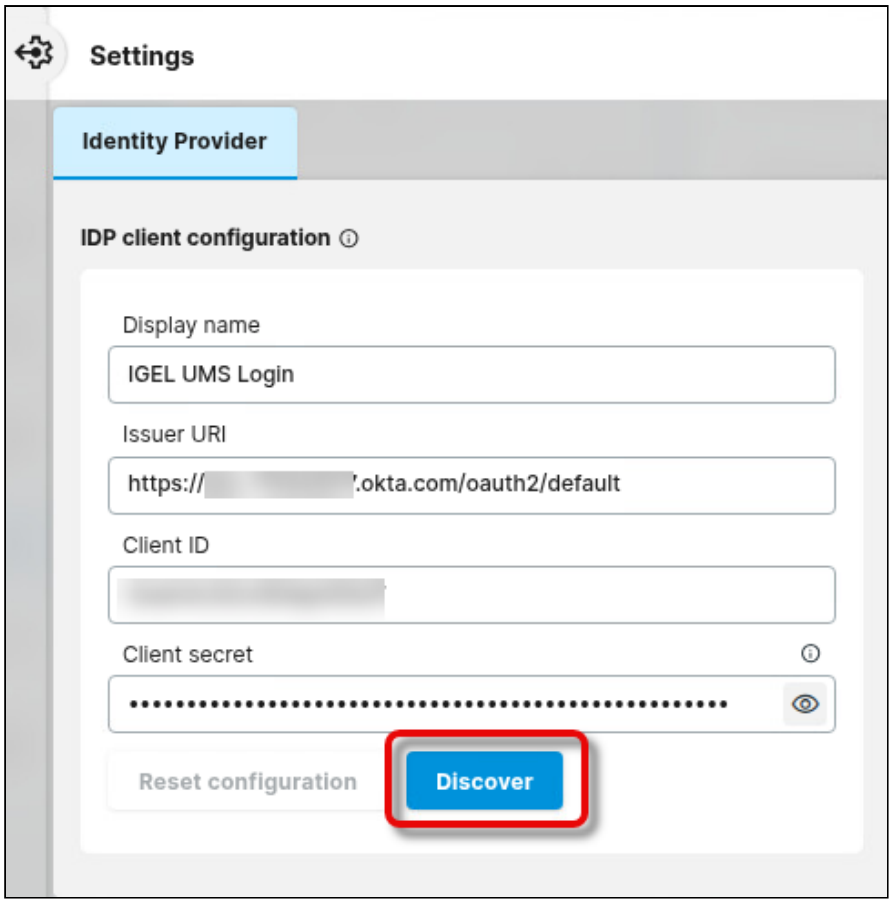


Configuring Your Connection to Okta in the UMS Web App

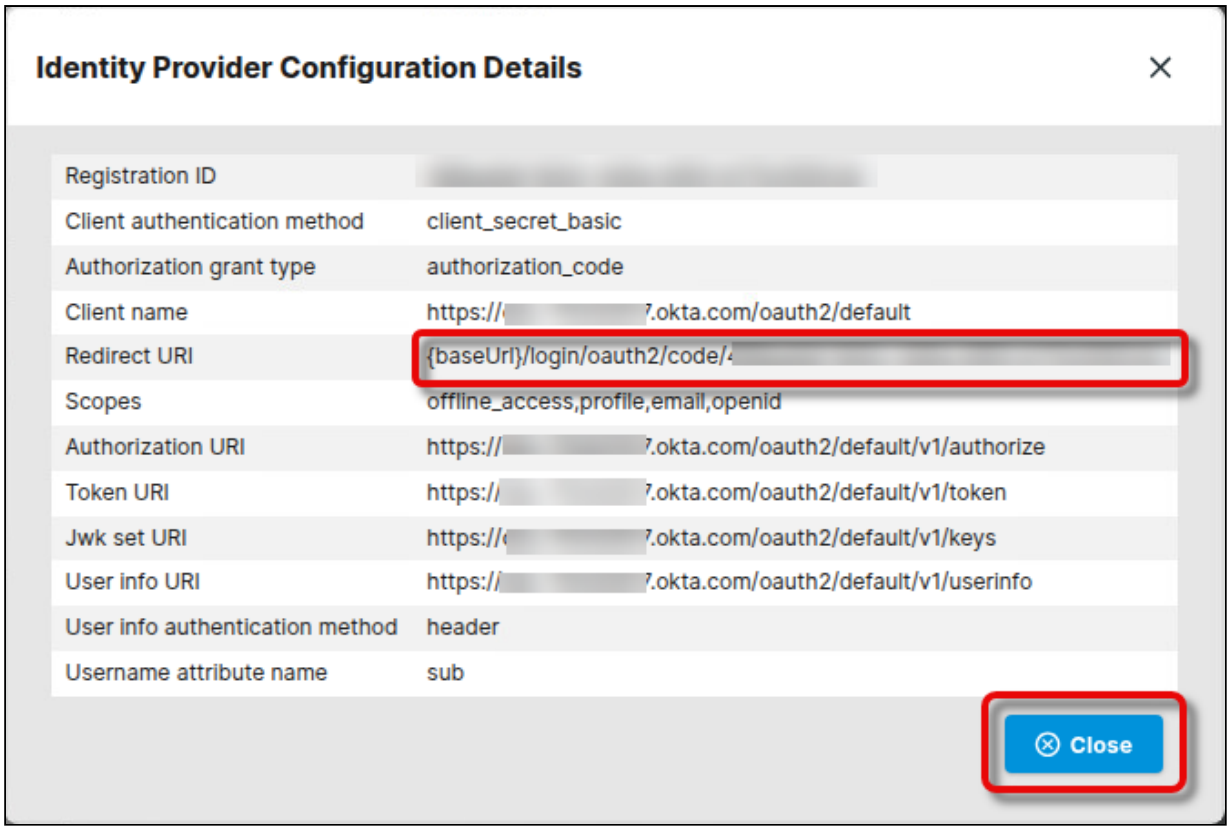
1. Open the UMS Web App, go to **User Management**, and click .



2. Enter the following data from the application you have created in Okta and click **Discover**.
    - **Display name**: The name of your application
    - **Issuer URI**: The issuer URI of your authentication server
    - **Client ID**: The client ID for your application
    - **Client secret**: The secret you have created for your application

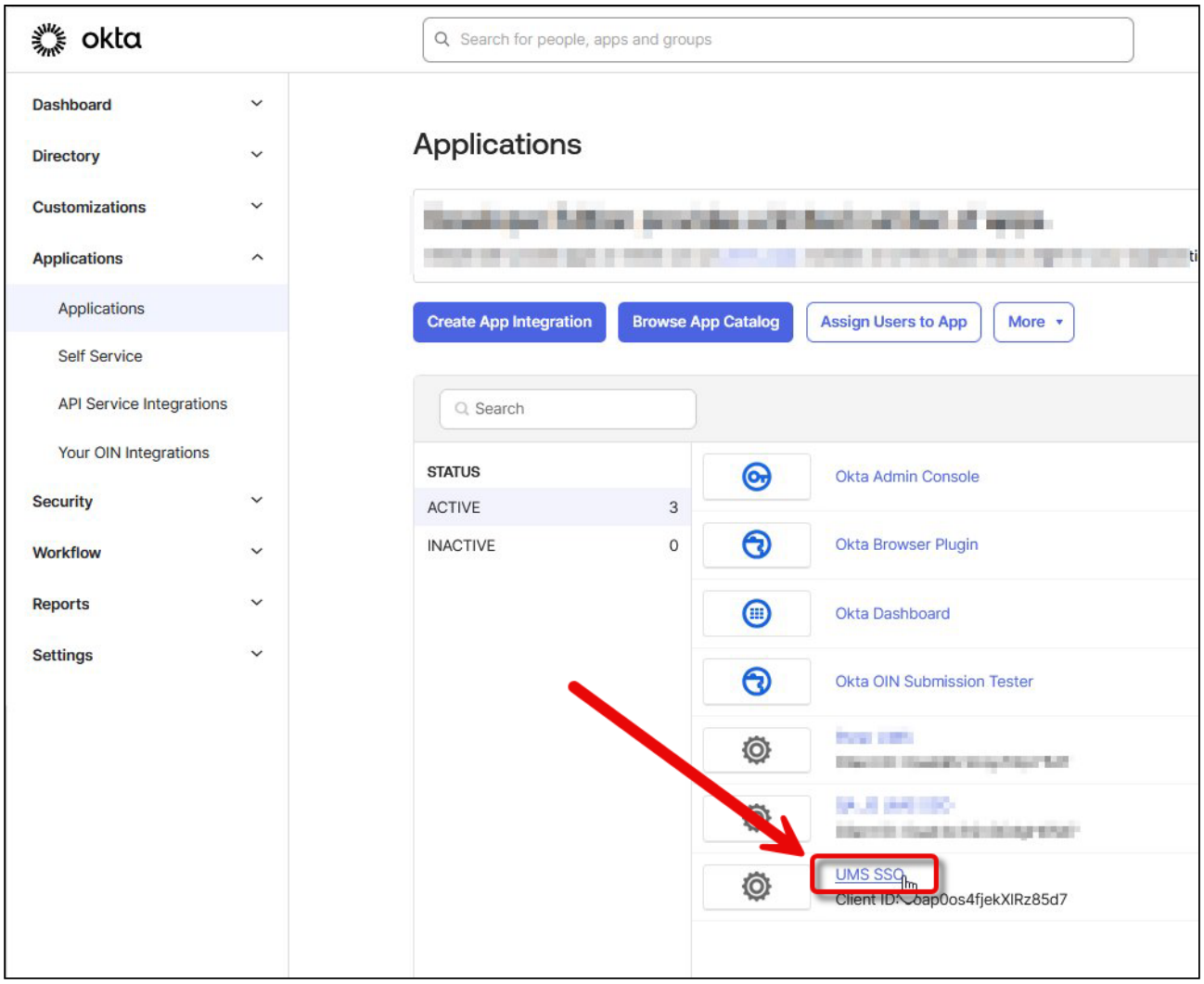


3. In the **Identify Provider Configuration Details** window, copy the **Redirect URI** and close the window.

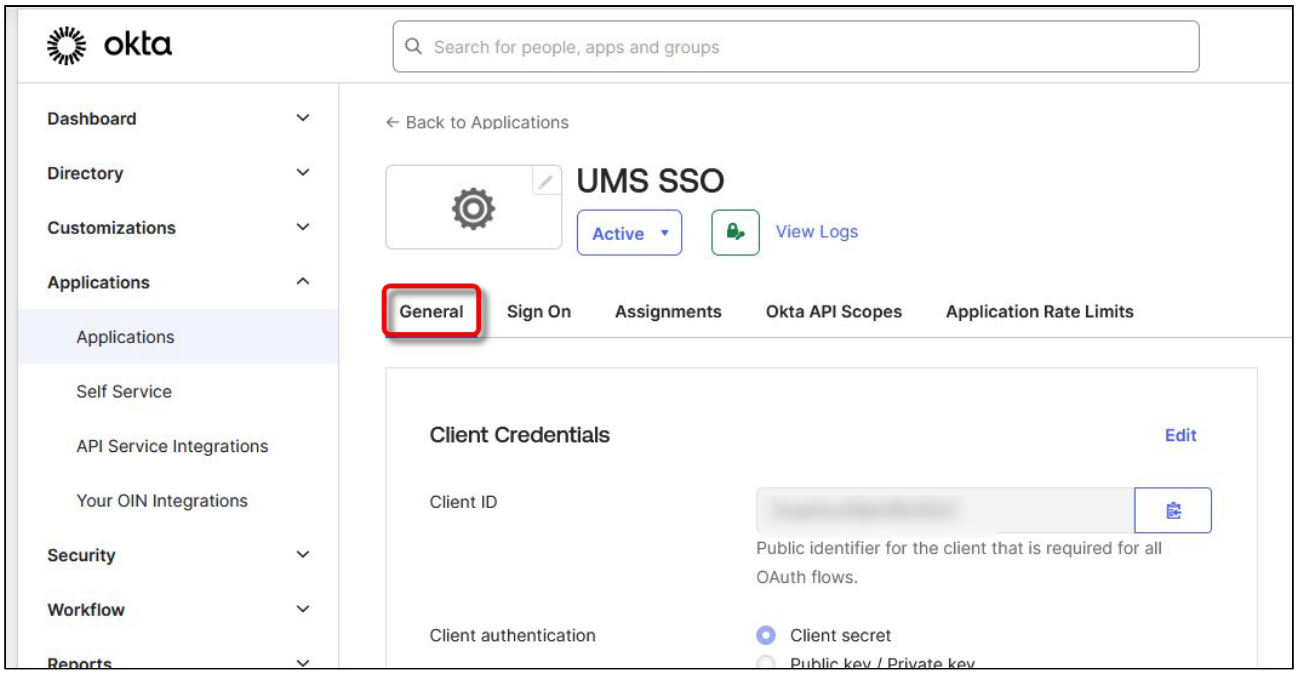


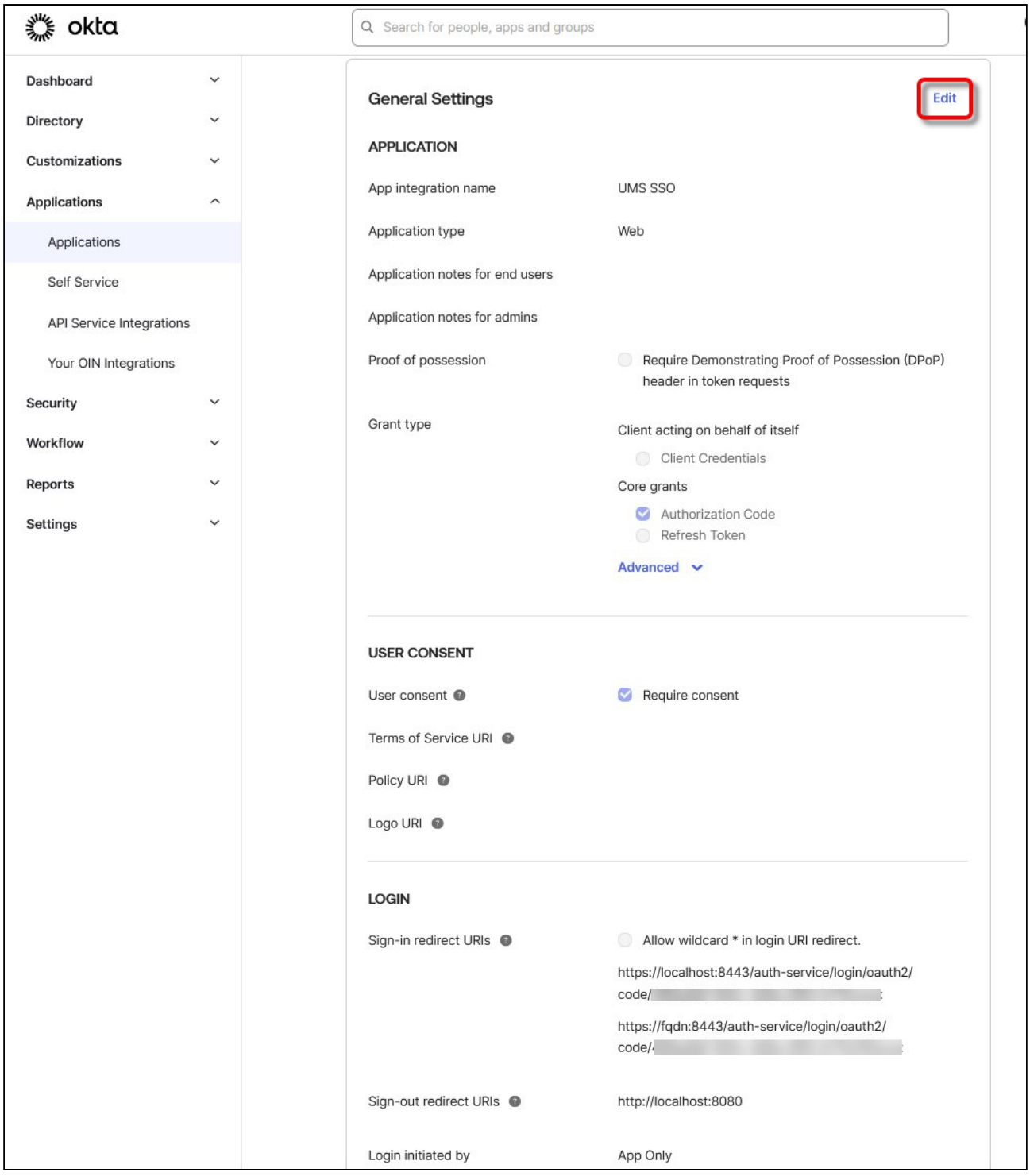
Configuring the Redirect URL of the UMS in Okta

1. In the Okta portal, go to **Applications > Applications** and open your application.



2. Select the tab **General**, scroll down to **General Settings**, and click **Edit**.

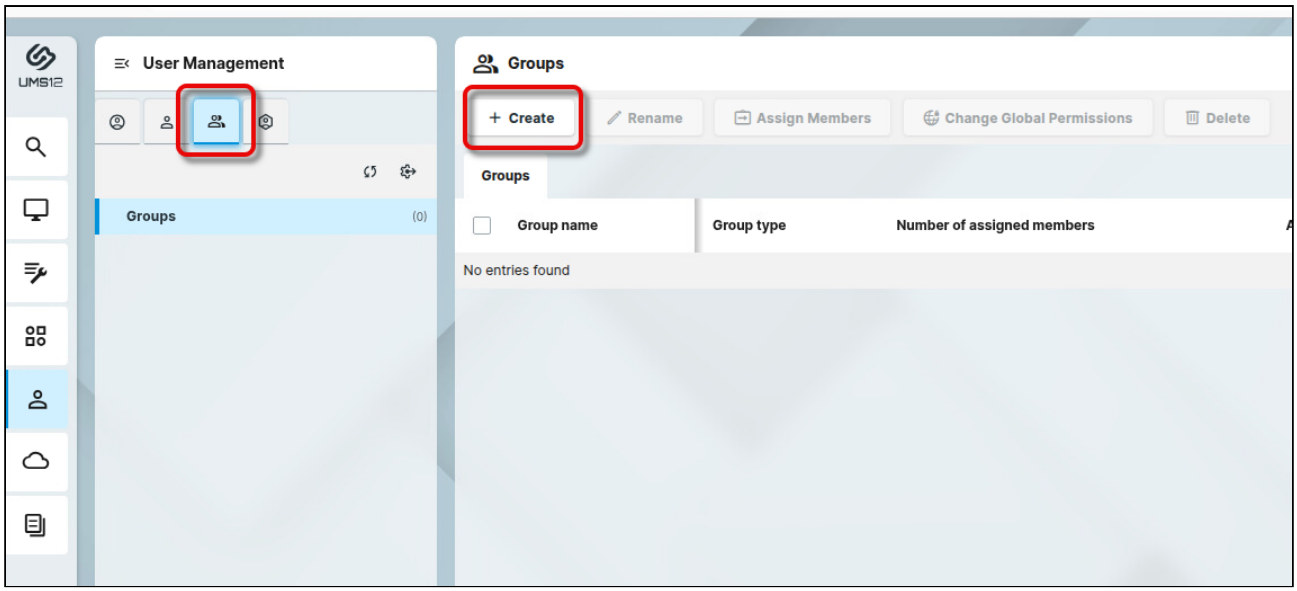

okta
Search for people, apps and groups
Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security
Workflow
Reports
← Back to Applications
UMS SSO
Active
View Logs
General
Sign On
Assignments
Okta API Scopes
Application Rate Limits
Client Credentials
Edit
Client ID
Public identifier for the client that is required for all OAuth flows.
Client authentication
Client secret
Public key / Private key


okta
Search for people, apps and groups
Dashboard
Directory
Customizations
Applications
Applications
Self Service
API Service Integrations
Your OIN Integrations
Security
Workflow
Reports
Settings
General Settings
Edit
APPLICATION
App integration name
UMS SSO
Application type
Web
Application notes for end users
Application notes for admins
Proof of possession
Require Demonstrating Proof of Possession (DPoP) header in token requests
Grant type
Client acting on behalf of itself
Client Credentials
Core grants
Authorization Code
Refresh Token
Advanced
USER CONSENT
User consent
Require consent
Terms of Service URI
Policy URI
Logo URI
LOGIN
Sign-in redirect URIs
Allow wildcard * in login URI redirect.
https://localhost:8443/auth-service/login/oauth2/code/
https://fqdn:8443/auth-service/login/oauth2/code/
Sign-out redirect URIs
http://localhost:8080
Login initiated by
App Only

3. In the section **LOGIN**, under **Sign-in redirect URIs**, enter the login URIs. All URIs that can be used for login must be added here, according to the following patterns:
   - IP address of the UMS Server: `https://<IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://123.123.123.123:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - FQDN of the UMS Server: `https://<FQDN>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums.example.com:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - Short name of the UMS Server: `https://<SHORT NAME>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - Local IP address: `https://<LOCAL IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://127.0.0.1:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
   - “localhost” (used when the **Server** field in the login dialog of the UMS Console is empty): `https://localhost:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://localhost:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`

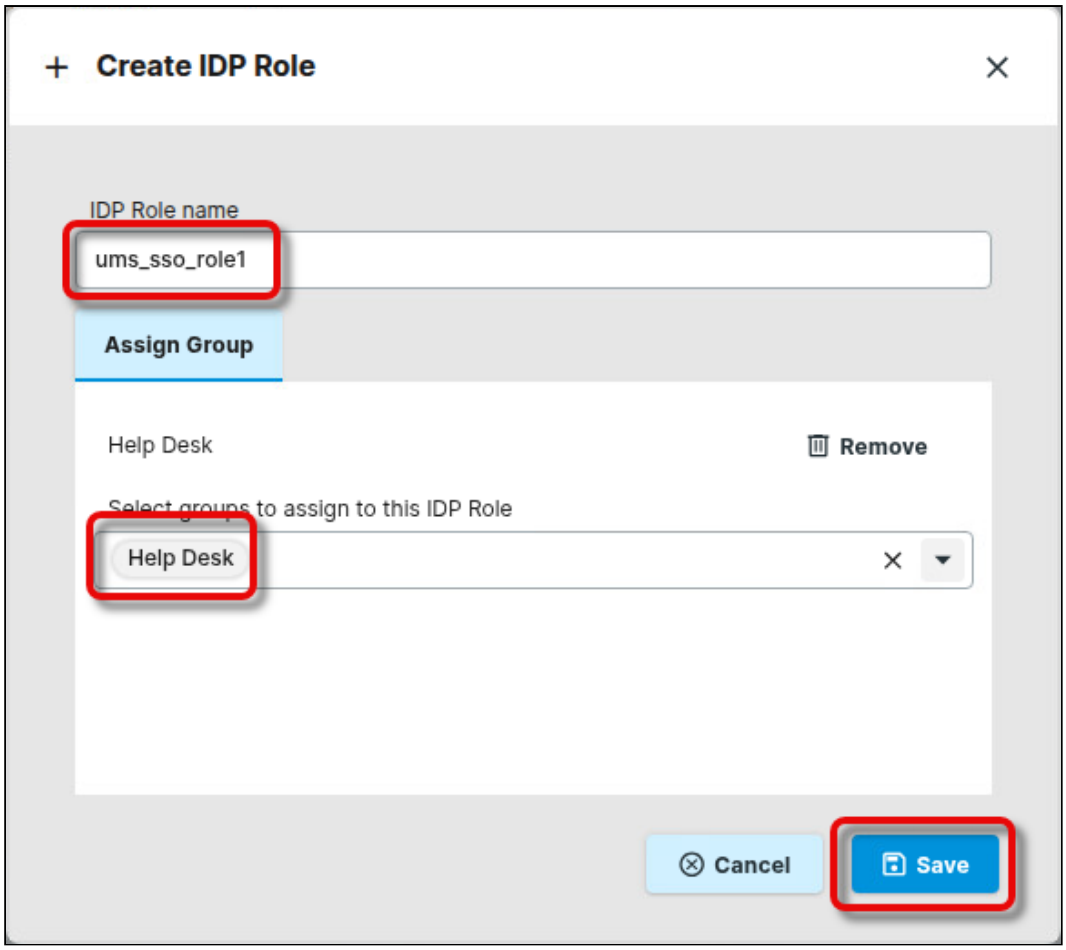
Mapping the Roles in Okta to UMS Groups

1. Open the UMS Web App, go to **User Management**, select  , and click **+ Create**.



2. Edit the settings as follows:

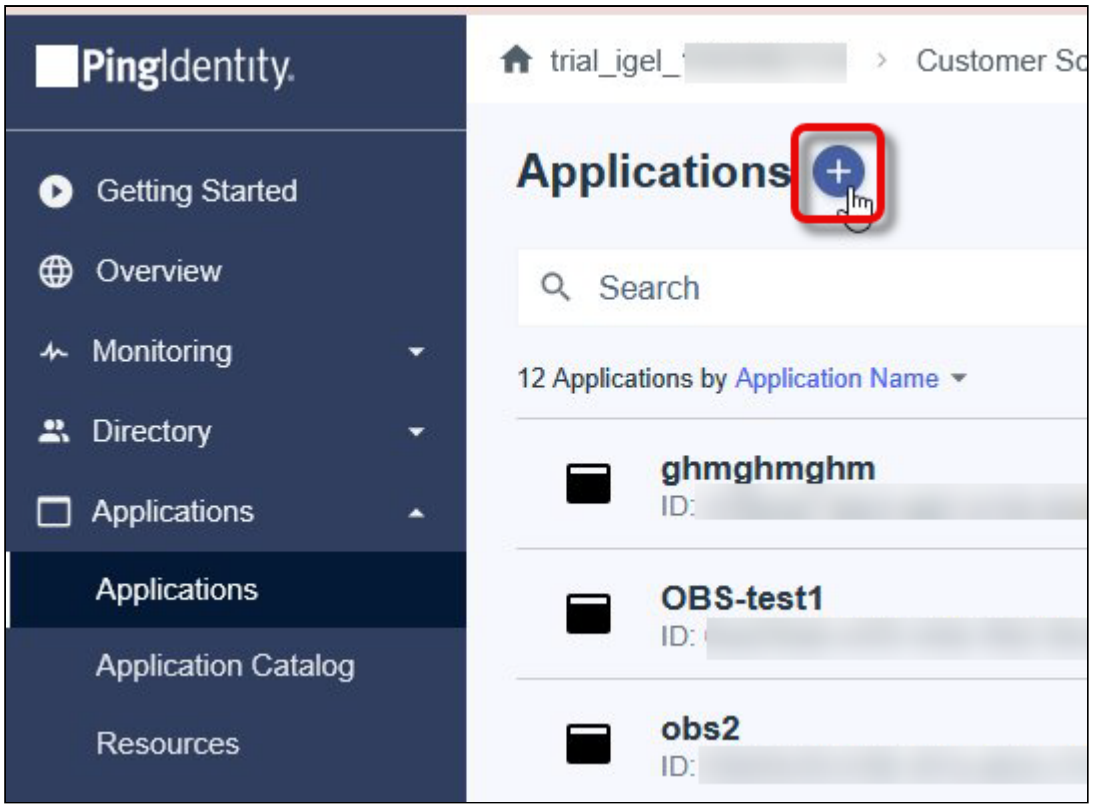
- **IDP Role name**: The **Name** of the app role you have configured in Okta. Please note that this value is case-sensitive.
- **Assign Group**: The UMS group you want to map to the app role



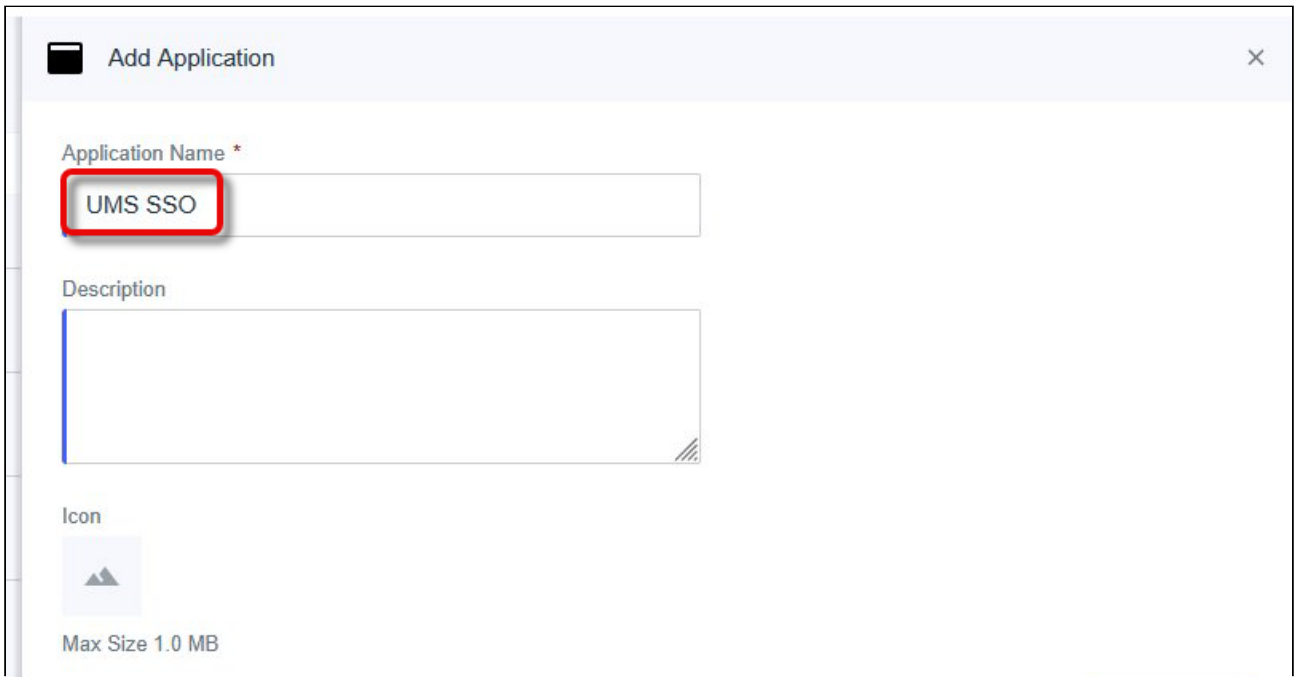
UMS Login with Ping Identity

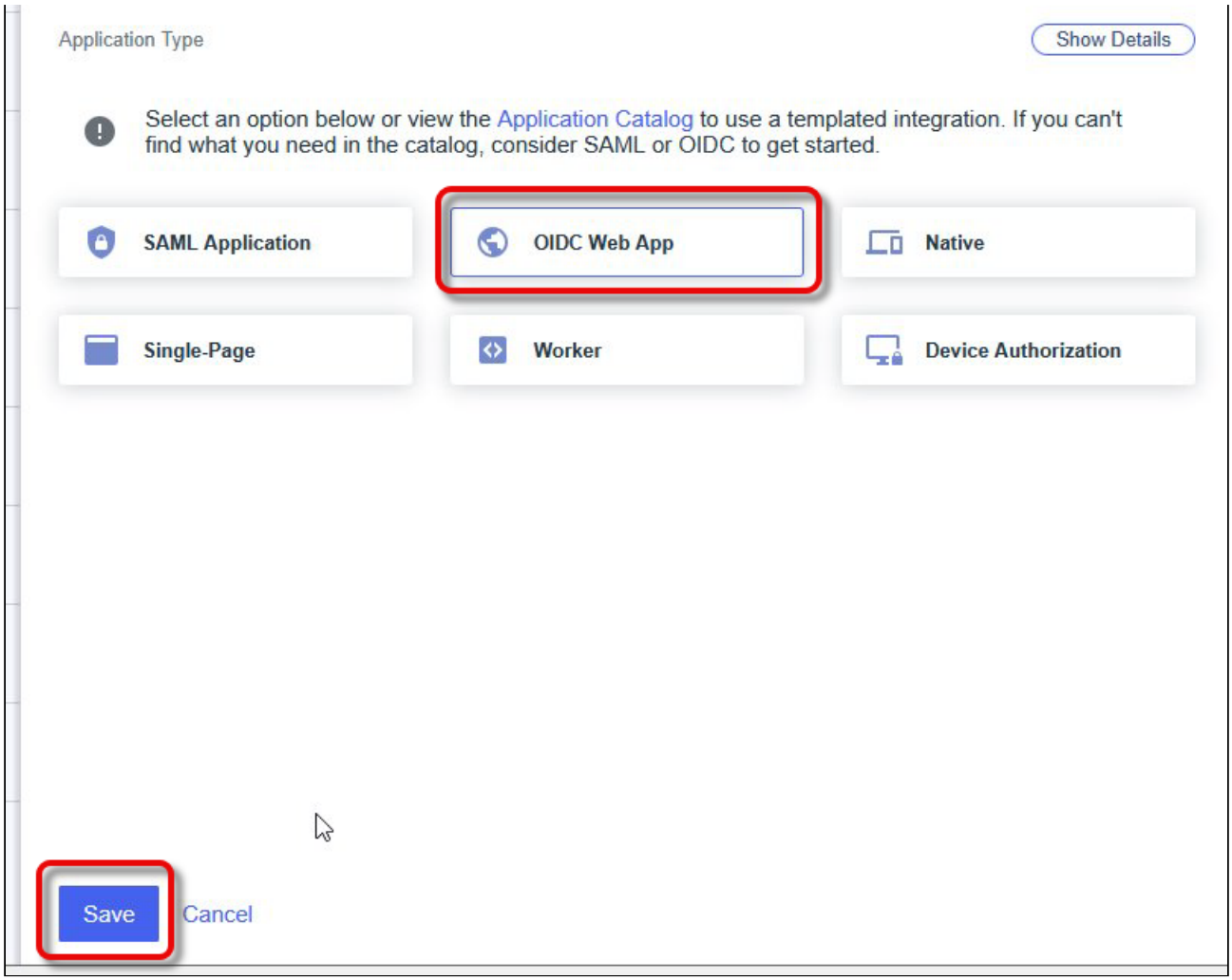
Creating an Application in PingIdentity

1. Log in to the PingIdentity portal, go to **Applications > Applications**, and click ⊕ to create a new application.

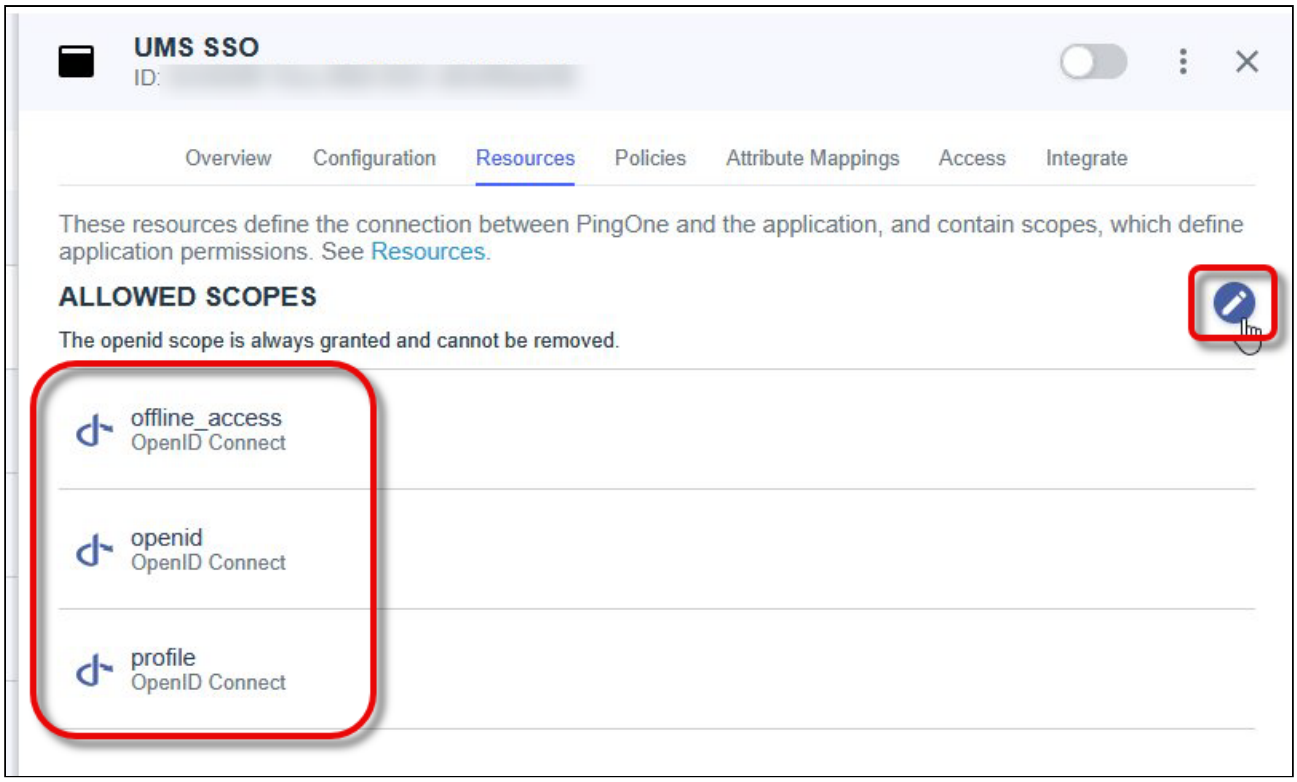


2. Define an **Application Name** and select **OIDC WebApp** as the app type.

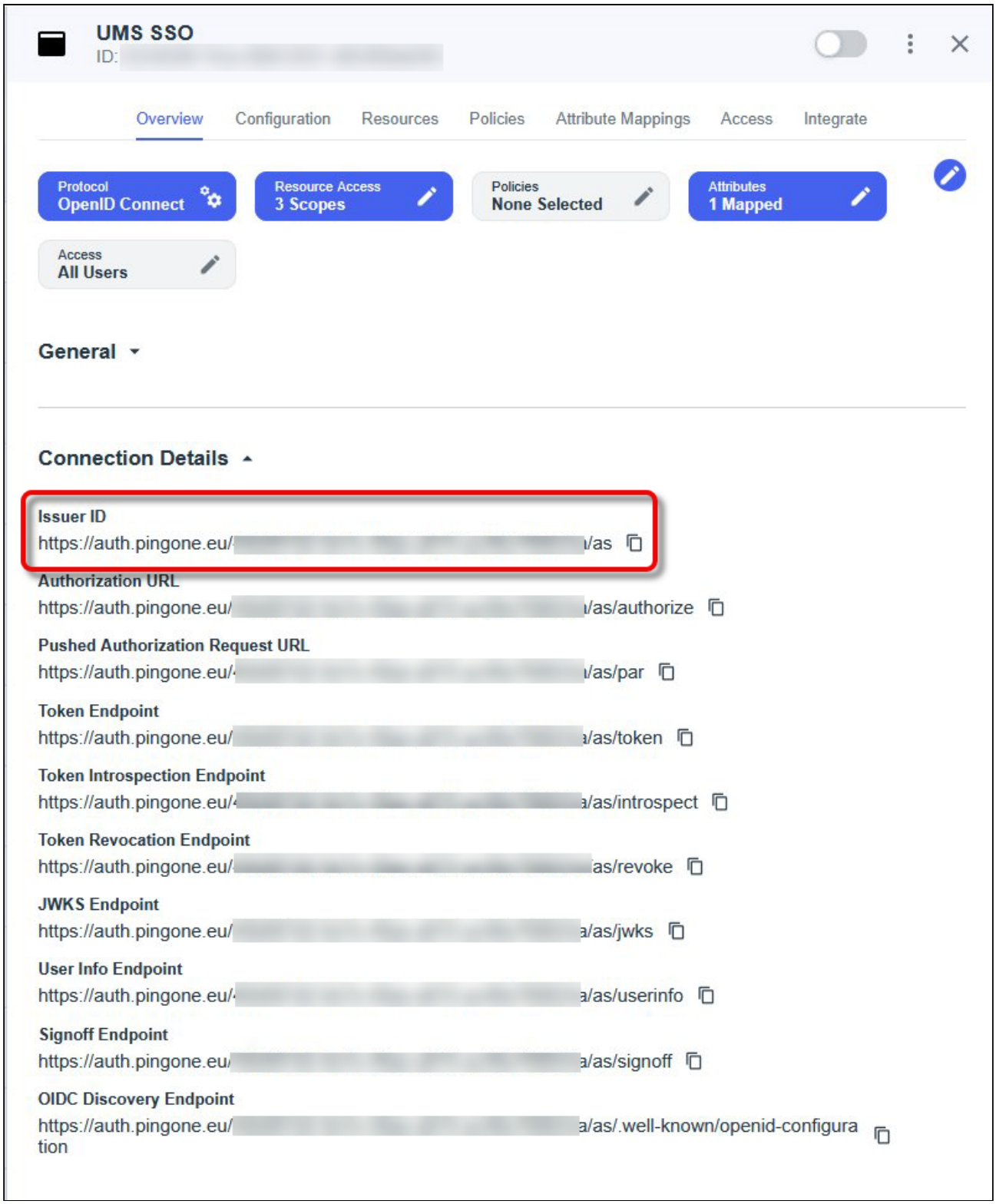




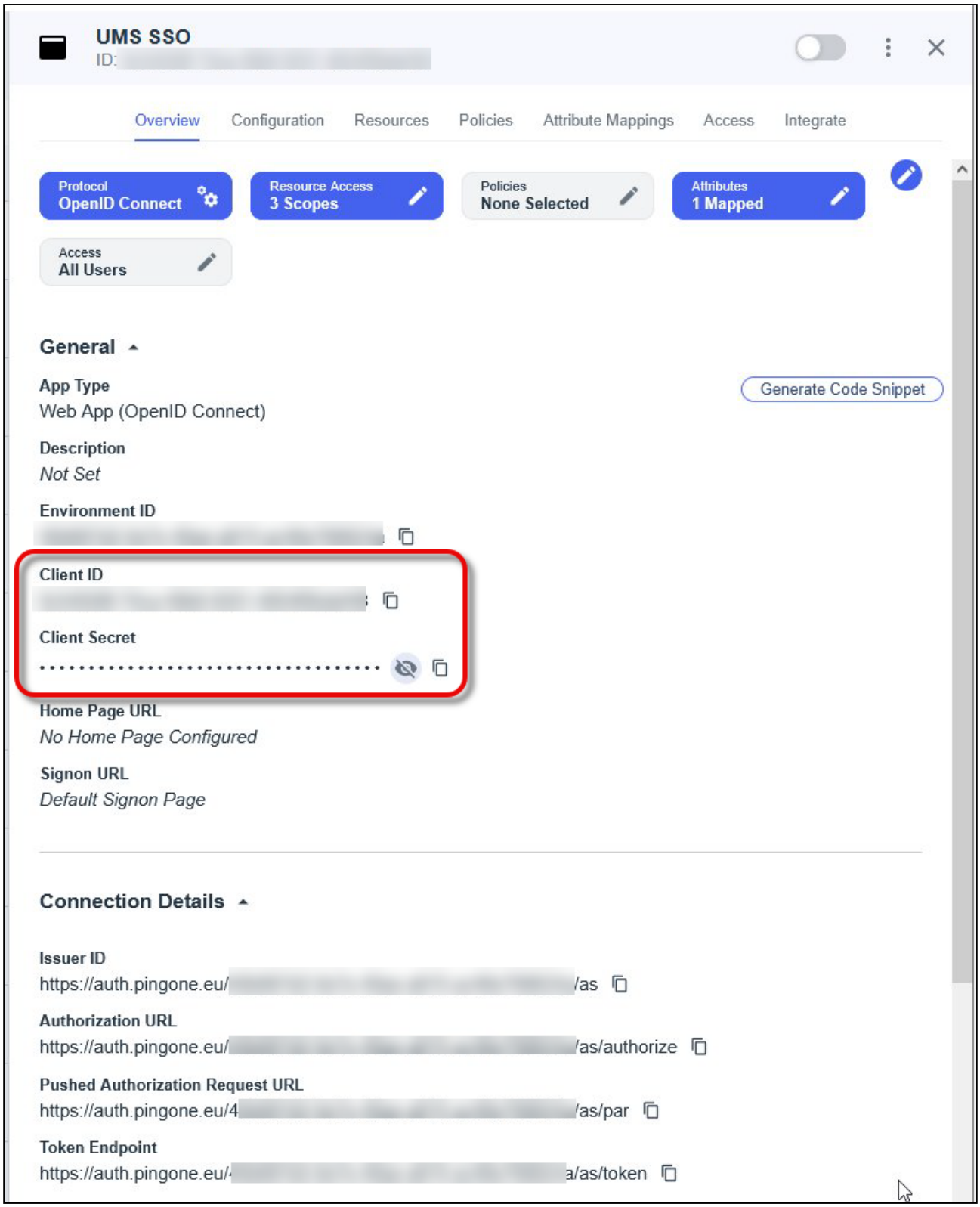
3. Go to Resources and select the following **Allowed Scopes**:
   - **offline_access**
   - **openid**
   - **profile**



4. Open the tab **Overview**, expand the connection details, and copy the **Issuer URI**.

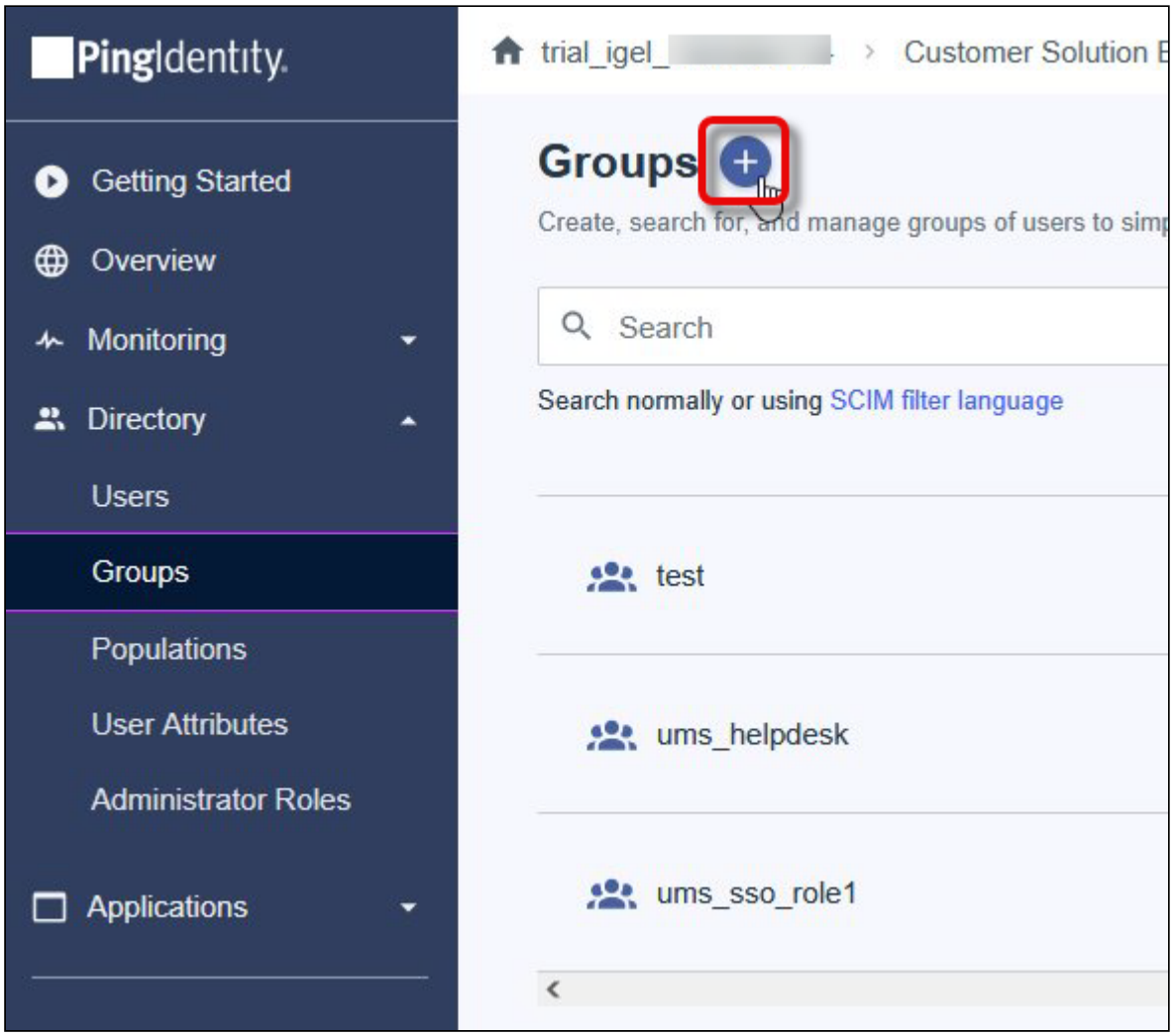

UMS SSO
ID:
Overview
Configuration
Resources
Policies
Attribute Mappings
Access
Integrate
Protocol
OpenID Connect
Resource Access
3 Scopes
Policies
None Selected
Attributes
1 Mapped
Access
All Users
General
Connection Details
Issuer ID
https://auth.pingone.eu/ /as
Authorization URL
https://auth.pingone.eu/ /as/authorize
Pushed Authorization Request URL
https://auth.pingone.eu/ /as/par
Token Endpoint
https://auth.pingone.eu/ /as/token
Token Introspection Endpoint
https://auth.pingone.eu/ /as/introspect
Token Revocation Endpoint
https://auth.pingone.eu/ as/revoke
JWKS Endpoint
https://auth.pingone.eu/ /as/jwks
User Info Endpoint
https://auth.pingone.eu/ /as/userinfo
Signoff Endpoint
https://auth.pingone.eu/ /as/signoff
OIDC Discovery Endpoint
https://auth.pingone.eu/ /as/.well-known/openid-configura
tion

5. From the section **General**, copy the following data:
    - **Client ID**
    - **Client Secret**

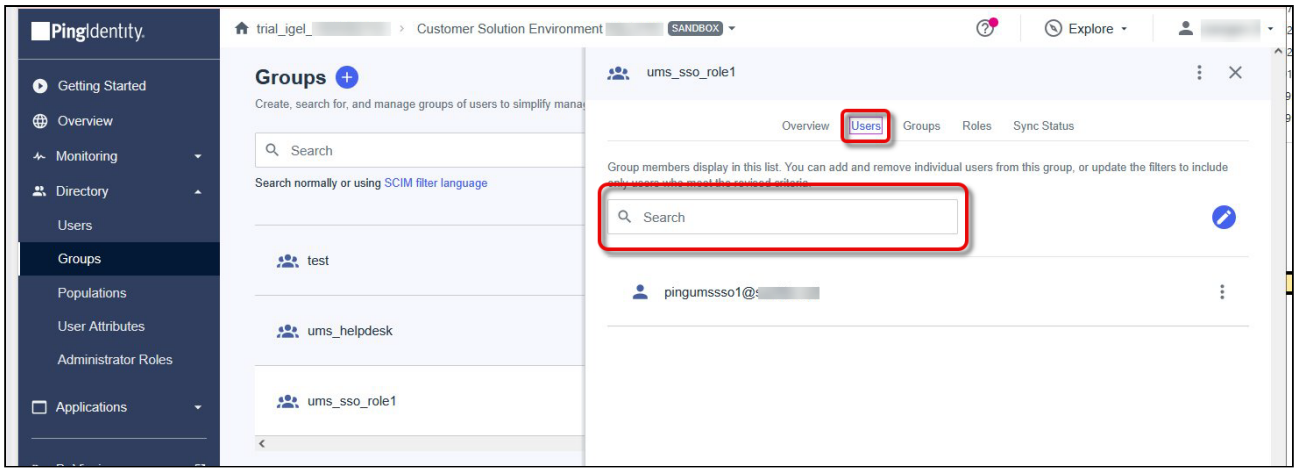

UMS SSO
ID:
Overview
Configuration
Resources
Policies
Attribute Mappings
Access
Integrate
Protocol
OpenID Connect
Resource Access
3 Scopes
Policies
None Selected
Attributes
1 Mapped
Access
All Users
General
App Type
Web App (OpenID Connect)
Generate Code Snippet
Description
Not Set
Environment ID
Client ID
Client Secret
Home Page URL
No Home Page Configured
Signon URL
Default Signon Page
Connection Details
Issuer ID
https://auth.pingone.eu/
/as
Authorization URL
https://auth.pingone.eu/
/as/authorize
Pushed Authorization Request URL
https://auth.pingone.eu/4
/as/par
Token Endpoint
https://auth.pingone.eu/
a/as/token

Configuring User Role Mapping in PingIdentity

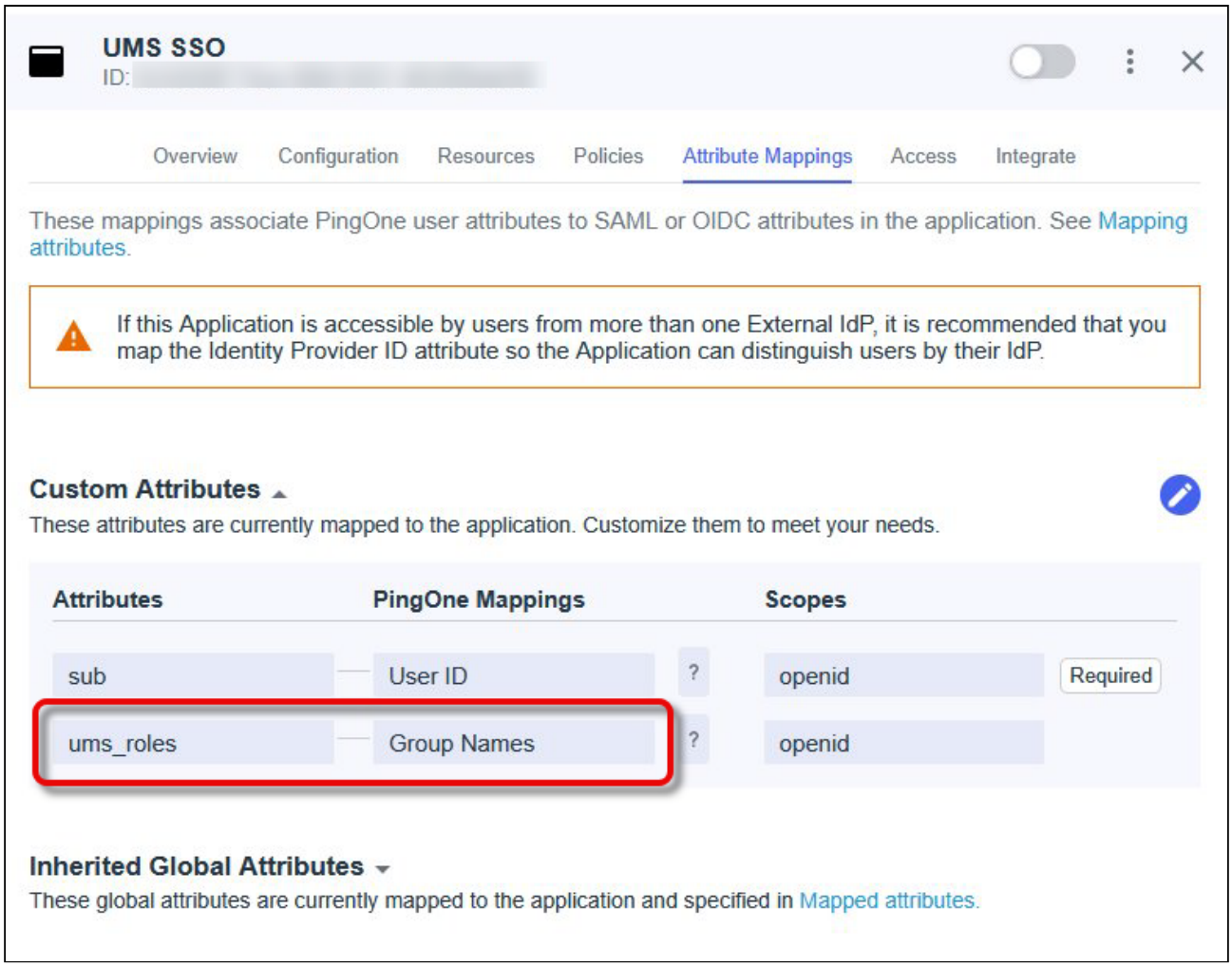
1. Go to **Directory > Groups** and create a group.



2. Open the tab **Users** and add users to your group.

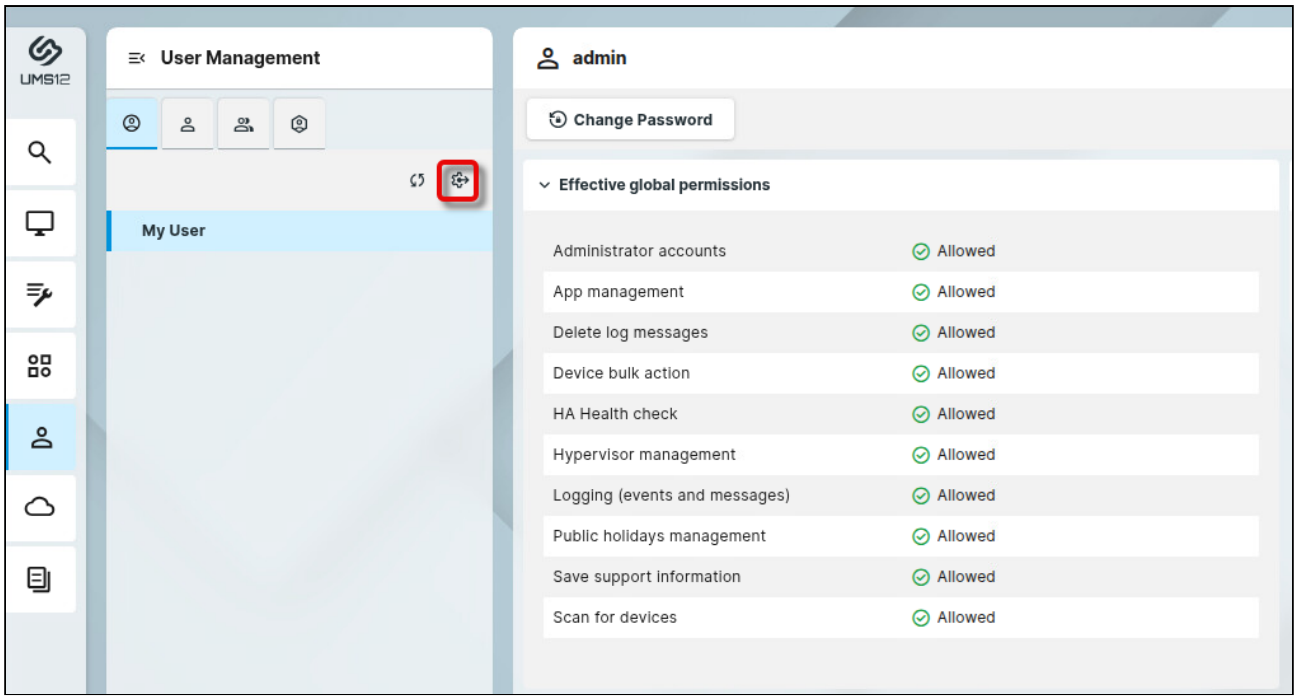


3. In your application, open the tab **Attribute Mappings** and map the attribute **ums_roles** to **Group Names**.

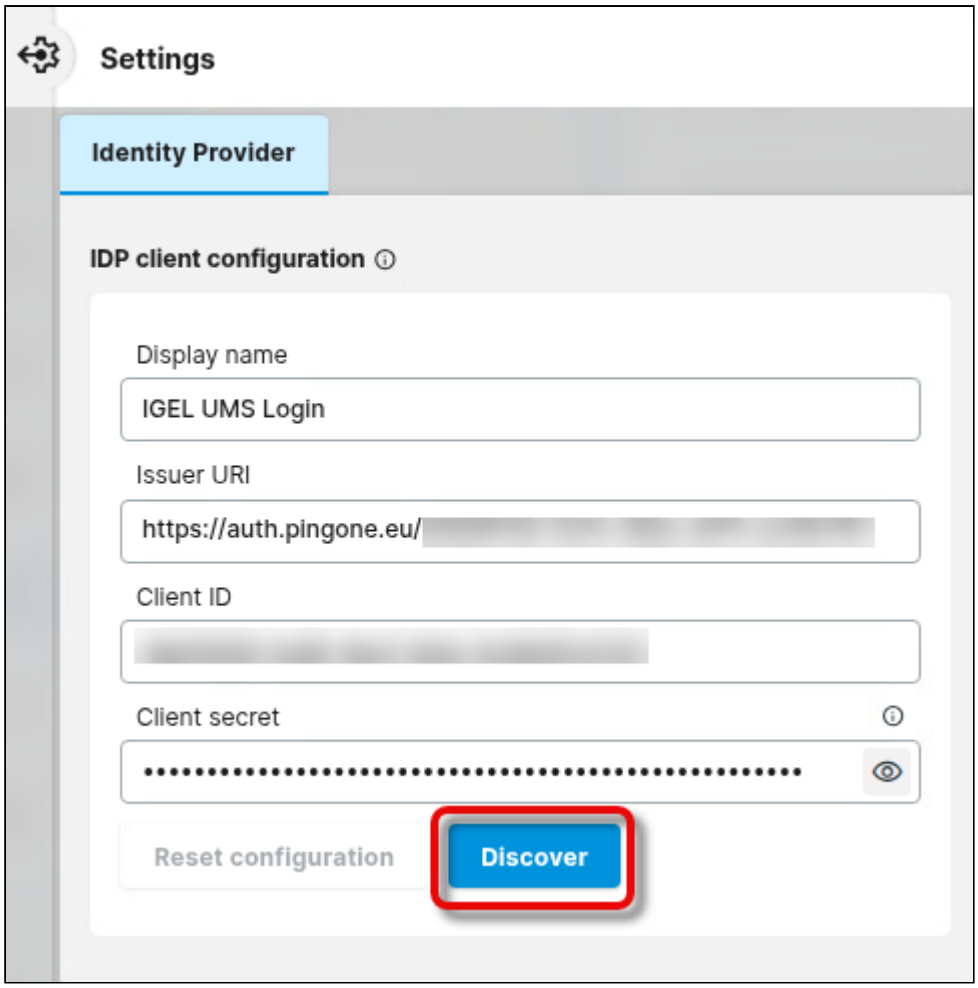


Configuring Your Connection to PingIdentity in the UMS Web App

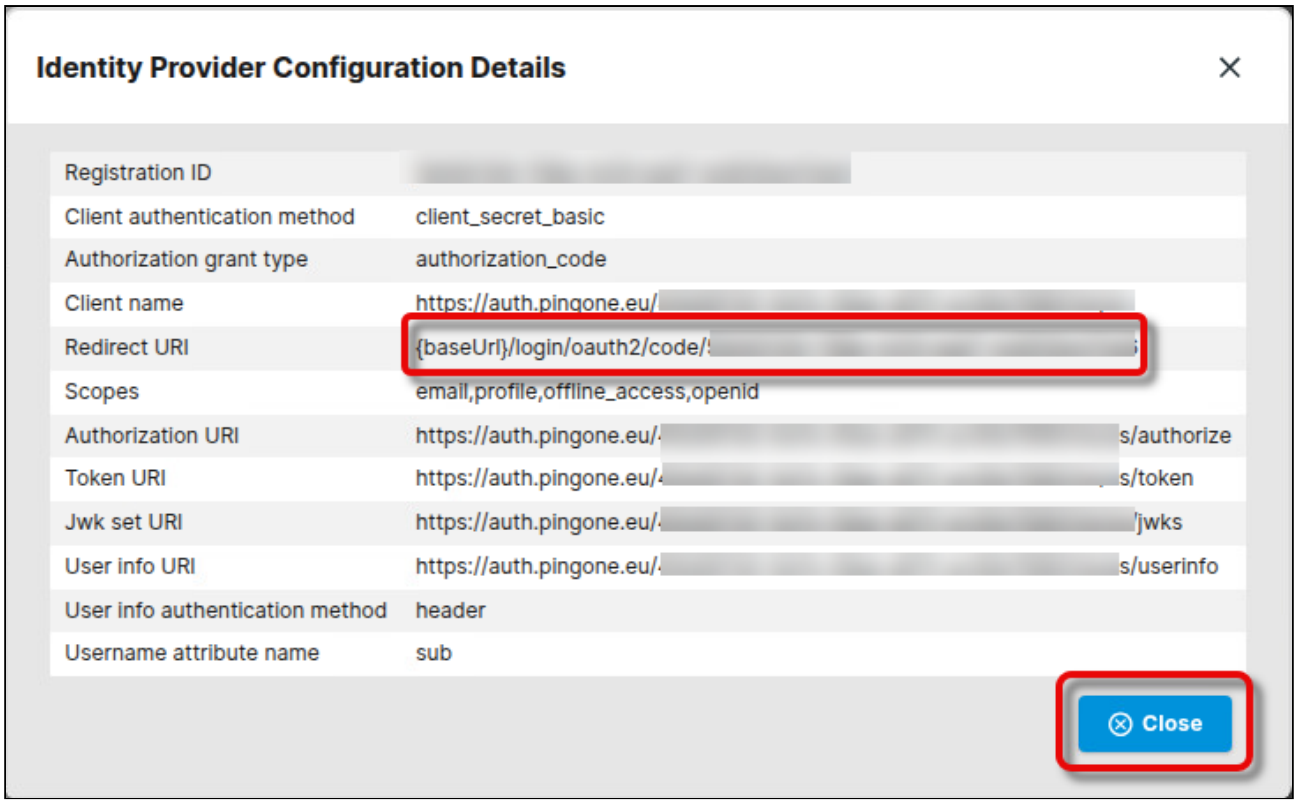
1. Open the UMS Web App, go to **User Management**, and click .



2. Enter the following data from the application you have created in Okta and click **Discover**.
    - **Display name**: The name of your application
    - **Issuer URI**: The issuer URI of your authentication server
    - **Client ID**: The client ID for your application
    - **Client secret**: The secret you have created for your application

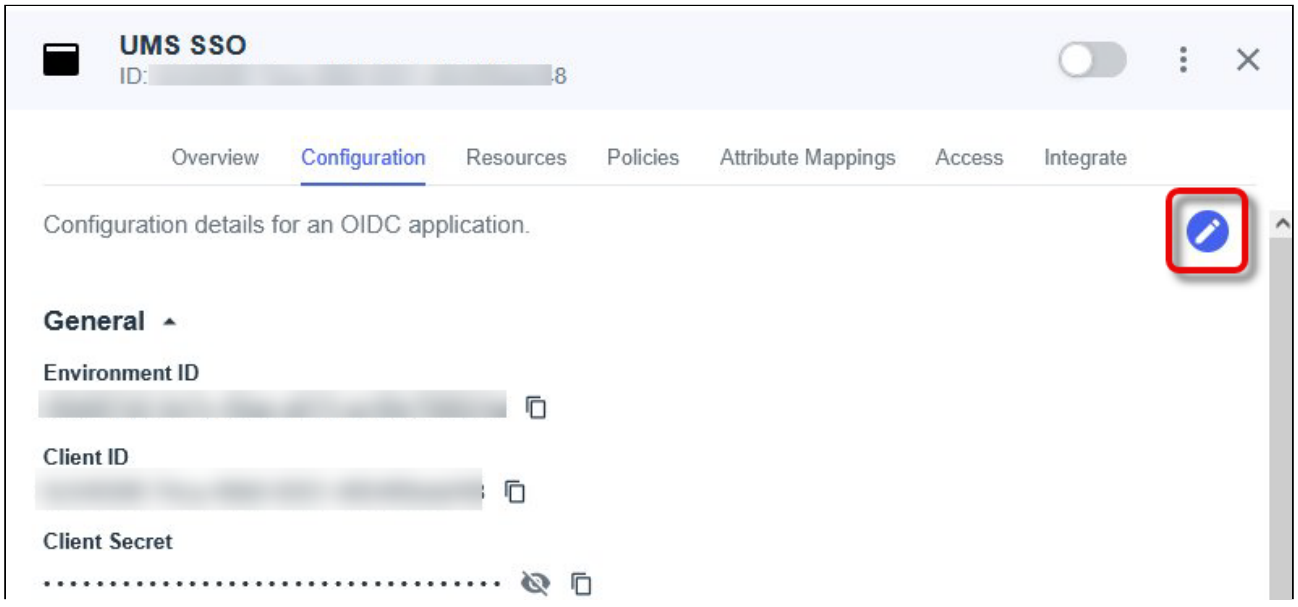


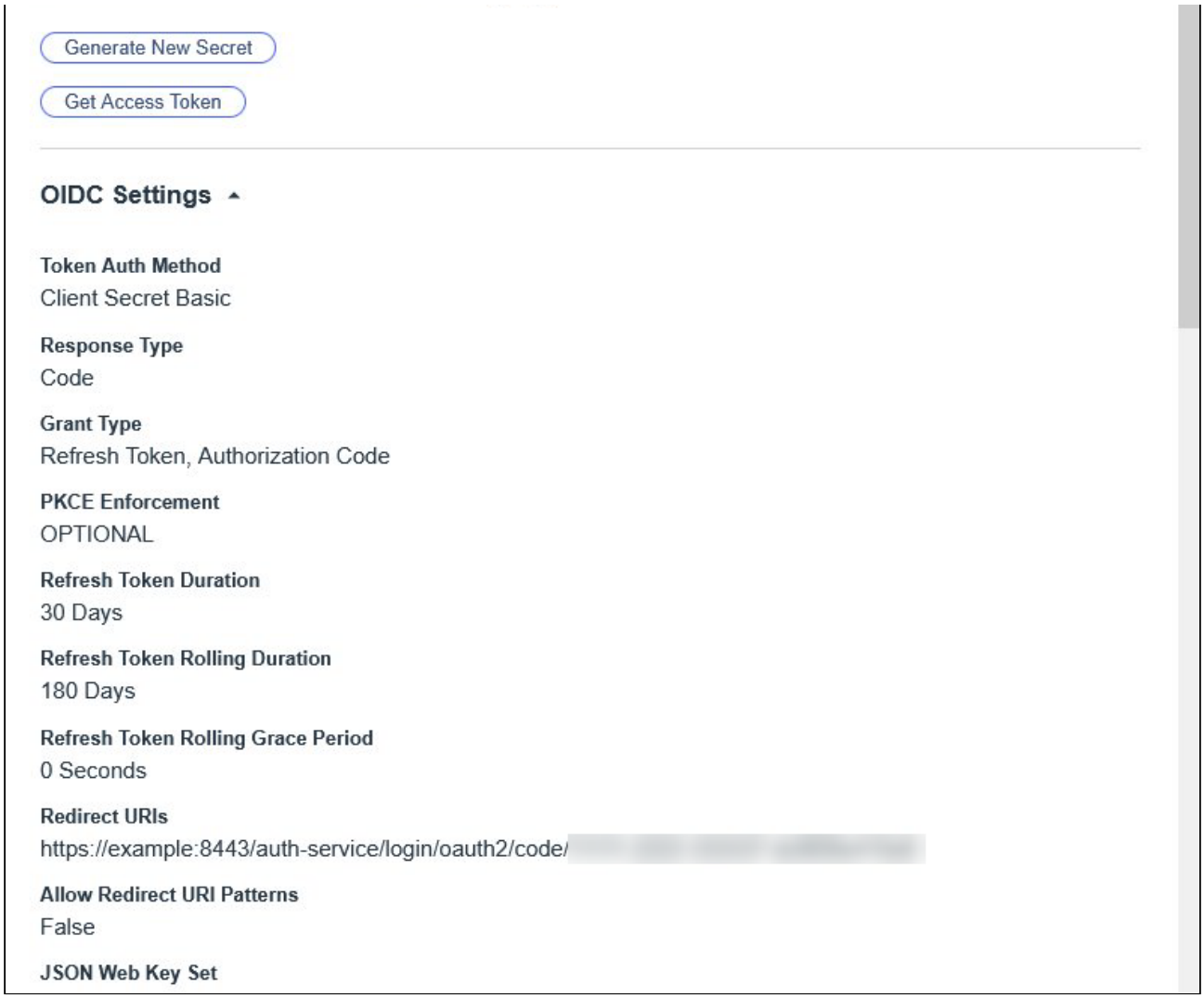
3. In the **Identify Provider Configuration Details** window, copy the **Redirect URI** and close the window.



Configuring the Redirect URL of the UMS in PingIdentity

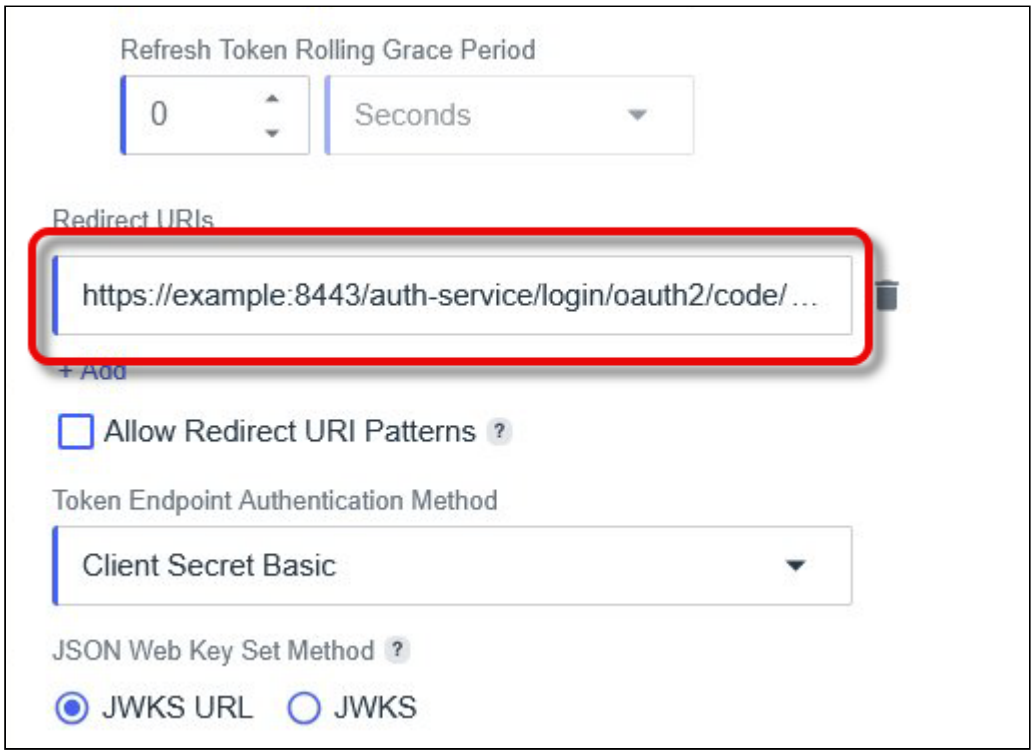
1. In the PingIdentity portal, open the tab **Configuration** and click to edit.



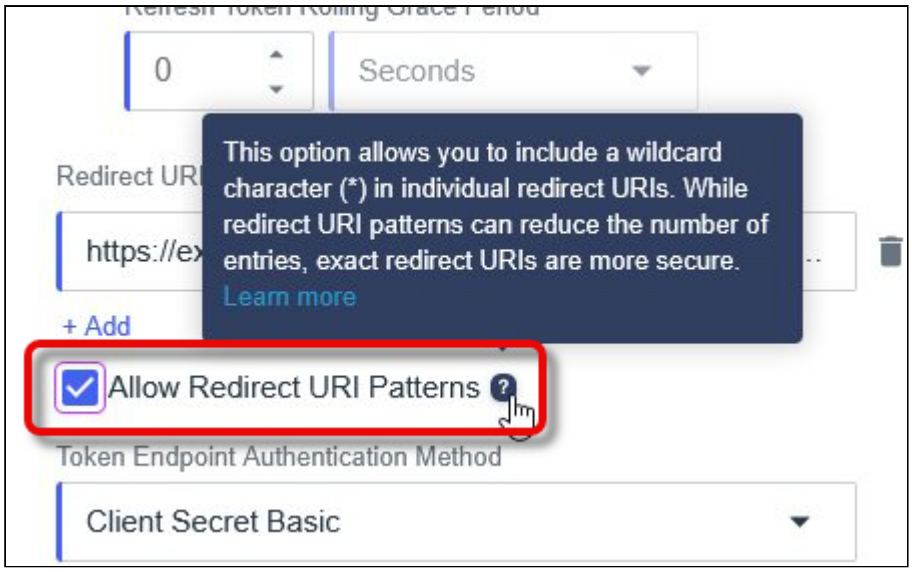


2. Add all URIs that can be used for login, according to the following patterns:
    - IP address of the UMS Server: `https://<IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://123.123.123.123:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
    - FQDN of the UMS Server: `https://<FQDN>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums.example.com:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`

- Short name of the UMS Server: `https://<SHORT NAME>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://myums:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
- Local IP address: `https://<LOCAL IP ADDRESS>:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://127.0.0.1:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`
- "localhost" (used when the **Server** field in the login dialog of the UMS Console is empty): `https://localhost:8443/auth-service/login/oauth2/code/<REGISTRATION ID>` - example: `https://localhost:8443/auth-service/login/oauth2/code/ik45379f-ea33-413c-ed06-649f52d1a64d`



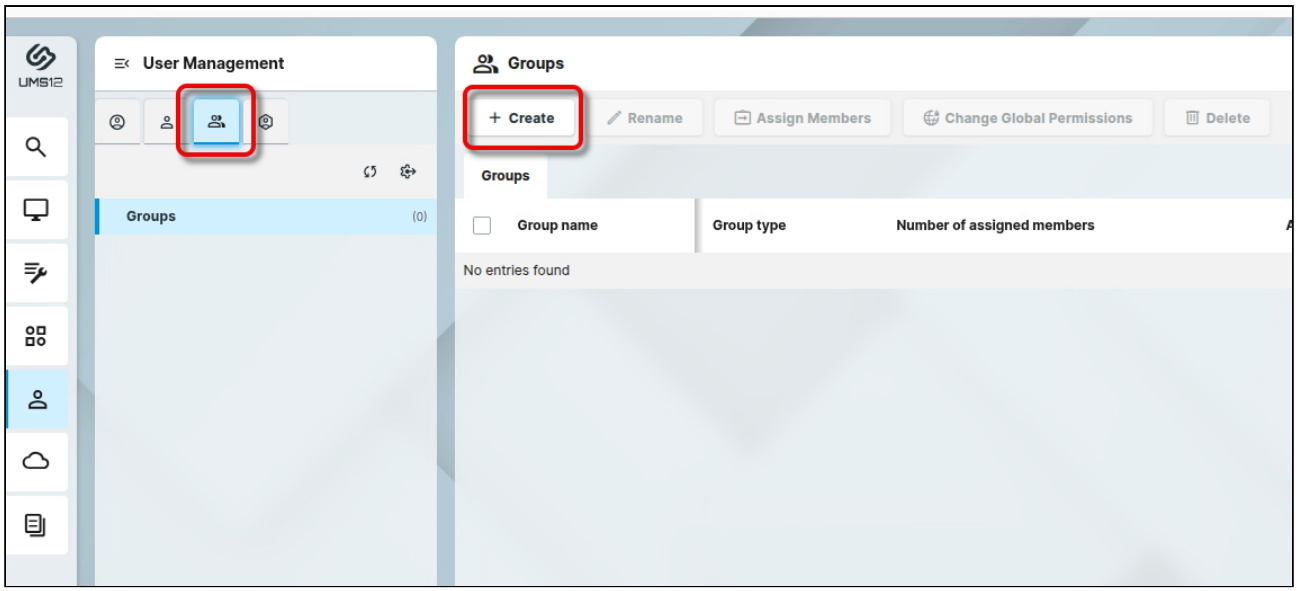
If you allow **Redirect URI patterns**, you can add wildcards (e.g., for subdomains or registration ID)



3. Open the tab **Overview** and enable the application.

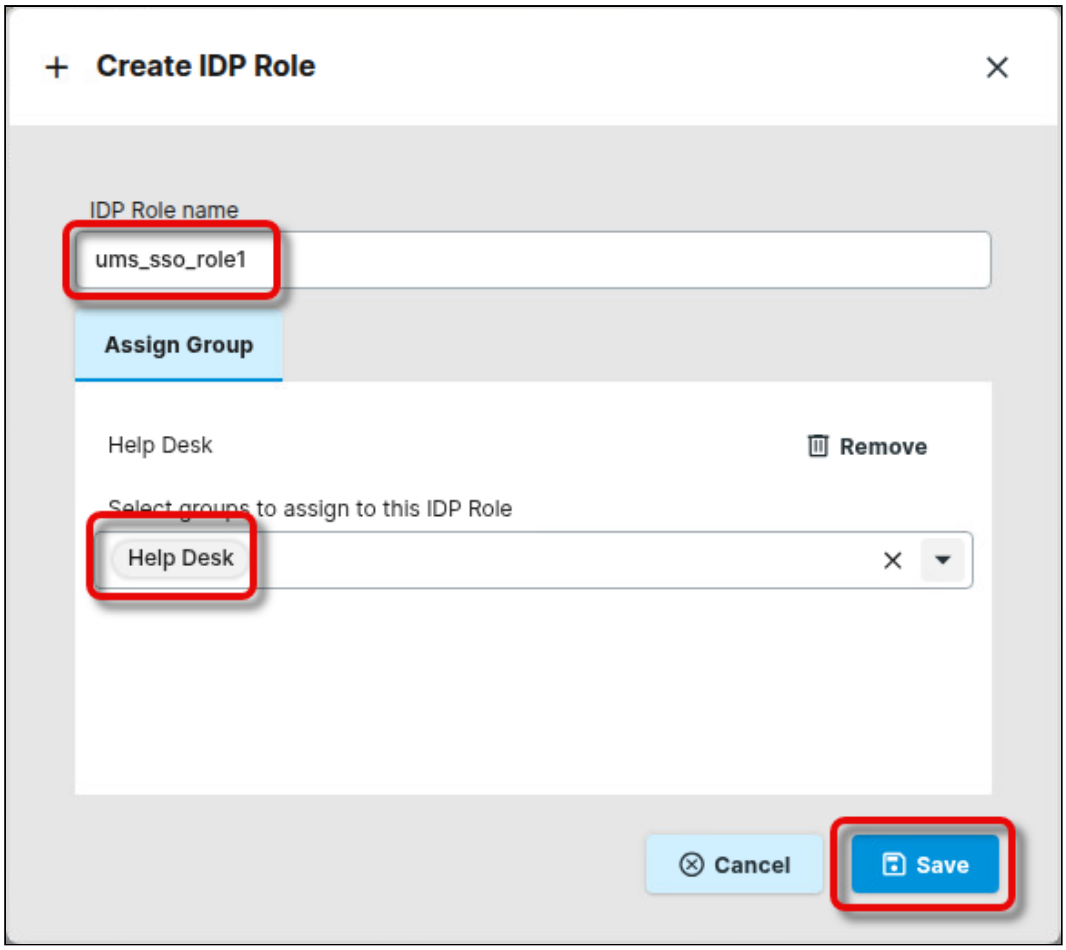
Mapping the Roles in PingIdentity to UMS Groups

1. Open the UMS Web App, go to **User Management**, select , and click **+ Create**.



2. Edit the settings as follows:

- **IDP Role name**: The name of the group you have configured in PingIdentity. Please note that this value is case-sensitive.
- **Assign Group**: The UMS group you want to map to the app role


Create IDP Role
IDP Role name
ums_sso_role1
Assign Group
Help Desk
Remove
Select groups to assign to this IDP Role
Help Desk
Cancel
Save

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 (see page 1407).

Update Instructions

- How to Update the IGEL UMS under Linux (see page 206)
- Updating the IGEL UMS under Windows (see page 211)

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.

If you have IGEL Cloud Gateways (ICGs) in use and perform a UMS update from version 12.04 or lower to 12.05 or higher, you must restart all existing ICGs after the update installation is completed. For more on how to restart the ICG, see IGEL Cloud Gateway - Managing an ICG Connection in the IGEL UMS[46] and Controlling the ICG Daemon[47] .

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.

Update Preparations

Before the installation, check that your hardware and software fulfill the installation requirements (see page 10). See also Devices Supported by IGEL Universal Management Suite (see page 255).

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 1050) and Creating a Backup of the IGEL UMS (see page 1051).

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.

46. https://kb.igel.com/en/universal-management-suite/current/igel-cloud-gateway-managing-an-icg-connection-in-t
47. https://kb.igel.com/en/igel-cloud-gateway/current/controlling-the-icg-daemon

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.

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.

WebDAV downloads (e.g. files, firmware updates) are stored in the `ums_filetransfer` directory. Custom file transfer directories are not supported.

How to Update the IGEL UMS under Linux

Before starting the update of the IGEL Universal Management Suite (UMS), read IGEL UMS Update (see page 204).

⚠ Create a backup of the database (see page 1050) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

⚠

Oracle

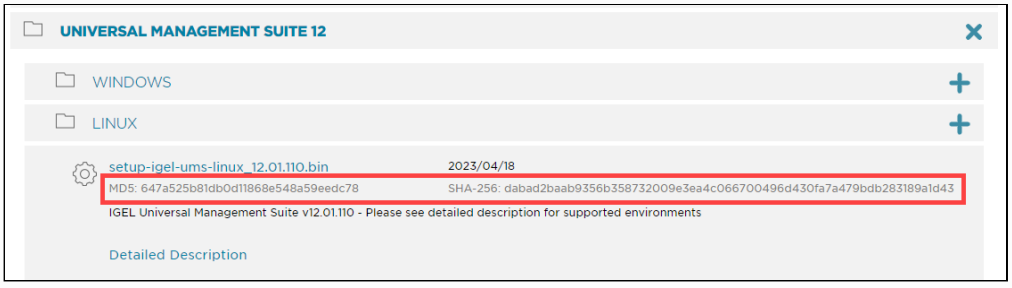
For the proper operation of the UMS with Oracle databases, particularly for the upgrade process, the number of `open_cursors` for the database must be adjusted. `open_cursors` is a system setting.

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[48].

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



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

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.

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.

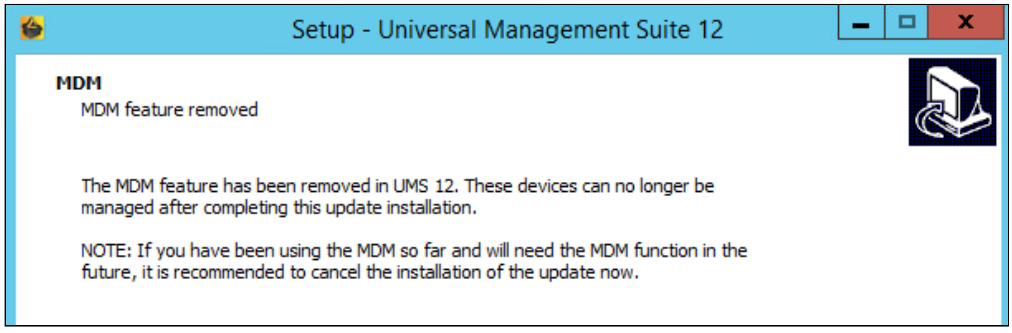
5. Start the installation procedure by pressing **Enter**.

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

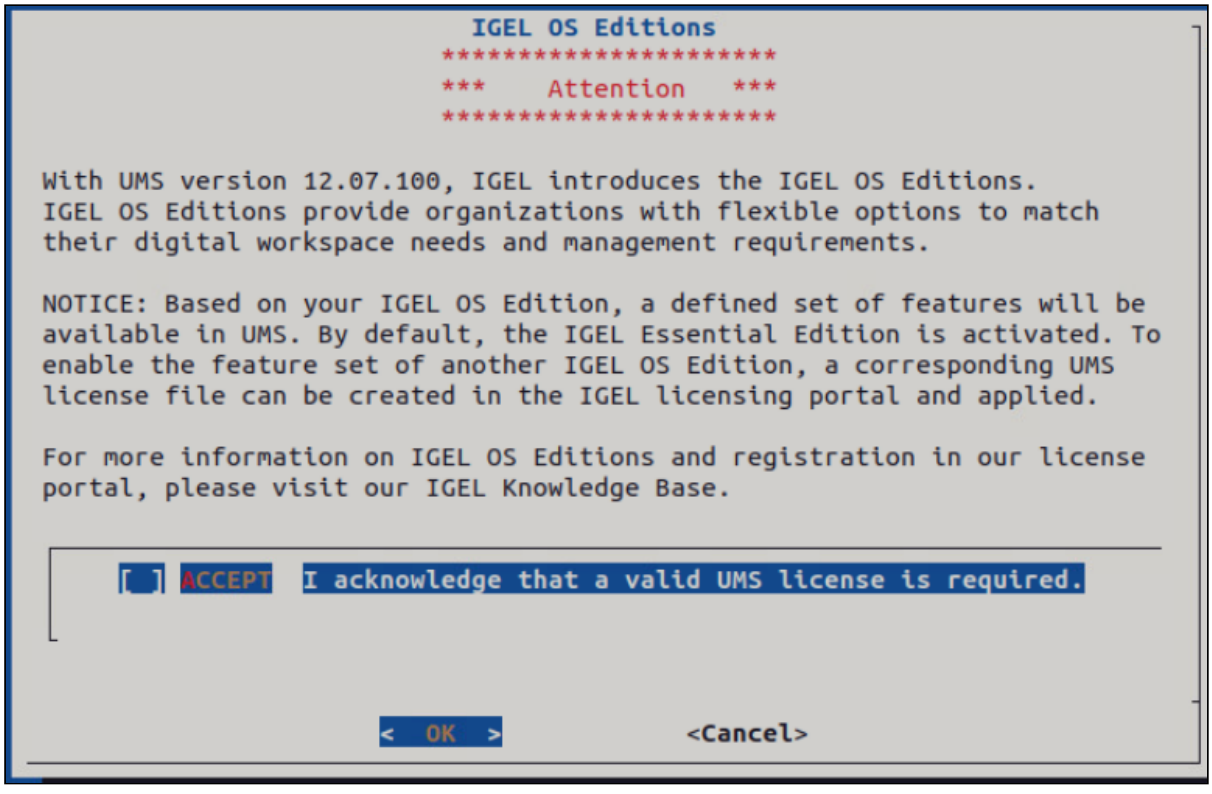


- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server 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
   - **HA net**: High Availability configuration
   - **Client only**: UMS Console only

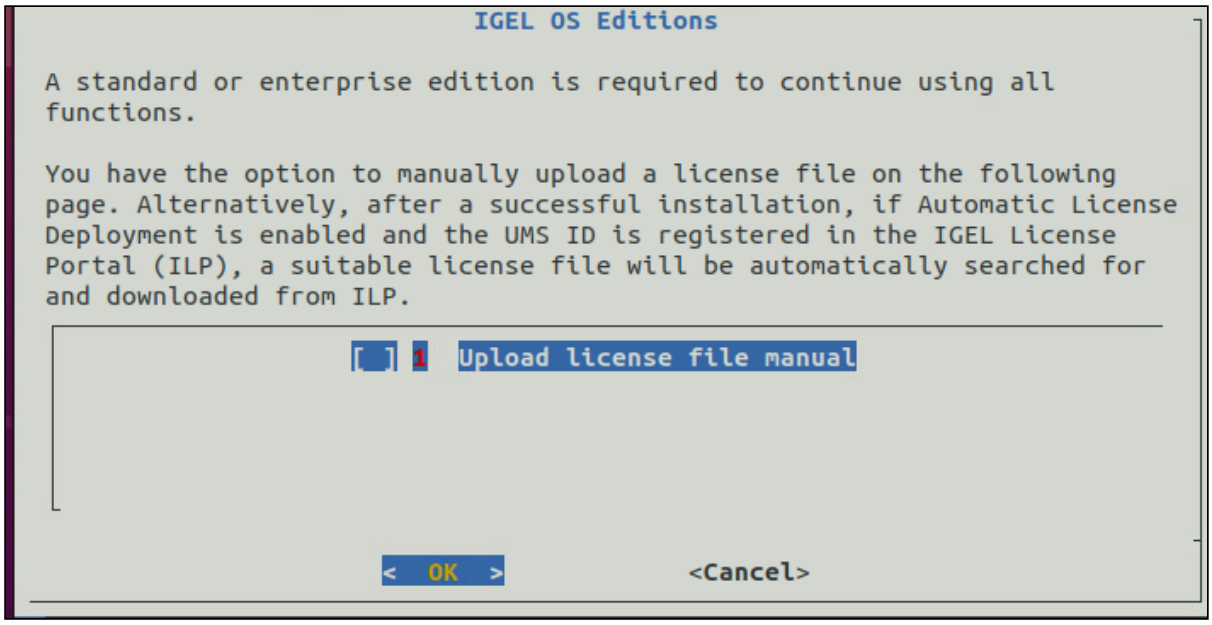
   For more information on installation types, see IGEL UMS Installation[49].
9. Choose whether the **UMS Web App** (see page 1154) should be installed. See Important Information for the IGEL UMS Web App (see page 1155).

10. Read and confirm the information regarding IGEL OS Editions[50] and UMS Licenses[51] .



49. https://kb.igel.com/en/universal-management-suite/current/igel-ums-installation
50. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions
51. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums

11. Select whether you want to manually upload the license file during installation or automatically.



⚠ The license will only be downloaded automatically if Automatic License Deployment (ALD) is activated. For the manual upload, you can download the license file from the IGEL License Portal (ILP). For details and further licensing options, see How to License the IGEL UMS[52].

12. If manual license upload is selected, upload the license file.

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

14. 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 Troubleshooting Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux (see page 404).

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

52. https://kb.igel.com/en/igel-subscription-and-more/current/how-to-license-the-igel-ums

16. 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.

17. 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`.

18. Connect the UMS Console to the UMS Server with the help of the existing access data. See Connecting the UMS Console to the IGEL UMS Server[53].

> **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 Universal Management Suite Network Configuration (see page 265)) 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 (see page 256).

53. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server

Updating the IGEL UMS under Windows

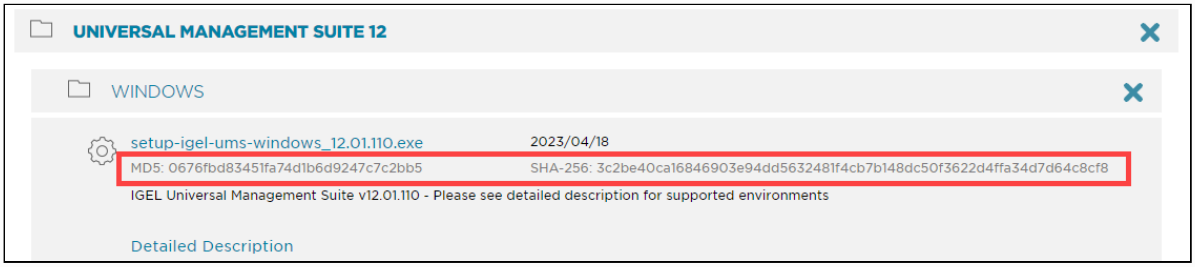
Before starting the update of IGEL Universal Management Suite (UMS), read IGEL UMS Update (see page 204).

⚠ Create a backup of the database (see page 1050) 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[54].

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**.

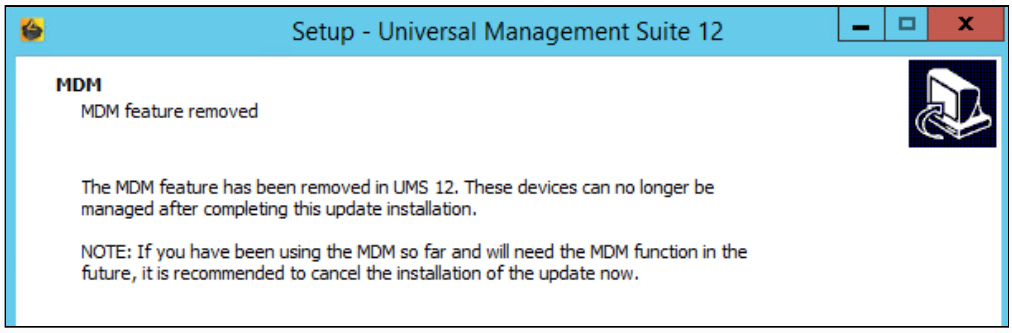
4. Read the **Information** regarding the installation process and click **Next**.

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**

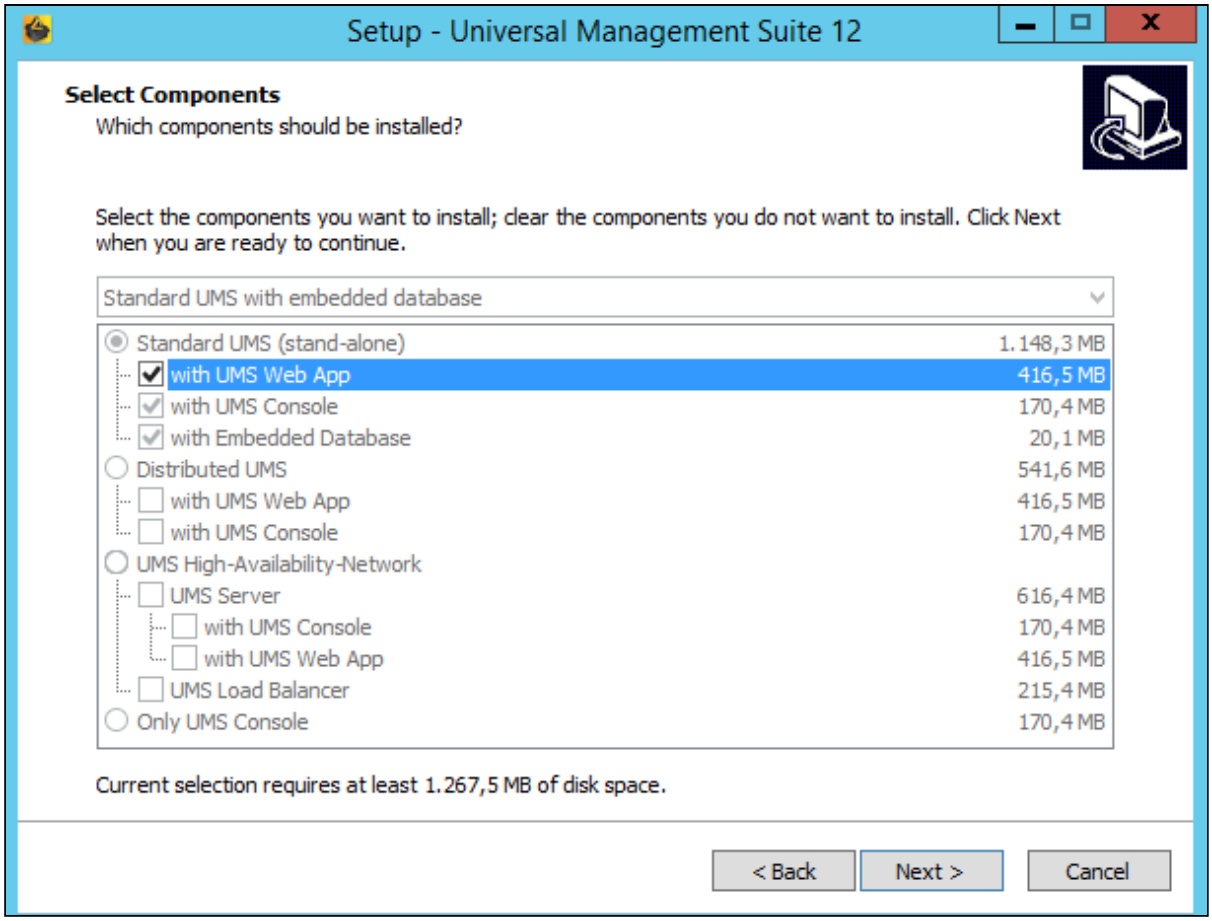
- As of UMS 12, the MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:

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



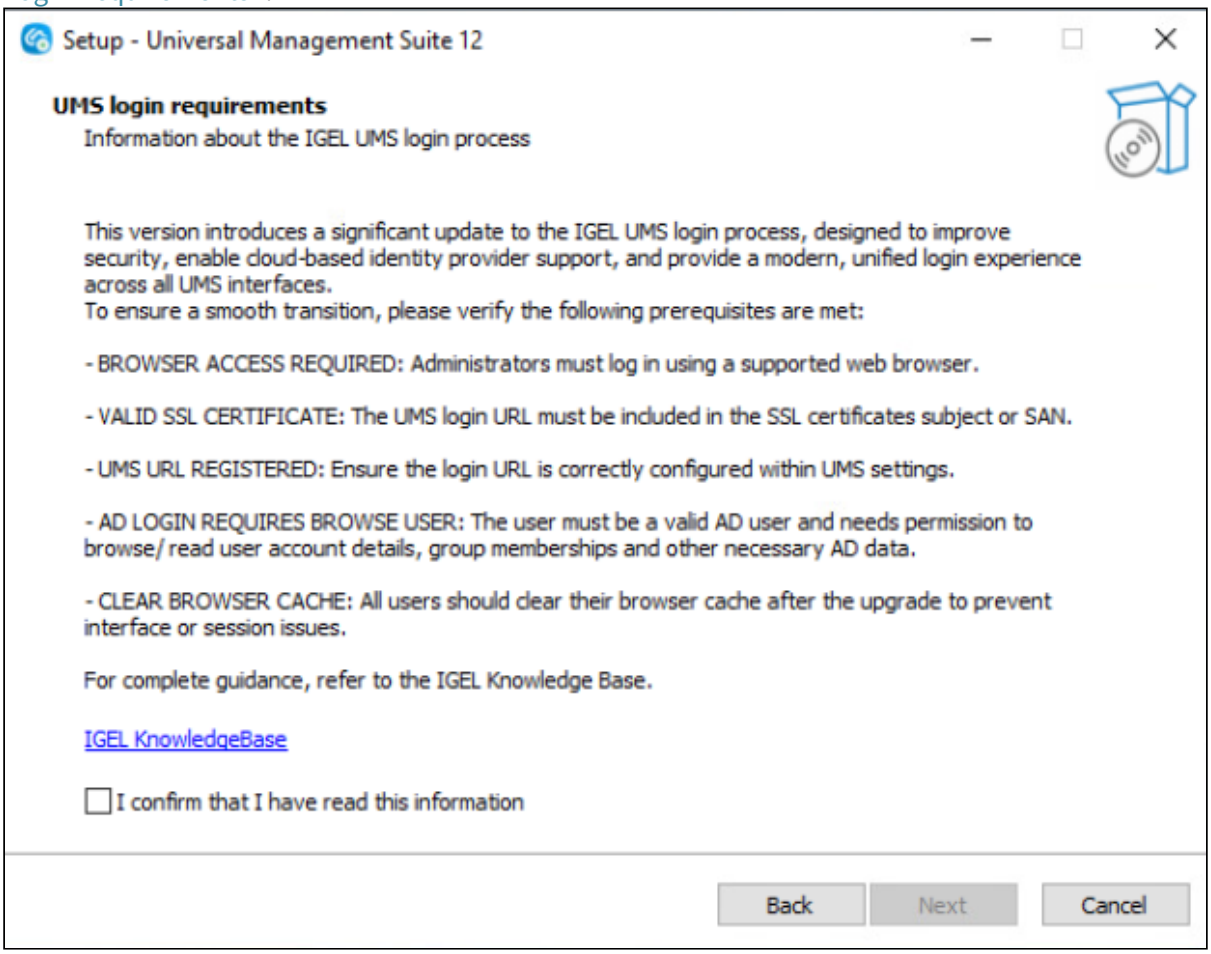
- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server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



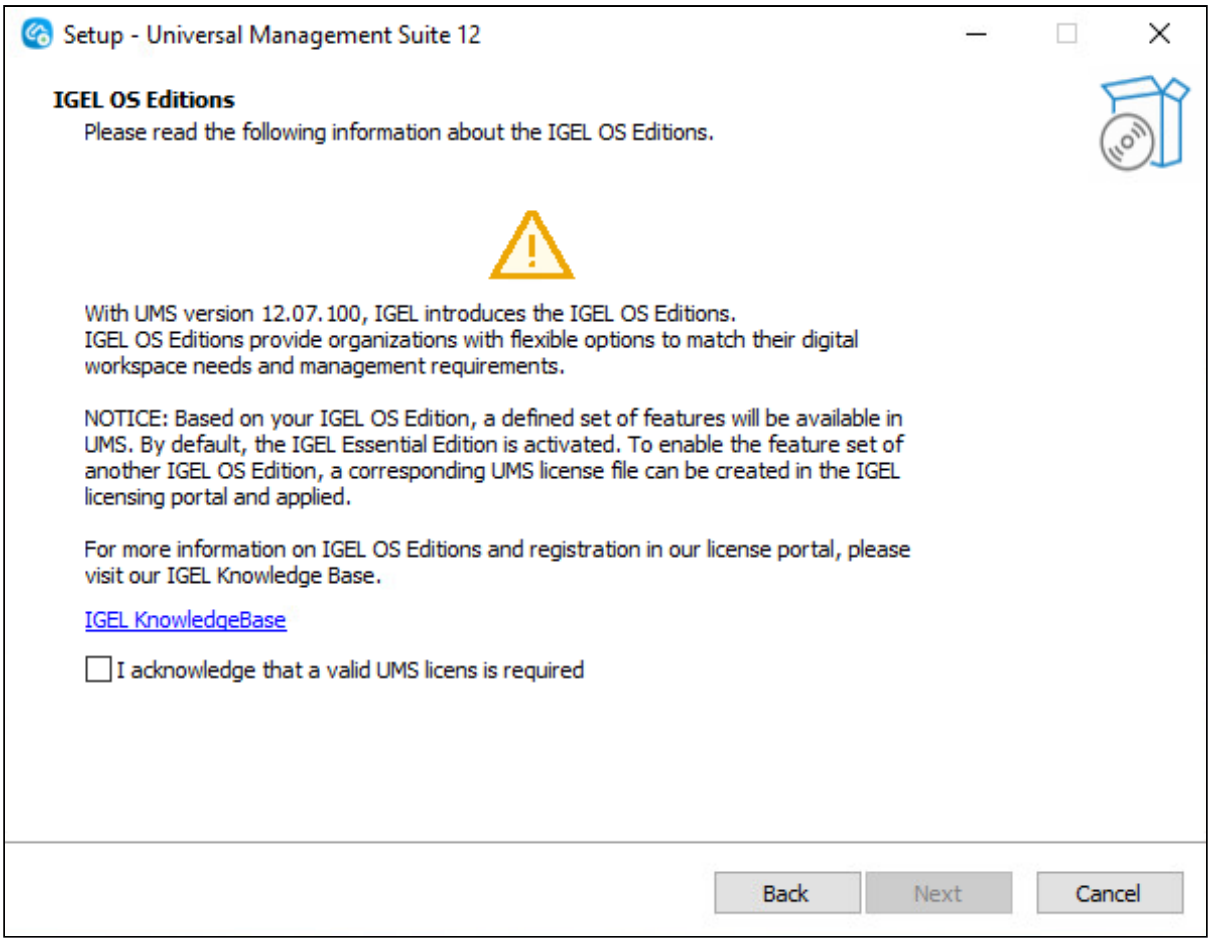
For information on the UMS installation types, see IGEL UMS Installation (see page 13).
For information on the UMS components, see Overview of the IGEL UMS (see page 661).

7. Read and confirm information about the **UMS login requirements**. For more information, see UMS Login Requirements[55].

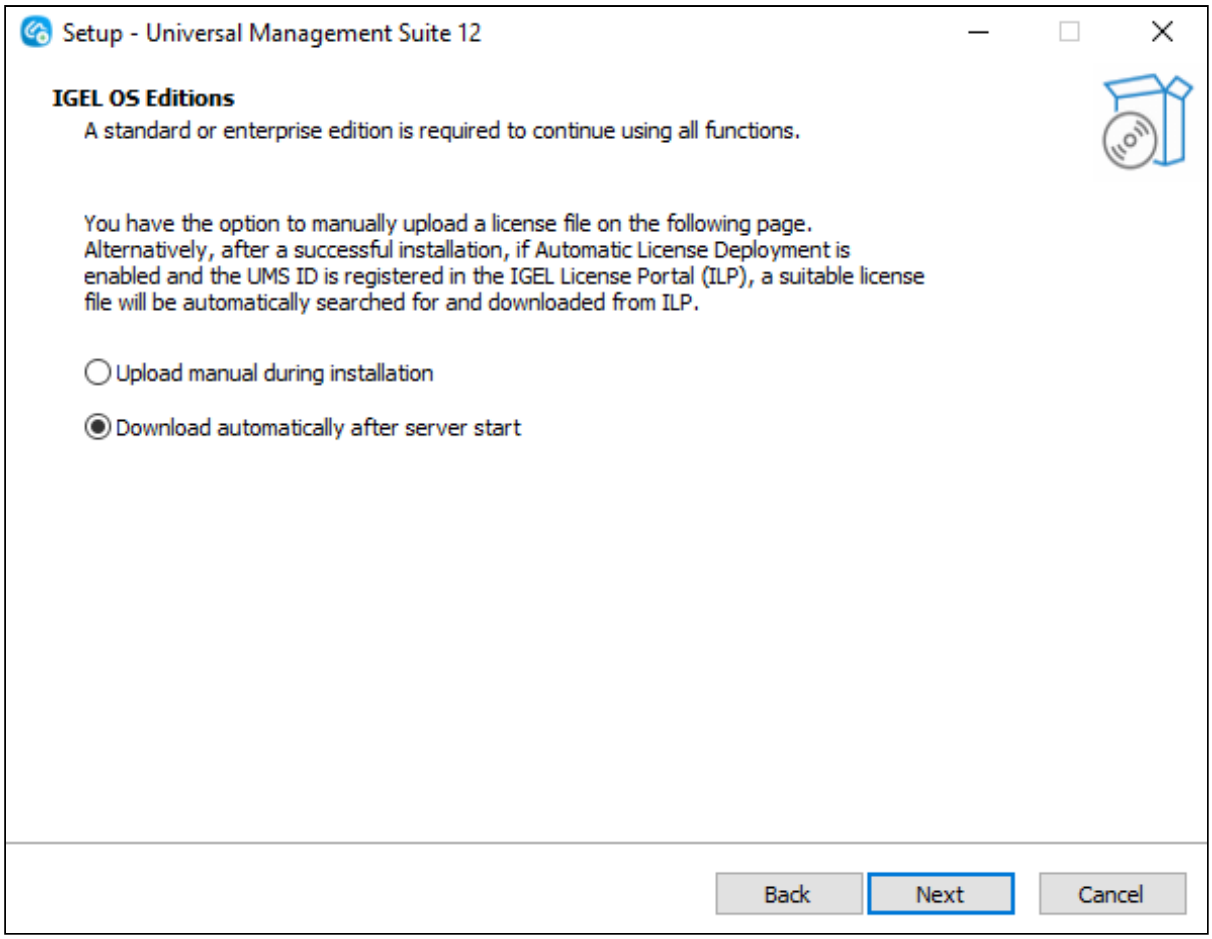


8. Read and confirm the information regarding IGEL OS Editions and UMS Licenses[56] and click **Next**.

55. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements
56. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums



9. Select whether you want to manually upload the license file during installation or automatically.



The license will only be downloaded automatically if Automatic License Deployment (ALD) is activated. For the manual upload, you can download the license file from the IGEL License Portal (ILP). For details and further licensing options, see How to License the IGEL UMS[57].

10. If manual license upload is selected, upload the license file.

11. Read the **Memory (RAM) requirements** and click **Next** if your system fulfills them.

12. 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:

57. https://kb.igel.com/en/igel-subscription-and-more/current/how-to-license-the-igel-ums

- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
  SSL can be terminated at the reverse proxy / external load balancer (see IGEL Universal Management Suite Network Configuration (see page 265)) 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 (see page 256).

13. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and UMS Administrator (see page 1037) on the desktop.

14. 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.

15. Close the program once the installation is complete by clicking on **Finish**.

16. Start the UMS Console.

17. Connect the UMS Console to the UMS Server with the help of the existing access data. See Connecting the UMS Console to the IGEL UMS Server[58].

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

If you use an external database, check the database connection in the **UMS Administrator** (see page 1037) > **Datasource** (see page 1061).

58. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server

Post-Installation Configuration of the IGEL UMS Server

This article covers the tasks that should be performed after installing a new IGEL Universal Management Suite (UMS) server.

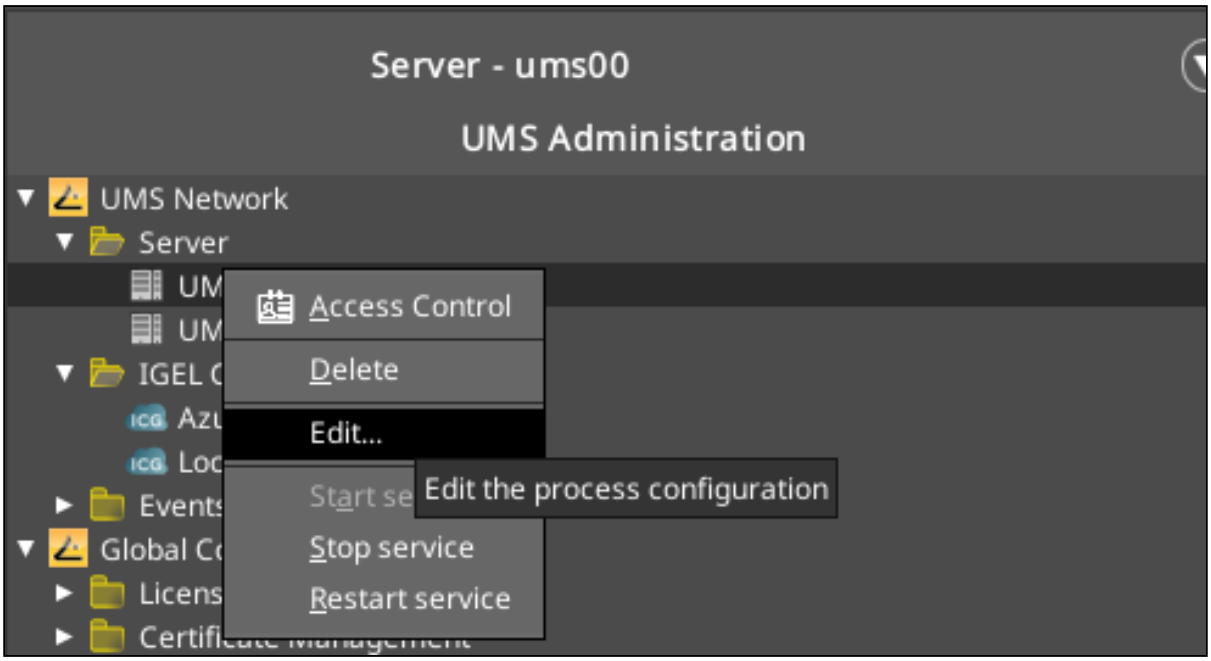
Set the Correct Public Address and Public Web Port for each UMS server

It is required to set the public address for your UMS servers in order for OS 12 devices to properly locate them. Thee steps below will need to be performed once for each UMS server in your cluster:

1. Open the **IGEL UMS Console**, and go to the **UMS Administration** section.

2. Navigate to **UMS Network > Server**.

3. Right-click the UMS server you wish to adjust, and select the **Edit...** button.

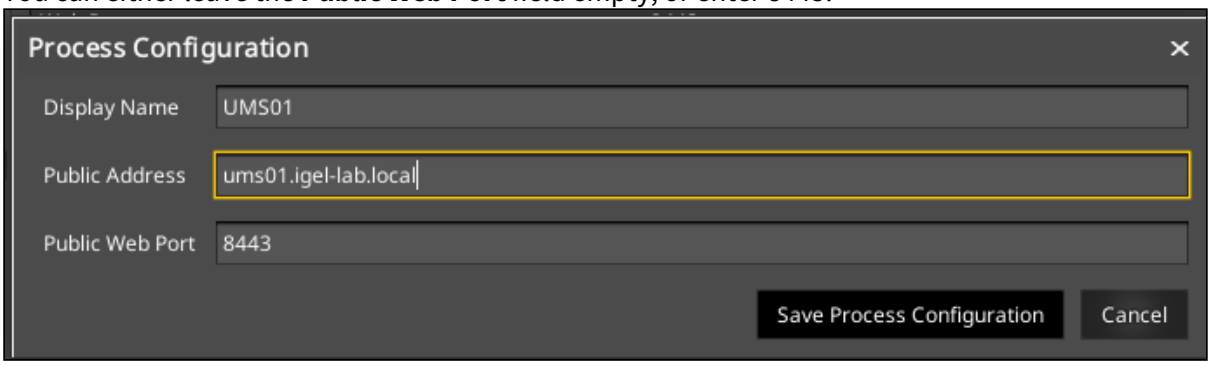


4. Enter a unique identifier into the **Display Name** field (this does not impact functionality, just how it appears in the UMS Console).

5. Enter the Fully Qualified Domain Name (FQDN) of your UMS server that the IGEL will connect to on from your local network into the **Public Address** field.

As a best practice, only use lowercase letters in the FQDN / **Public Address**. Using capital letters might lead to authentication issues or connection issues from OS 12 devices due to case sensitivity.

6. You can either leave the **Public Web Port** field empty, or enter 8443.

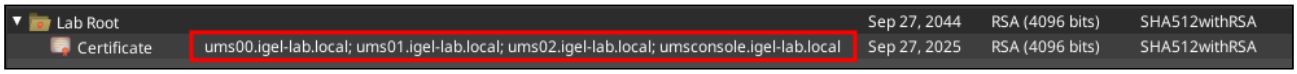


If you are using a reverse proxy, load balancer, or individual VIPs with Unique Addresses for your UMS servers that go through that proxy, you will need to make sure you have the correct port defined for that proxy, and that the **Public Address** is the URL of said VIP or reverse proxy server.

Validate UMS and ICG Certificates

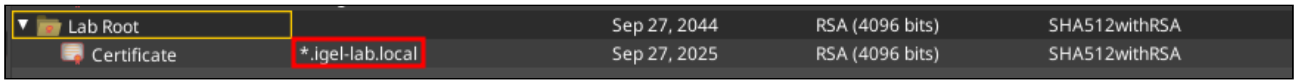
In order for the new Unified Protocol and UMS Web App to function properly, your UMS Web Certificates must contain either a list of all your UMS server public addresses in the SAN, or use a wild card certificate.

List of UMS Server SANs

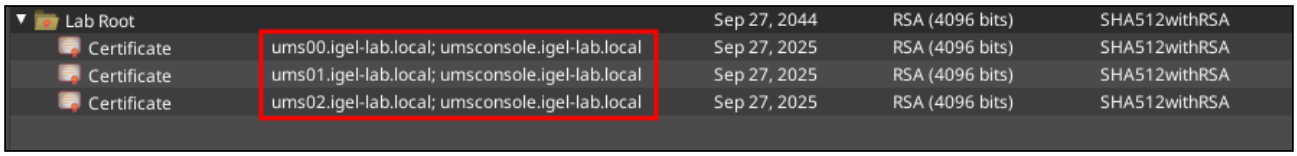


If you use any other URL's to access the UMS Web App, or an external load balancer/reverse proxy address, these will need to be added as well (i.e umsconsole.igel-lab.local).

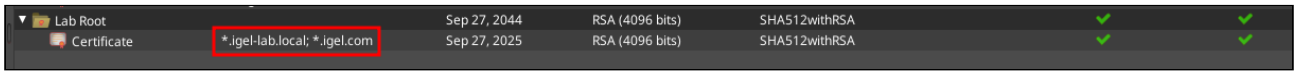
Wild Card Certificate



Individual Certificates



If you have multiple domains, it is possible to generate certificates from UMS containing multiple domain names.

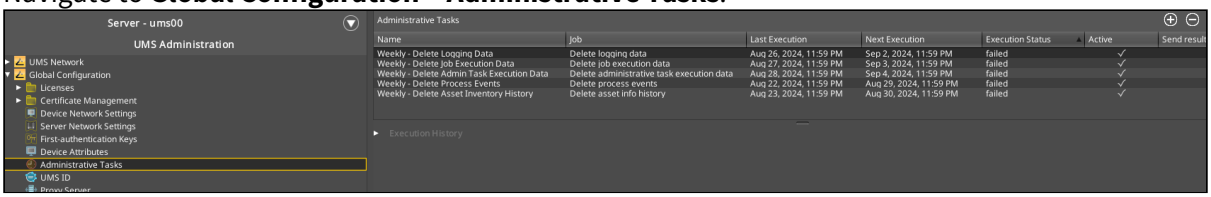


Configure Recommended Administrative Tasks

There are some recommended Administrative Tasks that should be deployed in all IGEL UMS environments:

1. Open the **IGEL UMS Console**, and go to the **UMS Administration** section.

2. Navigate to **Global Configuration > Administrative Tasks**.



3. Configure the Administrative Tasks described below.

Backup

The first item that should be configured is a daily backup of the UMS database. If you are using the embedded database, this can be configured via a UMS Administrative Task. If you are using an external database, then please refer to the documentation of that database to configure this.

Backup Best Practices
Backups should be run daily, and schedule 2 hours before any other UMS Administrative Tasks are scheduled to run.
Backups should be stored on separate storage than where your UMS server is running, or in accordance to your companies backup policies.
For the embedded database, it is recommended to mount external storage which you can then point to as your backup location. Please refer to your operating systems instructions on how to create a local mount for remote storage.

Cleanup Device Licenses

Configure it to run weekly or monthly at least 2 hours after the backup task. This task removes unused / expired licenses from the UMS database.

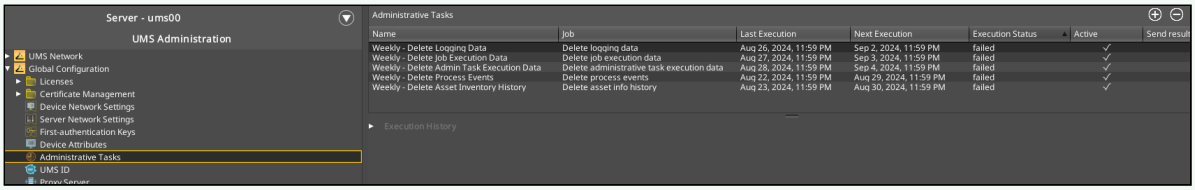
Additional Administrative Tasks

The following tasks should be configured to run one night a week, staggered by 24 hours, and scheduled to run 2 hours after your backup task or process is started:

- Delete Logging Data
- Delete Job Execution Data
- Delete Administrative Task Execution Data
- Delete Process Events
- Delete Asset Info History

Example
Backup is scheduled to run nightly at 09:00 PM

- Monday @ 11:59pm - Delete logging data
- Tuesday @ 11:59pm - Delete Job Execution Data
- Wednesday @ 11:59pm - Delete Administrative Task Execution Data
- Thursday @ 11:59pm - Delete Process Events
- Friday @ 11:59pm - Delete Asset Info History



Optional: Additional Administrative Tasks

Remove Unused Firmware (OS 11 Only)

If you have IGEL OS 11 in your environment, you can schedule a task to remove old update files and database entries.

Further tasks for performance optimization and maintenance are described in:

- IGEL UMS Maintenance Tasks (see page 221)
- Performance Optimizations in IGEL UMS (see page 225)

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

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

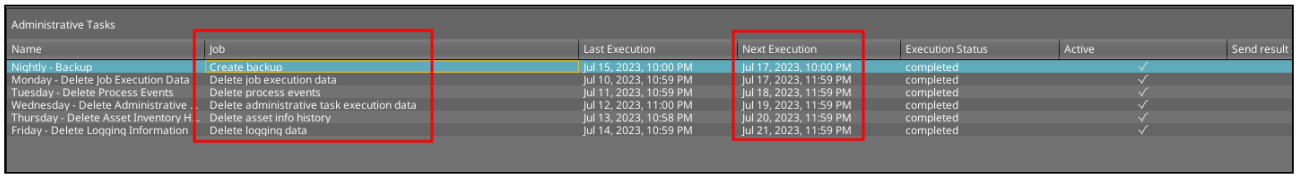
It is recommended to schedule each task on a different day, two hours after any backups are made. This will give each task enough time to complete and allow for a rollback via the backup if data is removed that is required.

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 932).
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 938).

	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 935).
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 history. For details, see Delete Asset Information History[59].
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 928).

Example:



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.

59. https://kb.igel.com/en/universal-management-suite/current/delete-asset-information-history-as-an-administrat

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 223).

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:

- **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 1068), 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. For details, see Create Data Backup as Administrative Task in the IGEL UMS[60]. If you want to create a backup manually, see Creating a Backup of the IGEL UMS[61].	• 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

60. https://kb.igel.com/en/universal-management-suite/current/create-data-backup-as-administrative-task-in-the-i
61. https://kb.igel.com/en/universal-management-suite/current/creating-a-backup-of-the-igel-ums

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[62] 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. See also IGEL UMS Maintenance Tasks[63].
- **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:**

62. https://kb.igel.com/en/universal-management-suite/current/administrative-tasks-configure-scheduled-actions-f
63. https://kb.igel.com/en/universal-management-suite/current/igel-ums-maintenance-tasks

    - 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[64] and How to Configure Java Heap Size for the UMS Console[65].
    - 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[66].
- **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.

64. https://kb.igel.com/en/universal-management-suite/current/how-to-configure-java-heap-size-for-the-ums-server
65. https://kb.igel.com/en/universal-management-suite/current/how-to-configure-java-heap-size-for-the-ums-consol
66. https://kb.igel.com/en/universal-management-suite/current/how-to-configure-java-heap-size-for-the-ums-server

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

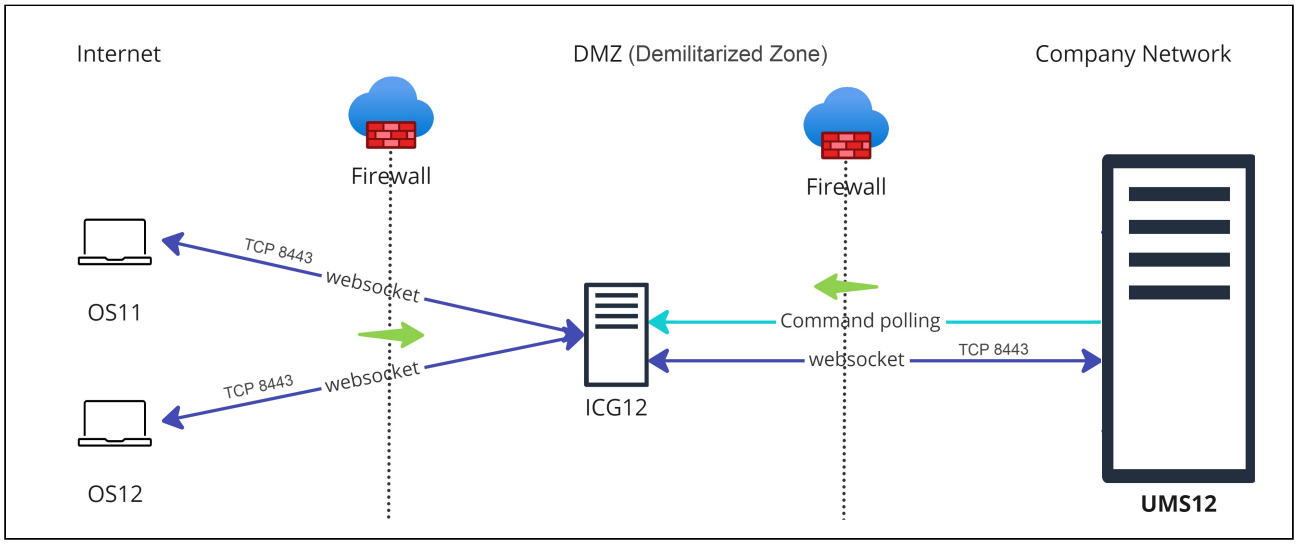
With the launch of IGEL Universal Management Suite (UMS) 12, the Unified Protocol used for all communication between the UMS and IGEL OS 12 devices was introduced, see Overview of the IGEL UMS (see page 661). The Unified Protocol is a secure protocol that uses TCP 8443, see IGEL UMS Communication Ports (see page 256). 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.

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 (see page 356). 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.



Legend to the image:

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

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

Advantages

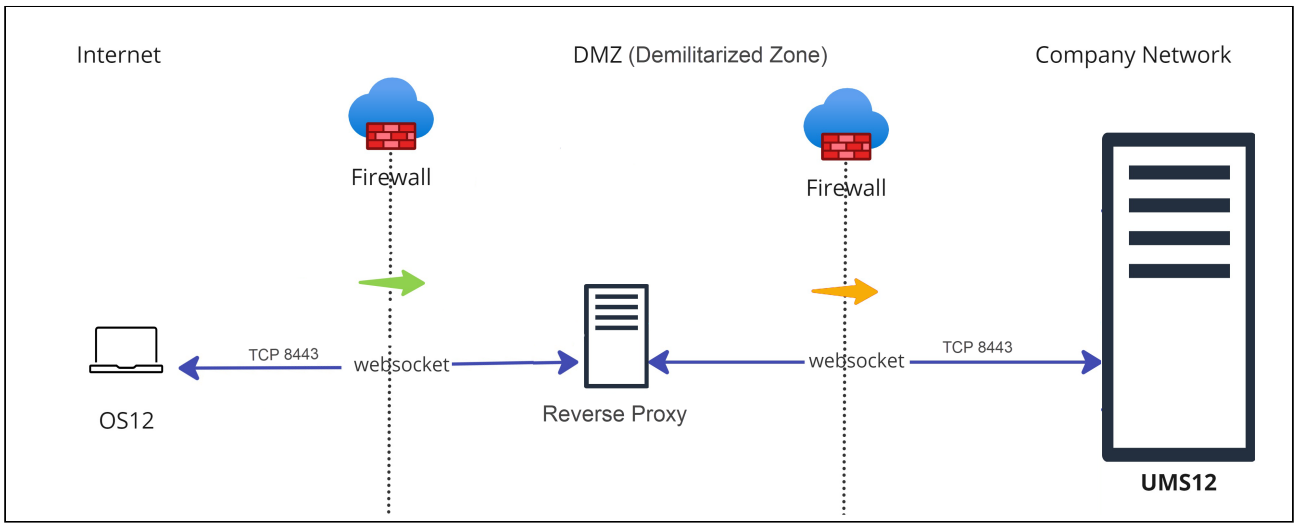
- Suitable for mixed environments when you manage both IGEL OS 12 and IGEL OS 11 devices.
- No inbound connection from the device to the UMS.
- Only the ICG is exposed to the Internet. Thus, if compromised, the UMS is NOT compromised at the same time.
- Simple and lightweight, which minimizes the attack 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 (see page 1342).
- 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.



Legend to the image:

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

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

Technical Details

- Reverse proxy with SSL offloading is possible as of UMS 12.02. See NGINX Example Configuration for Reverse Proxy in IGEL OS with SSL Offloading[67].

- 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 909).

> 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 (see page 265).

- 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 (see page 1342).
- Adds an extra layer of security (depending on the configuration)

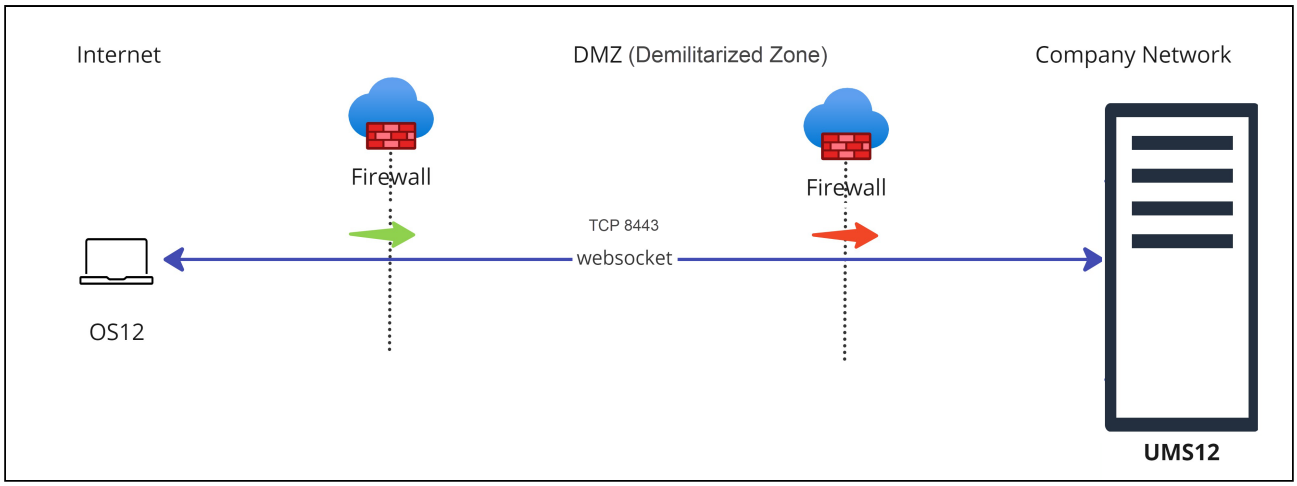
Disadvantages

- 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.
- If the reverse proxy gets compromised, it can provide access to the UMS. In comparison, if the ICG gets compromised, the UMS is NOT compromised at the same time.

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 (see page 359).

67. https://kb.igel.com/en/universal-management-suite/current/nginx-example-configuration-for-as-reverse-proxy-i



Legend to the image:

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

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

Advantages

- port 8443 (can be changed under **UMS Administrator > Settings > Web server port** (see page 1038)) 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[68] and Onboarding IGEL OS 12 Devices[69].

68. https://kb.igel.com/en/how-to-start-with-igel/current/initial-configuration-of-the-igel-onboarding-servi
69. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices

Installation and Sizing Guidelines for IGEL UMS Environments Managing IGEL OS 11

The contenct was updated to describe IGEL OS 12 environments, see Sizing Guidelines for IGEL UMS 12 and IGEL OS 12 (see page 5) .

If you need information on environments managing IGEL OS 11, reach out to igelcxm@igel.com[70].

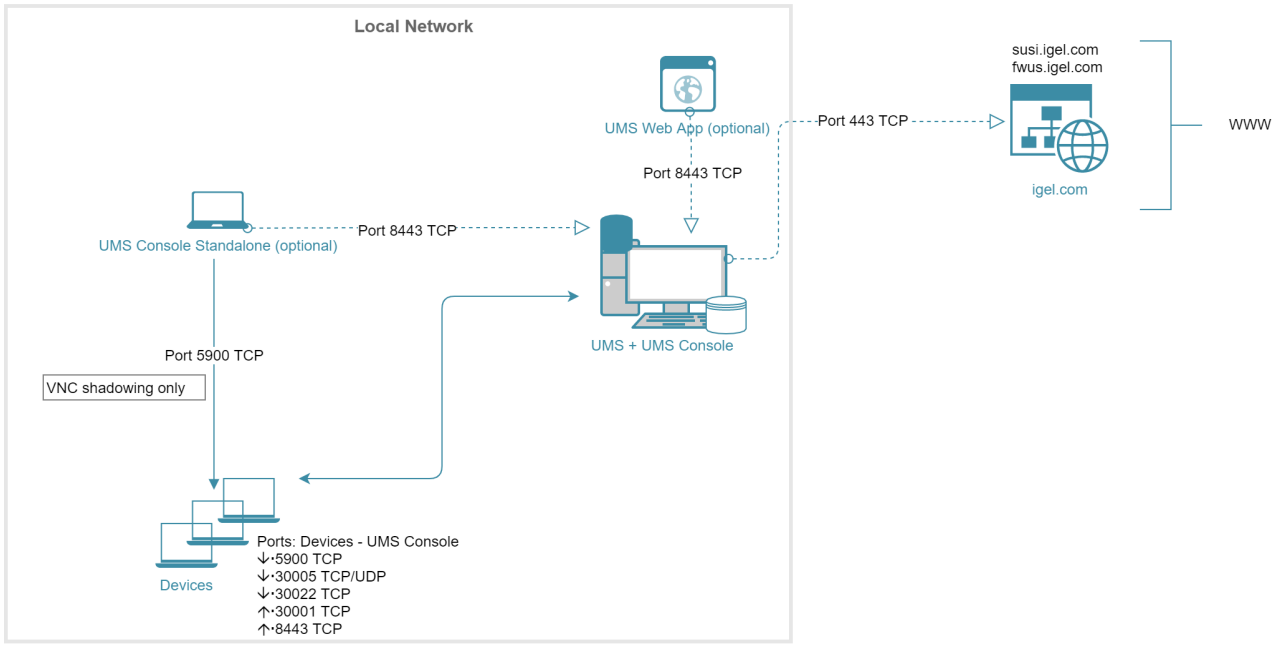
For architecture diagrams of environments managing IGEL OS 11, see:

- Small Environment: UMS S (see page 232)
- Small and Medium Environments: UMS M/S (HA) (see page 233)
- Medium Environment: UMS M (see page 234)
- Large Environment: UMS L (HA) (see page 235)
- Extra Large Environment: UMS XL (HA) (see page 236)

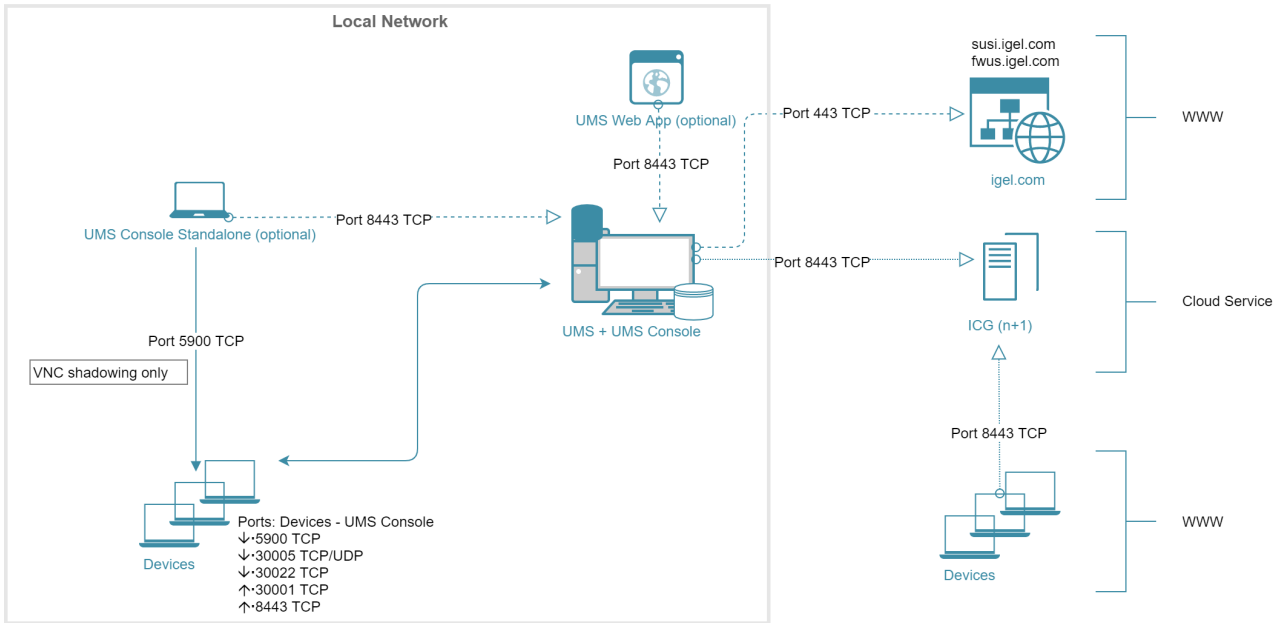
70. mailto:igelcxm@igel.com

Small Environment: UMS S

Architecture: Small Environment

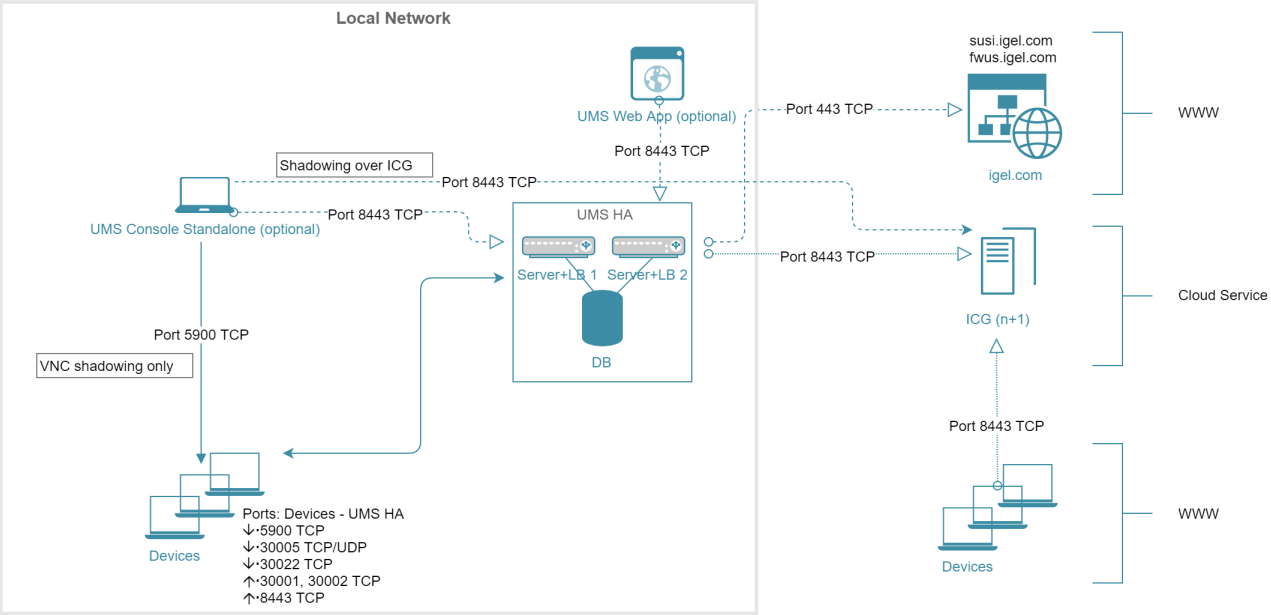


Architecture: Small Environment + ICG in Cloud



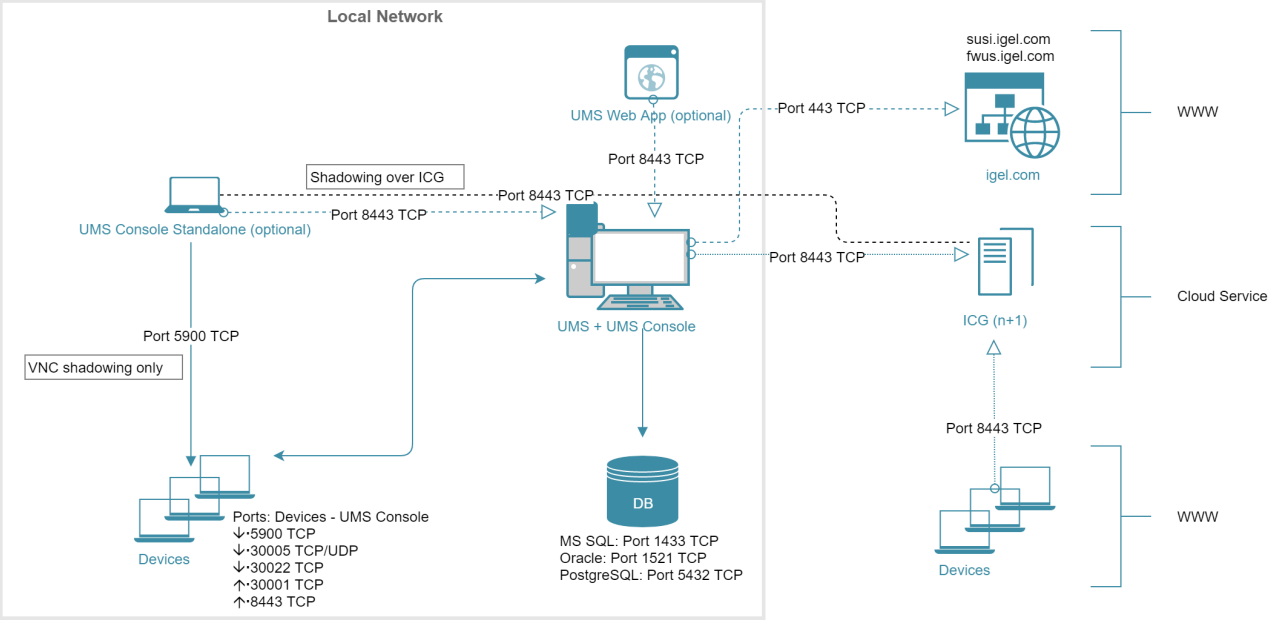
Small and Medium Environments: UMS M/S (HA)

Architecture: Small and Medium Environment (HA) + ICG



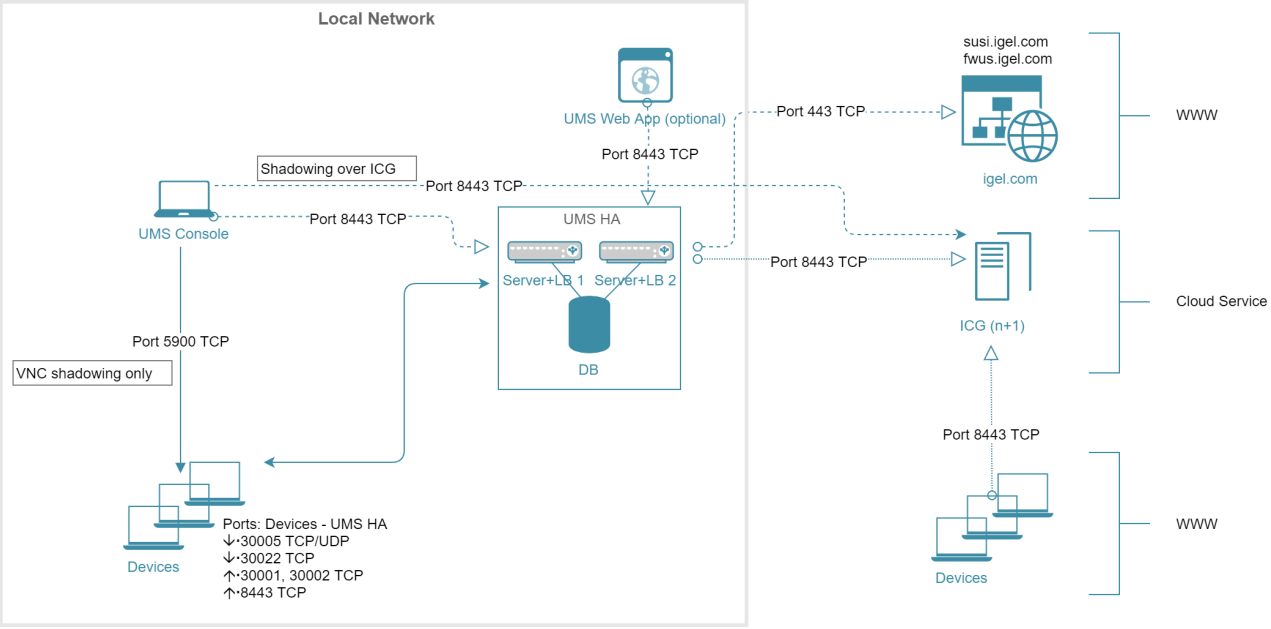
Medium Environment: UMS M

Architecture: Medium Environment + ICG



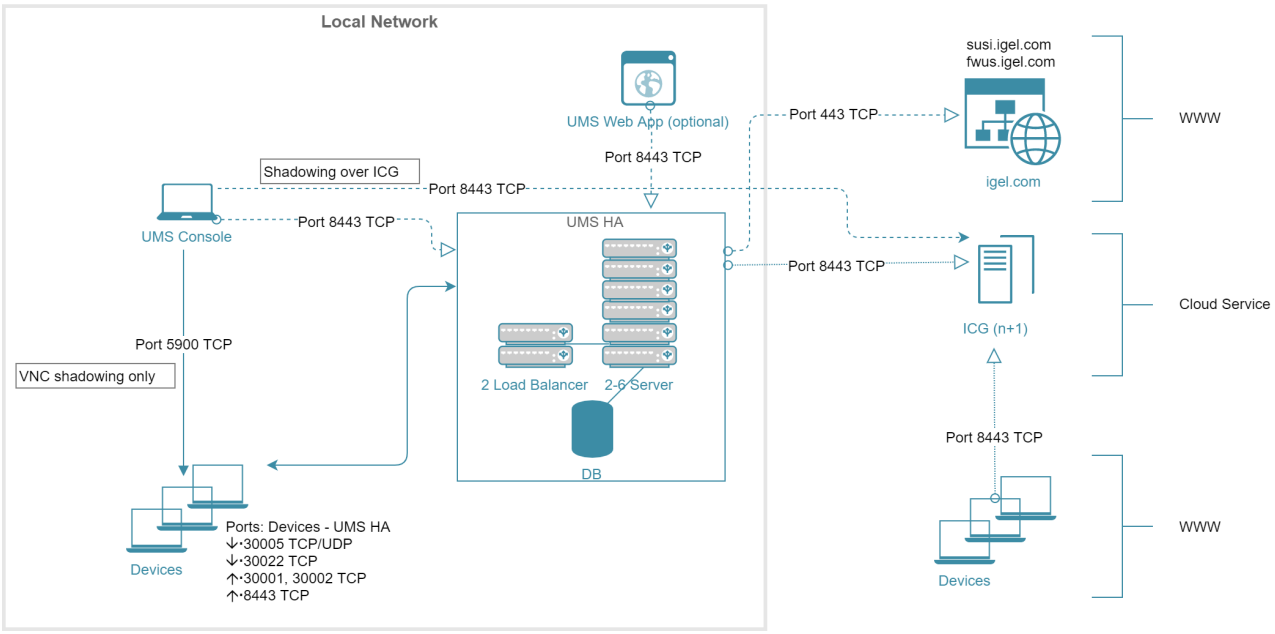
Large Environment: UMS L (HA)

Architecture: Large Environment (HA) + ICG



Extra Large Environment: UMS XL (HA)

Architecture: Extra Large Environment (HA) + ICG



Configuration of an AWS Application Loadbalancer (ALB) for Deploying the IGEL Universal Management Suite (UMS)

This article provides instructions for configuring an AWS Application Load Balancer (ALB) with mTLS support to prepare for installing an IGEL Universal Management Suite (UMS) Server on an Amazon Elastic Compute Cloud (EC2) instance.

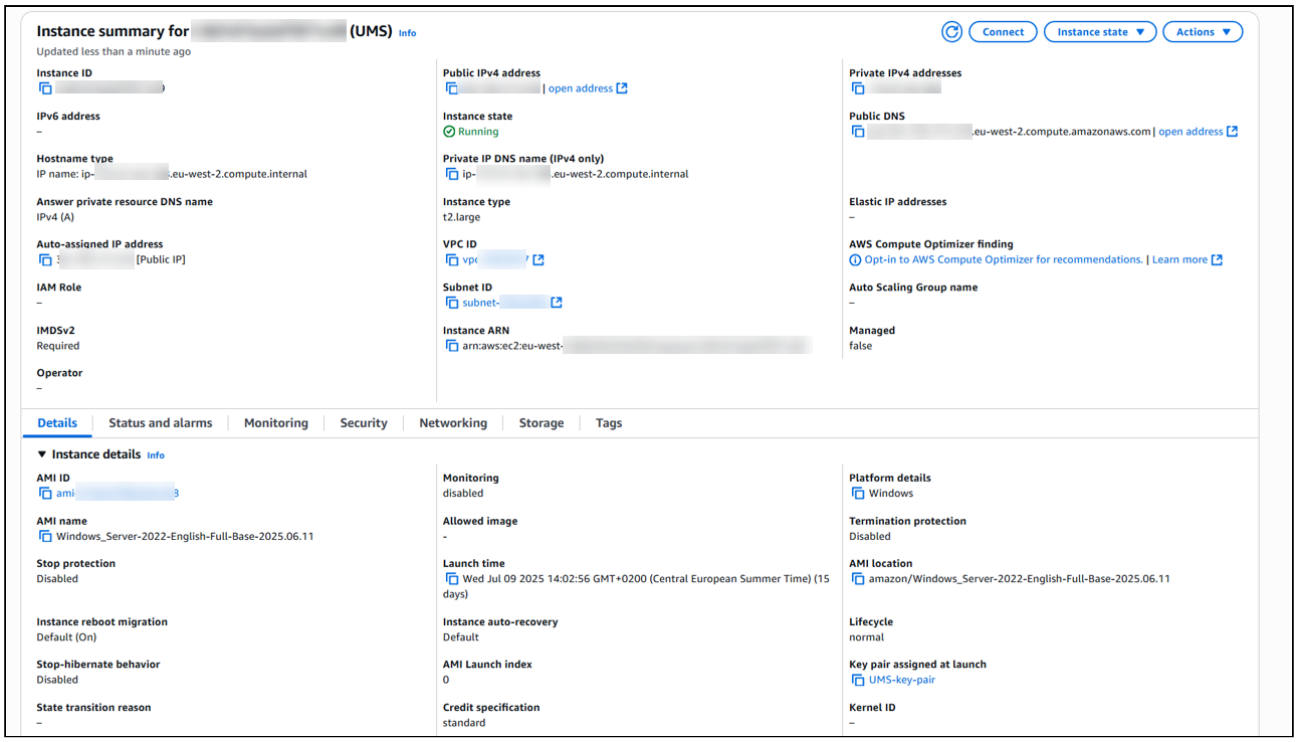
We set up an Application Load Balancer (ALB) in AWS to securely expose the UMS Server application, running on port 8443, with HTTPS and mTLS enabled. The ALB uses a trust store stored in S3 and forwards requests to a registered EC2 instance. To support client certificates forwarded from the ALB, the UMS Server must be configured to support Base64 decoding by setting the `encodingType` to `URL_AWS`.

Component	Value
ALB Type	Application Load Balancer
Scheme	Internet-facing
Listener Port	HTTPS 8443 & 443
Target	EC2 Instance running UMS
mTLS	Enabled (on port 8443)
Trust Store	Client Certificate Chain in S3 bucket
Encoding	`URL_AWS` handled at backend

AWS Configuration

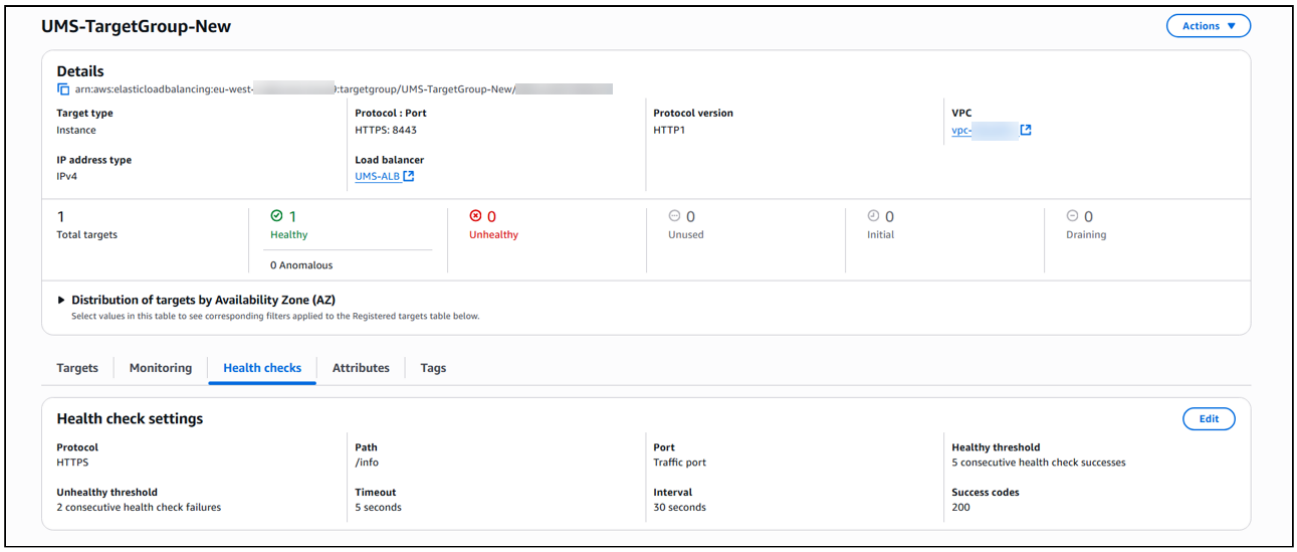
Setting up an EC2 Instance

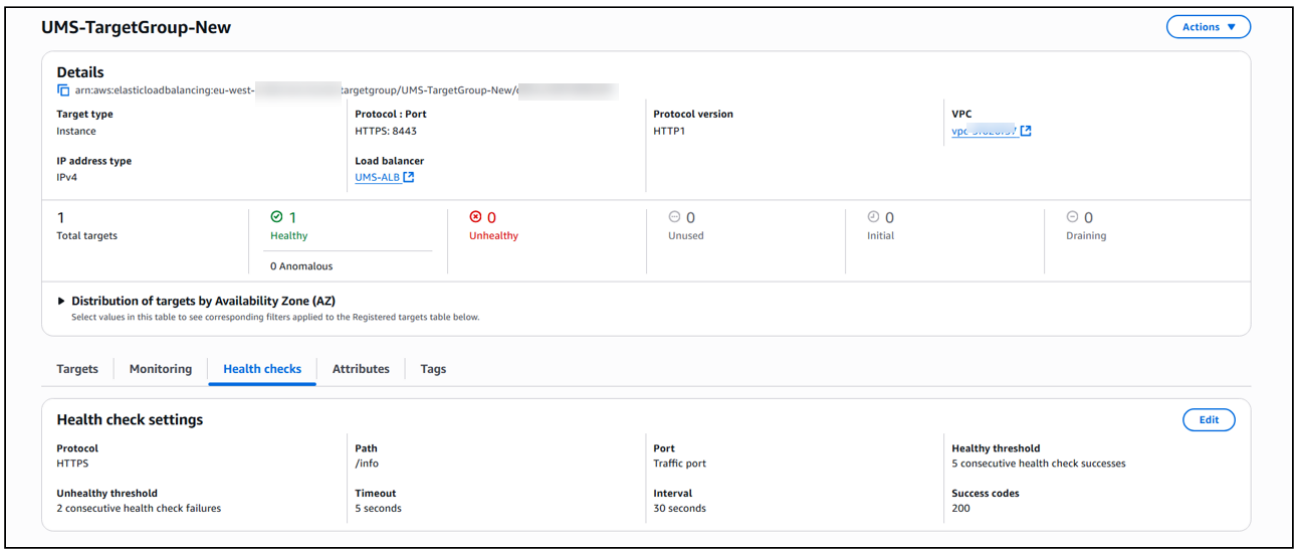
1. Launch a new EC2 instance using the Windows Server 2022 AMI with the following settings:
   - Ensure the instance has a security group allowing HTTPS (8443) inbound traffic from the ALB's security group.
   - Assign a static public IP address



Creating a Target Group

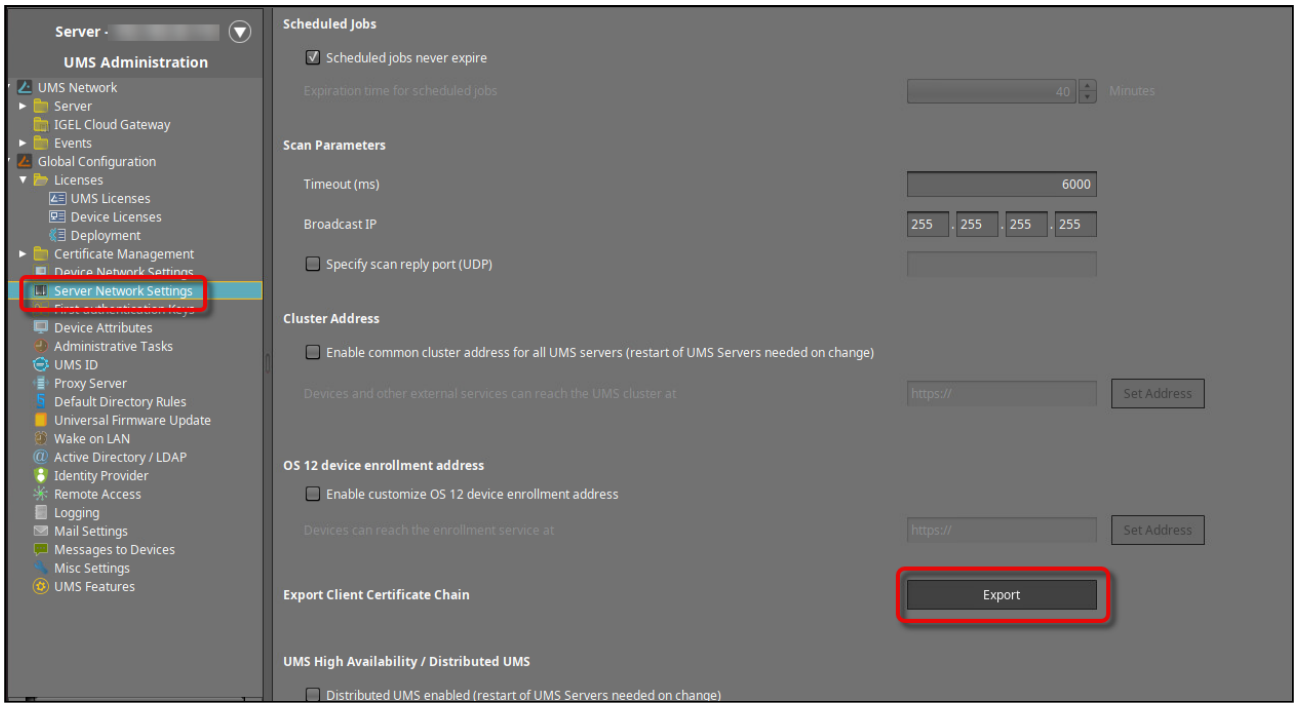
1. Create a new Target Group, e.g. with “UMS-TargetGroup“ as the name, with the following settings:
    - **Target type**: `Instance`
    - **Protocol : Port**: `HTTPS : 8443`
    - Health check path:
        - UMS: `/info`
        - ICG: `/usg/check-status`
    - **Success codes**: `200`

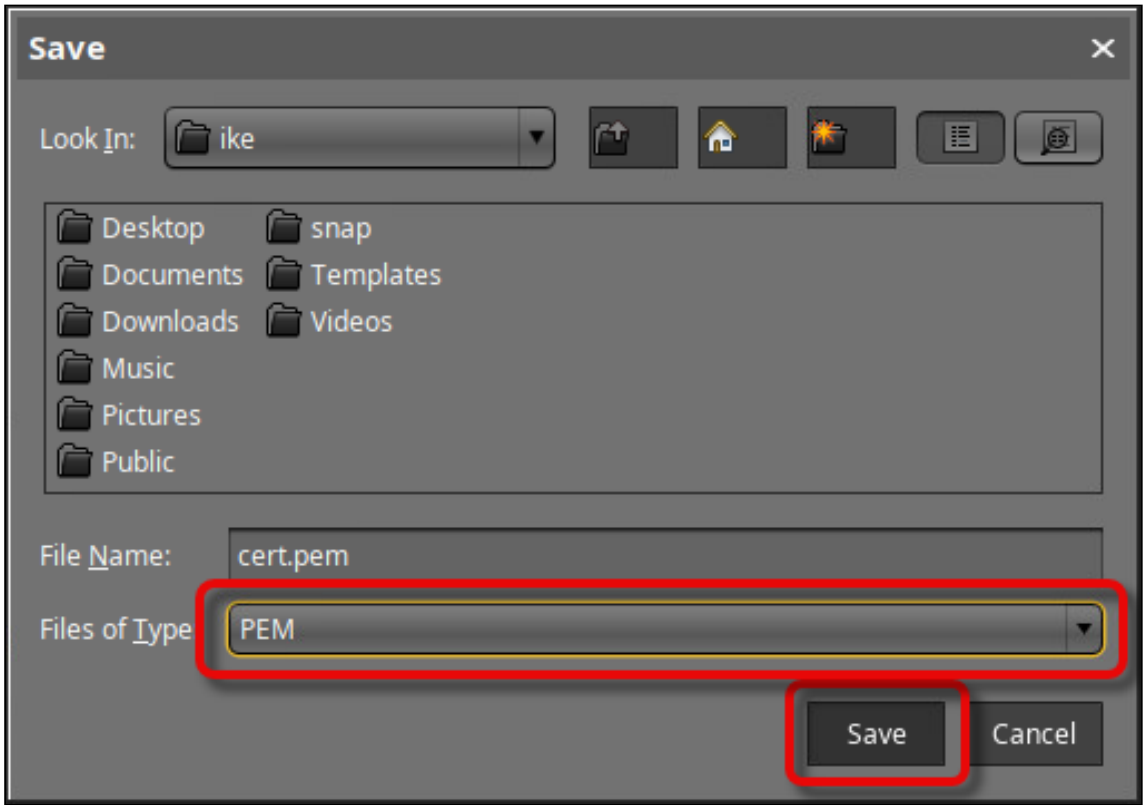




Exporting the CA Certificate Chain from the UMS

→ In the UMS Console, go to **UMS Administration > Global Configuration > Server Network Settings > Export Client Certificate Chain**, click **Export**, and save the certificate file in **PEM** format to a suitable location.


Server -
UMS Administration
UMS Network
Server
IGEL Cloud Gateway
Events
Global Configuration
Licenses
UMS Licenses
Device Licenses
Deployment
Certificate Management
Server Network Settings
Device Attributes
Administrative Tasks
UMS ID
Proxy Server
Default Directory Rules
Universal Firmware Update
Wake on LAN
Active Directory / LDAP
Identity Provider
Remote Access
Logging
Mail Settings
Messages to Devices
Misc Settings
UMS Features
Scheduled Jobs
Scheduled jobs never expire
Expiration time for scheduled jobs
40
Minutes
Scan Parameters
Timeout (ms)
6000
Broadcast IP
255 . 255 . 255 . 255
Specify scan reply port (UDP)
Cluster Address
Enable common cluster address for all UMS servers (restart of UMS Servers needed on change)
Devices and other external services can reach the UMS cluster at
https://
Set Address
OS 12 device enrollment address
Enable customize OS 12 device enrollment address
Devices can reach the enrollment service at
https://
Set Address
Export Client Certificate Chain
Export
UMS High Availability / Distributed UMS
Distributed UMS enabled (restart of UMS Servers needed on change)

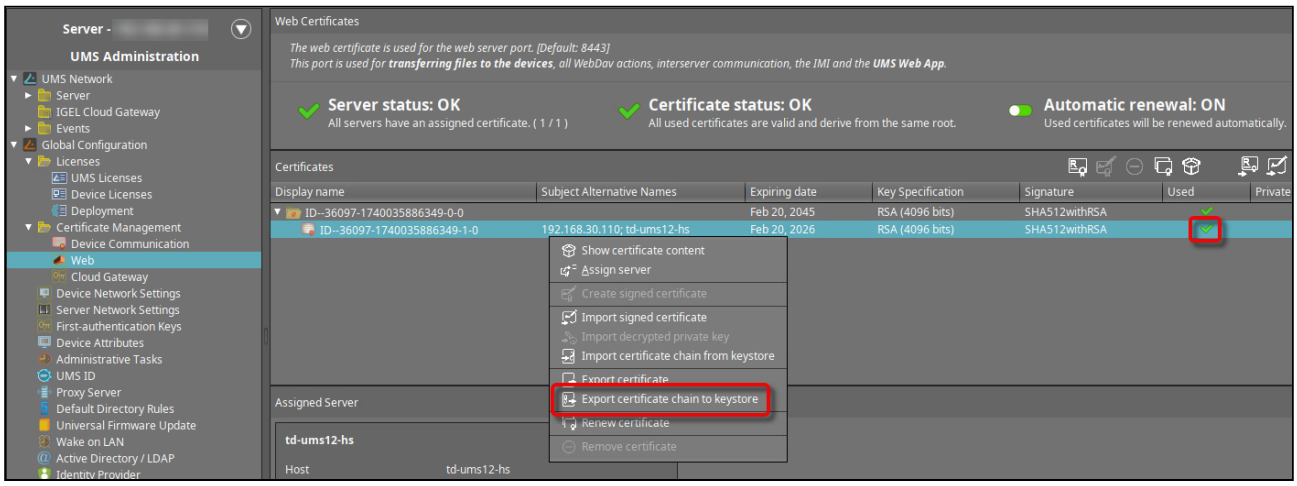

Save
Look In:
ike
Desktop
Documents
Downloads
Music
Pictures
Public
snap
Templates
Videos
File Name:
cert.pem
Files of Type
PEM
Save
Cancel

Creating a Trust Store with the UMS CA Certificate Chain via S3

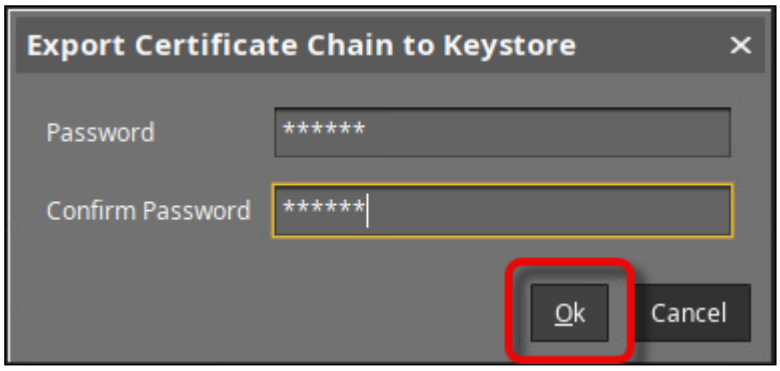
→ Create an S3 bucket and upload the CA certificate chain you have just created.

Exporting the UMS Web Certificate Chain

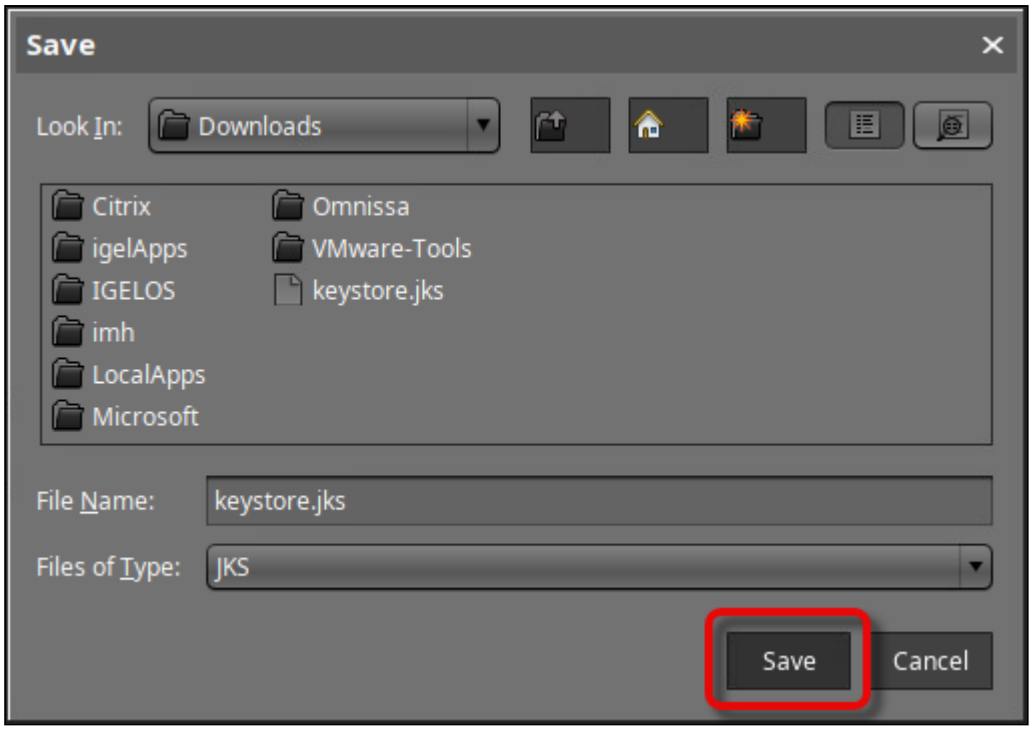
1. Select the web certificate that is currently in use, open the context menu, and click **Export certificate chain to keystore**.



2. Set a password for the keystore.



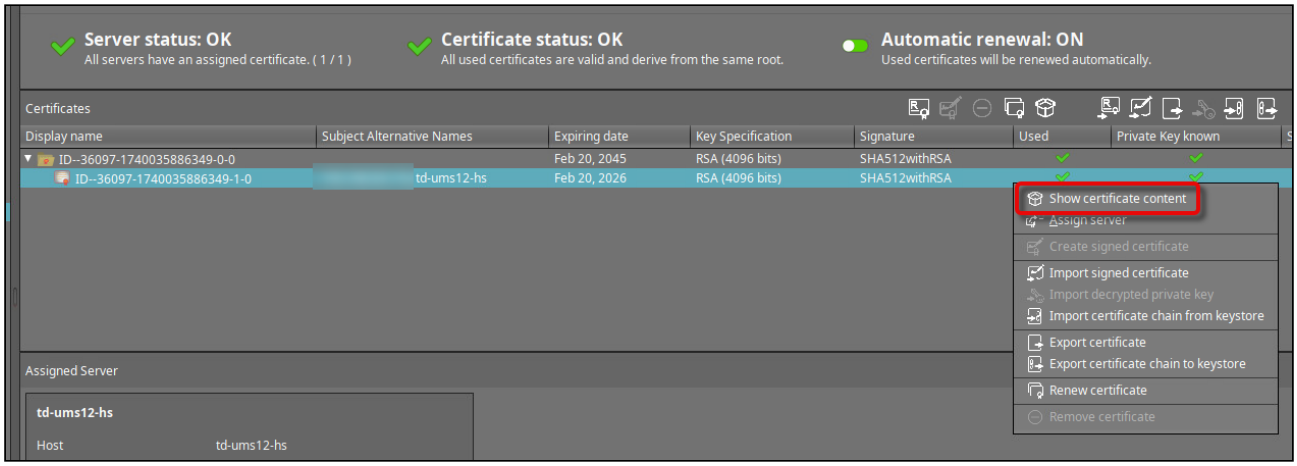
3. Save the keystore file to a suitable location.

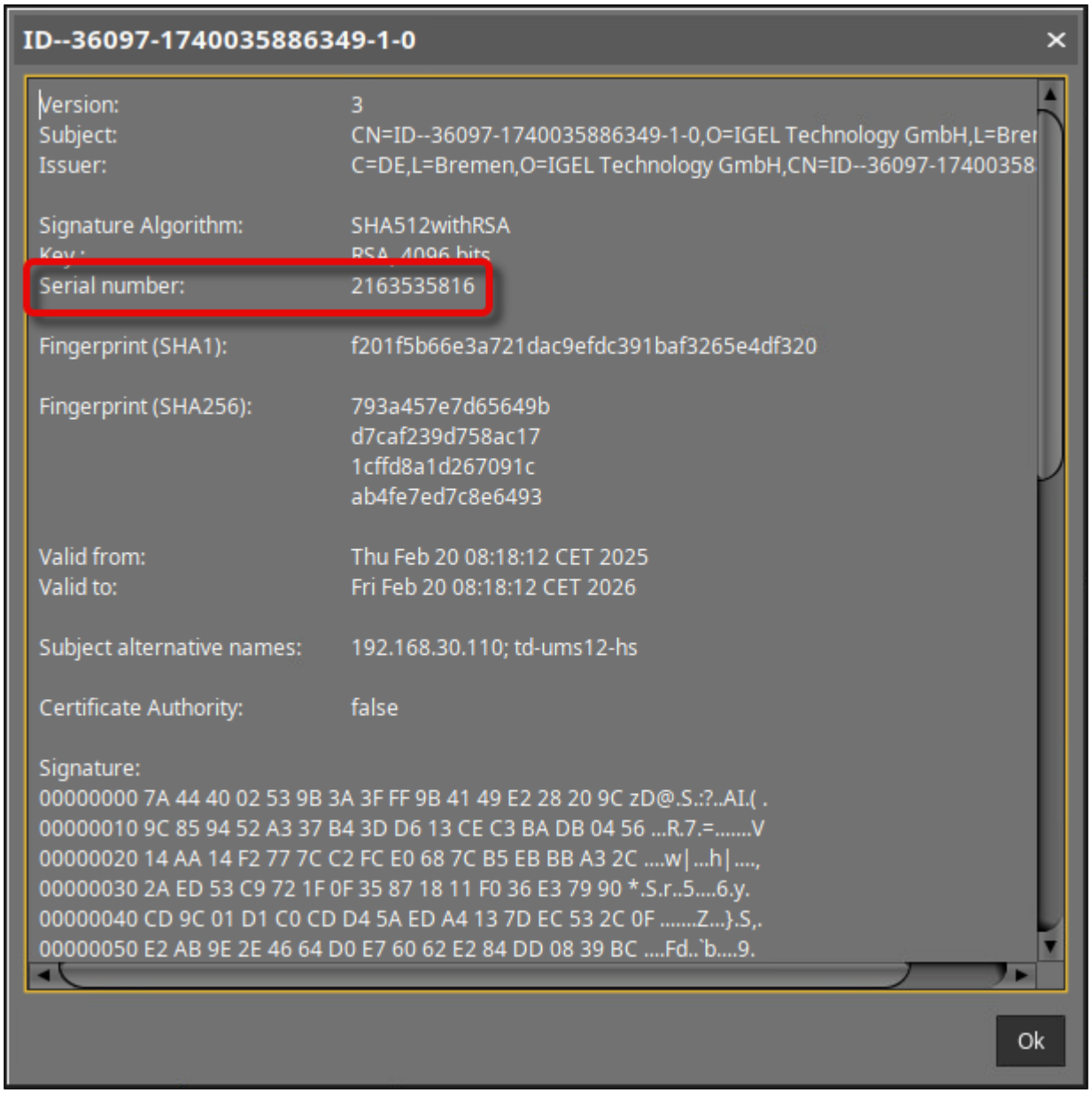


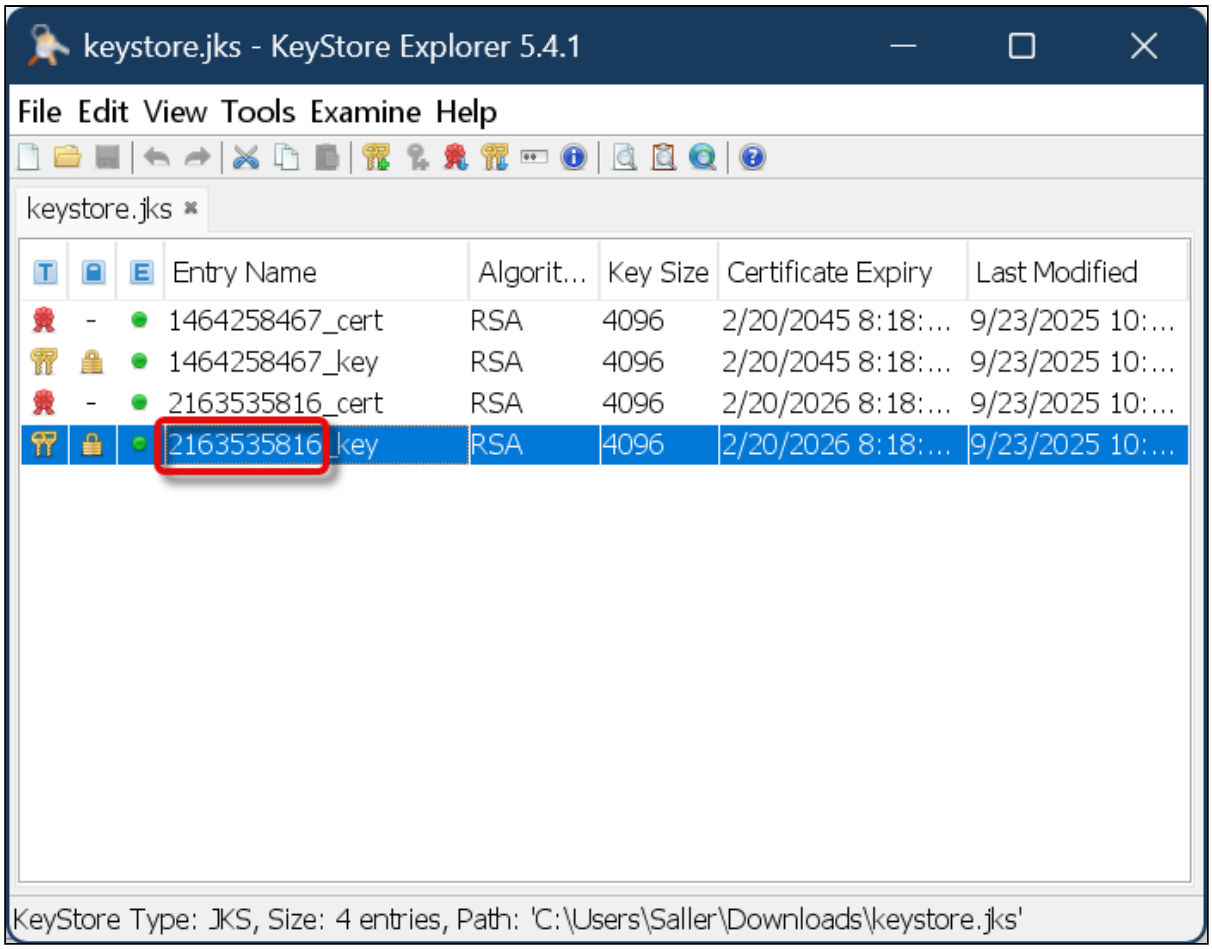
4. Open the keystore file with a suitable tool, e.g., KeyStore Explorer.

5. Enter the password you have defined during the export from the UMS.

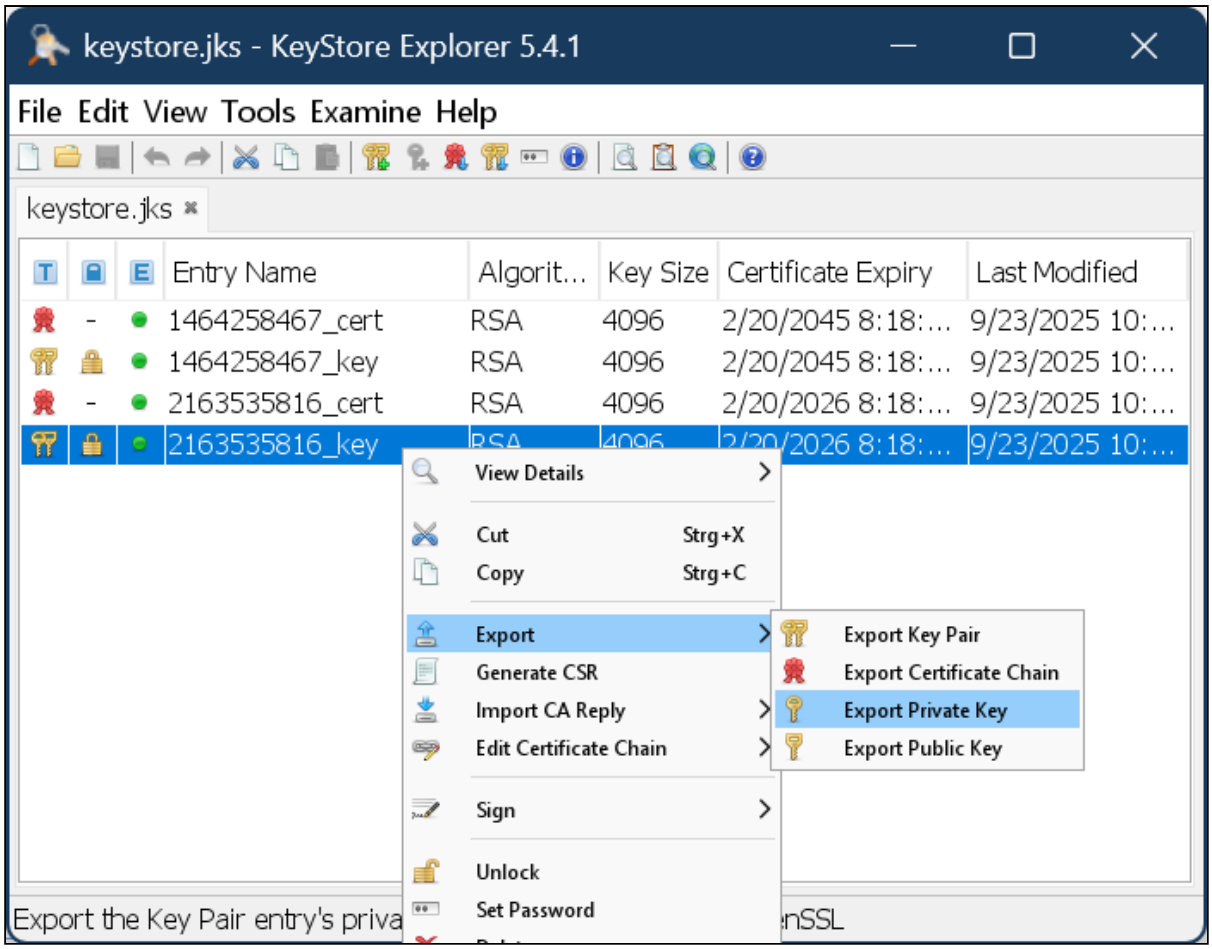
6. Select the correct key pair by comparing the entry name in the keystore tool with the serial number displayed in the UMS when you click **Show certificate content**.

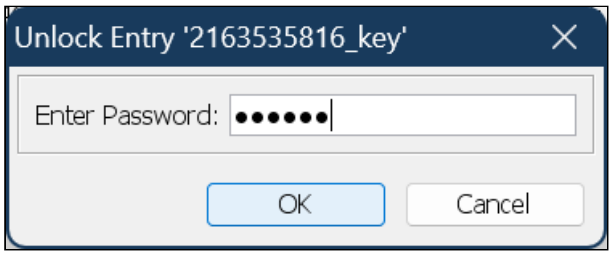


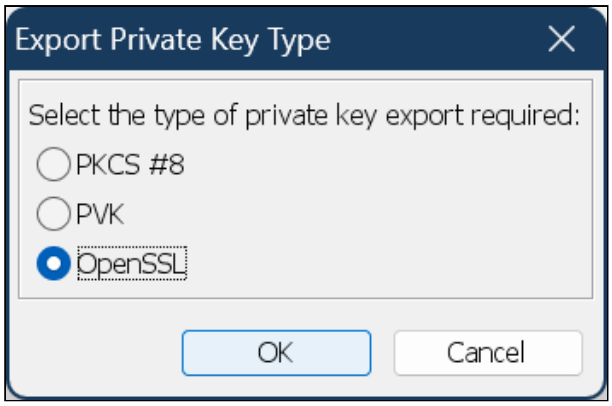

ID--36097-1740035886349-1-0
Version: 3
Subject: CN=ID--36097-1740035886349-1-0,O=IGEL Technology GmbH,L=Bre
Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--36097-17400358
Signature Algorithm: SHA512withRSA
Serial number: 2163535816
Fingerprint (SHA1): f201f5b66e3a721dac9efdc391baf3265e4df320
Fingerprint (SHA256): 793a457e7d65649b d7caf239d758ac17 1cffd8a1d267091c ab4fe7ed7c8e6493
Valid from: Thu Feb 20 08:18:12 CET 2025
Valid to: Fri Feb 20 08:18:12 CET 2026
Subject alternative names: 192.168.30.110; td-ums12-hs
Certificate Authority: false
Signature:
00000000 7A 44 40 02 53 9B 3A 3F FF 9B 41 49 E2 28 20 9C zD@.S.:?..AI.(.
00000010 9C 85 94 52 A3 37 B4 3D D6 13 CE C3 BA DB 04 56 ...R.7.=.....V
00000020 14 AA 14 F2 77 7C C2 FC E0 68 7C B5 EB BB A3 2C ....w|...h|....,
00000030 2A ED 53 C9 72 1F 0F 35 87 18 11 F0 36 E3 79 90 *.S.r..5....6.y.
00000040 CD 9C 01 D1 C0 CD D4 5A ED A4 13 7D EC 53 2C 0F .....Z...}.S,.
00000050 E2 AB 9E 2E 46 64 D0 E7 60 62 E2 84 DD 08 39 BC ....Fd..`b....9.
Ok

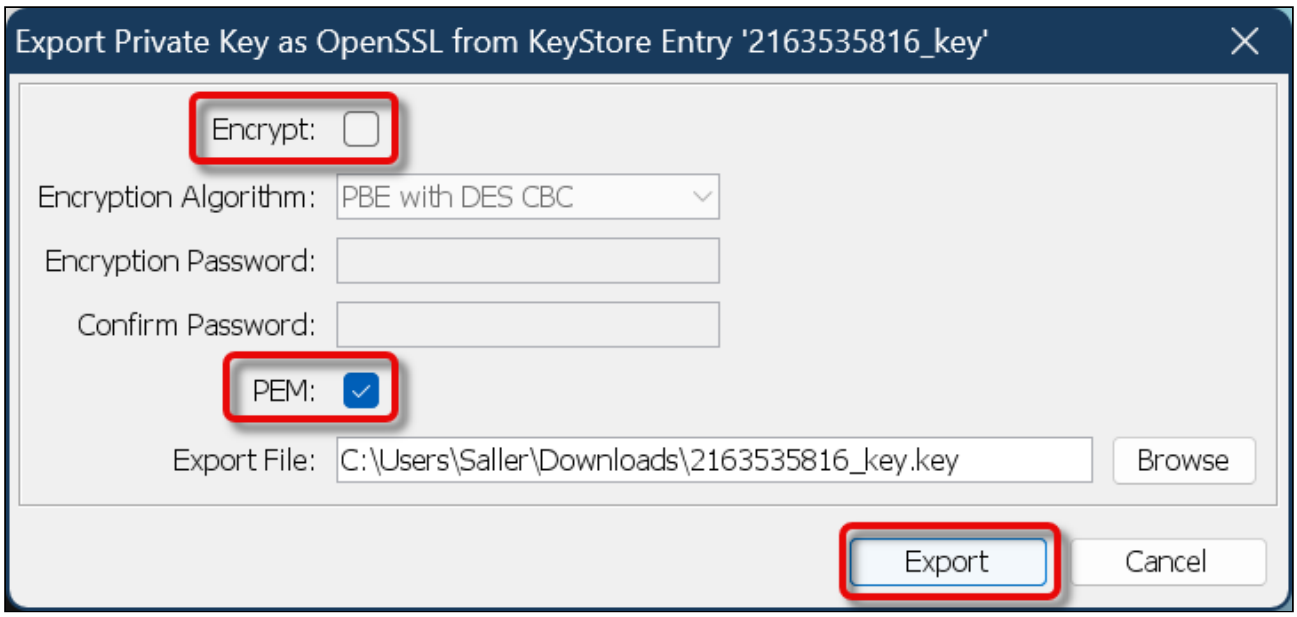


7. Export the private key with the following properties:
    - Type: OpenSSL
    - Unencrypted
    - PEM is activated
    - Appropriate filename, e.g., something with “private_key”

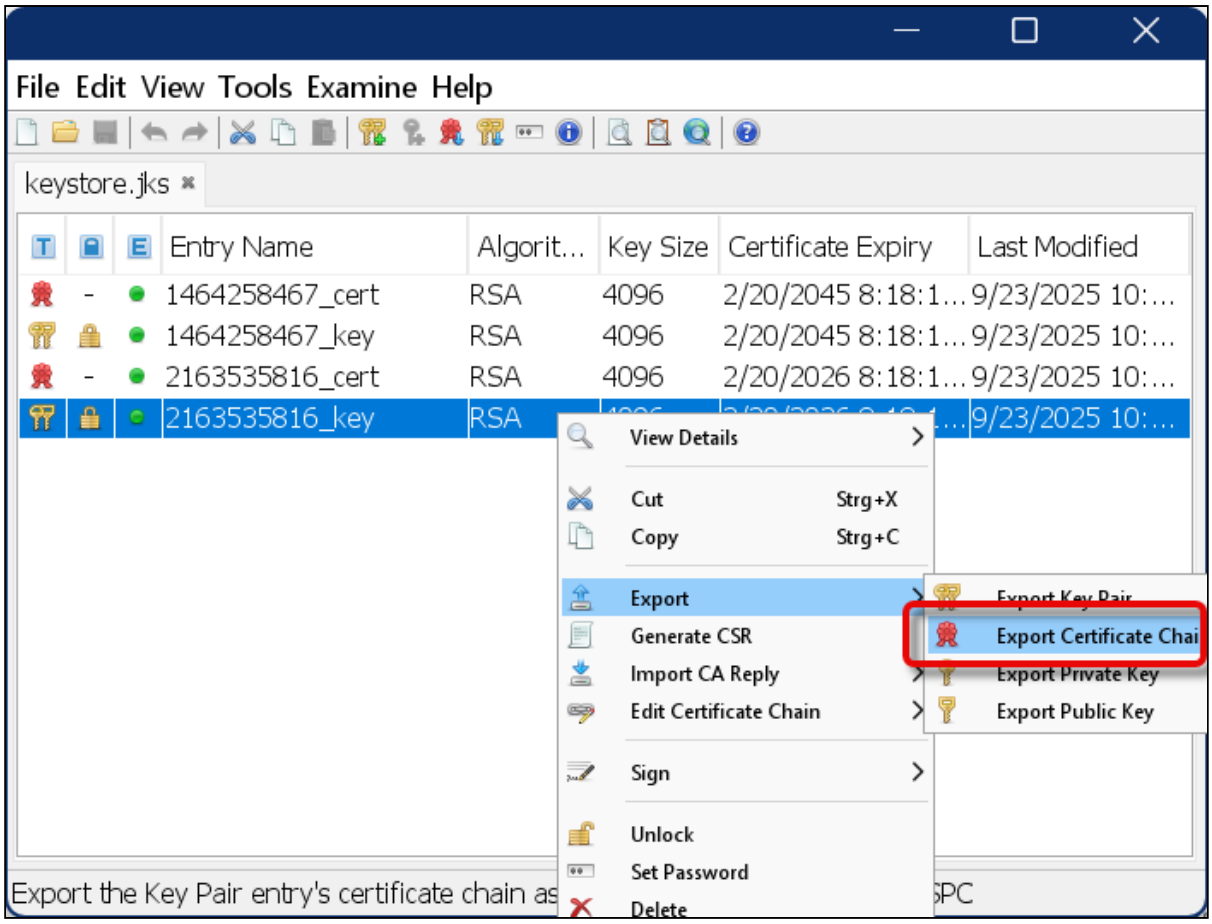

keystore.jks - KeyStore Explorer 5.4.1
File Edit View Tools Examine Help
keystore.jks
Entry Name
Algorit...
Key Size
Certificate Expiry
Last Modified
1464258467_cert
RSA
4096
2/20/2045 8:18:...
9/23/2025 10:...
1464258467_key
RSA
4096
2/20/2045 8:18:...
9/23/2025 10:...
2163535816_cert
RSA
4096
2/20/2026 8:18:...
9/23/2025 10:...
2163535816_key
View Details
Cut Strg+X
Copy Strg+C
Export
Generate CSR
Import CA Reply
Edit Certificate Chain
Sign
Unlock
Set Password
Export Key Pair
Export Certificate Chain
Export Private Key
Export Public Key
Export the Key Pair entry's priva

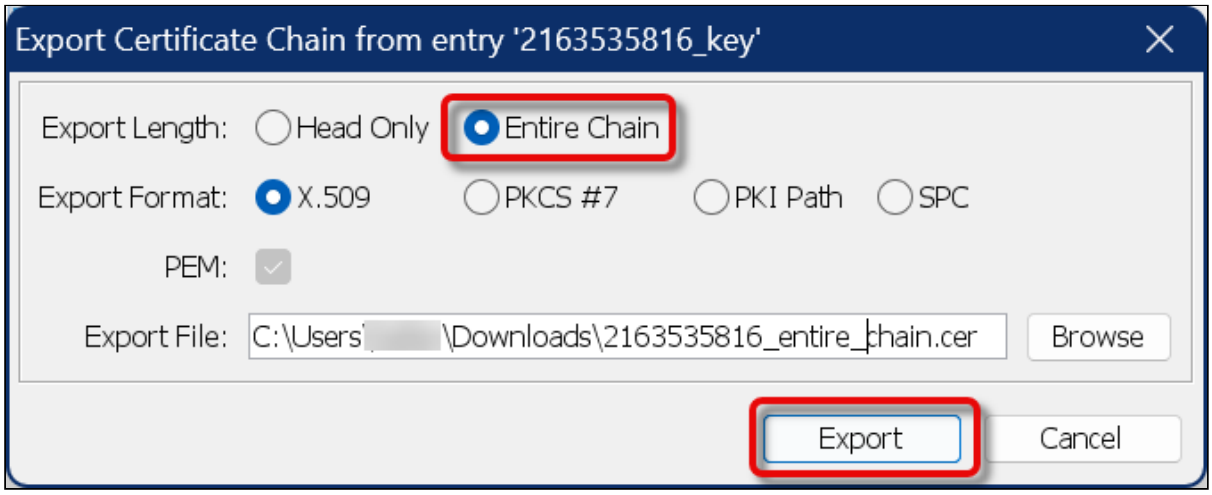

Unlock Entry '2163535816_key'
Enter Password:
OK
Cancel





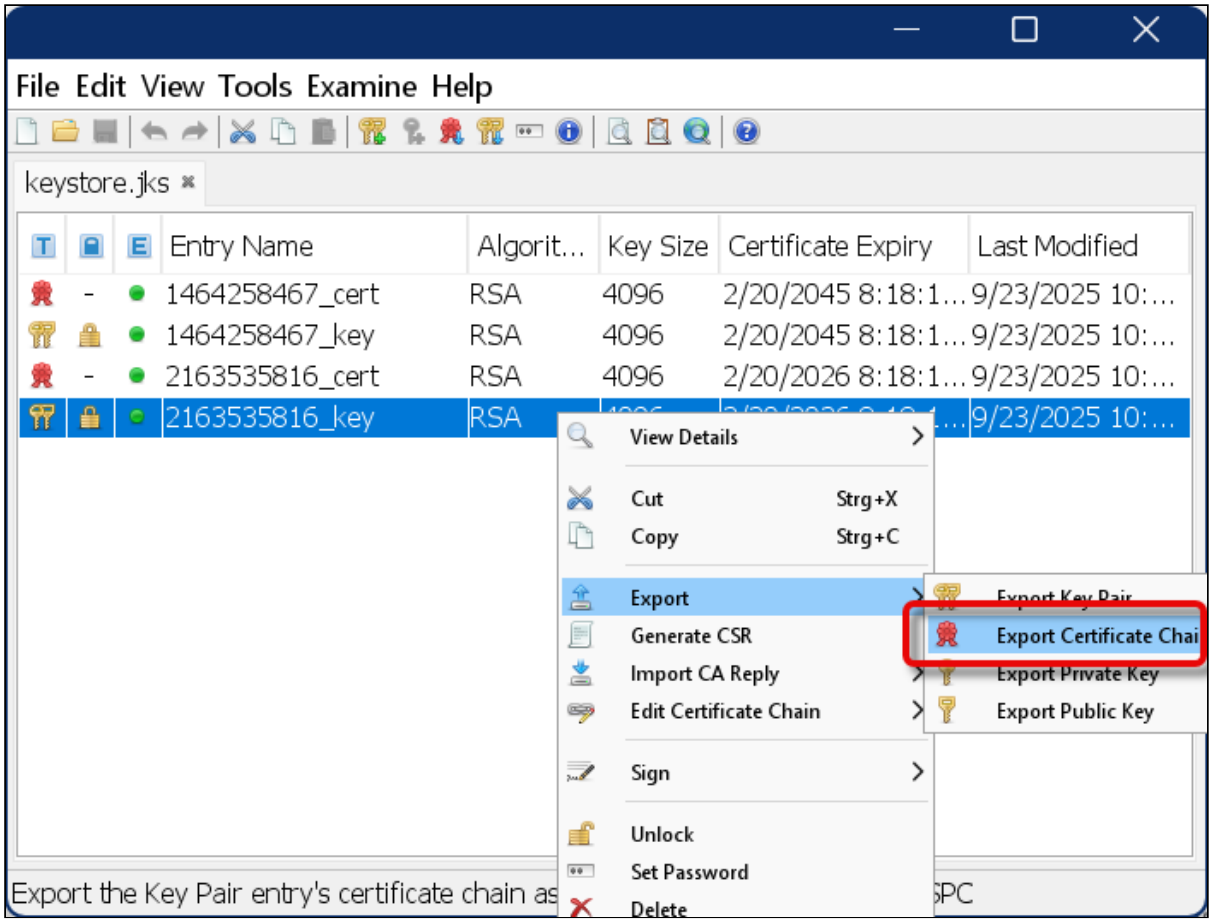
8. Export the certificate chain with the following properties:
   - Export length: Entire chain
   - PEM is activated
   - Appropriate filename, e.g., something with “entire_chain”

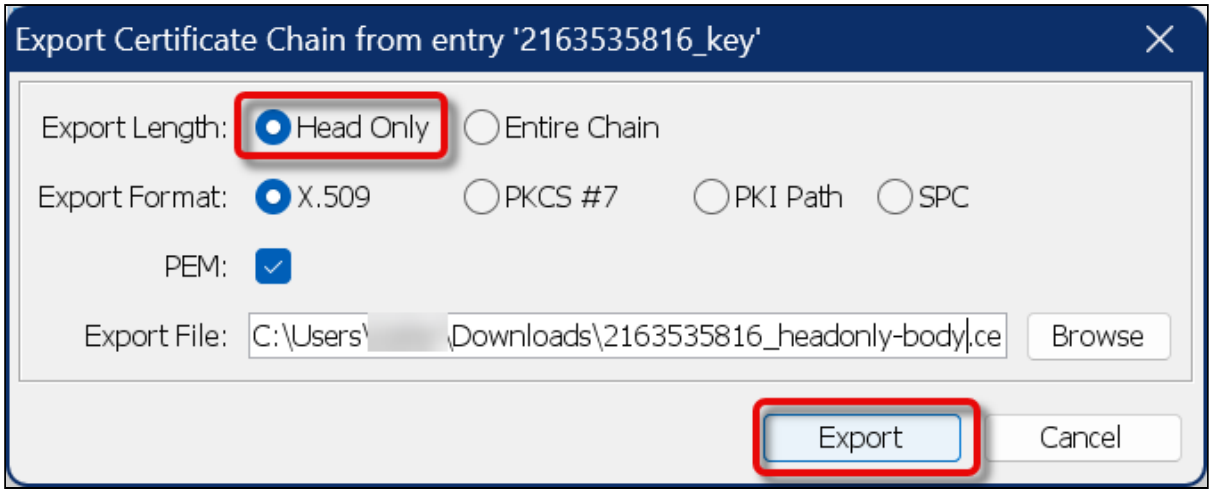




9. Export the certificate chain, this time with the following properties:
   - Export length: Head only
   - PEM is activated

- Appropriate filename, e.g., something with “headonly-body”





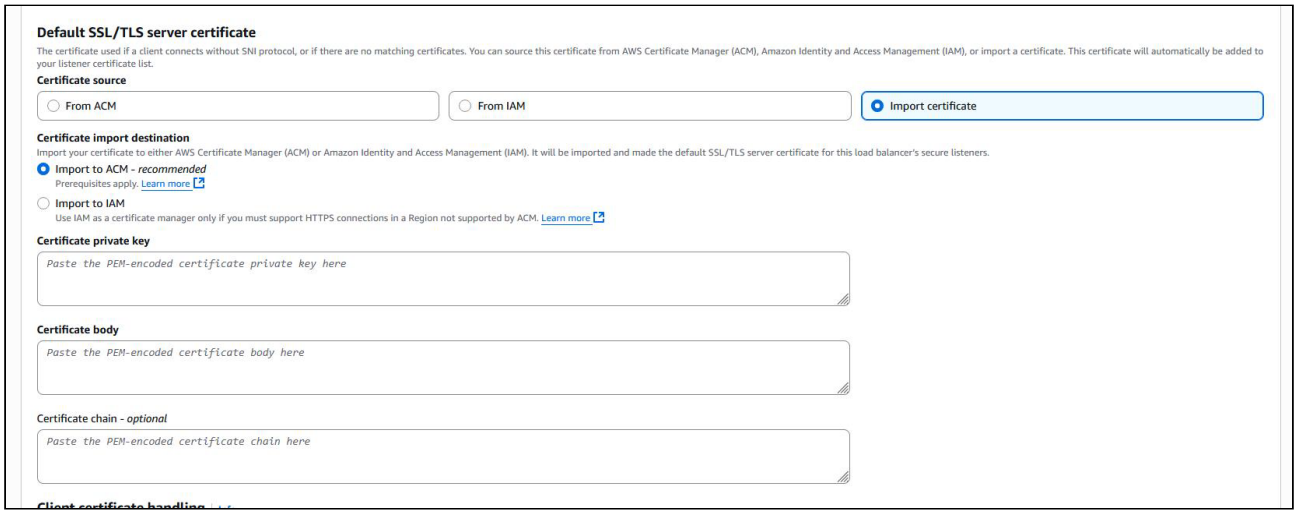
Configuring the ALB Listeners

In the following, we will create an ALB with two listeners

1. Create an Internet-facing ALB.

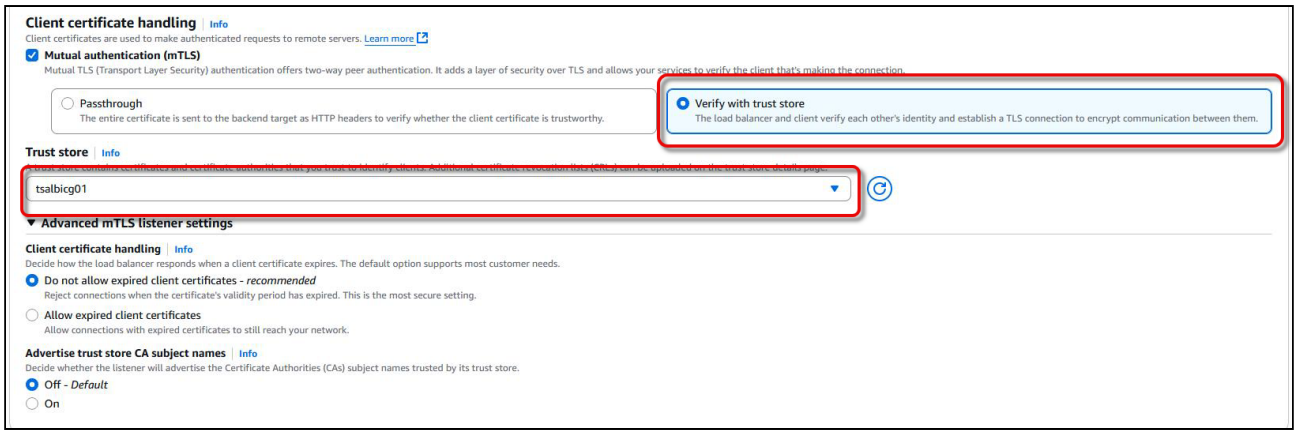
2. Create a listener that listens for HTTPS connections with mTLS on port 8443 and forwards traffic to the UMS target group.

3. Click **Import a certificate** and paste the complete contents of the files we have exported from the keystore:
   - **Certificate private key**: Paste the content of the file we created in Exporting the UMS Web Certificate Chain (see page 241), step 7 (see page 244).
   - **Certificate chain (optional)**: Paste the content of the file we created in Exporting the UMS Web Certificate Chain (see page 241), step 8 (see page 246).
   - **Certificate body**: Paste the content of the file we created in Exporting the UMS Web Certificate Chain (see page 241), step 9 (see page 247).



Once imported, the certificate becomes available in the AWS Certificate Manager (ACM).

4. Under **mTLS settings**, enable **Verify with Trust Store** and link to the S3 bucket with the UMS CA certificate chain you have created beforehand.



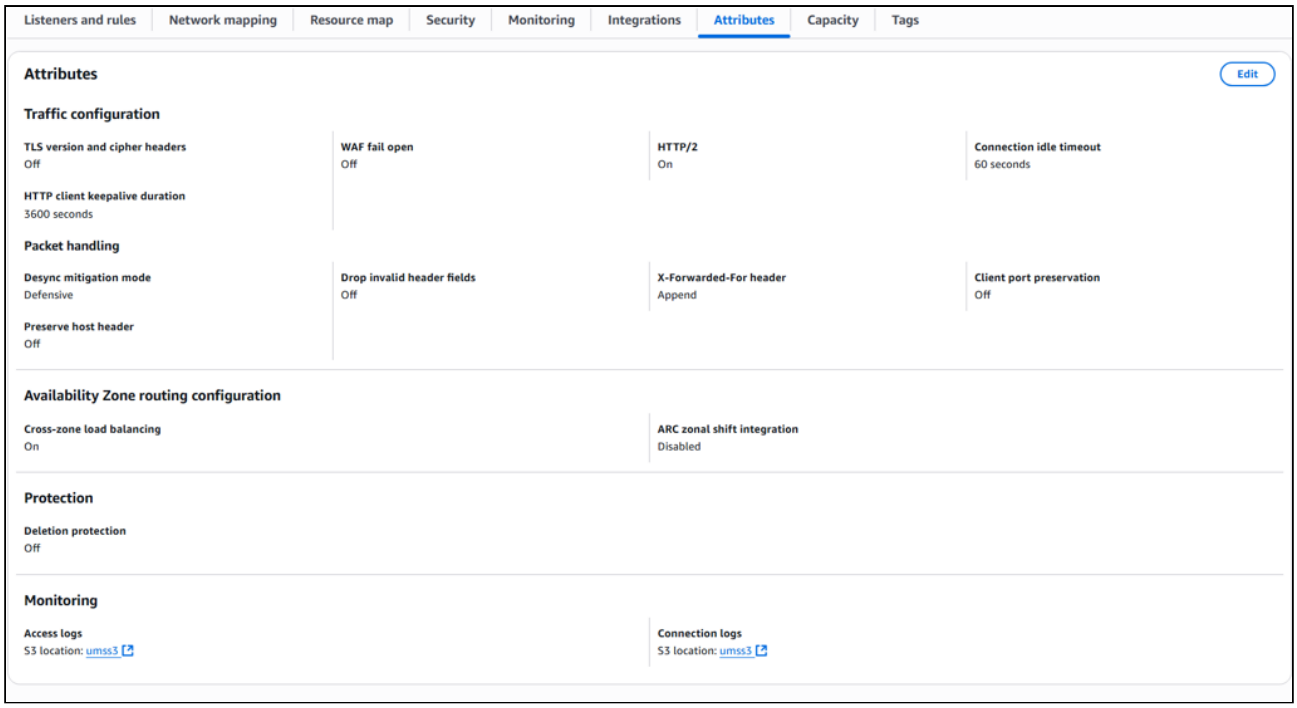
5. Create another listener that listens for HTTPS connections with standard TLS (no mTLS) on port 443 and forwards traffic to the UMS target group.

6. Click **Import a certificate** and provide the same certificate configuration as you did for the first listener in step 4.

Configuring Logging and Monitoring

1. Enable **Access Logs** and **Connection Logs** for the ALB.

2. Set the log destination to the S3 bucket that is used for the trust store or another one as needed.



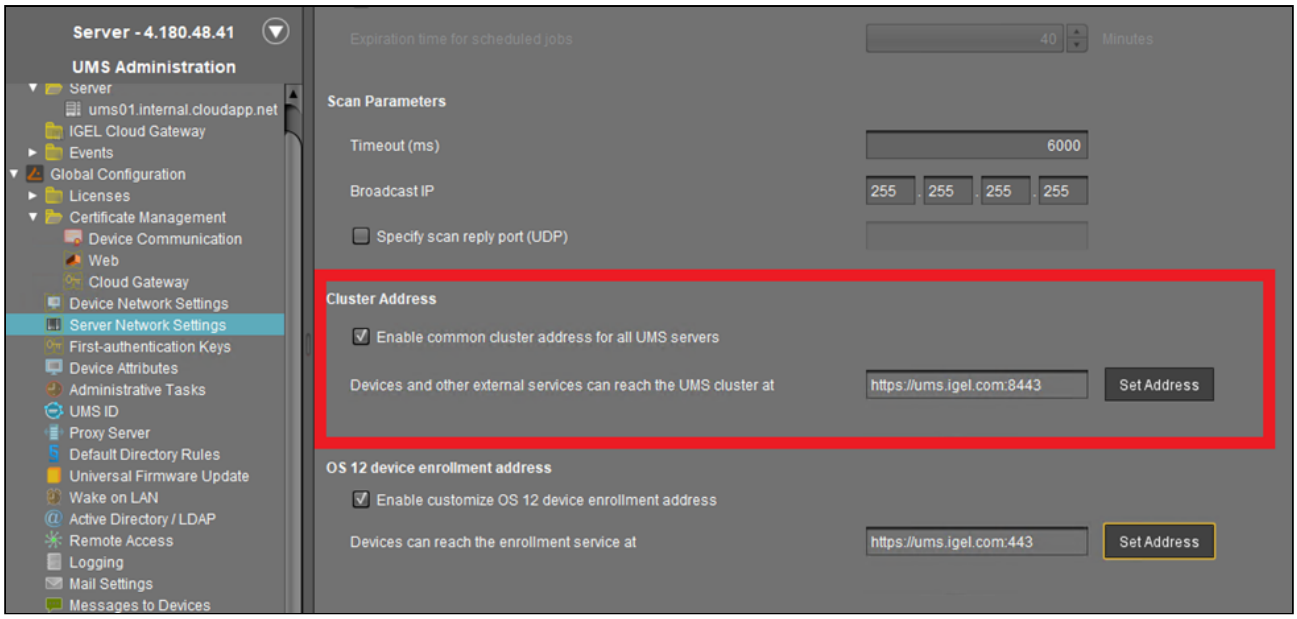
Configuring the UMS Server

Adjusting the Server Network Settings

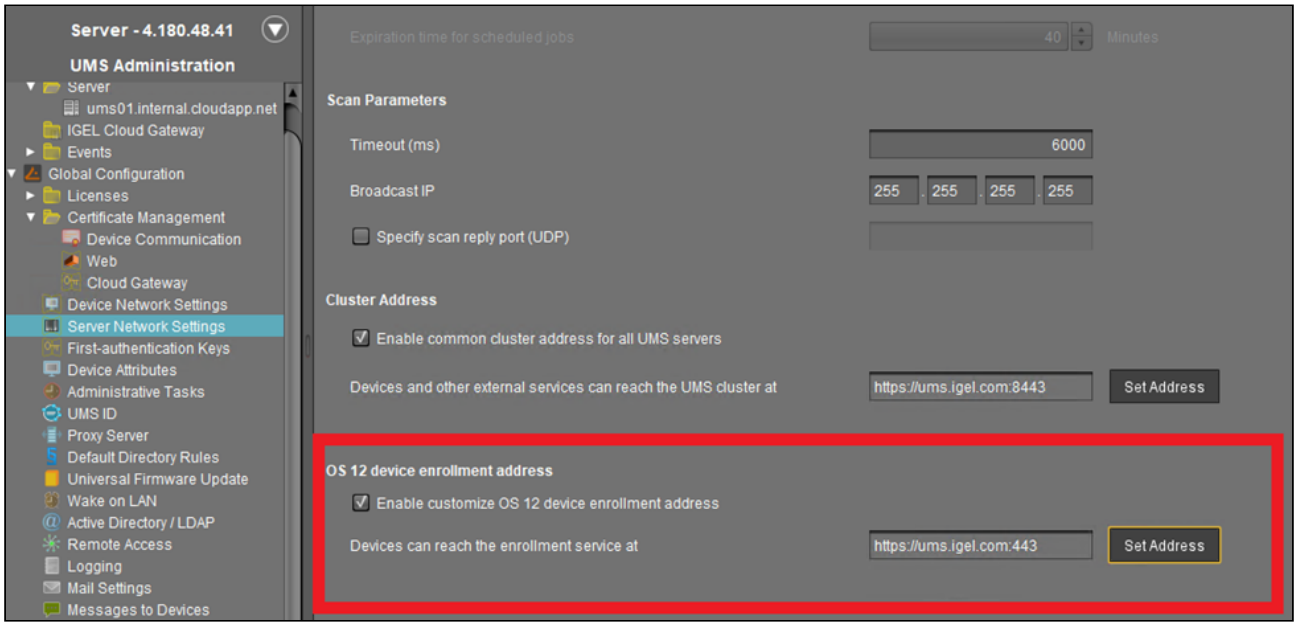
The FQDN of the UMS cluster must be set as the external address. This FQDN of the UMS cluster must be included in your web certificate, and the corresponding certificate must be assigned to all UMS servers:

1. Go to **UMS Administration > Global Configuration > Server Network Settings**.

2. Set the **Cluster Address** to the external address of your AWS ALB.

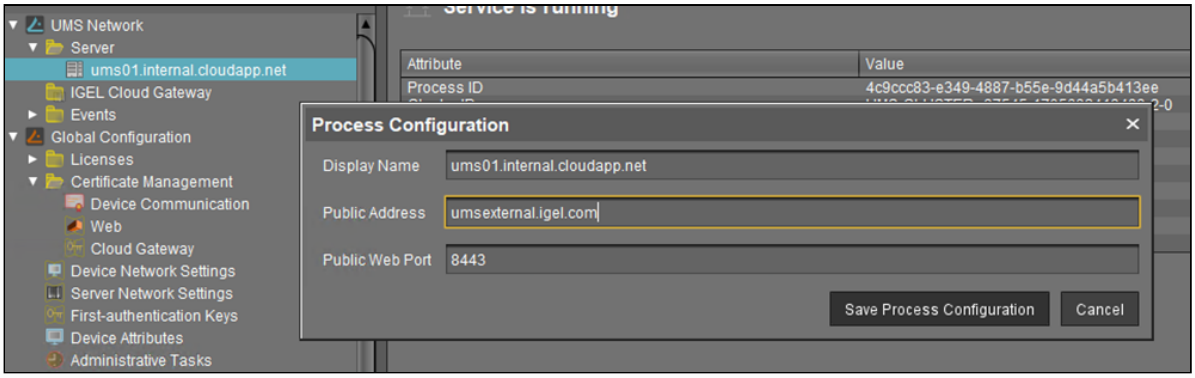


3. Set the **OS 12 device enrollment address** to the external address of your AWS ALB.



Set Public Address and Port of the UMS Process Configuration

If the public address of the UMS differs from the UMS address, the public address and port must be set. This option can be set under **UMS Administration > UMS Network > Server**. This is essential for device shadowing.



Create UMS Web Certificate / Cloud Gateway Ce

Setting the UMS Server to Accept the Certificate from the AWS ALB

The AWS ALB sends a header (`X-Amzn-Mtls-Clientcert-Leaf`) that contains only the client certificate, not the full certificate chain. Therefore, the UMS Server must be configured accordingly.

1. Edit the file `<UMS installation path>\rmguiserver\conf\appconfig\application.yml` according to the example below:

```
igel:
  client-cert-forwarding:
    enabled: true
    encodingType: URL_AWS
    client-cert-forwarded-header: X-Amzn-Mtls-Clientcert-Leaf
```

The `encodingType` must be explicitly set to `URL_AWS` to properly decode the certificate format used by the ALB, which URL-encodes the PEM-formatted certificate.

2. Restart the UMS Server.

UMS Articles

Devices Supported by IGEL Universal Management Suite (UMS)

Question

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

Answer

> ⚠ To ensure that you can use all new features of IGEL OS:
> → Update your UMS to the current version.
> → For all relevant OS 11 profiles (see page 701), set **Based on** to the appropriate firmware version.
> → For OS 12 profiles (see page 1252), note the following: An OS 12 profile configures ALL versions of an app, unless a specific version is set under **Show Versions**.

The latest UMS version supports

- all IGEL devices that have not yet reached their end of maintenance
- devices converted with IGEL OS Creator (OSC)

Older UMS releases support

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

IGEL UMS Communication Ports

The following table shows the default ports which are used by the components of the IGEL Universal Management Suite (UMS) and a UMS infrastructure. Some of these ports are configurable, e.g. web server port 8443, device communication port 30001 for IGEL OS 11 devices, etc. (see Settings - Change Server Settings in the IGEL UMS Administrator (see page 1038)).

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
443 (TCP)	IGEL App Portal https://app.igel.com/	Cloud Service	UMS Server	The UMS Server imports apps from the IGEL App Portal.
443 (TCP)	(en) Initial Configuration of the IGEL Onboarding Service (OBS) https://obs.services.igel.com[71]	Cloud Service	UMS Server	The UMS Server validates the onboarding token.
443 (TCP)	(en) IGEL Insight Service	Cloud Service	UMS Server	The UMS Server transfers analytical and usage data to IGEL.
443 (TCP)	Automatic License Deployment (ALD)	IGEL licensing server (at susi.igel.com)	UMS Server	The UMS Server requests licenses; see UMS Contacting the Licensing Server (see page 390) .

71. https://obs.services.igel.com/

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
443 (TCP)	Automatic License Deployment (ALD)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	The UMS Server requests the connection details required for connecting to the IGEL license server (at susi.igel.com). See UMS Contacting the Licensing Server (see page 390).
8443 (TCP)	Core	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Console / UMS Web App	See UMS with Internal Database (see page 351) or UMS with External Database (see page 352).
8443 (TCP)	Unified Protocol	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device opens a WebSocket for data exchange (all communication incl. registration via IGEL Onboarding Service or One-Time Password method, file transfer, firmware customization and license transfer, secure shadowing, secure terminal) For more information on Unified Protocol, see Overview of the IGEL UMS (see page 661).
8443 (TCP)	UMS as an Update Proxy	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device contacts the UMS Server to download app updates.

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
30002 (TCP)	Core (directly, without ICG)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	HA Load Balancer	If the UMS Server and the HA Load Balancer are running on the same host, the UMS Server will use port 30002 instead of 30001, and the HA Load Balancer will use port 30001 (relevant for IGEL OS 11 only).
30001 (TCP)	Unified Protocol (automatic registration or registration after scanning)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device requests a registration token if the UMS Server was detected in the company network (see Registering Devices Automatically on the IGEL UMS (see page 1151) and Importing Devices (see page 1143)) or the device received a registration request after it was scanned (see Scanning the Network for Devices and Registering Devices on the IGEL UMS (see page 1136)).
30001 (TCP)	Core (direct device communication, not used with communication via ICG)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	See Devices Contacting UMS (see page 359).
8443 (TCP)	Core (file transfer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device requests a file from the UMS; see UMS and Devices: File Transfer[72].

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
8443 (TCP)	Core (firmware customization)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The UMS provides files for customizing the look and feel of the device's GUI; see UMS and Devices: File Transfer[73].
88 (TCP/ UDP)	Core (if Active Directory is used), Shared Workplace	MS Active Directory Service	UMS Server	The UMS Server sends a Kerberos request to MS Active Directory.
389 (TCP)	Core (if Active Directory is used), Shared Workplace	MS Active Directory Service	UMS Server	The UMS Server sends an LDAP request to MS Active Directory.
1527 (TCP)	Core (if Apache Derby is used)	Apache Derby database (Derby Network Server)	UMS Server	See UMS with External Database (see page 352).
636 (TCP)	Core (if LDAPS server is used)	LDAPS server (other than MS Active Directory)	UMS Server	The UMS Server sends an LDAP request over SSL.
1433 (TCP)	Core (if MS SQL Server is used)	Microsoft SQL Server database	UMS Server	See UMS with External Database (see page 352).

72. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-file-transfer-communication-f
73. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-file-transfer-communication-f

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
1521 (TCP)	Core (if Oracle is used)	Oracle database	UMS Server	See UMS with External Database (see page 352).
5432 (TCP)	Core (if PostgreSQL is used)	PostgreSQL database	UMS Server	See UMS with External Database (see page 352).
8443 (TCP)	Core (licenses)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The UMS provides license files for the devices; see UMS and Devices: File Transfer[74].
Auto ("high port") (UDP)	Core (online check)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device responds to a message sent by the UMS to check if the device is online. The port number to be used is contained in the UDP packet sent by the UMS.
30005 (TCP/UDP)	Core (scanning for device)	Device (OS 12 & OS 11)	UMS Server	The UMS sends a broadcast. The UDP package is sent to the given port number. In case TCP is selected and an IP range is given this port is used to build up an TCP connection to the device.

74. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-file-transfer-communication-f

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
Auto ("high port") (UDP)	Core (scanning for device)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device (OS 12 & OS 11)	The device responds to a broadcast sent by the UMS during a scan. The port number to be used is contained in the UDP packet sent by the UMS.
30022 (TCP)	Core (secure terminal)	IGEL OS 11 device (UMS agent)	UMS Server	See IGEL UMS and Devices: Secure Terminal Communication Flow[75] .
5900 (TCP)	Core (shadowing)	IGEL OS 11 device (UMS agent)	UMS Console	The UMS Console initiates a VNC session for shadowing; see IGEL UMS and Devices: Shadowing Communication Flow[76]
5900 (TCP)	Core (shadowing) via UMS Web App	IGEL OS 11 device (UMS agent)	UMS Server	The UMS Web App triggers the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; see IGEL UMS and Devices: Shadowing Communication Flow[77]

75. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-secure-terminal-communication
76. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-shadowing-communication-flow
77. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-shadowing-communication-flow

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
9080 (TCP)	Core (unencrypted, no SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device requests a file from the UMS (regular file transfer or Universal Firmware Update). This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.
Auto ("high port")	Core (unencrypted, no SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Console	The GUI is started via Java Webstart console. This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.
443 (TCP)	Core (Universal Firmware Update)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	See UMS Contacting the Download Server to Check for New Updates (see page 385).
8443 (TCP)	Core (Universal Firmware Update)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	In the course of a Universal Firmware Update, the device requests a file from the UMS; see UMS and Devices: File Transfer[78].

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications /Service Binding to Port	Who is Talking? Applications/ Services Initiating Communications	Description
9 (UDP)	Core (Wake on LAN)	Device (OS 12 & OS 11)	UMS Server	The UMS Server sends magic packets to the devices.
8443 (TCP)	Core (with ICG)	ICG (IGEL Cloud Gateway)	UMS Server	See Devices and UMS Server Contacting Each Other via ICG (see page 356) or UMS Server (see page 661).
8443 (TCP)	Core (with ICG)	ICG (IGEL Cloud Gateway)	Device (OS 12 & OS 11)	See Devices and UMS Server Contacting Each Other via ICG (see page 356).
6155 (UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 6155 and use it for communication.
8443 (TCP)	High Availability (HA) and Distributed UMS	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	File synchronization between UMS Servers
61616 (TCP/UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 61616 and use it for communication.
8443 (TCP)	IMI	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	3rd party component using IMI (IGEL Management Interface)	See IGEL Management Interface (IMI) (see page 354).

78. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-file-transfer-communication-f

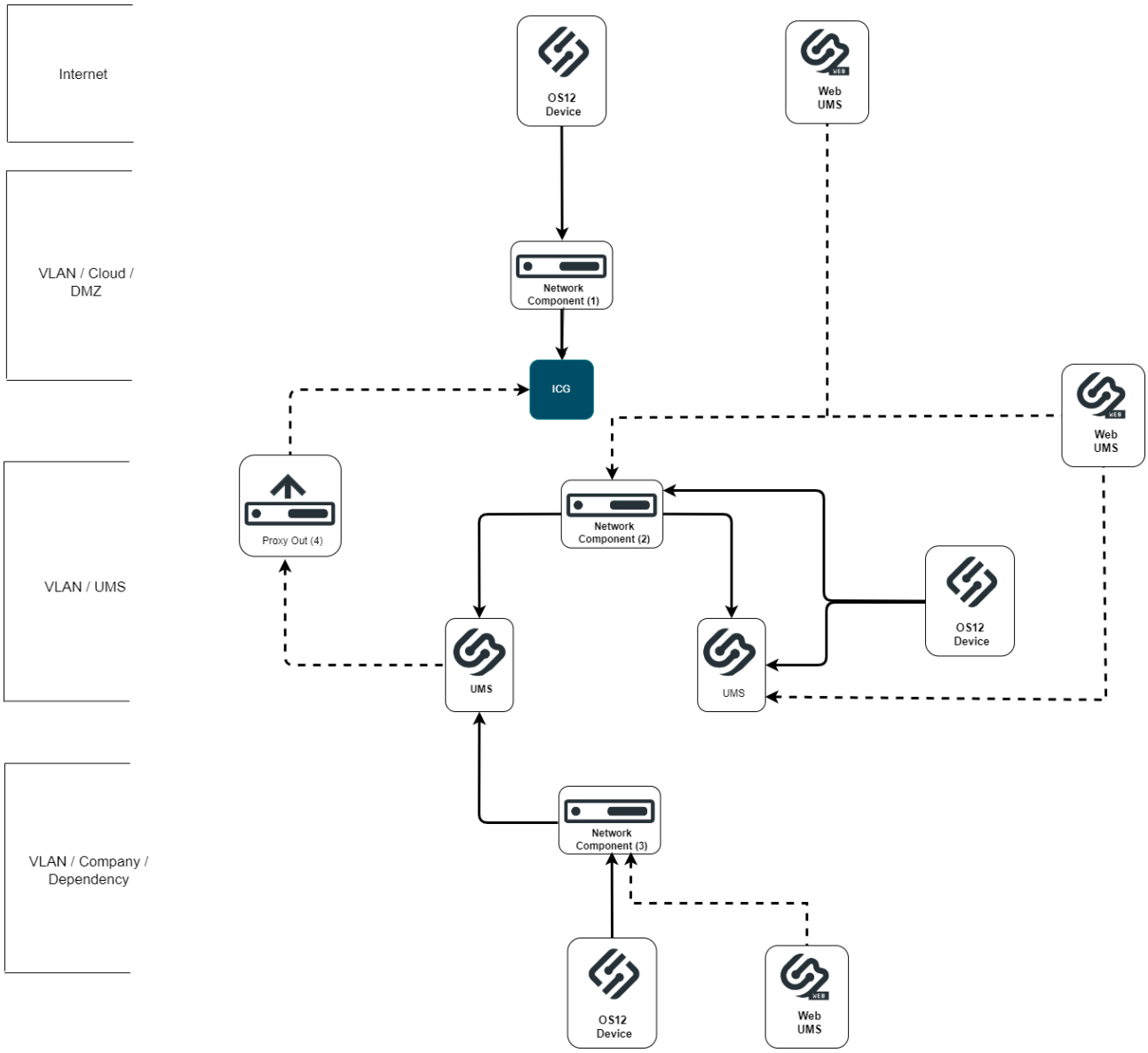
IGEL Universal Management Suite Network Configuration

This article describes the Universal Management Suite (UMS) and IGEL Cloud Gateway (ICG) Integration with Network components like Firewalls and Reverse Proxies.

For Reverse Proxy configuration examples, see:

UMS Network Configurations

The diagram shows a network configuration with possible network boundaries where network components like Reverse Proxies, Proxies, Firewalls and Loadbalancer can be placed.



There are typically three different positions for these components:

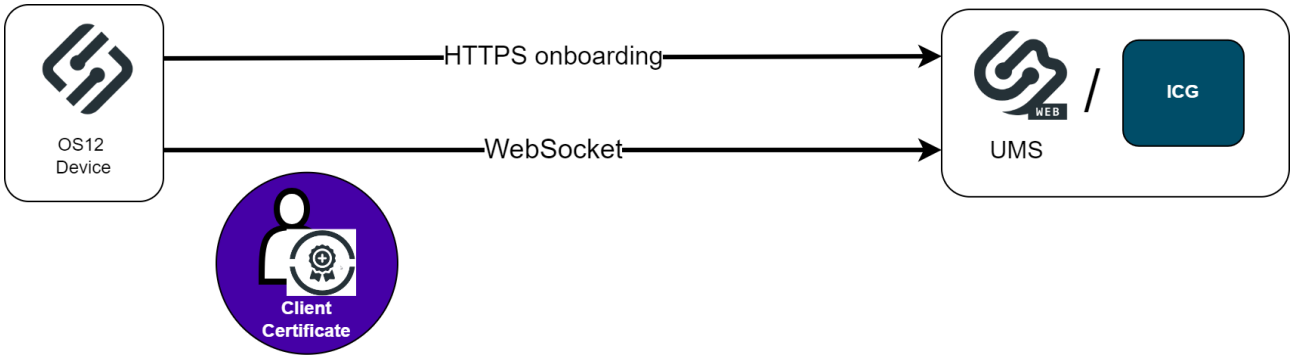
- Device and ICG Server
- Device and UMS Server
- ICG and UMS Server

Connection Types Between Device and UMS

For a successful configuration it is important to understand the different connection types.

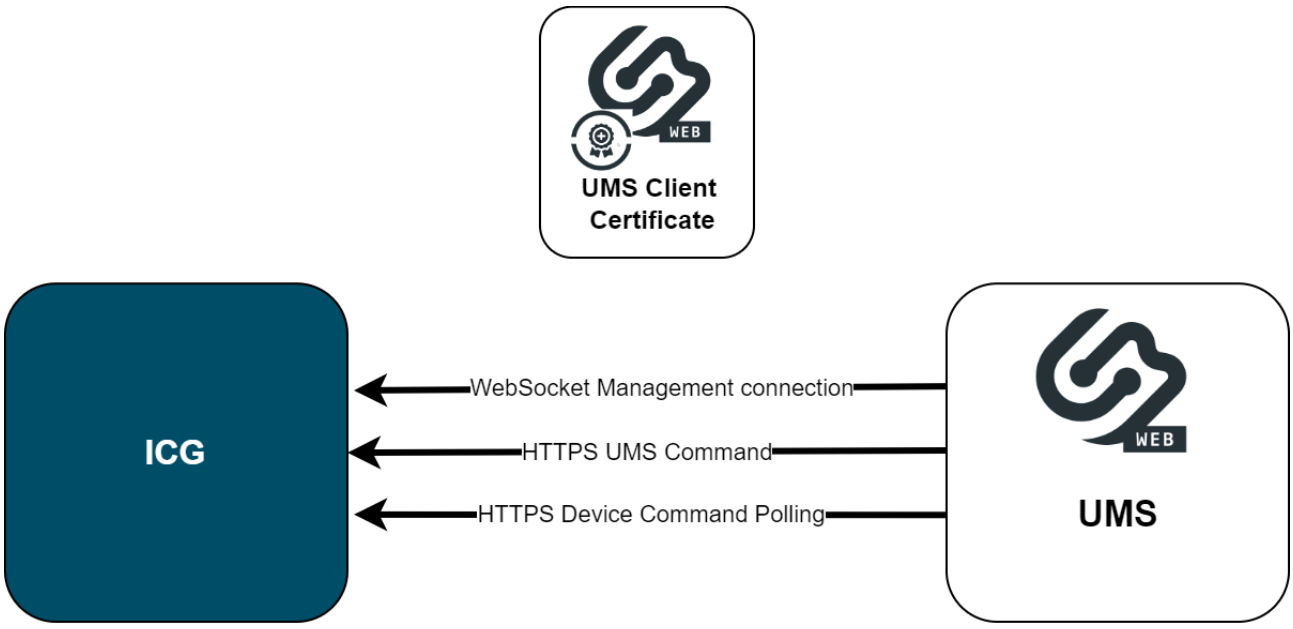
Device to ICG / UMS Communication

The communication of the devices to UMS or ICG consists of two different types. Regular HTTPS calls for the device registration and a WebSocket connection with Mutual TLS for device management. These must be considered for Proxy, Reverse Proxy and Firewall configuration.



UMS to ICG Communication

The communication of the UMS to the ICG is also based on WebSocket and regular HTTPS calls. Every request is initialized by the UMS and uses Mutual TLS. A HTTPS Proxy can be configured for these connections in the UMS.

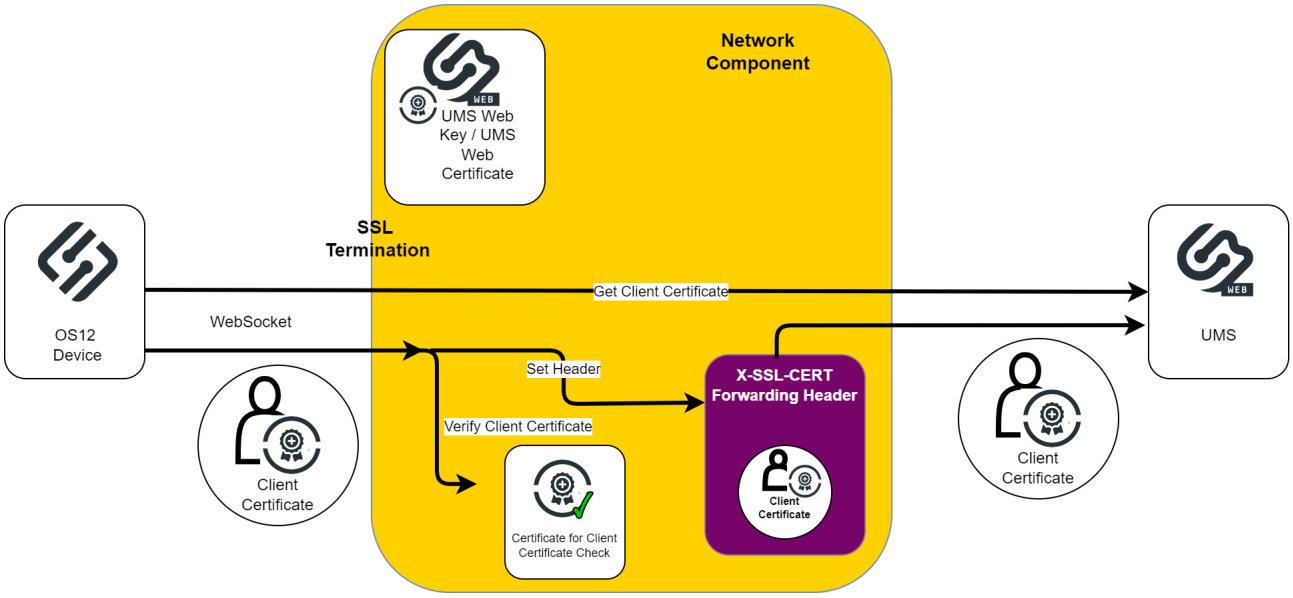


In case a Network Component is placed between these servers be aware of these connections. Connection problems could be observed when Deep Packet Inspection (DPI) is activated on a Firewall. The chapter SSL Offloading is only applicable for device to UMS / ICG connections. It is not supported for the communication between ICG and UMS.

Communication via Reverse Proxy

The diagram shows the device to UMS connection via a Network Component like Azure Application Gateway. The required connections are listed for SSL Offloading. The diagram shows one HTTPS connection which is necessary

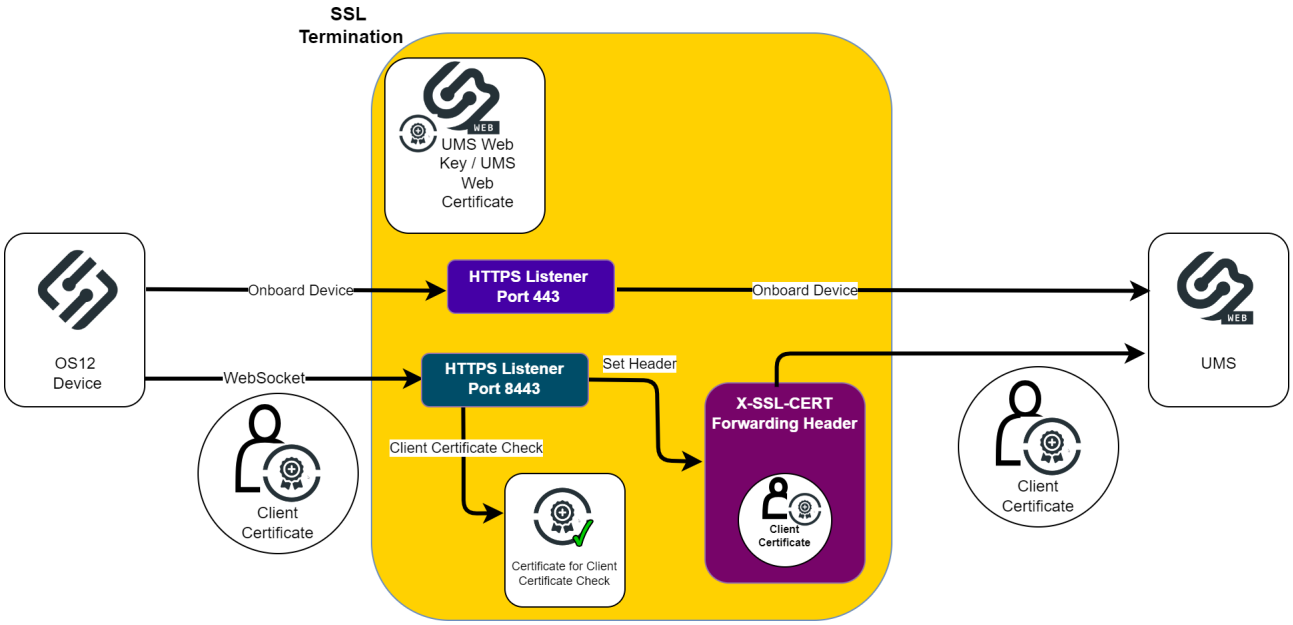
for device onboarding (Client Certificate request) and the following WebSocket connection where Mutual TLS and Client Certificate forwarding is required.



Communication via Azure Application Gateway

Some Reverse Proxies like NGINX support a Mutual TLS configuration with optional Client Certificate check. These Reverse Proxies can handle both required UMS connections with one configured listener. The Azure Application Gateway does not support this feature. The two types of connections used must be handled separately. According to this the Azure Application Gateway configuration must contain two separate listeners with corresponding rules.

The UMS supports the separation of the Onboarding and the WebSocket connections. The following diagram shows an overview of a device to UMS connection via the Application Gateway.



The HTTPS listener for device onboarding could use the standard https Port (443) and forwards direct to UMS.
In this example, the HTTPS listener for WebSocket connection listens on Port 8443 and uses mutual TLS for the Client Certificate Check and adds it to the Request Header, so that the UMS can verify it.

SSL Passthrough

SSL Passthrough passes encrypted HTTPS traffic from a client to the server and back again without any decryption or deep packet inspection. The HTTPS traffic is not manipulated so this configuration of network components shouldn't have any impact on the ICG or UMS functionality. Please refer to the documentation of your Web Component for the appropriate settings.

Example

nginx – one possible configuration of passthrough:

```
## tcp LB and SSL passthrough for backend ##
stream {
    upsream umsserver{
        server 192.168.1.100:8443 max_fails=3 fail_timeout=10s;
        server 192.168.1.100:8443 max_fails=3 fail_timeout=10s;
    }
    server{
        listen 443;
        proxy_pass umsserver;
        proxy_next_upstream on;
    }
}
```

The configuration must be added to the nginx config file:

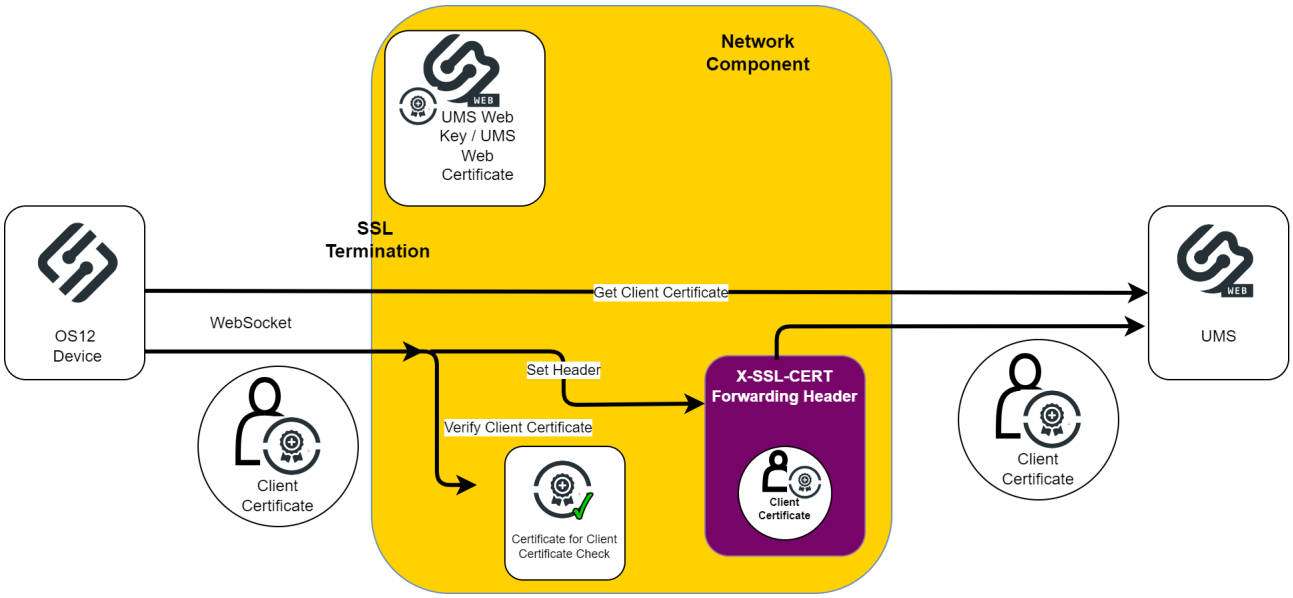
```
user nginx;
worker_process auto;
error_log /var/log/nginx/error.log warn;
pid       /var/run/nginx.ped;
events{
    worker_connections 1024;
}
http {
    include     /etc/nginx/mime.types;
    default_type application/octet-stream;
    sendfile    on;
    #tcp_nopush     on;
    keepalive_timeout 65;
    #gzip on;
    include/etc/nginx/conf.d/*.conf;
```

```
}
include/etc/nginx/passthrough.conf;
```

SSL Offloading

SSL Offloading means that the network component terminates the SSL connection and decrypts the data. This decrypted data could be sent directly to the Server which also sends decrypted data to the network component which handles the encryption.

The Network component could also inspect the decrypted traffic und encrypt it again before sending it to the server. The UMS supports only this type of communication with encrypted data until now. The diagram shows the required tasks for SSL Offloading on the Network Component for the device to UMS direction.



The Steps to configure SSL Offloading of a Network Component:

- Configure Listener for SSL Termination. This includes:
  - **Port**: UMS Web Port
  - Key and Certificate: UMS Web Key and UMS Web Certificate
- Configure Client Certificate Check and Client Certificate Forwarding. This includes:
  - SSL Client Certificate Check
  - Read SSL Client Certificate and add it to a Forwarded Header
- If necessary, configure the WebSocket Upgrade Header

The processing of forwarded Client Certificates must be activated on UMS side. The configuration file is `(Install Dir)/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml`.

```
igel:
```

```
client-cert-forwarding:
   enabled: false
   client-cert-forwarded-header: X-SSL-CERT
```

Set client-cert-forwarding -> enabled to true.

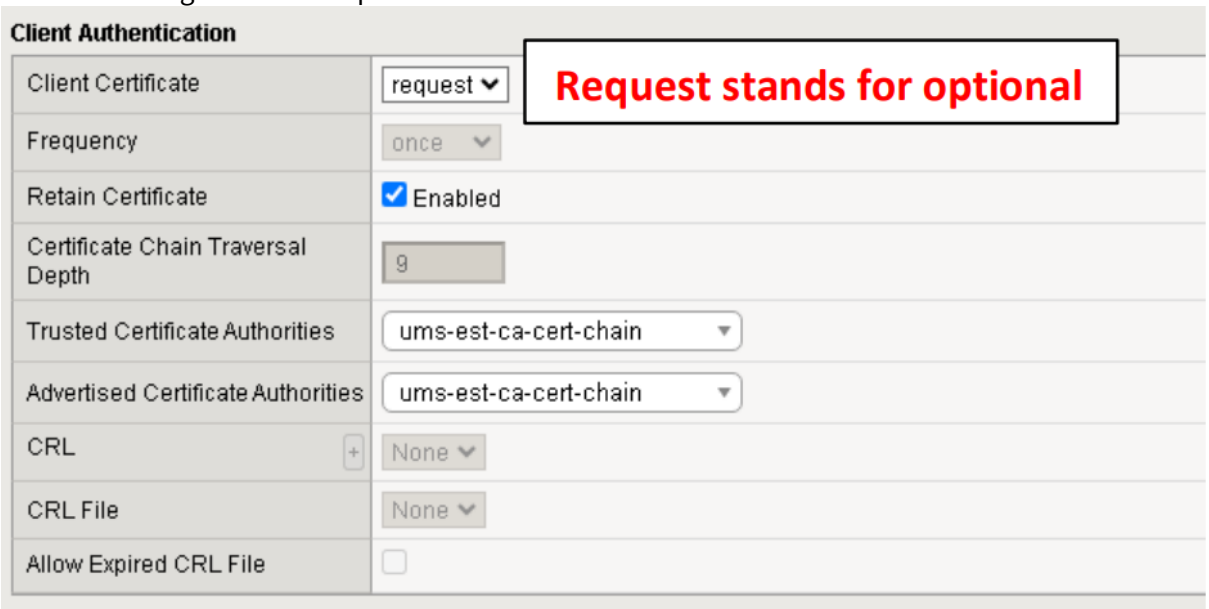
The forwarding Header can be configured. The X-SSL-CERT Header value can be changed but be aware to change the corresponding value in the network component configuration.
The ICG configuration is analog except for the ICG Port, ICG KEY and ICG Certificate parameters.
The processing of forwarded Client Certificates must also be activated on ICG side.
The configuration file is (Install Dir)/IGEL/icg/usg/conf/application-prod.yml

Required Features of the Network Component

Client Certificate check and forwarding

The OS12 device uses two types of connections to the UMS. One is a direct https connection to onboard the device and get a Client Certificate. The other one is a WebSocket connection for managing the device with mutual TLS. So, the used Reverse Proxy must at least implement one of the following configuration options:

- The **Client Certificate check is optional**, so the connection will always be forwarded but the certificate is only added when a valid certificate has been sent. Additionally, the WebSocket Upgrade must be supported.
  F5 BIG-IP configuration example:



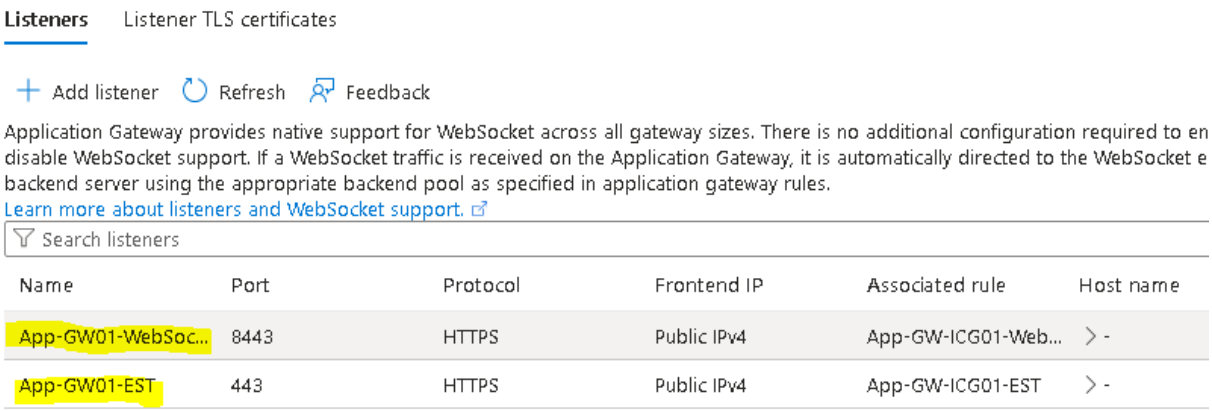
- **Path dependent forwarding** configuration must be supported. The NGINX Reverse Proxy supports this type. The listing shows a configuration for the WebSocket endpoint which requires

the Client Certificate, add it to the http header and add the WebSocket Upgrade header. See also, NGINX Example Configuration for Reverse Proxy in IGEL OS with SSL Offloading[79] .
The other configuration is required for the onboarding endpoint.
NGINX configuration example:

```
# Configuration for WebSocket Endpoints
 location~/device-connector/device/(ws-connect|portforwarding) {
    proxy_pass https://umsserver;
    proxy_set_header X-SSL-CERT $ssl_client_escaped_cert;# client certificate
in current connection
    proxy_set_header Upgrade $http_upgrade; #Set upgrade header
    proxy_set_header Connection $connection_upgrade;
}
#Configuration for all other endpoints
 location / {
    proxy_pass https//umsserver;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    proxy_ssl_protocols TLSv1.3;
}
```

- **Configuration of two endpoints** (that is, two Virtual Servers / Listeners) on the Reverse Proxy / Loadbalancer. One endpoint is configured for the device onboarding and another one for the WebSocket connection.

Azure Application Gateway configuration example:



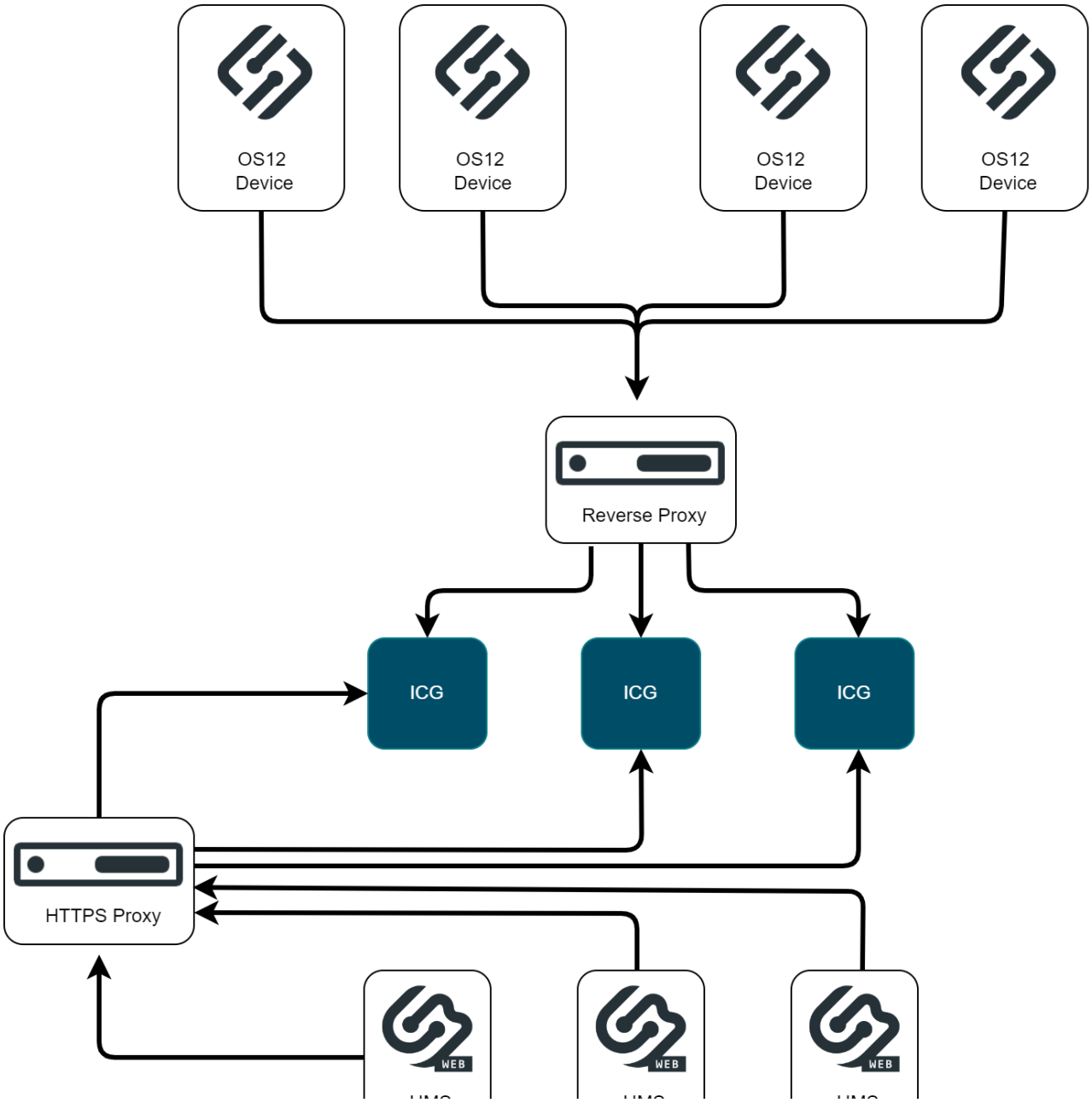
UMS HA environment with Reverse Proxy, Loadbalancer

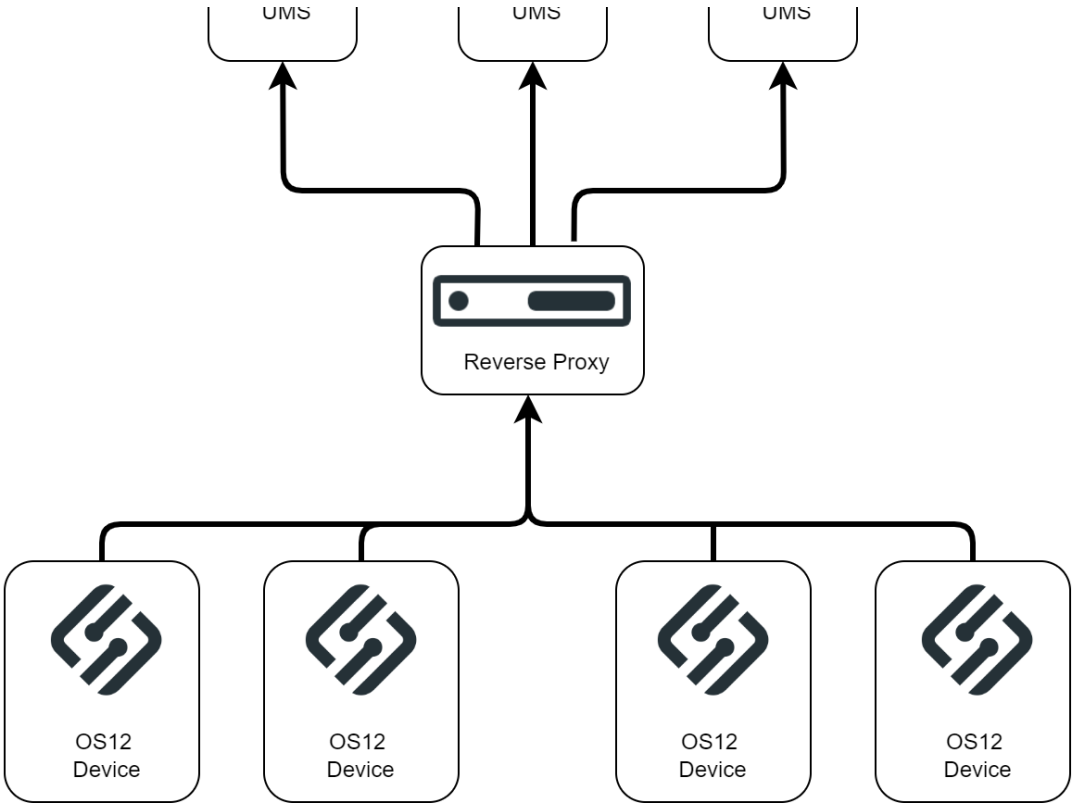
The device to UMS / ICG connection can be load balanced.
The UMS Web certificate and ICG certificate must correspond to the IP or Fully Qualified Domain Name of the servers and configured network component. Consider the Subject Alternative Names of the certificate. Wildcard

79. https://kb.igel.com/en/universal-management-suite/current/nginx-example-configuration-for-as-reverse-proxy-i

certificates are possible. Be aware to set the UMS cluster address and the UMS public address.
The example shows a nginx upstream server configuration with multiple UMS server entries.

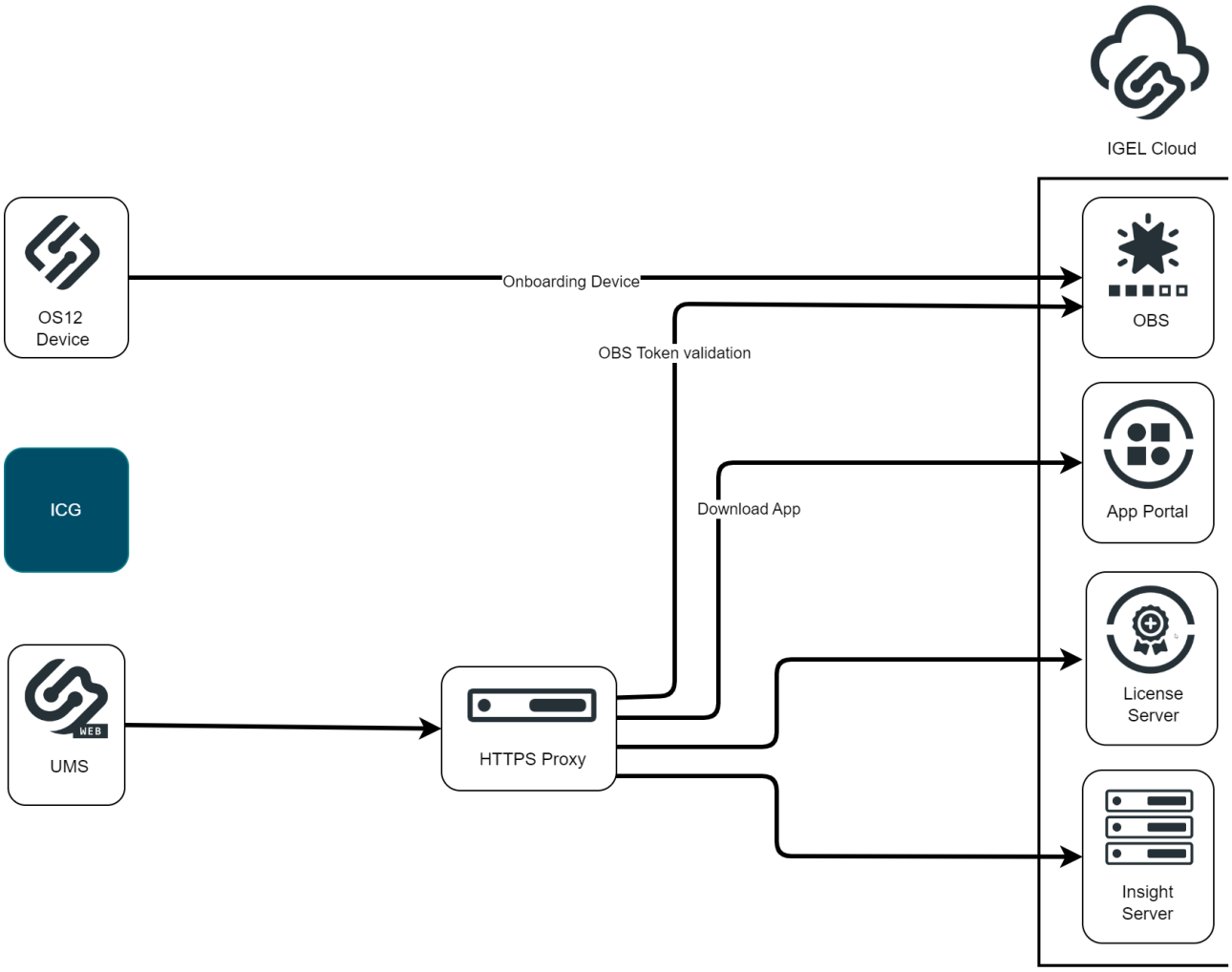
```
upstream umsserver {
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
 }
```





IGEL Cloud Service Configuration

The communication to the IGEL Cloud might be influenced also by network components. In case of the device onboarding via the Onboarding Service, the OBS must be reachable for the device. The UMS server also connects to the IGEL Cloud Services. Here the required reachable services are the Onboarding Service (OBS), the IGEL License Portal (ILP), the IGEL App Portal and the Insight Service. These connections can go over a Proxy but must be configured in the UMS. A network component like a firewall with Deep Packet Inspection could result in connection problems.



UMS Endpoint Paths for Reverse Proxy Integration

The paths required for OS 12 device connections to the UMS (via a reverse proxy) are:

- Root path: `/device-connector/device/*`
- Detailed paths:
  - `/device-connector/device/ws-connect`
  - `/device-connector/device/portforwarding`
  - `/device-connector/device/.well-known/est/*`
- App proxy path: `/ums-appproxy/*`

The device communication is always TLSv1.3.

In case the UMS Web App should be used via a reverse proxy, the following paths are required:

- `/wums-app/*`
- `/webapp/*`

The device communication is TLSv1.2 or TLSv1.3.

Configure the UMS to Integrate Reverse Proxy with SSL Offloading

This article describes the general configurations of the IGEL Universal Management Suite (UMS) for SSL offloading with a load balancer / reverse proxy. You can use this document when you want the SSL to be terminated not at the UMS Server, but at the load balancer / reverse proxy.

> A reverse proxy / external load balancer can be used if you manage IGEL OS 12 devices only. See https://igel-jira.atlassian.net/wiki/pages/createpage.action?spaceKey=enliteumsp&title=%2812.09.110-en%29%20IGEL%20Cloud%20Gateway%20vs.%20Reverse%20Proxy%20for%20the%20Communication%20between%20UMS%2012%20and%20IGEL%20OS%20Devices&linkCreation=true&fromPageId=540640731 .

Requirements of Reverse Proxy Configuration

- IGEL UMS version 12.04.100 or higher
- IGEL OS version 12.3.2 or higher
- If the ICG is used: ICG version 12.04.100 or higher
- In the case of the Distributed UMS or High Availability installations (see page 13), the time must be synchronized on all servers.

> For extracting keys and certificate chains, you will require a suitable tool like "Keystore Explorer". Please use the latest version of such tools.
> Please also make sure that you use Java 17.

Limitations

- The scan and register command 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, the scan and register feature might not be usable.

Process Overview

We advise you to follow the process presented here. Before starting the UMS configuration, take a look at the UMS network connection types described in IGEL Universal Management Suite Network Configuration[80] .

- Configure your UMS / ICG:
  a. Activate forwarding client certificate processing on UMS / ICG.
  b. Modify server network settings and set process configuration.

- Configure and export the certificates for the reverse proxy:
  a. Configure UMS Web Certificate. / If ICG is used, configure Cloud Gateway certificate.
  b. Export the UMS Web certificate chain / If ICG is used, Cloud Gateway certificate chain.
    - Extract private key and certificate chain from the exported certificate. (The necessary file formats depend on the reverse proxy.)
  c. Export the EST CA Client Certificate.

80. https://kb.igel.com/en/universal-management-suite/current/igel-universal-management-suite-network-configurat

d. Export UMS Web Root Certificate / If ICG is used, Cloud Gateway Root Certificate. (Only needed for Azure Application Gateway if trust to the backend server must be verified.)

The next step is the configuration of the reverse proxy. For example configurations, see:

- NGINX Example Configuration for Reverse Proxy in IGEL OS with SSL Offloading[81]
- F5 BIG IP Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading[82]
- Azure Application Gateway Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading[83]
- Citrix Netscaler Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading[84]

Monitoring - Health Probe of UMS / ICG

Load balancers use health probes for detecting the online state of the backends to distribute data to them. If a custom HTTP probe should be used for monitoring the UMS/ICG service, the following URLs can be configured for testing:
UMS:

- `https://UMS_URL:8443/info` or
- `https://UMS_URL:8443/ums/check-status`

ICG:

- `https://UMS_URL:8443/usg/server-status` or
- `https://UMS_URL:8443/usg/check-status`

Activate Forwarding Client Certificate Processing on UMS / ICG

If no ICG is used, the processing of forwarded Client Certificates must be activated on UMS side. In case only an ICG is used behind an Azure Application Gateway, activate the processing of forwarded Client Certificates on ICG side.

To activate forwarding Client Certificate processing on UMS:

1. Open the configuration file `[UMS installation directory]/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml`.
   You will see:

```
igel:
    client-cert-forwarding:
        enabled: false
        client-cert-forwarded-header: X-SSL-CERT
```

81. https://kb.igel.com/en/universal-management-suite/current/nginx-example-configuration-for-as-reverse-proxy-i
82. https://kb.igel.com/en/universal-management-suite/current/f5-big-ip-example-configuration-as-reverse-proxy-i
83. https://kb.igel.com/en/universal-management-suite/current/azure-application-gateway-example-configuration-as
84. https://kb.igel.com/en/universal-management-suite/current/citrix-netscaler-example-configuration-as-reverse-

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

```
client-cert-forwarding:
    enabled: true
```

3. If required, the forwarding header can be configured. The X-SSL-CERT Header value can be changed but be aware to change the corresponding value in the proxy configuration.
4. Save the configuration changes and restart the UMS Server service. For details on how you can restart the service, see https://igel-jira.atlassian.net/wiki/pages/createpage.action?spaceKey=enliteumsp&title=%2812.09.110-en%29%20IGEL%20UMS%20HA%20Services%20and%20Processes&linkCreation=true&fromPageId=540640731 .

To activate the processing of forwarded Client Certificates on ICG side:

1. Open the configuration file `[UMS installation directory]/IGEL/icg/usg/conf/application-prod.yml`.
   You will see:

```
igel:
    client-cert-forwarding:
        enabled: false
        client-cert-forwarded-header: X-SSL-CERT
```

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

```
client-cert-forwarding:
    enabled: true
```

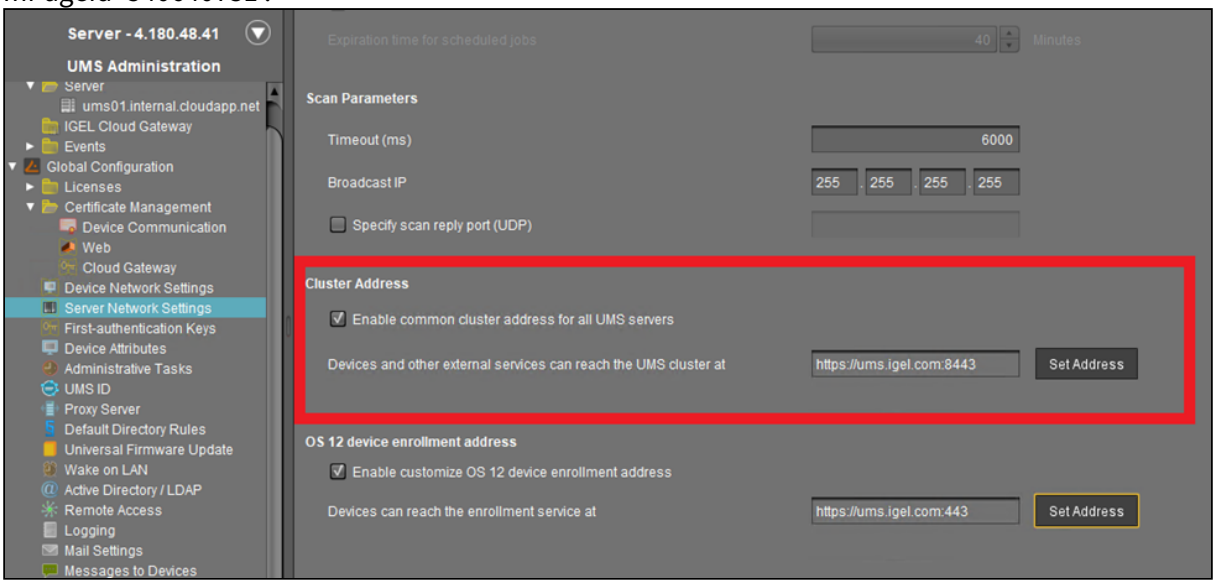
3. If required, the forwarding header can be configured. The `X-SSL-CERT` header value can be changed but be aware to change the corresponding value in the proxy configuration.
4. Save the configuration changes and restart the ICG server.

Modify Server Network Settings

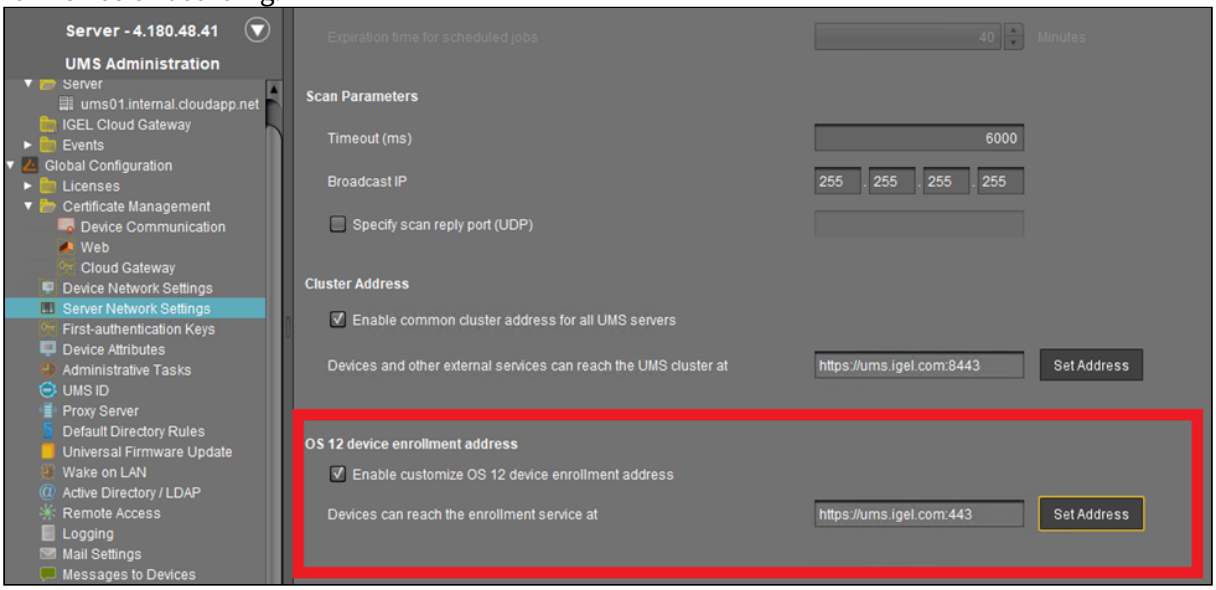
If you are using an external load balancer / reverse proxy, you have to update the FQDN of the UMS cluster as an external address. This FQDN of the UMS cluster must be included into your web certificate, and the corresponding certificate must be assigned to all UMS servers:

1. Go to **UMS Administration > Global Configuration > Server Network Settings**.
2. Set the **Cluster Address**.
   If you are using a Reverse Proxy, you will need to update the FQDN of the UMS cluster as external

address. This value must be set to the FQDN and Port of the Reverse Proxy. For detailed information, see https://igel-jira.atlassian.net/wiki/pages/createpage.action?spaceKey=enliteumsp&title=%2812.09.110-en%29%20Server%20Network%20Settings%20in%20the%20IGEL%20UMS&linkCreation=true&fromPageId=540640731 .

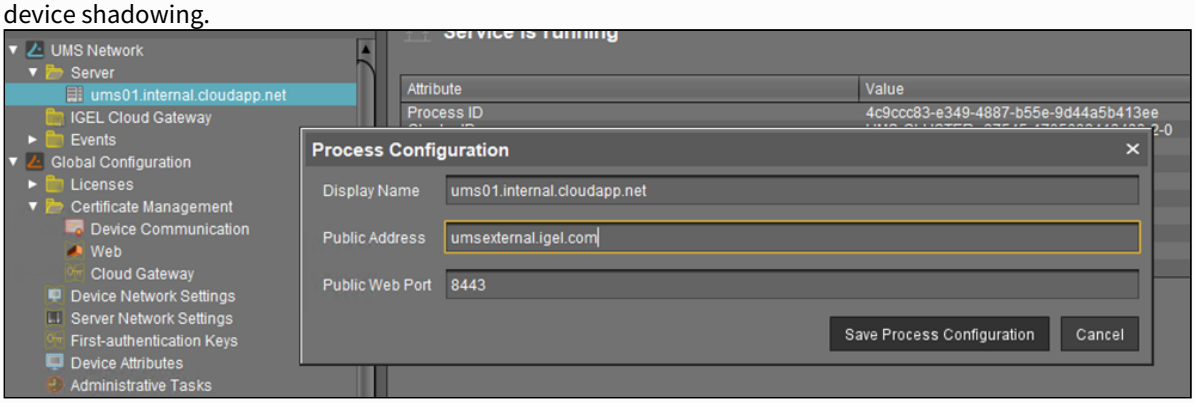


3. Set the **OS 12 device enrollment address** (this is the address used for device onboarding). This configuration must be set for Reverse Proxy without optional Client Certificate verification option like Azure Application Gateway. Set it to the FQDN / IP and Port of the configured listener for Device onboarding.



Set Public Address and Port of the UMS Process Configuration

In case the public address of the UMS differs from the UMS address, the public address and port must be set. This option can be set under **UMS Administration > UMS Network > Server**. This is essential for device shadowing.



Create UMS Web Certificate / Cloud Gateway Certificate

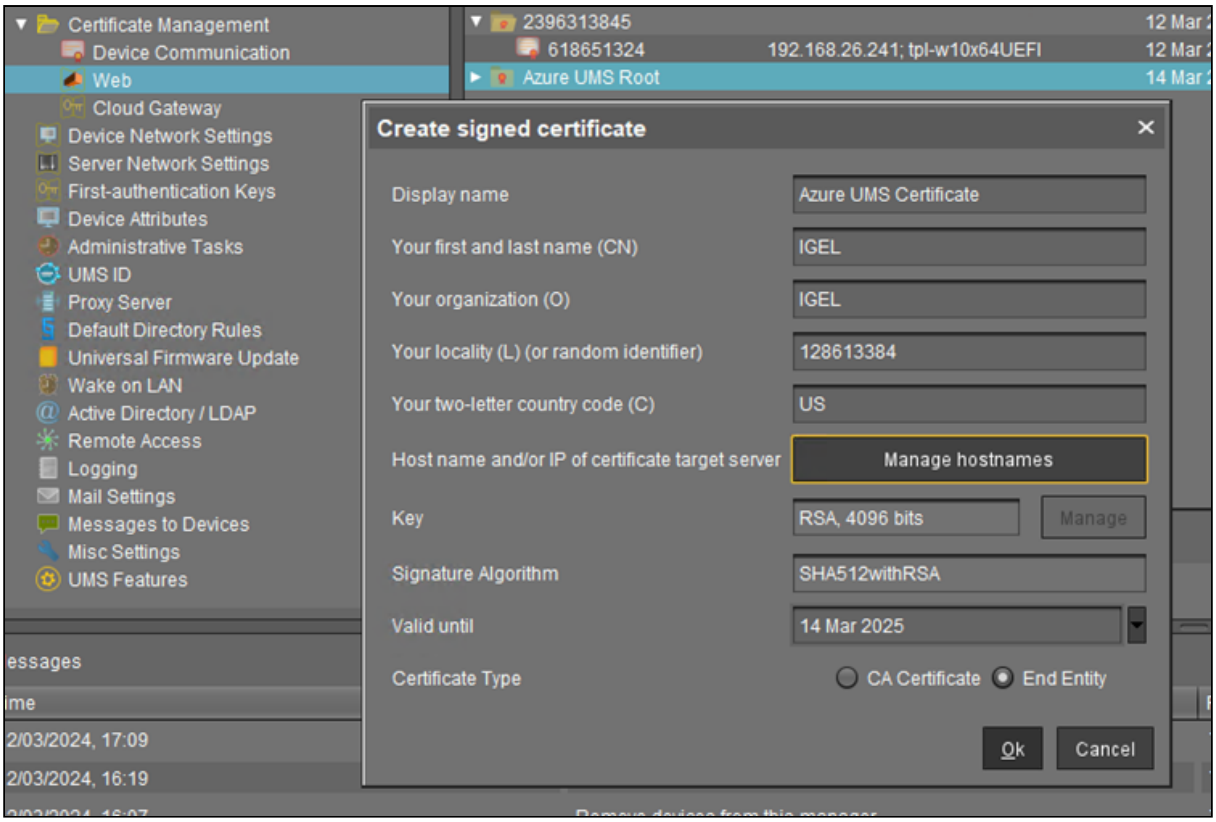
UMS Web Certificate

Web Certificate from Public CA

In case a Web Certificate from a public CA is used, the issuer public certificate must also be imported as Web Certificate.
The onboarding of OS 12 devices will only be successfull with a complete certificate chain.

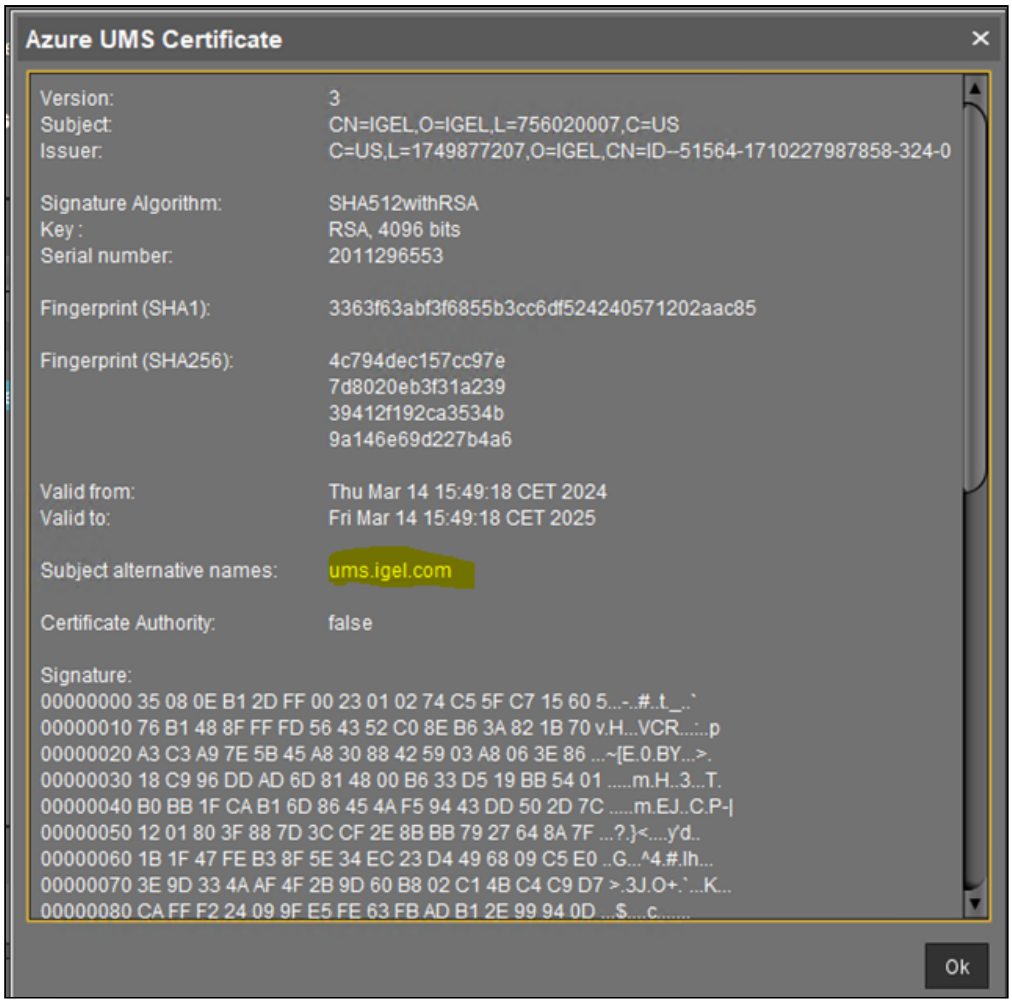
You need to create and use a valid certificate for UMS and Loadbalancer. The suggested approach is to use an own certificate for the Reverse Proxy:

1. Go to **UMS Administration > Certificate Management > Web** in the UMS Console.
2. Create the certificate. For details, see https://igel-jira.atlassian.net/wiki/pages/createpage.action?spaceKey=enliteumsp&title=%2812.09.110-en%29%20How%20to%20Use%20Your%20Own%20Certificates%20for%20Communication%20over%20the%20Web%20Port%20%28Default%208443%29%20in%20IGEL%20UMS&linkCreation=true&fromPageId=540640731 . For general information on web certificates, see https://igel-jira.atlassian.net/wiki/pages/createpage.action?spaceKey=enliteumsp&title=%2812.09.110-en%29%20Web%20Certificates%20in%20the%20IGEL%20UMS&linkCreation=true&fromPageId=540640731 .



3. The proxy FQDN must be added as Hostname so that in the Certificate it is listed as a Subject Alternative Name.

Use subject alternative names (SAN) if the IP addresses or hostnames that are used for the UMS and your load balancer / reverse proxy are different. For information on hostnames, Cluster Address, FQDNs, see also (en) Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device .



Cloud Gateway Certificate

> Certificate from Public CA
>
> In case a certificate from a public CA is used, the issuer public certificate must also be imported as Cloud Gateway certificate.
> The onboarding of OS 12 devices will only be successfull with a complete certificate chain.

When you use the reverse proxy with ICG:

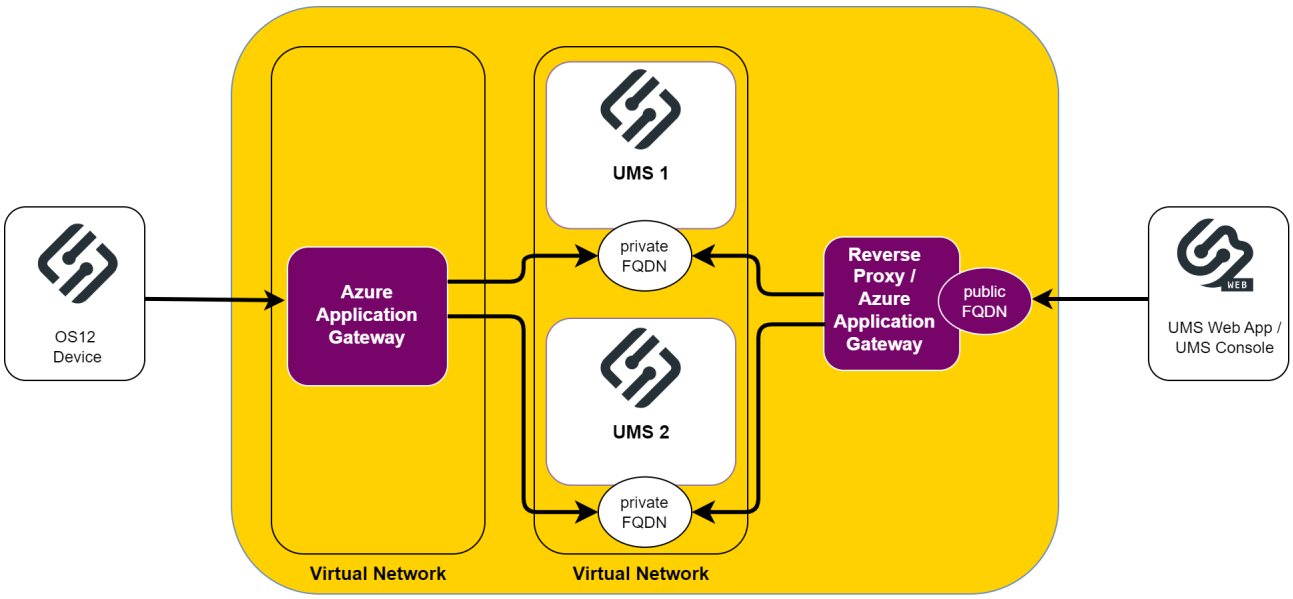
1. Go to **UMS Administration > Certificate Management > Cloud Gateway** in the UMS Console.
2. Create the certificate and add the IP or Hostname of the Loadbalancer at the ICG Certificate generation. Use a semicolon to separate the values.

UMS and ICG Certificates Examples

The network integration of Reverse Proxies and Loadbalancers with the UMS and ICG is a wide area with a lot of possible network settings. Here are two Azure Application Gateway examples listed with appropriate certificate details:

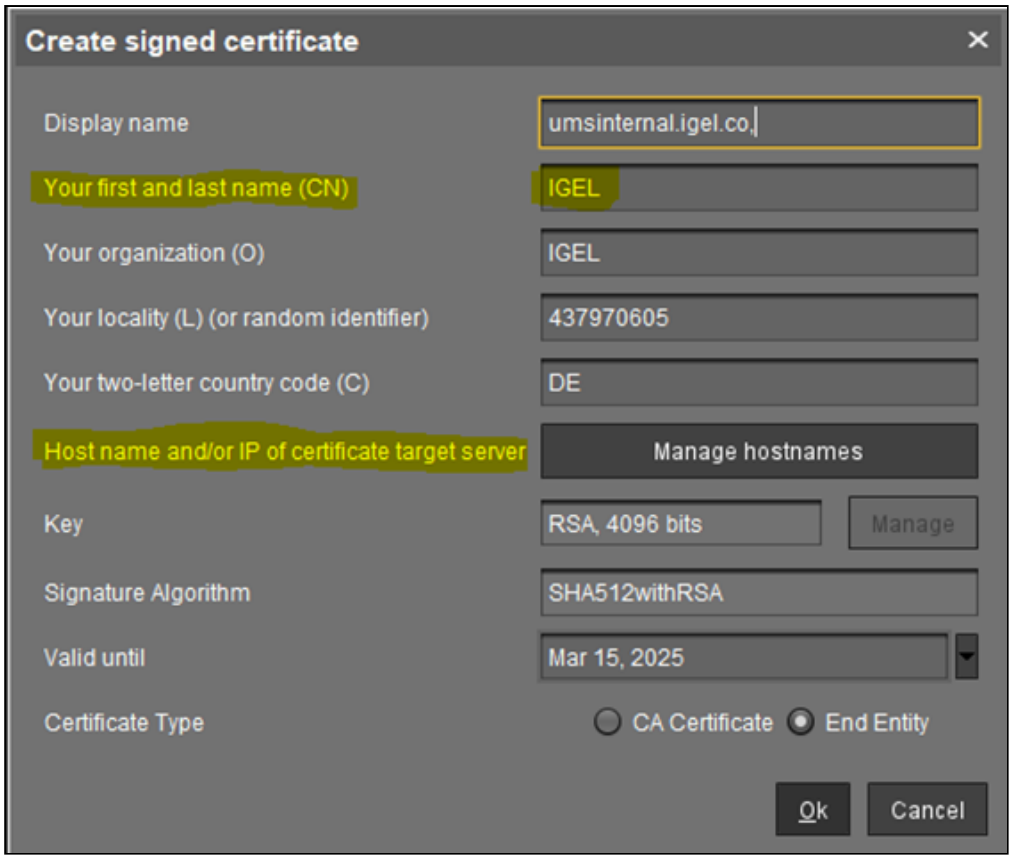
UMS Example

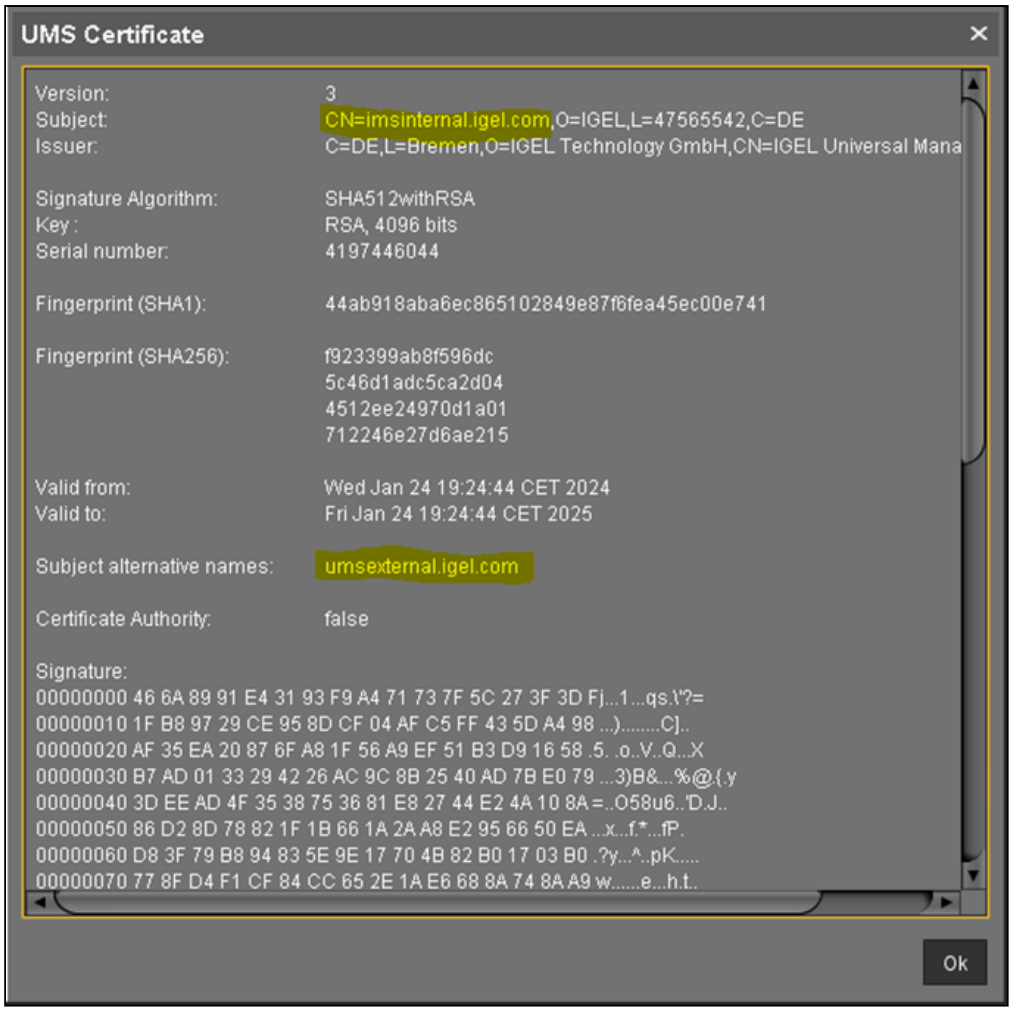
This diagram shows an Azure Application Gateway in front of UMS servers.



These UMS servers are within a Virtual Network and only reachable by a private FQDN. There is one Azure Application Gateway for incoming Device requests and another Reverse Proxy / Loadbalancer (Azure Application Gateway) for UMS Web App and Console requests. So the UMS server is reachable by two different addresses. This must be considered for **Web** certificate generation.

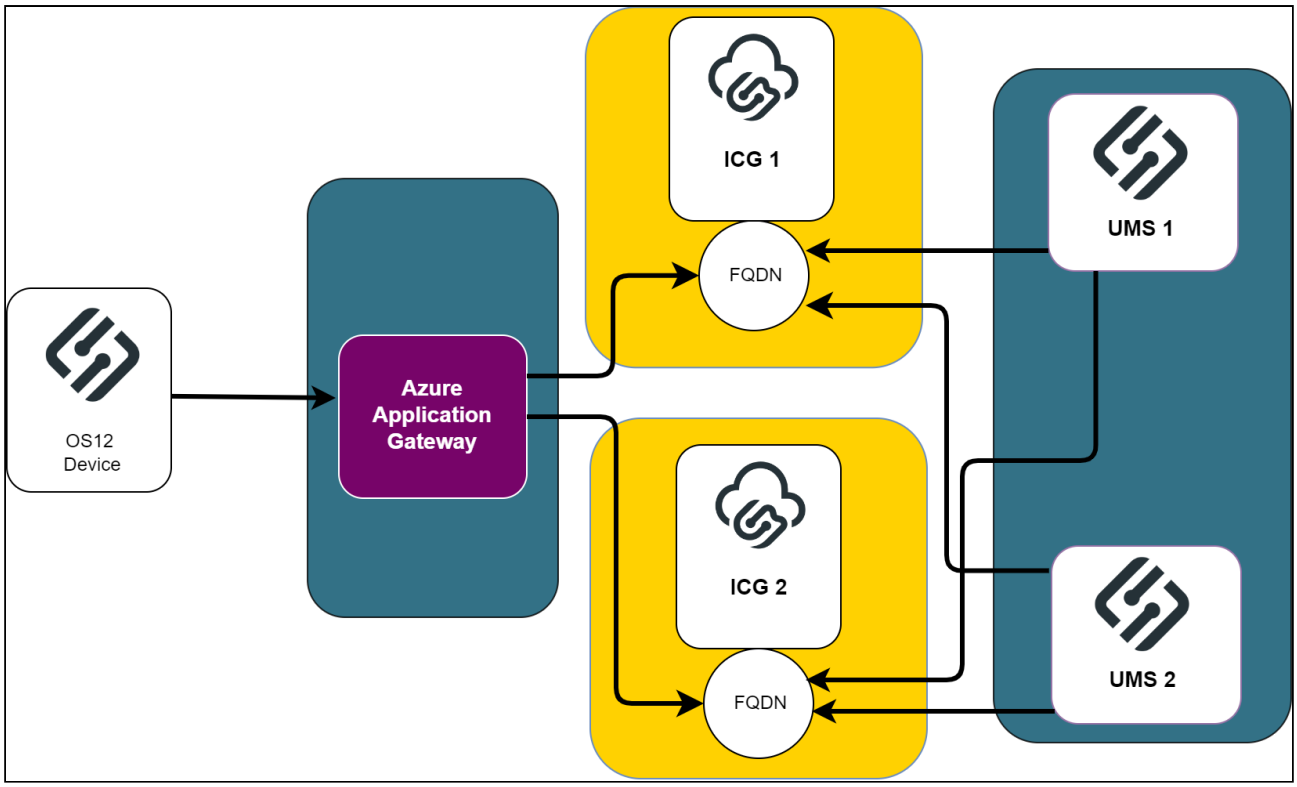
The private FQDN address is used by the Azure Application Gateway for UMS connection. This address **must be set as Common Name (CN)** to the UMS Web certificate. The public FQDN must be set for UMS Web App / Console connections to the UMS as Hostname (Subject Alternative Name).


Create signed certificate
Display name
umsinternal.igel.co
Your first and last name (CN)
IGEL
Your organization (O)
IGEL
Your locality (L) (or random identifier)
437970605
Your two-letter country code (C)
DE
Host name and/or IP of certificate target server
Manage hostnames
Key
RSA, 4096 bits
Manage
Signature Algorithm
SHA512withRSA
Valid until
Mar 15, 2025
Certificate Type
CA Certificate
End Entity
Ok
Cancel



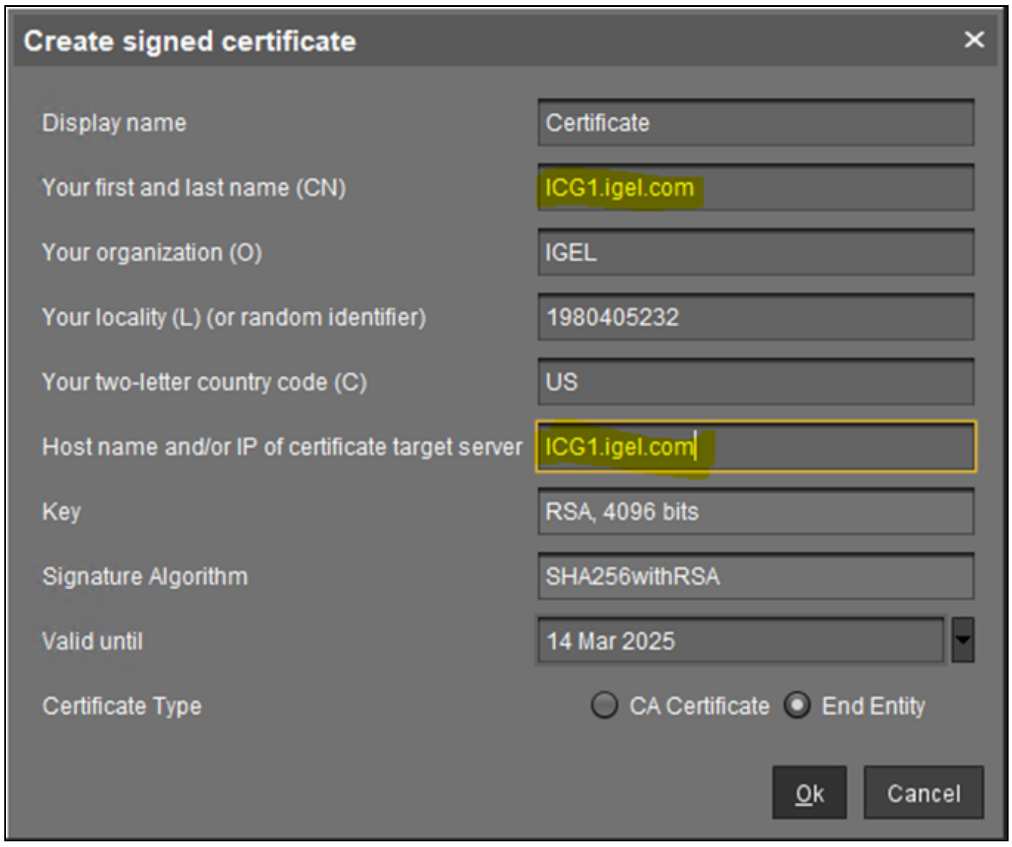
ICG Example

The diagram shows an example of Azure Application Gateway and ICG integration.



In this scenario the Azure Application Gateway connects to the ICG via the same FQDN as the UMS server. The ICG might be in a DMZ so only one FQDN is required.

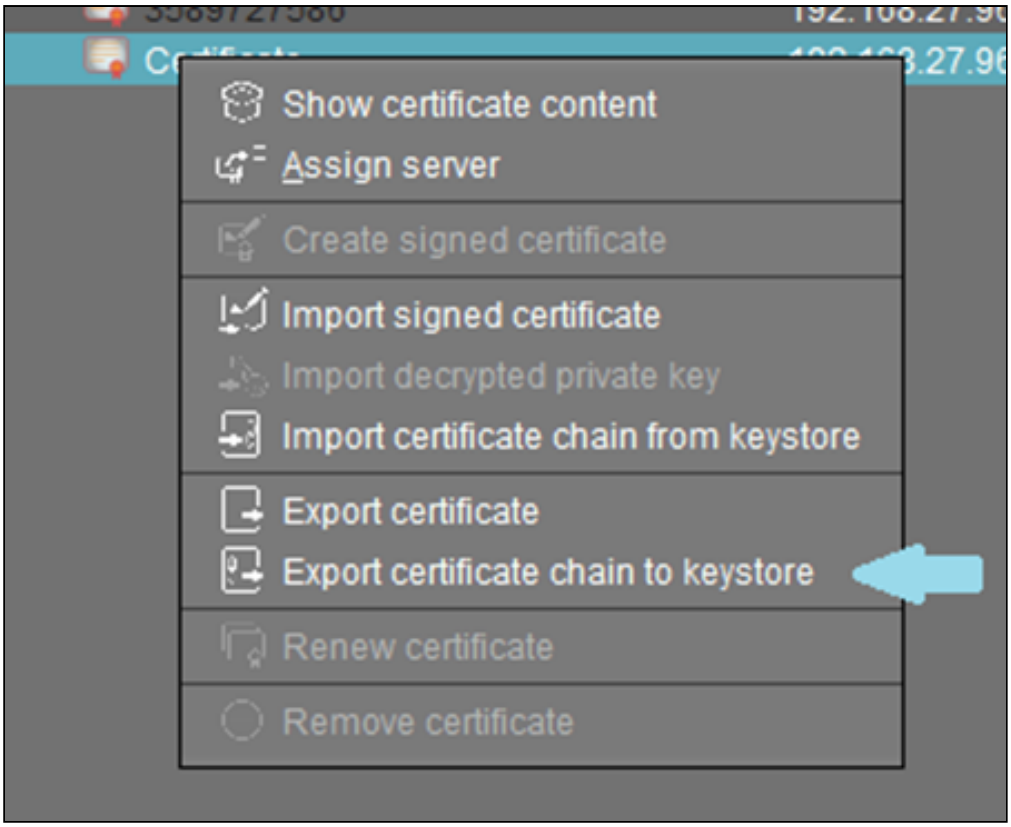
The **Cloud Gateway** certificate requires the **FQDN as Common Name** and as **Subject Alternative Name** for UMS management.



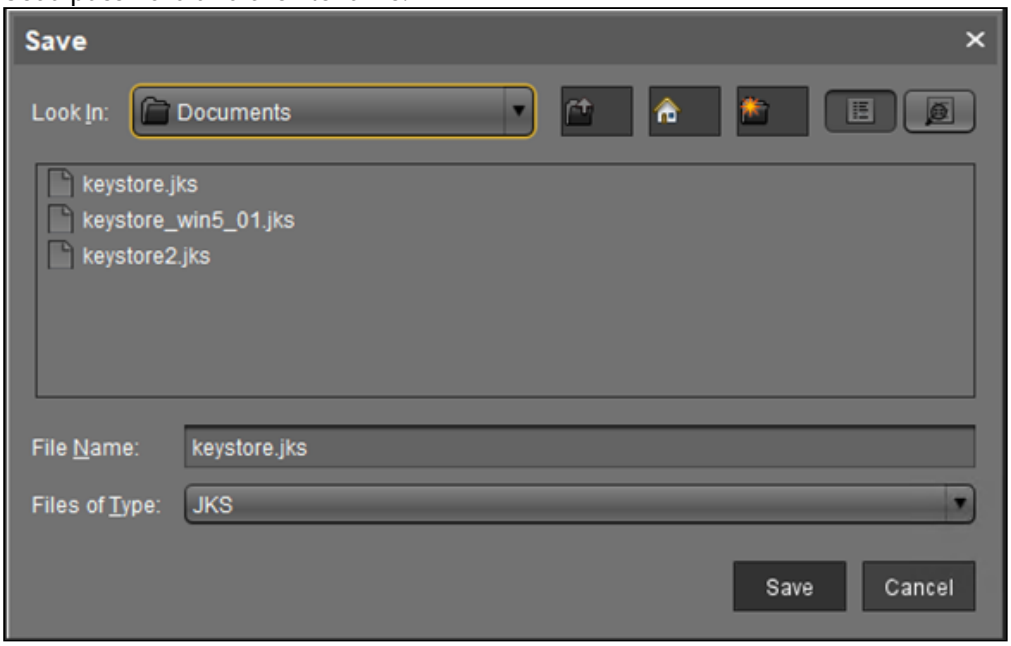
Export UMS Web Certificate Chain

This certificate must be exported for use in the Listener configuration.

1. Select the previously configured certificate and click **Export certificate chain to keystore**.

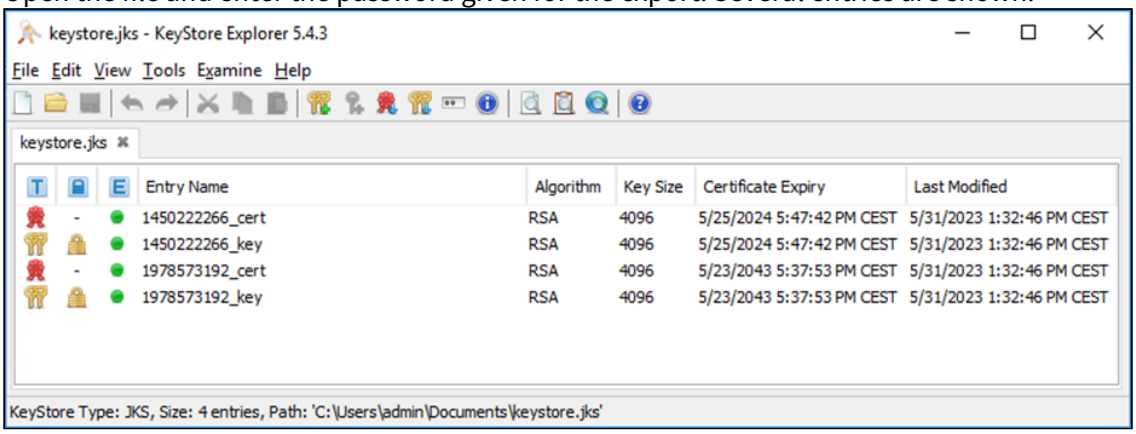


2. Set a password and the filename.

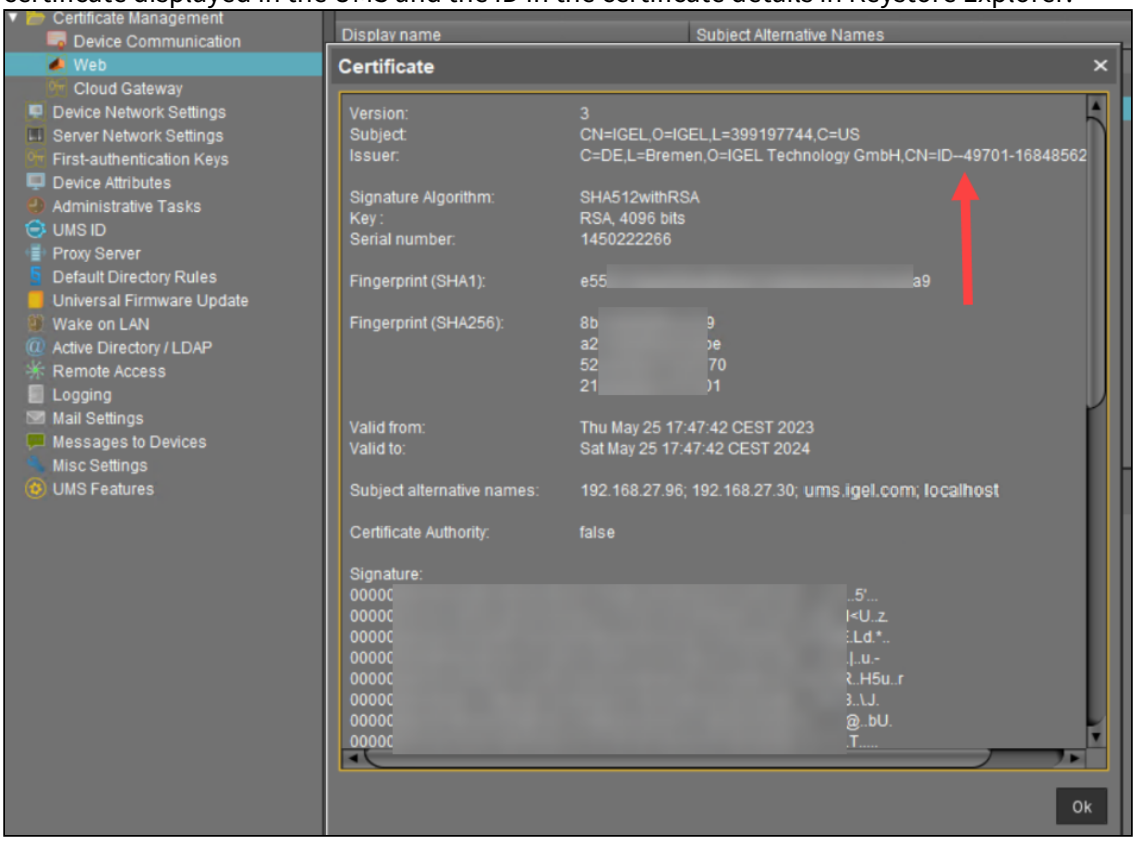


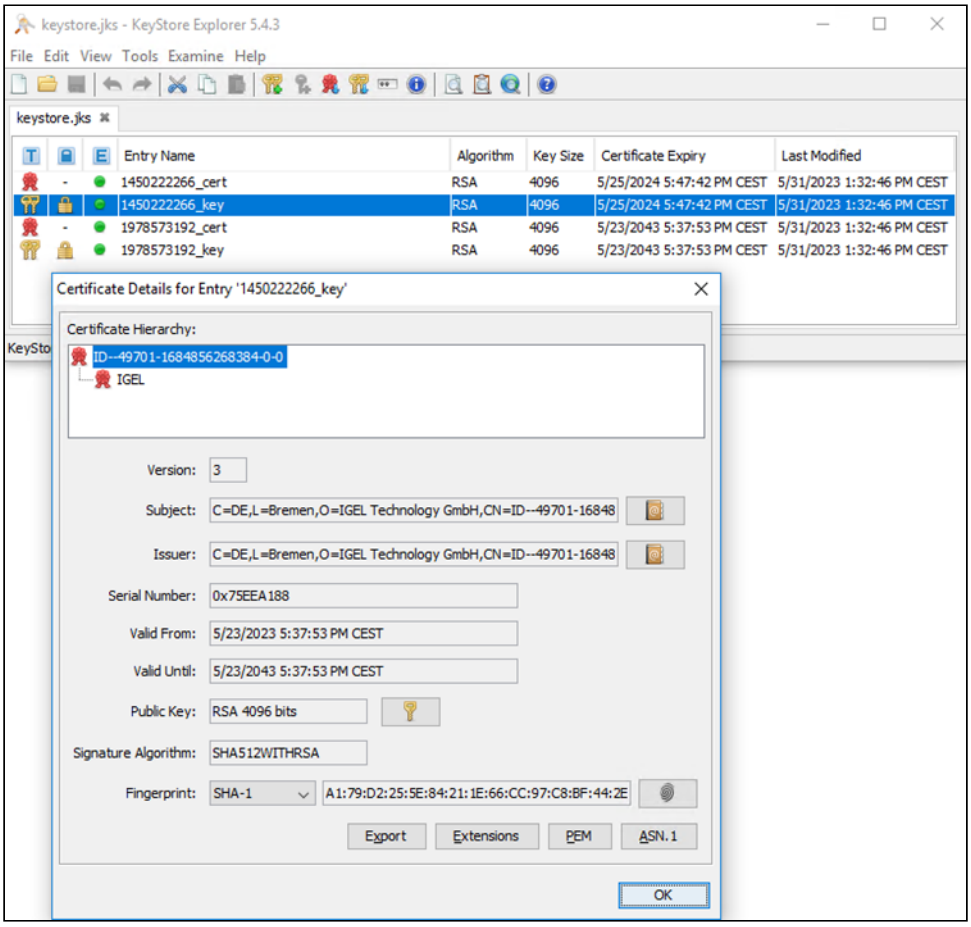
3. Identify the Web key.
   The exported keystore file contains several keys and certificates, at least the root and the currently used keys and certificates. A tool like Keystore Explorer can be used to identify the currently used Web key.
   How to find the currently used web key with Keystore Explorer

   a. Open the file and enter the password given for the export. Several entries are shown:



   b. Find the currently used key. For this, you can simply compare the ID of the currently used certificate displayed in the UMS and the ID in the certificate details in Keystore Explorer.





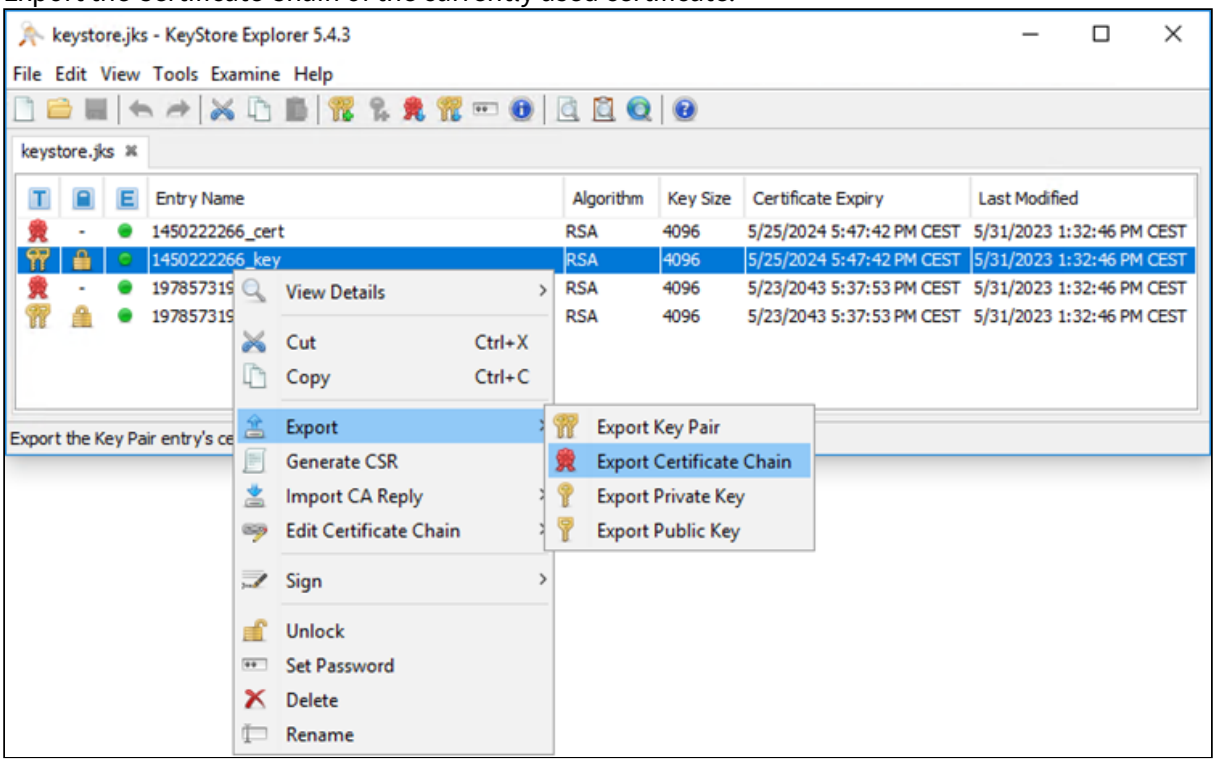
Extract Private Key and Certificate Chain

Different reverse proxies require different certificate files. For Azure Application Gateway, the key for the listener configuration is required in a `PFX` formatted file. Parse the exported keystore file to the `PFX` format. The java keytool command can be used. The command line tool can be found in the UMS installation: `(Install Dir)/IGEL/RemoteManager/_jvm/bin`
The **key alias** must be added to the call of command.

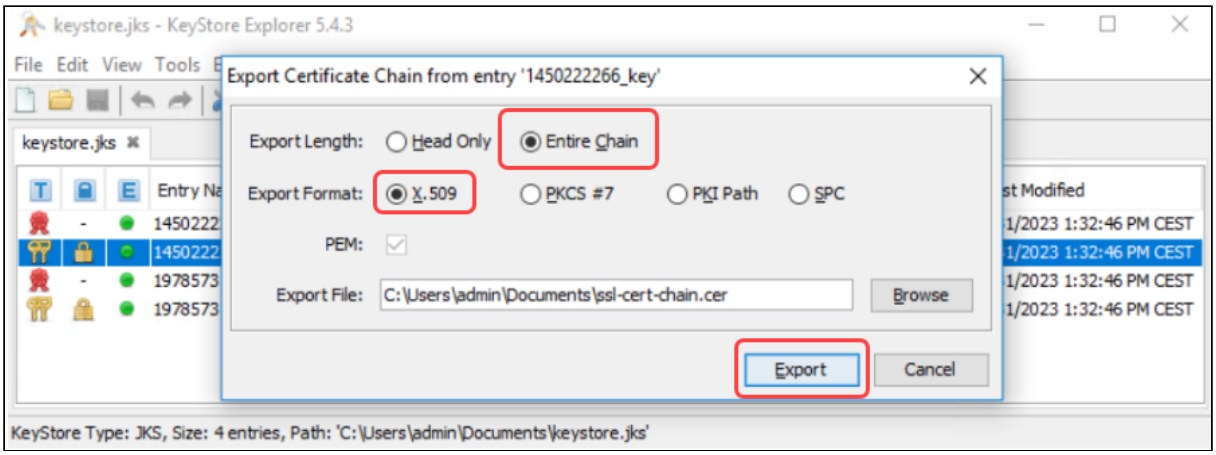
```
keytool -v -importkeystore -srckeystore  yourkeystore.keystore -srcalias mykey
-destkeystore myp12file.pfx -deststoretype PKCS12
```

For Citrix Netscaler, F5 Big IP and NGINX the certificate chain and the private key need to be exported:

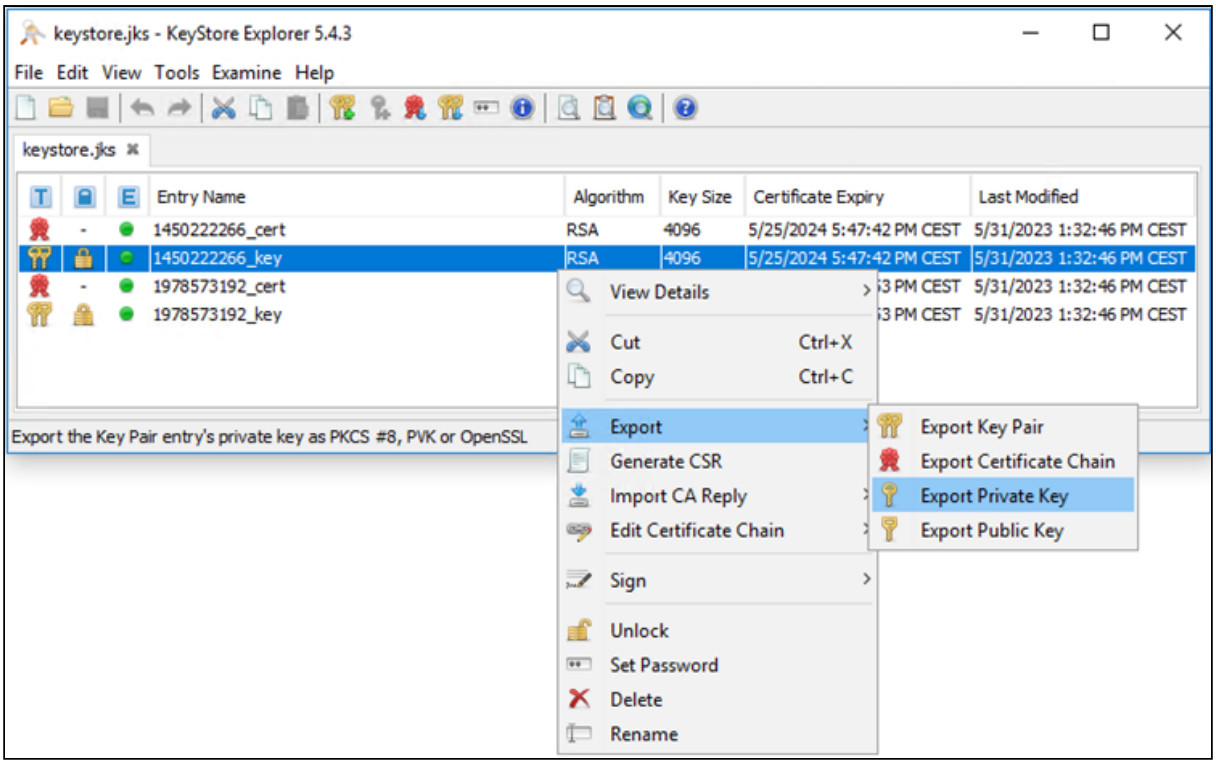
1. Export the Certificate Chain of the currently used certificate.



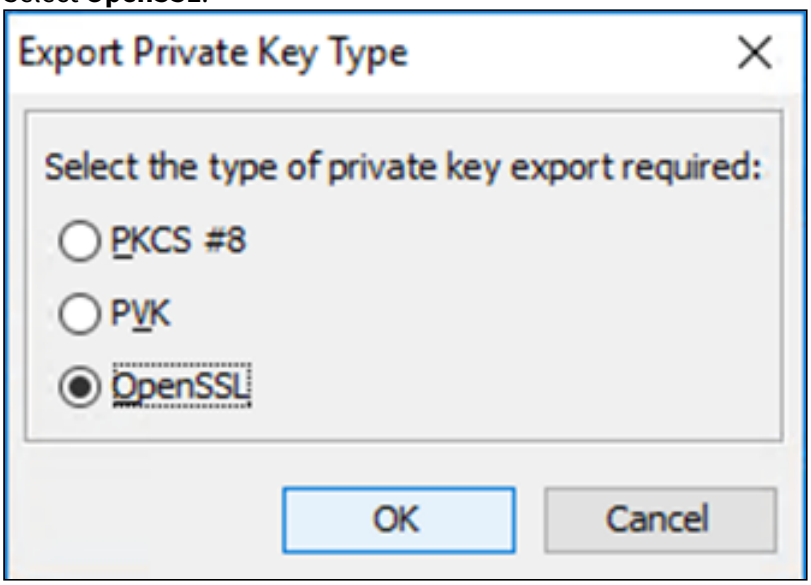
2. Select **Entire Chain** and **X.509** format.



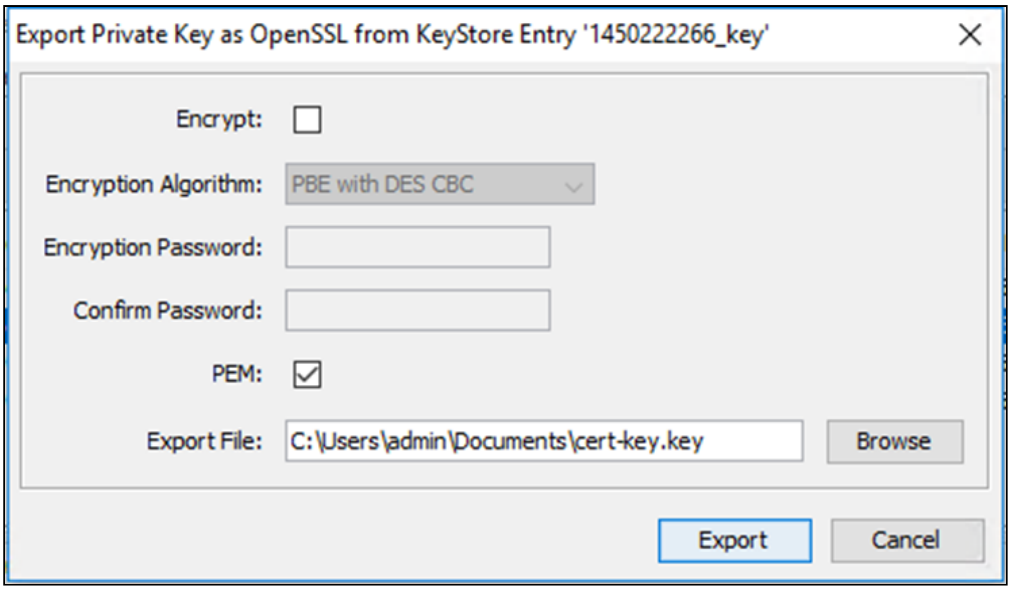
3. Click **Export**.
4. For F5 Big IP: Also select **Head only** and export the certificate to another file for example: `ssl-cert.cer`
5. Export the Private Key.



6. Enter the password you used in the UMS for the export.
7. Select **OpenSSL**.



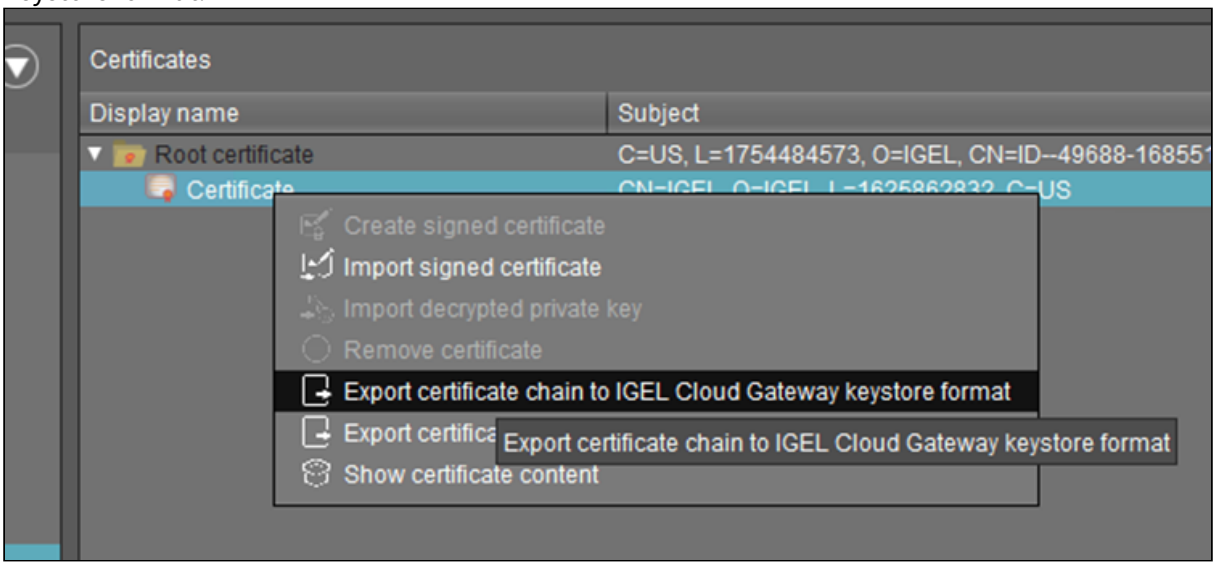
8. If required, select **Encrypt** and enter the corresponding data. In this example, we will use a not encrypted key file.



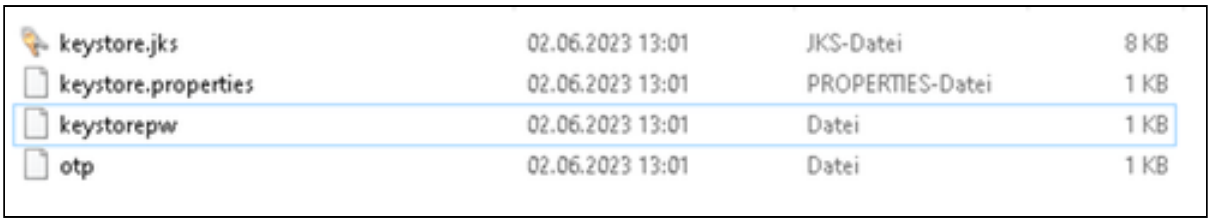
9. Click **Export**.

Export Cloud Gateway Certificate Chain and Extract Key and Certificate Chain

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** and export the ICG certificate chain to IGEL Cloud Gateway keystore format:



   The `keystore.icg` file will be saved.
2. Unzip the file.
3. Open the keystore.jks file and use the password from the `keystorepw` file.

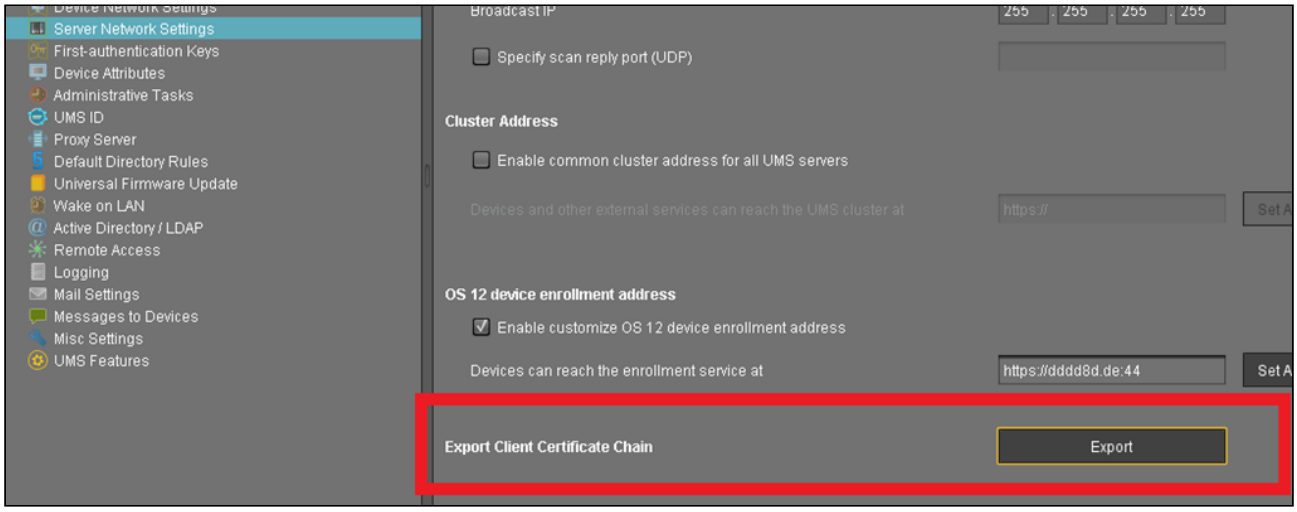


4. Select the configured key entry and export the private key and certificate chain as described in the section Extract Private Key and Certificate Chain (see page 291).

Export EST CA Client Certificate Chain

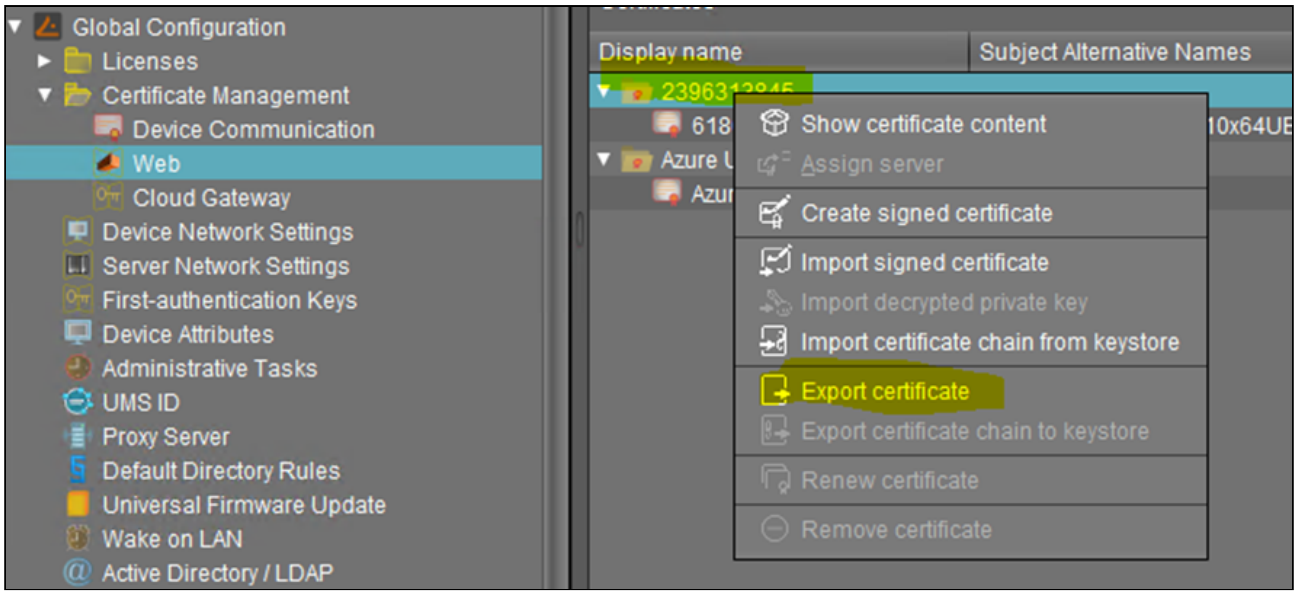
The EST CA Client Certificate is required for the Client Certificate check.

The Client Certificate Chain export can be found under: **UMS Administration > Server Network Settings > Export Client Certificate Chain**.



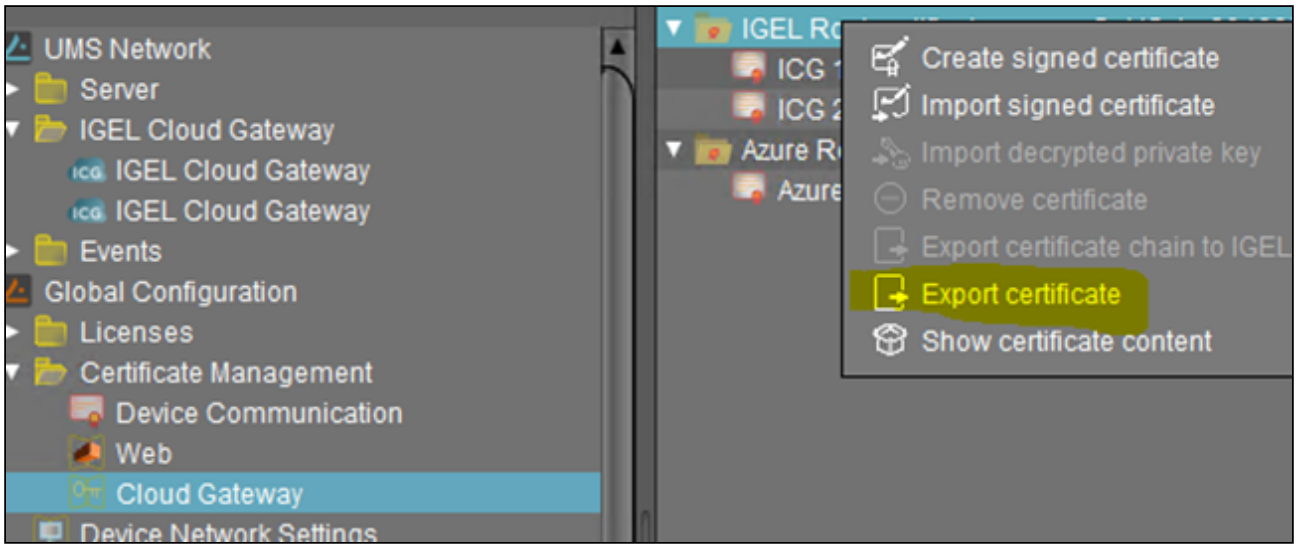
Export UMS Web Root Certificate for Azure

In the Azure Application Gateway, the Root Certificate is used for the Backend Settings configuration. The root certificate of the used Web certificate must be exported under **UMS Administration > Global Configuration > Certificate Management > Web**.



Export Cloud Gateway Root Certificate for Azure

In the Azure Application Gateway, the Root Certificate is used for the Backend Settings configuration. The root certificate of the used Cloud Gateway Root certificate under **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**.



Next Step: Managing Devices Connected through Reverse Proxy

You can find a list of useful features that support the management of devices connected through a reverse proxy under Useful IGEL UMS Features for Managing Reverse Proxy Connected Devices[85].

85. https://kb.igel.com/en/universal-management-suite/current/useful-igel-ums-features-for-managing-reverse-prox

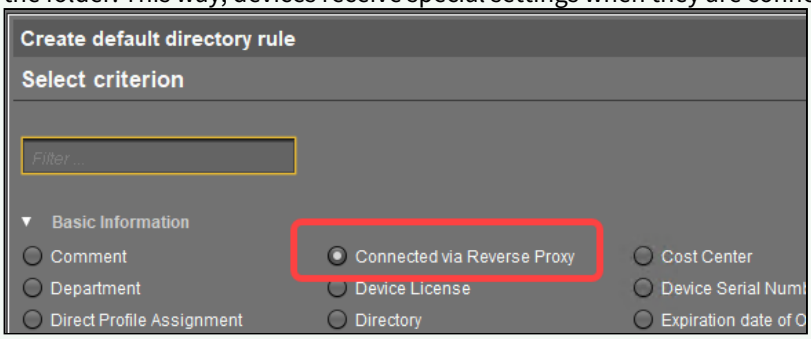
NGINX Example Configuration for Reverse Proxy in IGEL OS with SSL Offloading

This article describes the configuration of the IGEL Universal Management Suite (UMS) and NGINX for SSL offloading. You can use this document when you want the SSL to be terminated not at the UMS Server, but at the load balancer / reverse proxy. The article is based on the example of NGINX. For more information on NGINX, see https://www.nginx.com/resources/glossary/nginx/.

⚠ General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
As the reverse proxy is an external software we cannot provide full support for each version.

✓ Default Directory Rules for Devices Connected via Reverse Proxy

If you integrate a reverse proxy, you can create a default directory rule to sort devices connected through the reverse proxy into a dedicated folder. You can do this by using the **Connected via Reverse Proxy** criterion. You can use the dedicated folder to assign objects (files, profiles, etc.) to the devices included in the folder. This way, devices receive special settings when they are connected through a reverse proxy.



For more on default directory rules, see How to Create a Default Directory Rule[86].

Requirements

Requirements for UMS and certificate configuration for reverse proxy are summarized in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).

Process Overview

The configuration tasks of the reverse proxy are:

- UMS / ICG configuration and certificate export as described in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277)
- NGINX Installation (example based on Ubuntu)
- NGINX Configuration

86. https://kb.igel.com/en/universal-management-suite/current/how-to-create-a-default-directory-rule

NGINX Installation (Example Based on Ubuntu)

→ Install NGINX on your system:

```
sudo apt update
sudo apt install nginx
```

→ If a firewall is used, check the configuration:

1. Check the firewall configuration:

   ```
   sudo ufw app list
   ```

   The output of the command should look like this:

   ```
   Output
   Available applications:
       Nginx Full
       Nginx HTTP
       Nginx HTTPS
       OpenSSH
   ```

2. Enable 'Nginx Full':

   ```
   sudo ufw allow ‘Nginx Full’
   ```

3. Check the firewall configuration with

   ```
   sudo ufw status
   ```

4. For the UMS support, it might be necessary to open further ports. For more information on UMS ports, see IGEL UMS Communication Ports (see page 256).
5. Get the current state of NGINX:

   ```
   sudo systemctl status nginx
   ```

6. Check the current configuration of NGINX:

```
sudo nginx -t
```

NGINX Configuration

The configuration of the server is done in configuration files. In an Ubuntu installation, the main configuration file is `/etc/nginx/nginx.conf`.

In this example, a separate configuration file `umsSSLOffloading.conf` is used. This file has to be included in the `nginx.conf` file:

```
http {

##
# Basic Settings
##
sendfile on;
        ...
##
# Virtual Host Configs
##

include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
include /etc/nginx/umsSSLOffloading.conf; # used for configuration
}
```

The keys and certificates extracted in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277) can be copied to a directory under `/etc/nginx`: for example, `/etc/nginx/ssl` – create the directory if it does not exist.

TLSv1.3 Protocol in SSL Settings

IGEL OS devices are using TLSv1.3 connections. Check if the protocol is enabled in the SSL Settings part of the configuration file `/etc/nginx/nginx.conf`.

```
##
# SSL Settings
##

ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
```

NGINX Configuration File for SSL Offloading

→ Create a new config file `umsSSLOffloading.conf`.

This file must contain

- **upstream server** configuration
- **server** configuration
- **location** configuration

This is an example configuration to use with UMS 12 and IGEL OS 12:

- The **upstream umsserver** block defines the UMS Server in the backend.

```
upstream umsserver {
    server 192.168.27.96:8443 max_fails=3 fail_timeout=10s;
}
```

- The **server** block contains the configuration for the NGINX listener and the location.
  The UMS web certificate and the client certificate validation should be added here.
  Server common configuration:

```
server {
    listen       8443 ssl; # 'ssl' parameter tells NGINX to decrypt the traffic
    ssl_certificate             ssl/ssl-cert-chain.cer; # The Certificate File
(Web)
    ssl_certificate_key         ssl/cert-key.key; # The Private Key File (Web)
    ssl_verify_client           optional; ## Client Certificate check must be
optional
    ssl_client_certificate      ssl/estca.cer; #certificate for Client
Certificate Check

    access_log                  /var/log/nginx/ssl-access.log;
    error_log                   /var/log/nginx/ssl-error.log;
```

- At least two **location** definitions are required:
  - Location definition for all connections via WebSocket. The WebSocket connection requires the forwarding of the client certificate within the header. A second header information to add is the upgrade header which is required for WebSockets.

```
# Configuration for connections via WebSocket, the upgrade header
information must be written by NGINX
  location ~ /device-connector/device/(ws-connect|portforwarding) {
        proxy_pass https://umsserver;
        proxy_set_header X-SSL-CERT $ssl_client_escaped_cert; # client
certificate in current connection
        proxy_set_header Upgrade $http_upgrade; # Set upgrade header
```

```
        proxy_set_header Connection $connection_upgrade;
        proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer; #trusted
Cert Chain for UMS connection

        # TLSv1.3 configuration is recommended but not necessary
        proxy_ssl_protocols TLSv1.3;
 }
```

- Location definition for all other connections.

```
# Configuration for all other connections
  location / {
        proxy_pass https://umsserver;
        proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
        proxy_ssl_protocols TLSv1.3;
        proxy_set_header Host $Host;
 }
```

The whole configuration file:

```
#map upgrade header
map %https_upgrade $connection_upgrade {
default upgrade;
'' close;
}

    upstream umsserver {
        server 192.168.27.96:8443 max_fails=3 fail_timeout=10s;
    }

server {
    listen      8443 ssl; # 'ssl' parameter tells NGINX to decrypt the traffic
    ssl_certificate             ssl/ssl-cert-chain.cer; # The Certificate File (Web)
    ssl_certificate_key         ssl/cert-key.key; # The Private Key File (Web)
    ssl_verify_client           optional; ## Client Certificate check must be
optional
    ssl_client_certificate      ssl/estca.cer; #certificate for Client Certificate
Check

    access_log                  /var/log/nginx/ssl-access.log;
    error_log                   /var/log/nginx/ssl-error.log;

# Configuration for connections via WebSocket, the upgrade header information must be
written by NGINX
  location ~ /device-connector/device/(ws-connect|portforwarding) {
    proxy_pass https://umsserver;
    proxy_set_header X-SSL-CERT $ssl_client_escaped_cert;
```

```
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection $connection_upgrade;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    # TLSv1.3 configuration is recommended but not necessary
    proxy_ssl_protocols TLSv1.3;
 }

# Configuration for all other connections
  location / {
    proxy_pass https://umsserver;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection $connection_upgrade;
    proxy_ssl_protocols TLSv1.3;
    proxy_set_header Host $Host;
  # proxy_ssl_session_reuse on;
  }
}
```

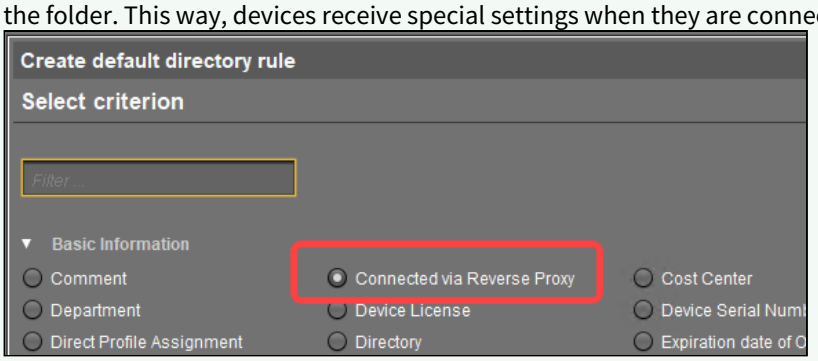
F5 BIG IP Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

In this article. you can find an example configuration of F5 BIG IP for SSL Offloading in the IGEL Universal Management Suite (UMS).

General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
As the reverse proxy is an external software we cannot provide full support for each version.

Default Directory Rules for Devices Connected via Reverse Proxy

If you integrate a reverse proxy, you can create a default directory rule to sort devices connected through the reverse proxy into a dedicated folder. You can do this by using the **Connected via Reverse Proxy** criterion. You can use the dedicated folder to assign objects (files, profiles, etc.) to the devices included in the folder. This way, devices receive special settings when they are connected through a reverse proxy.



For more on default directory rules, see How to Create a Default Directory Rule[87].

Requirements

Requirements for UMS and certificate configuration for reverse proxy are summarized in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).

To use remote management functions over the F5 BIG IP Reverse Proxy, you need to use IGEL OS 12.3.2 or higher and UMS 12.04.120 or higher.
The reason for this is that F5 BIG IP did not support the EC key used in the device certificate, so this was changed to RSA keys starting from these versions. (The device certificate key type can be changed in IGEL Setup using the registry key **system.remotemanager.device_key_type**.)

Process Overview

The configuration tasks of F5 BIG IP are:

- UMS / ICG configuration and certificate export as described in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277)

87. https://kb.igel.com/en/universal-management-suite/current/how-to-create-a-default-directory-rule

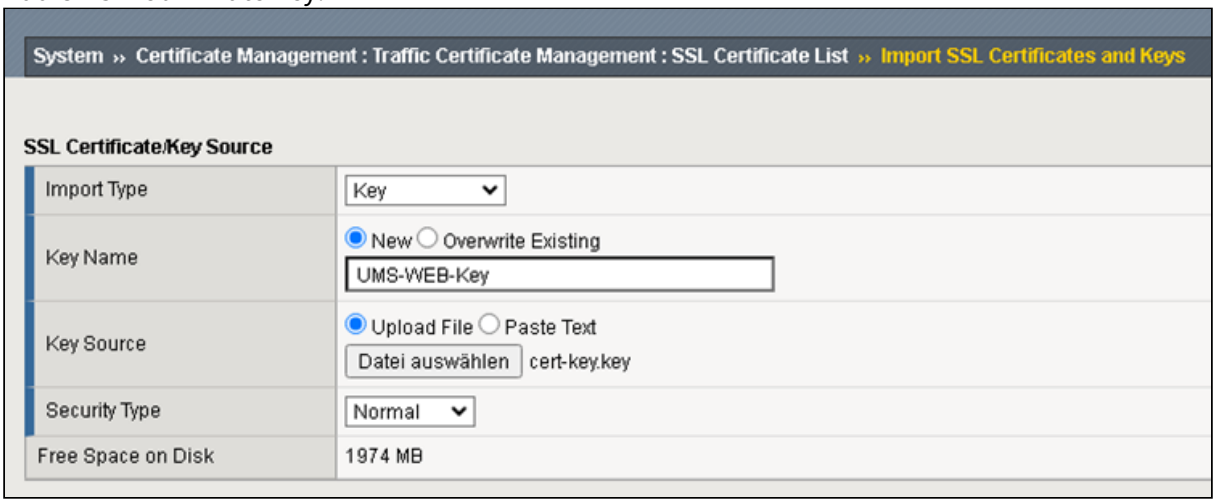
- UMS certificate management (Web UMS and EST CA)
- UMS backend node and pool configuration
- iRule configuration for client certificate forwarding
- SSL client profile configuration
- SSL server profile configuration
- Virtual server configuration

Certificate Management

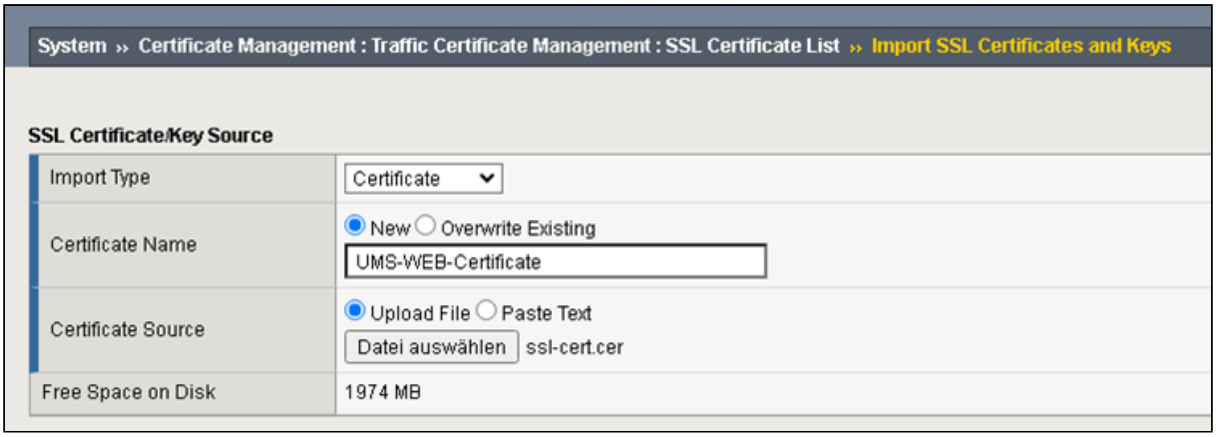
The certificates created in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277) must be added in the F5 BIG IP application. BIG IP offers a common Certificate Management.

To configure the UMS Web Certificates / Keys:

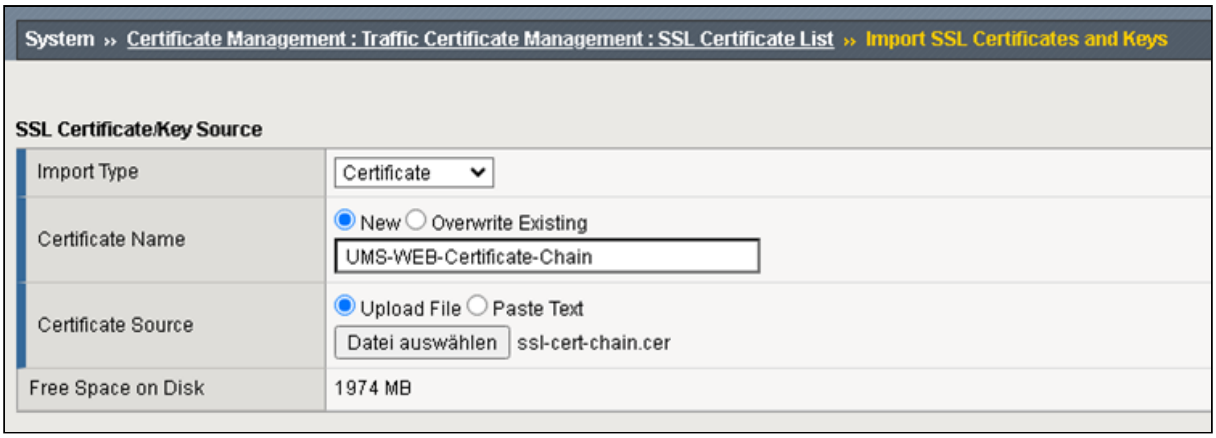
1. Add UMS Web Private Key.



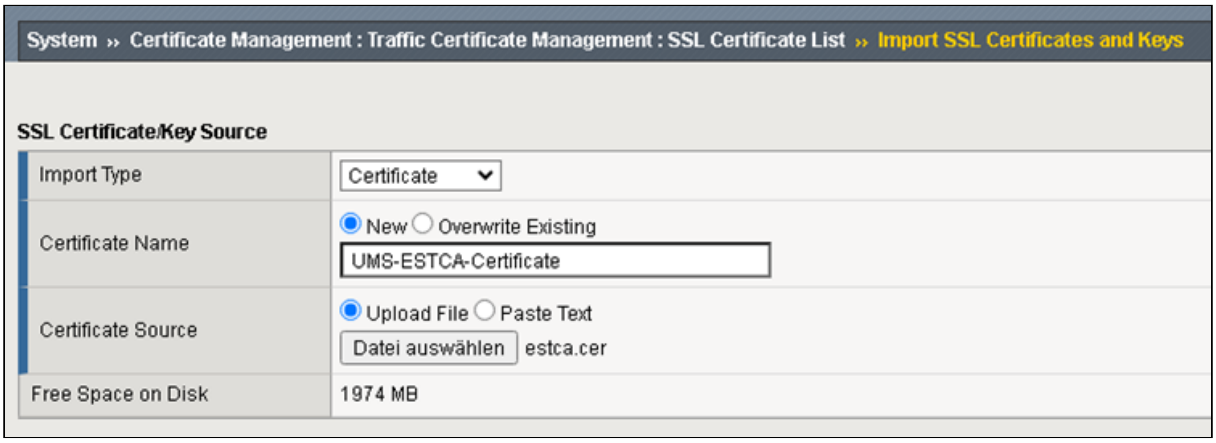
2. Add UMS Web Certificate.



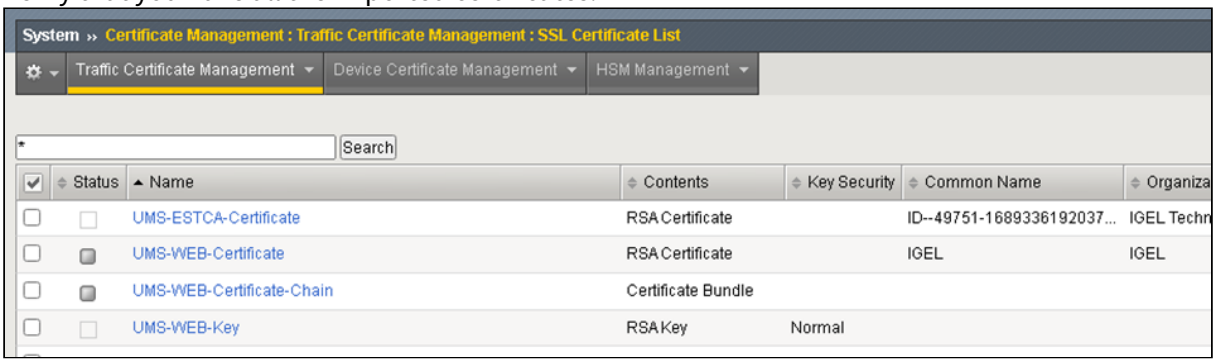
3. Add UMS Web Certificate Chain.



4. Add UMS EST CA Certificate



5. Verify that you have all the imported certificates.

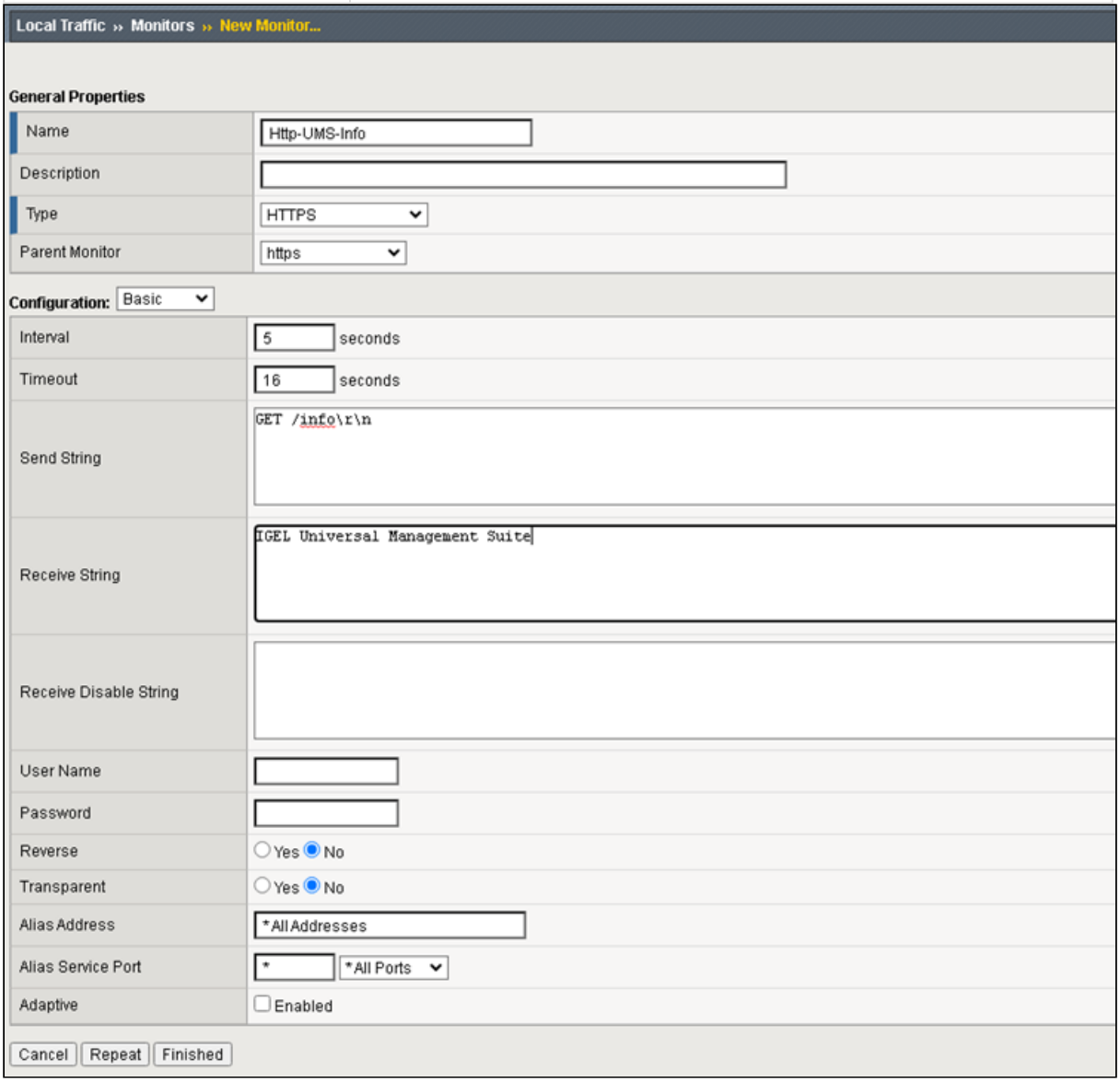


Backend Node and Pool Configuration

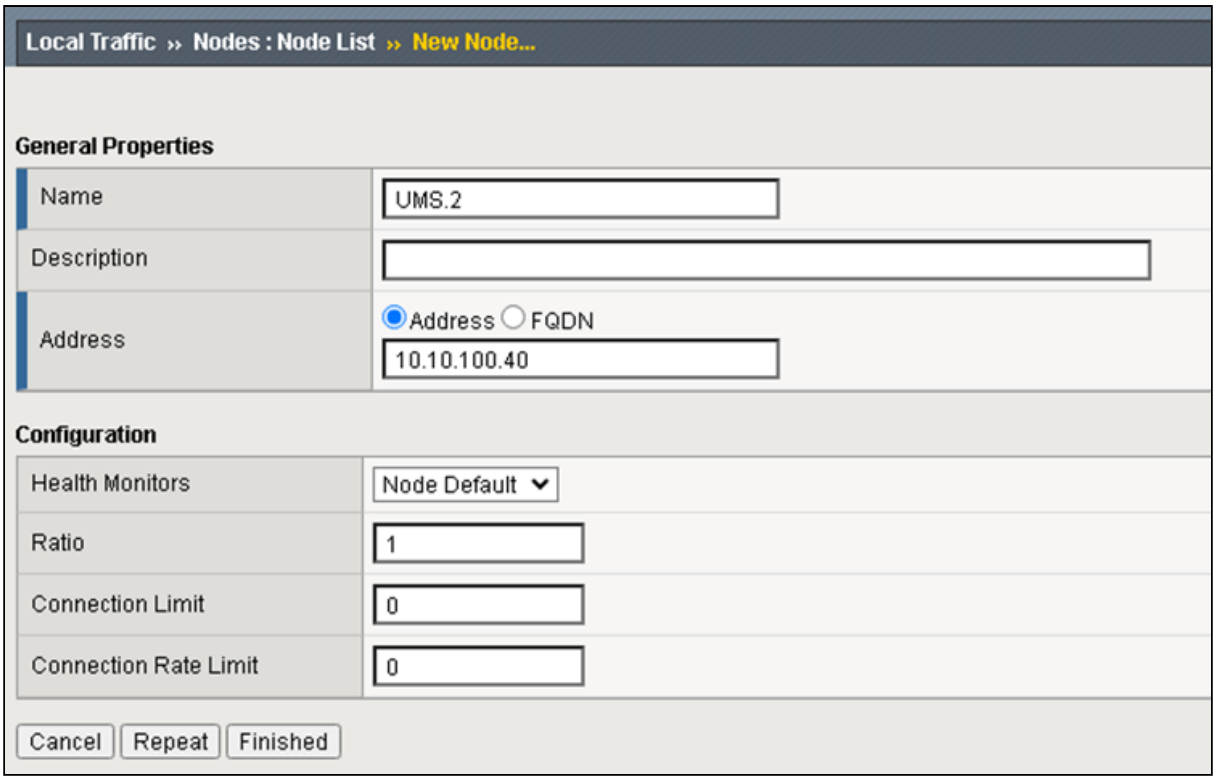
The UMS Server must be configured as backend server.

1. Add a Monitor and configure it for testing if the UMS info URL is online.
   The following properties must be set:

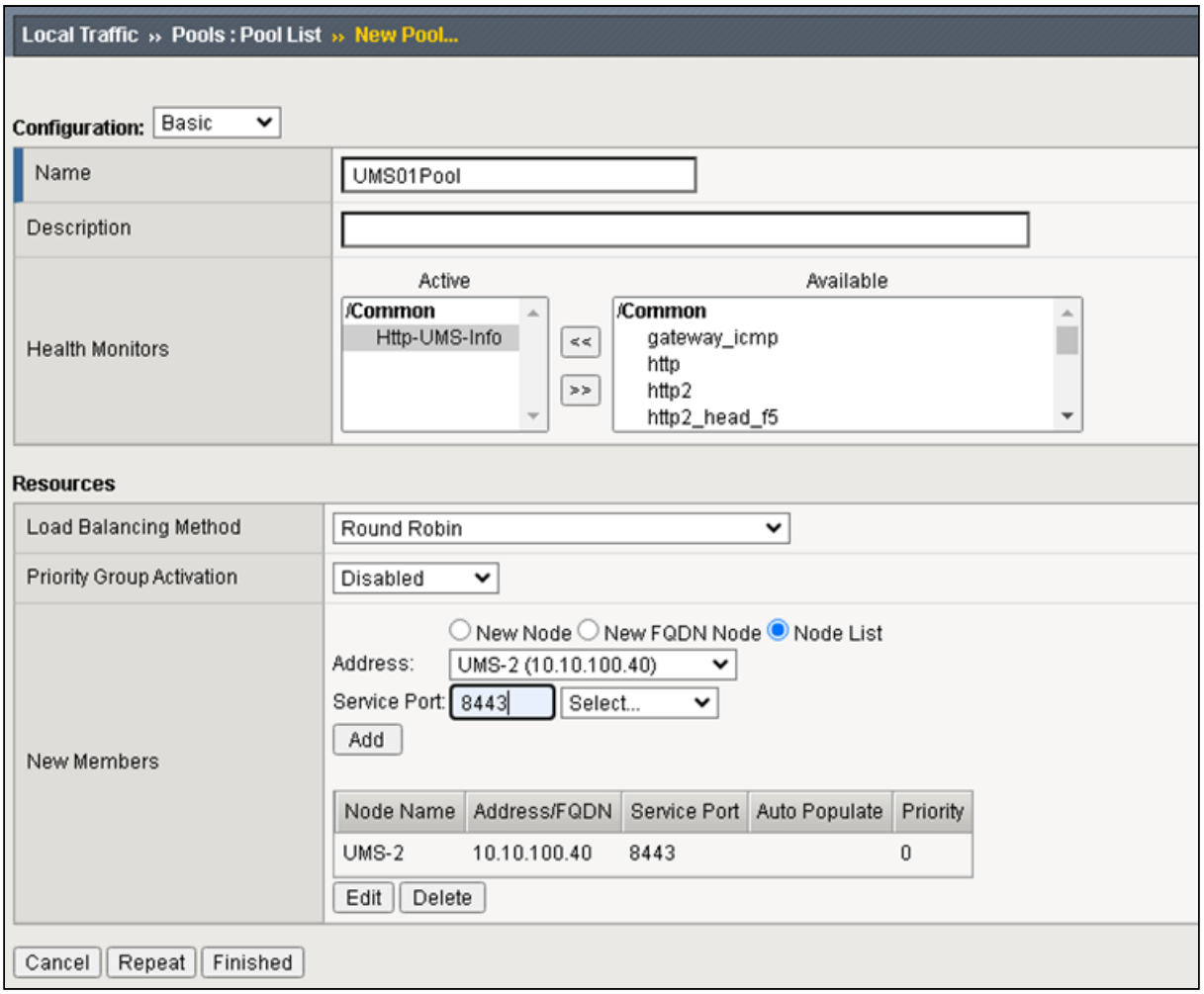
Type	HTTPS
Send String	GET /info\r\n
Receive String	IGEL Universal Management Suite



2. Create a new Node and set the Address of the UMS Server.



3. Add Pool. In the pool configuration the monitor and the node server must be at least configured. There is no specific Load Balancing Method recommended.

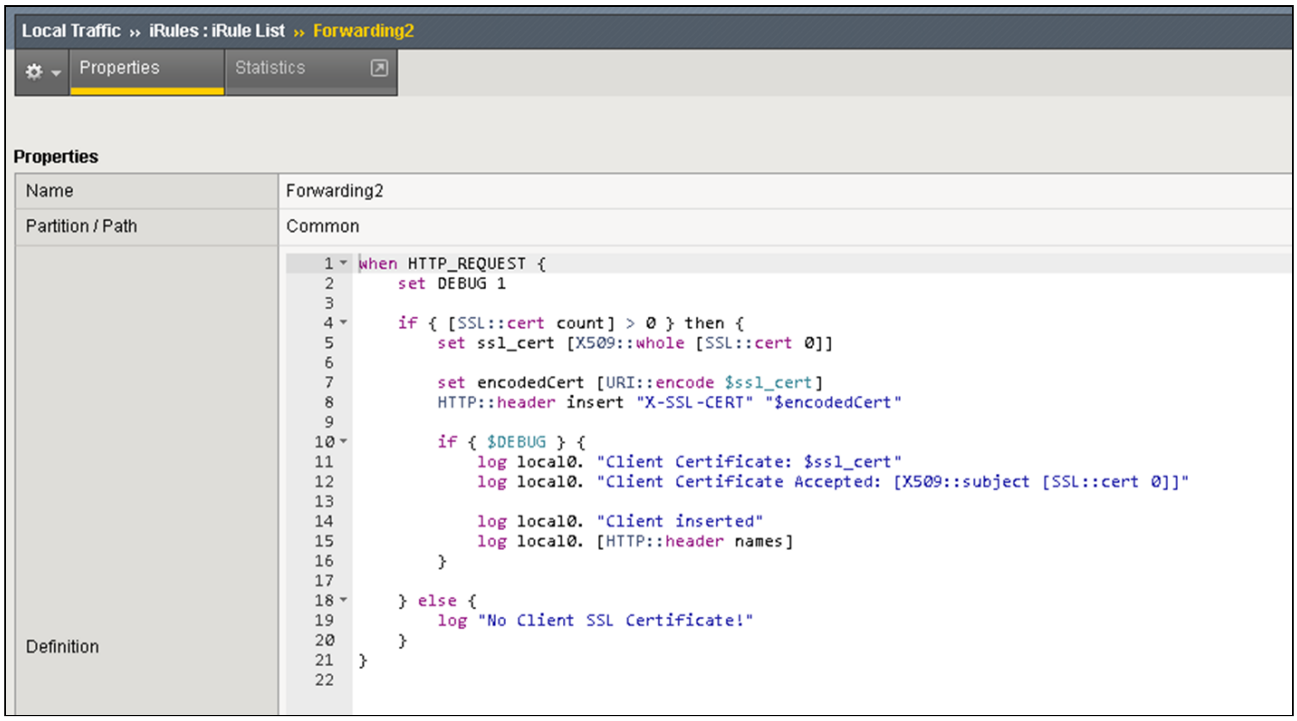


IRULE Configuration to Forward the Client Certificate in HTTP Header

Irules is the Script support of F5 BIG-IP.

The Client Certificate can be read from the HTTP_REQUEST. The variable `[X509::whole [SSL::cert 0]]` contains it in `PEM` format.

The UMS expects the certificate URL Encoded so it must be encoded: `[URI::encode $ssl_cert]`



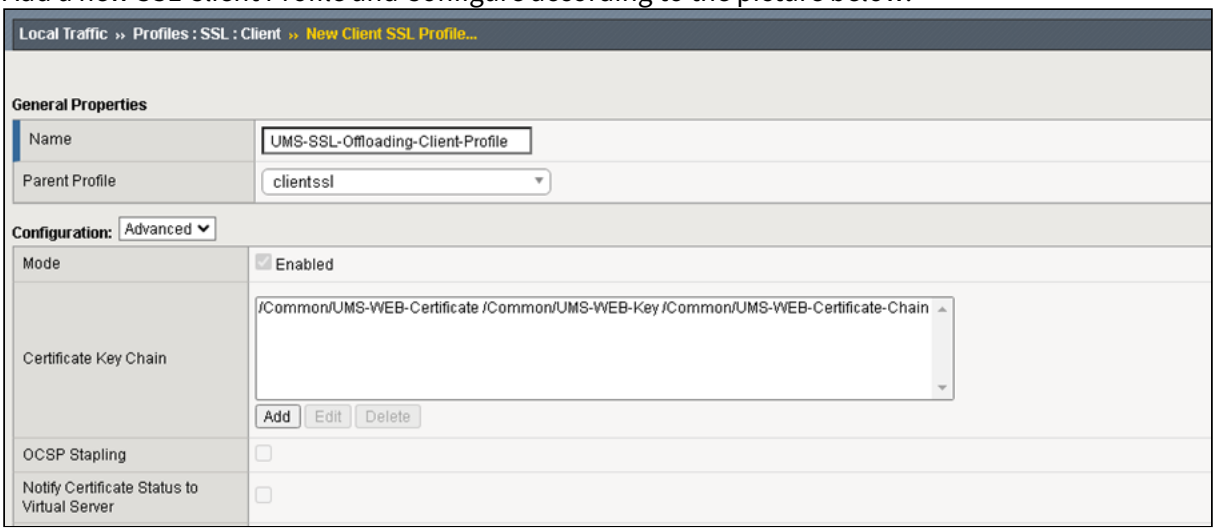
Forwarding Header Example:

```
when HTTP_REQUEST {
    set DEBUG 1

    if { [SSL::cert count] > 0 } then {
        set ssl_cert [X509::whole [SSL::cert 0]]

        set encodedCert [URI::encode $ssl_cert]
        HTTP::header insert "X-SSL-CERT" "$encodedCert"

        if { $DEBUG } {
            log local0. "Client Certificate: $ssl_cert"
            log local0. "Client Certificate Accepted: [X509::subject [SSL::cert 0]]"

            log local0. "Client inserted"
            log local0. [HTTP::header names]
        }

    } else {
        log "No Client SSL Certificate!"
    }
}
```

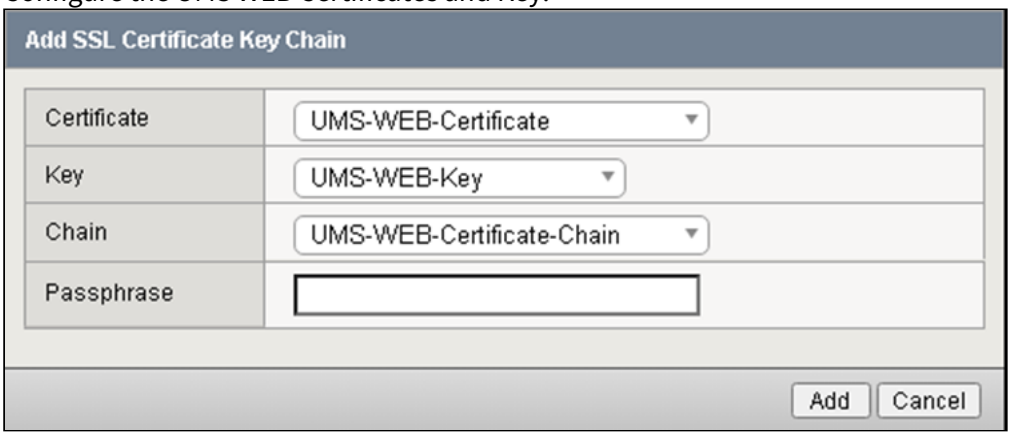
SSL Client Profile Configuration

The SSL Client Profile is used to set the SSL configuration for all incoming requests to the Virtual Servers.

1. Add a new SSL Client Profile and Configure according to the picture below.

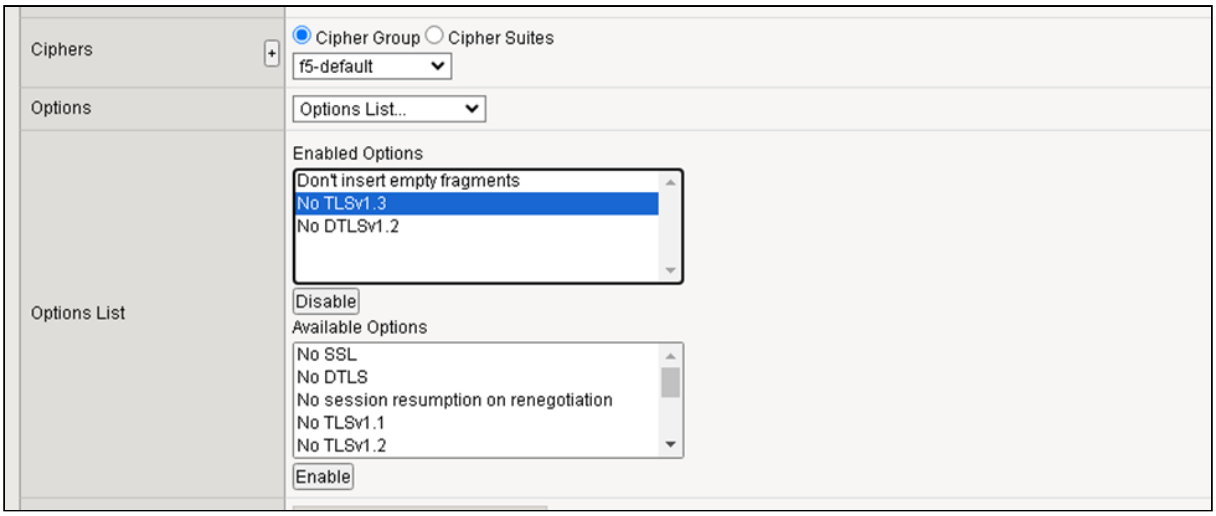


2. Configure the UMS WEB Certificates and Key.



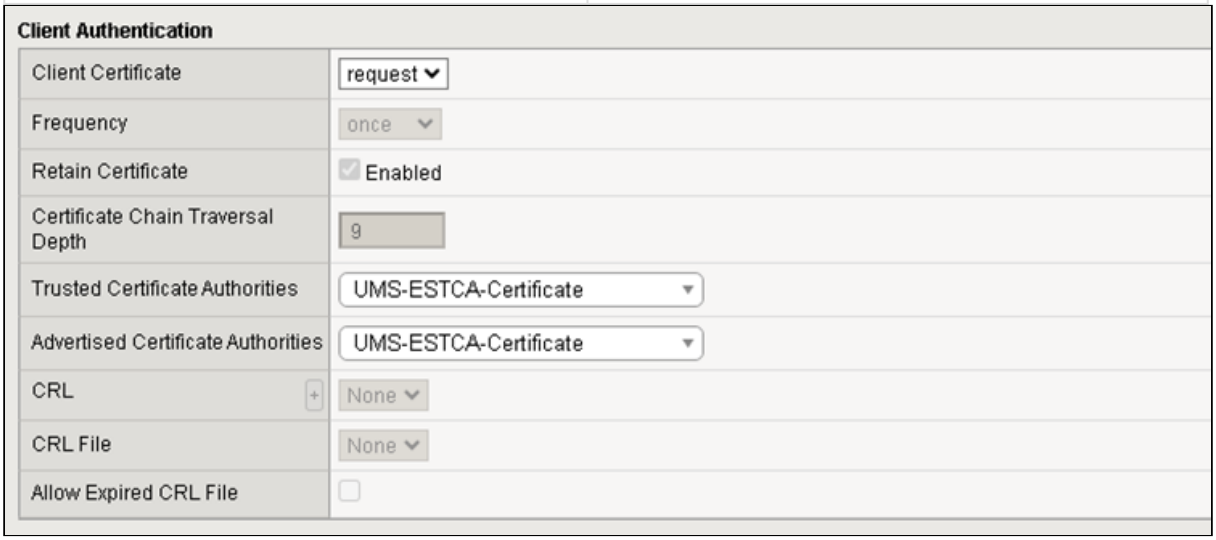
3. TLSv1.3 is used in the connection from the Device to UMS so the ciphers must be customized.

Ciphers	**f5-default** can be used as Cipher Group
Options List	disable the “No TLSv1.3” entry in the Enabled Options list



4. The necessary customizations for Client Certificate Authentication are:

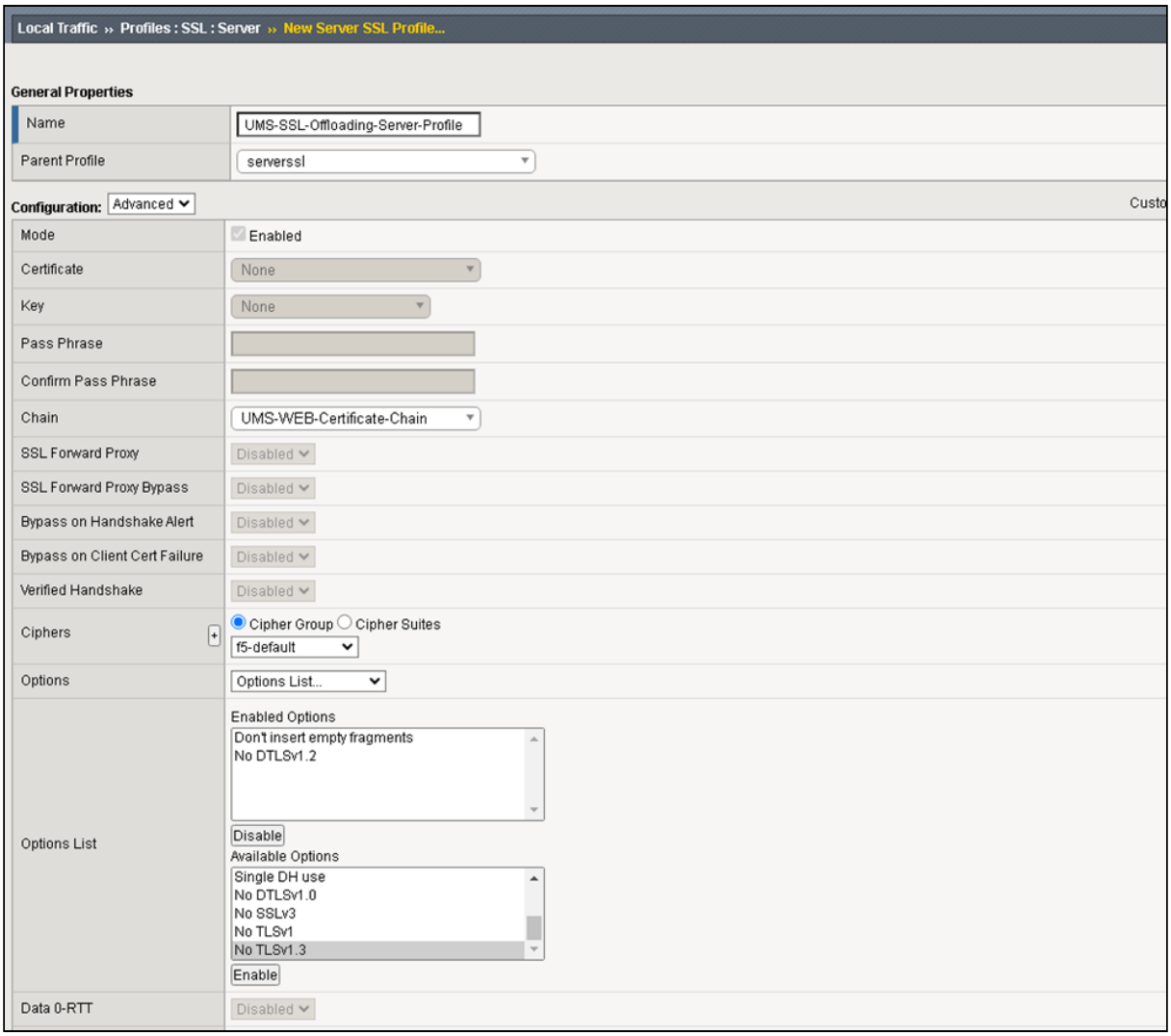
Client Certificate	This value must be set to **request**
Trusted Certificate Authorities	Set to **UMS-ESTCA-Certificate**
Advertised Certificate Authorities	Can be set to **UMS-ESTCA-Certificate**



SSL Server Profile Configuration

The SSL Server Profile is used to set the SSL configuration for all requests to the Backend Servers (UMS).

1. Create a new SSL Server Profile.
2. Set the Chain value to **UMS Web Certificate Chain**.
3. Set the TLSv 1.3 configuration the same as for the SSL Client Profile above.

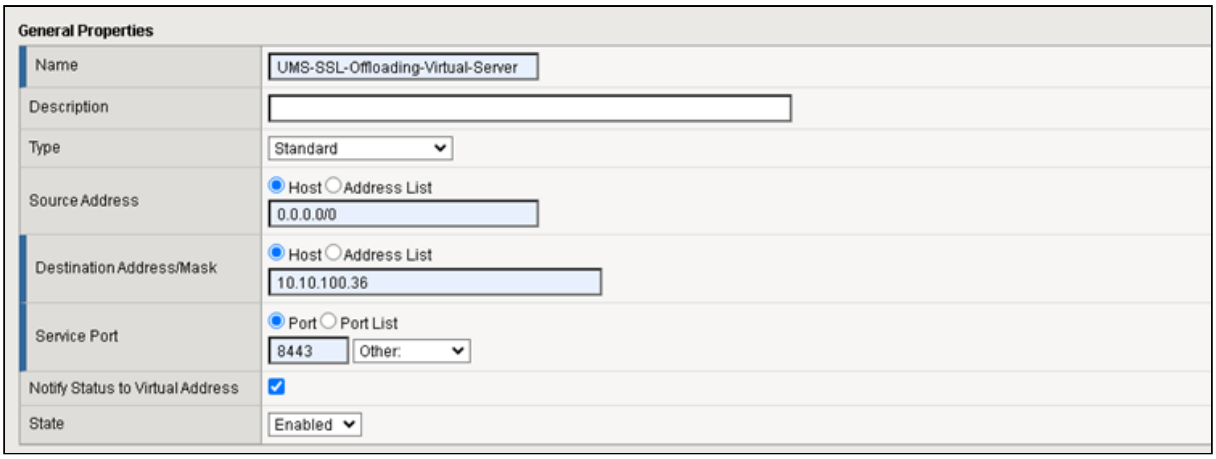


Virtual Server Configuration

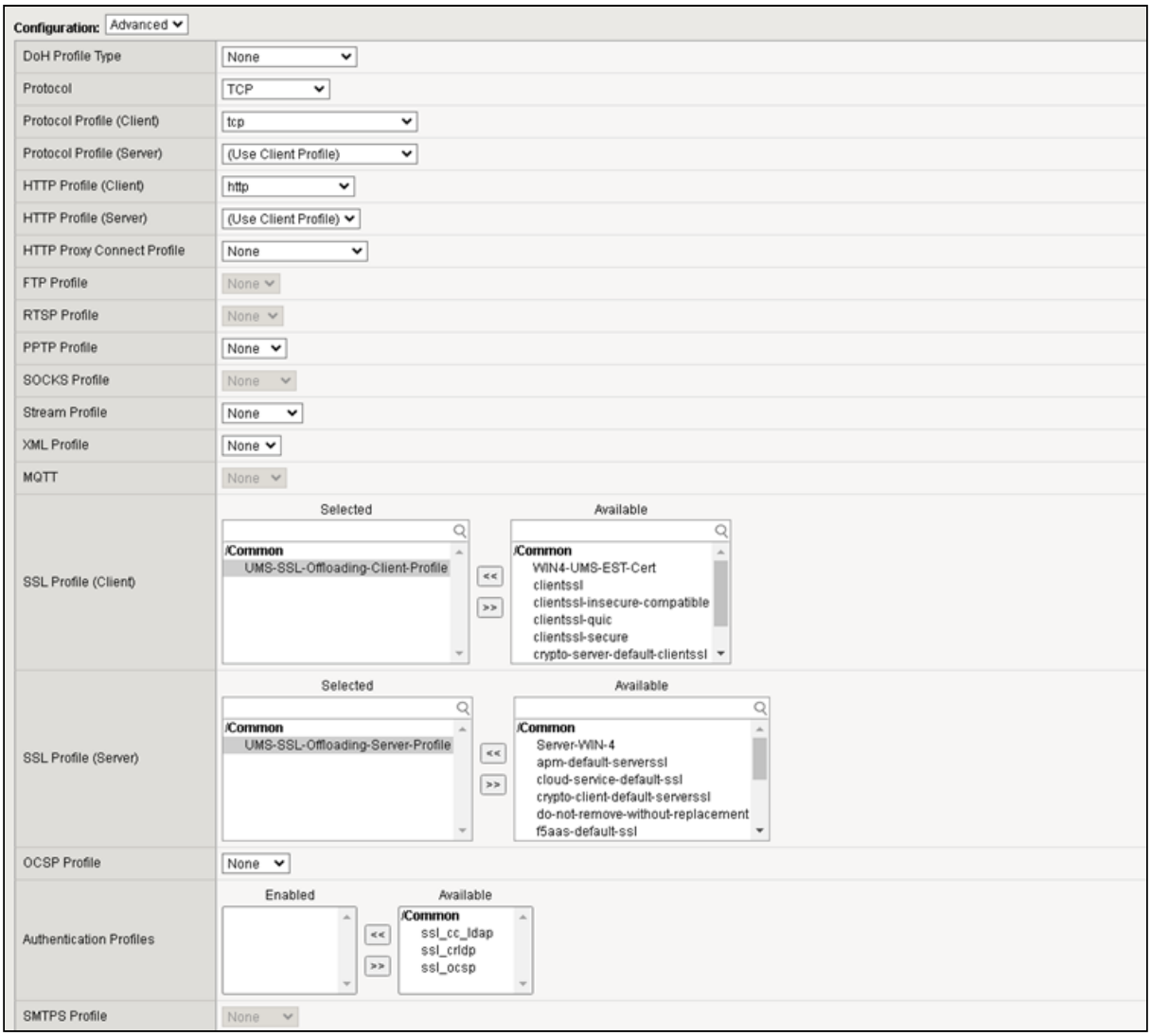
The Virtual Server defines the Listener in F5 BIG-IP.

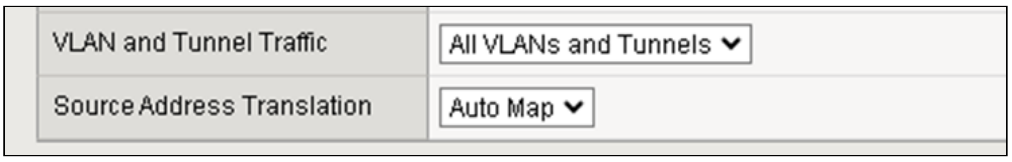
1. Set the following values:

Type	Standard
Source Address	From which IP are requests allowed. Set it to * if this shouldn't be evaluated
Destination Address	The Address under which this Virtual Server is reachable
Service Port	Select the UMS Port

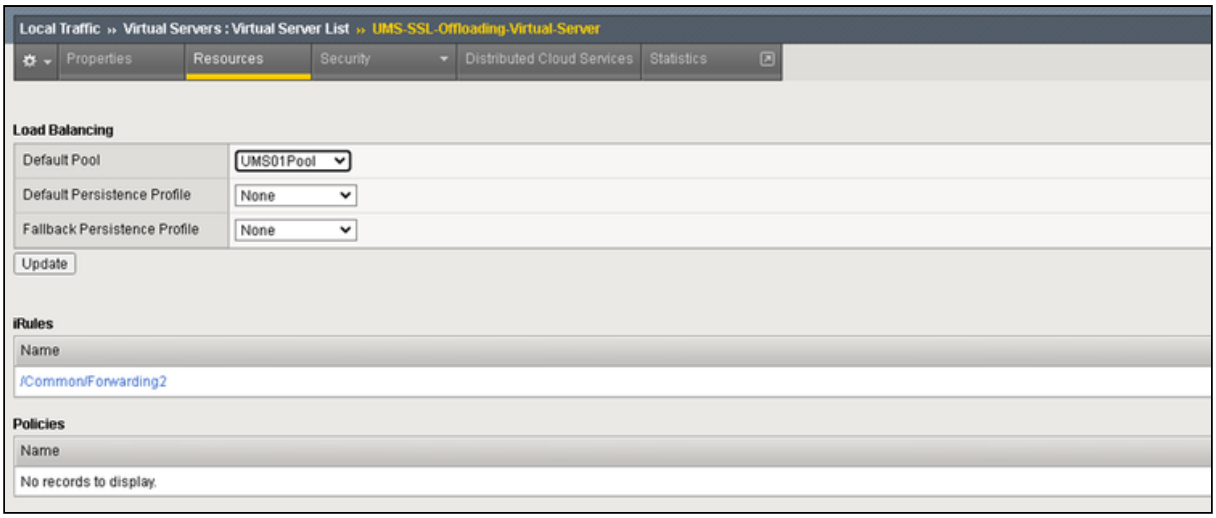


Protocol	TCP
HTTP Profile	http, required to evaluate the HTTP Header
SSL Profile (Client)	Add the earlier created Client SSL Profile
SSL Profile (Server)	Add the earlier created Server SSL Profile
Source Address Translation	Set it to Auto Map





2. Add the Pool and iRule to the Virtual Server.


Local Traffic ›› Virtual Servers : Virtual Server List ›› UMS-SSL-Offloading-Virtual-Server
Properties
Resources
Security
Distributed Cloud Services
Statistics
Load Balancing
Default Pool
UMS01Pool
Default Persistence Profile
None
Fallback Persistence Profile
None
Update
iRules
Name
/Common/Forwarding2
Policies
Name
No records to display.

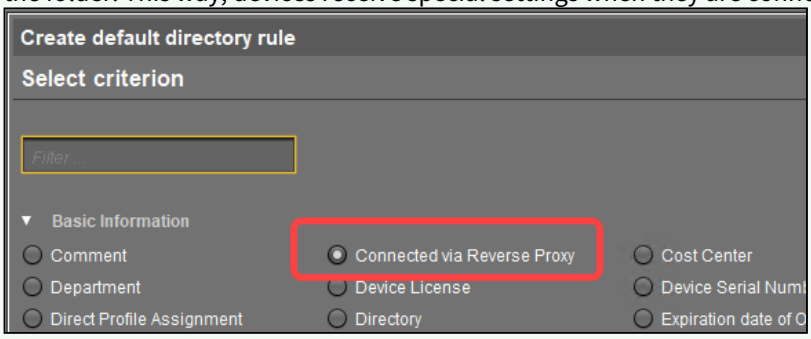
Azure Application Gateway Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

This article describes the IGEL Unified Management Suite (UMS) configurations and the Azure Application Gateway configurations you need for SSL Offloading.

General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
As the reverse proxy is an external software we cannot provide full support for each version.

Default Directory Rules for Devices Connected via Reverse Proxy

If you integrate a reverse proxy, you can create a default directory rule to sort devices connected through the reverse proxy into a dedicated folder. You can do this by using the **Connected via Reverse Proxy** criterion. You can use the dedicated folder to assign objects (files, profiles, etc.) to the devices included in the folder. This way, devices receive special settings when they are connected through a reverse proxy.



For more on default directory rules, see How to Create a Default Directory Rule[88].

Requirements

Requirements for UMS and certificate configuration for reverse proxy are summarized in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).

Process Overview

The configuration tasks of the reverse proxy are:

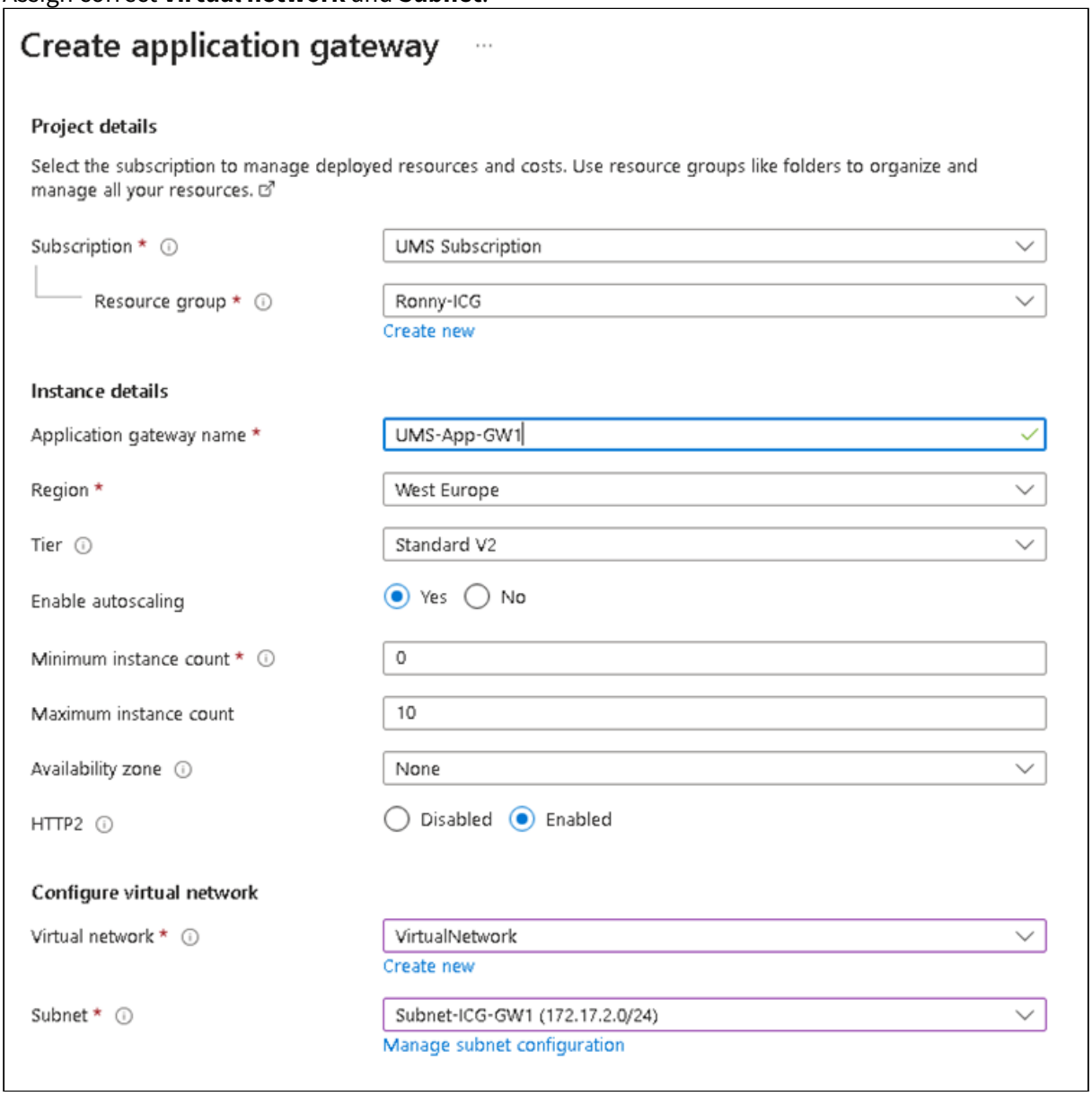
- UMS / ICG configuration and certificate export as described in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277)
- Azure application gateway creation
- Routing rule creation for onboarding connection
- Routing rule creation for the Websocket connection
- Network security group check
- Mutual authentication creation for WebSocket connection

88. https://kb.igel.com/en/universal-management-suite/current/how-to-create-a-default-directory-rule

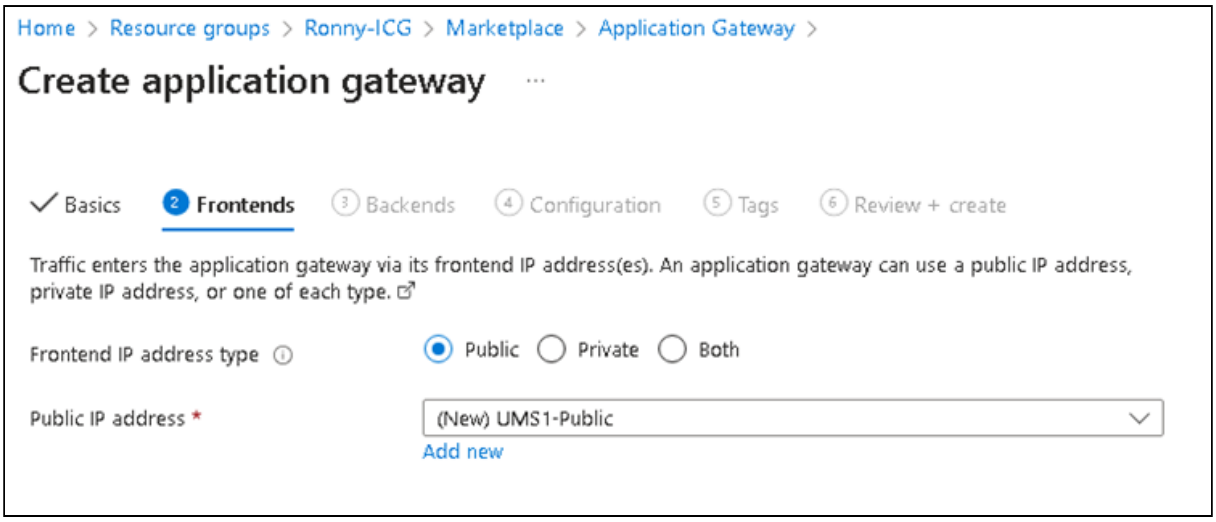
- Rewrite configuration for client certificate forwarding
- Troubleshoot certificate error (if needed)

Create Azure Application Gateway

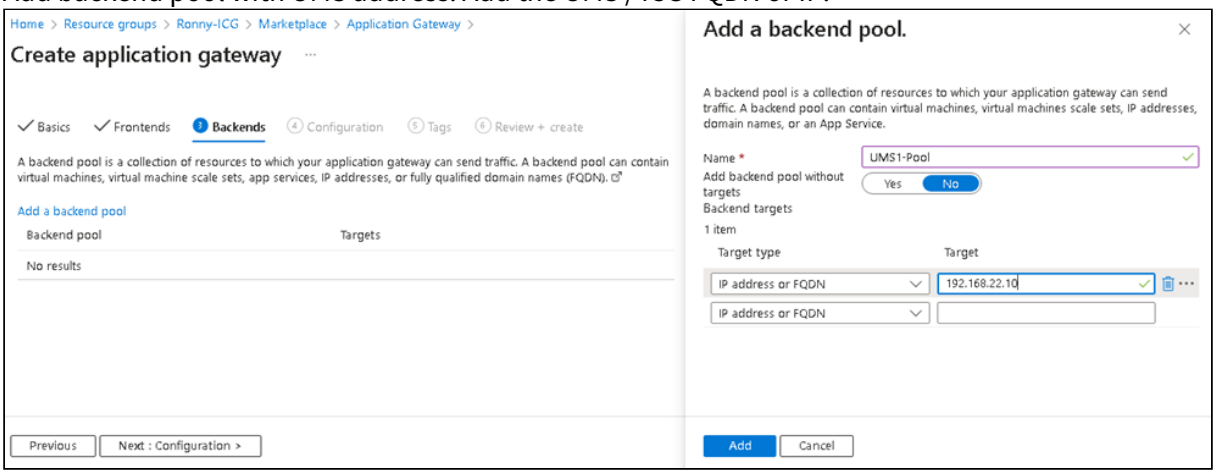
1. Assign correct **Virtual network** and **Subnet**.



2. Provide Frontend IP address.

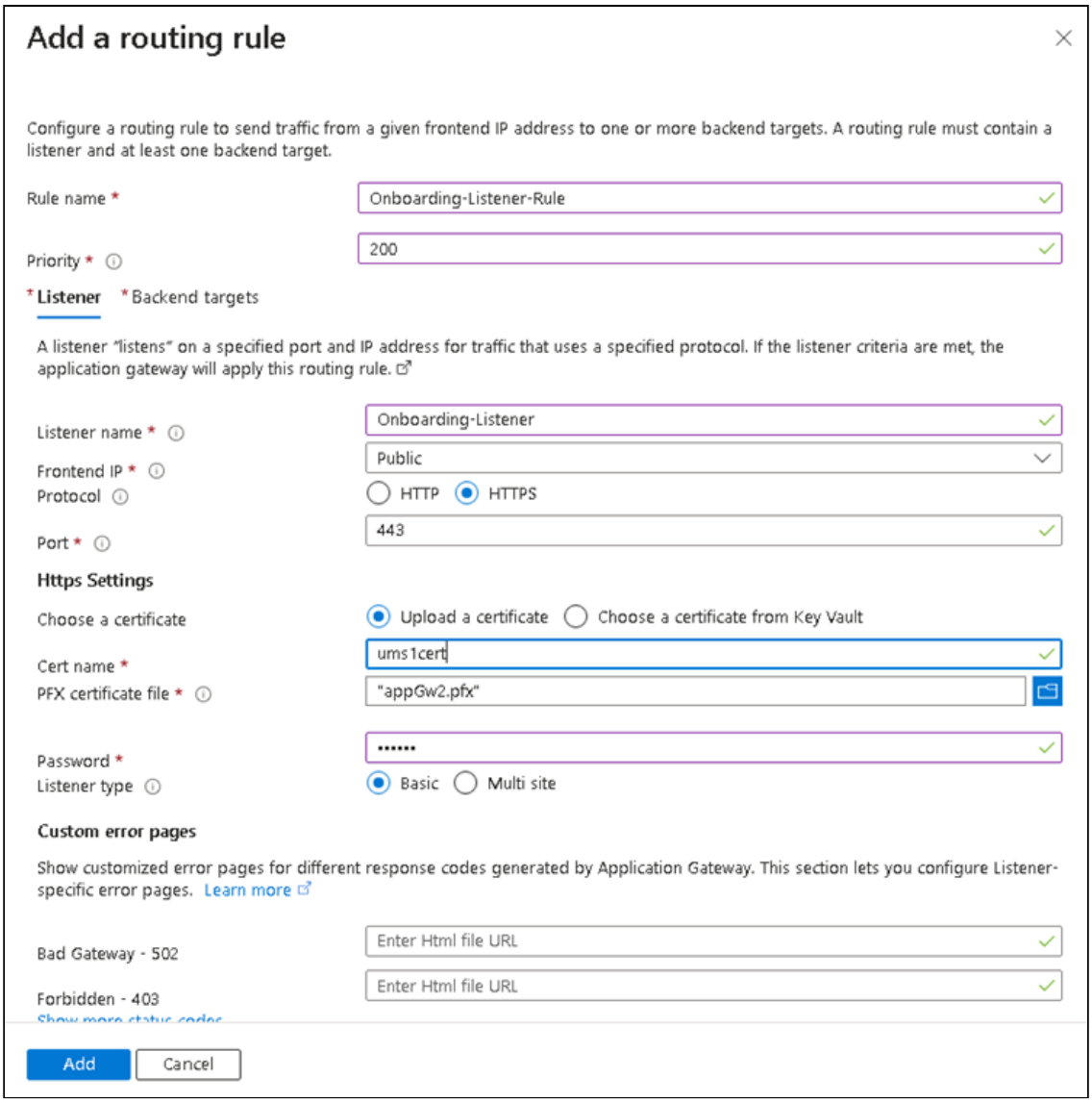


3. Add backend pool with UMS address. Add the UMS / ICG FQDN or IP.



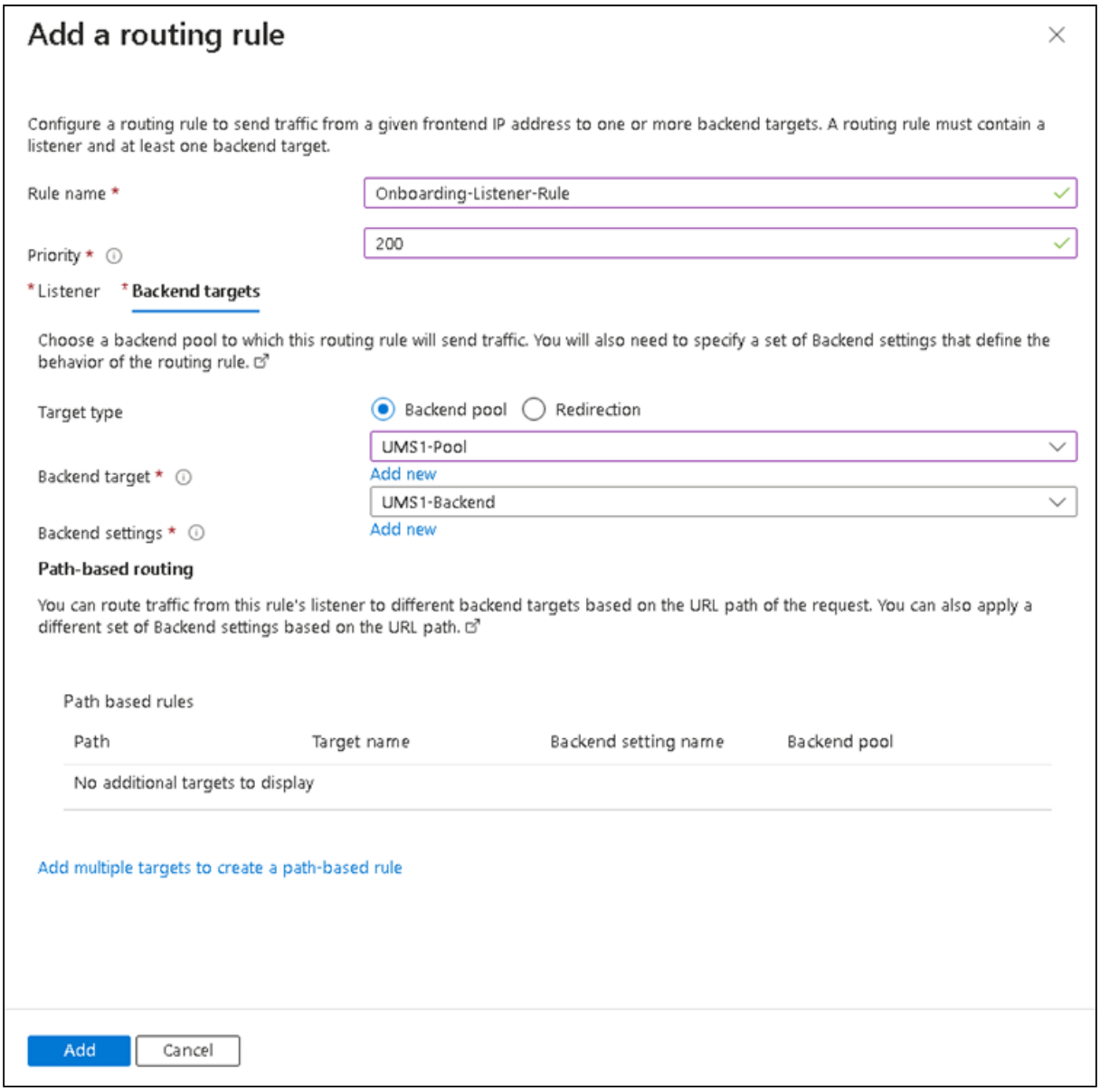
Add a Routing Rule for Onboarding Connection

1. Configure a listener:
   - Set the **Protocol** to **HTTPS**.
   - Set the **Public** IP address.
   - The recommended **Port** value is **443**.

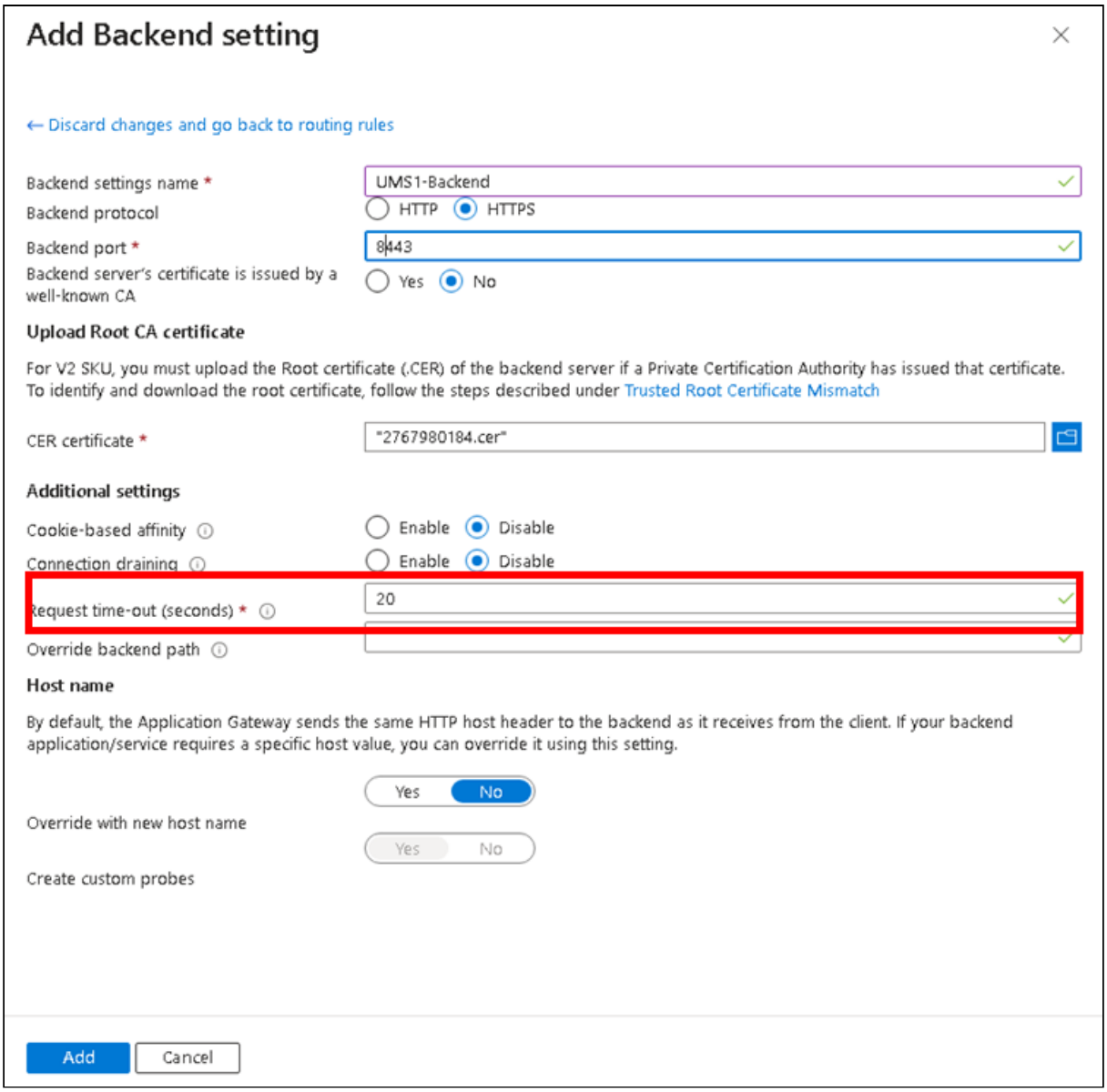


2. Select the `PFX` file created in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277) and enter the appropriate password.

3. Configure **Backend targets**. The already inserted Backend pool can now be selected and the Backend settings must be added.



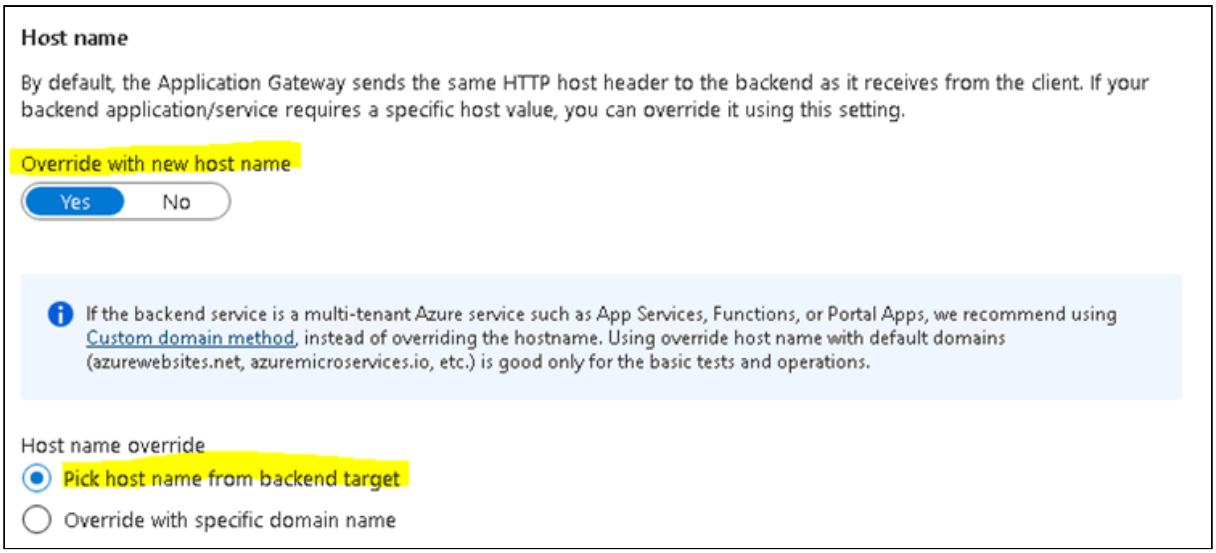
4. Under **Add Backend settings**, set the **Backend protocol** to **HTTPS** and add the **UMS Web Port** as **Backend port**.



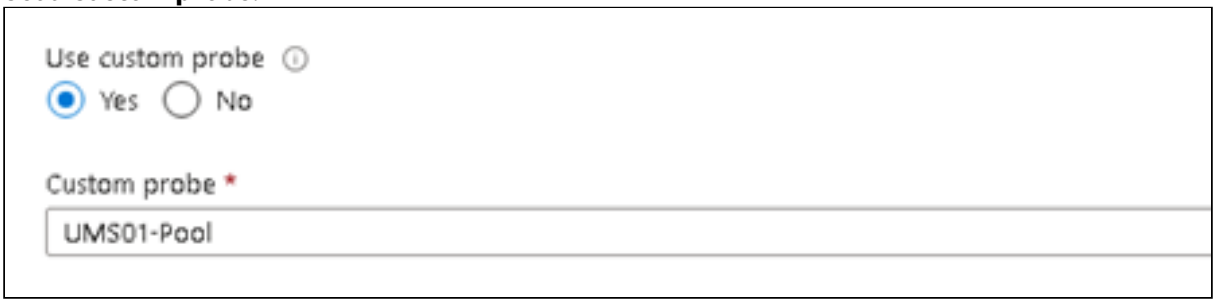
5. Select the UMS Web/Cloud Gateway Root Certificate exported in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).

6. Set the value for **Request time-out (seconds)** to a value at least **130** seconds.

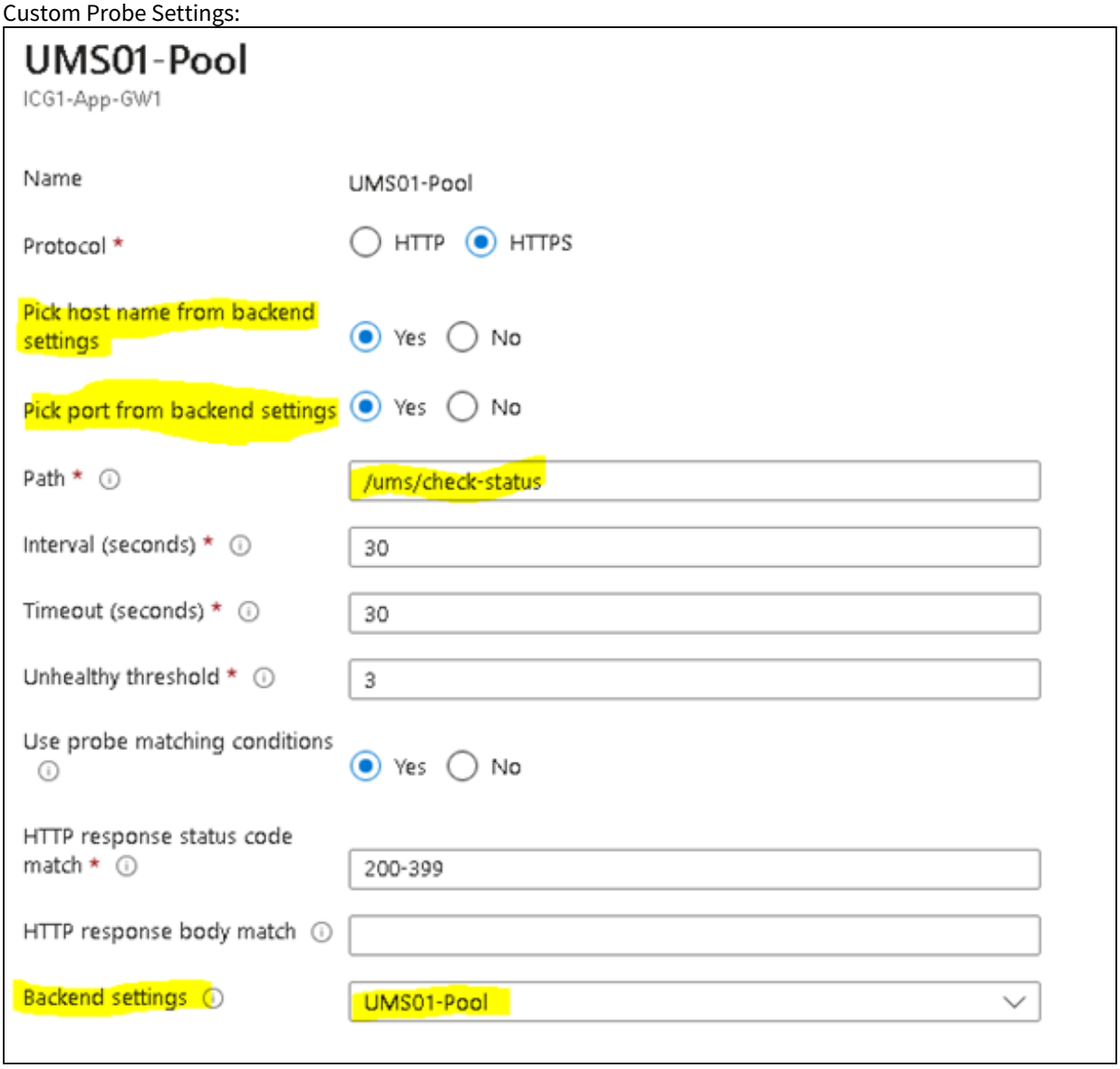
7. Verify that the **Override with new host name** is activated and set **Host name override**.



8. Set a **Custom probe**.

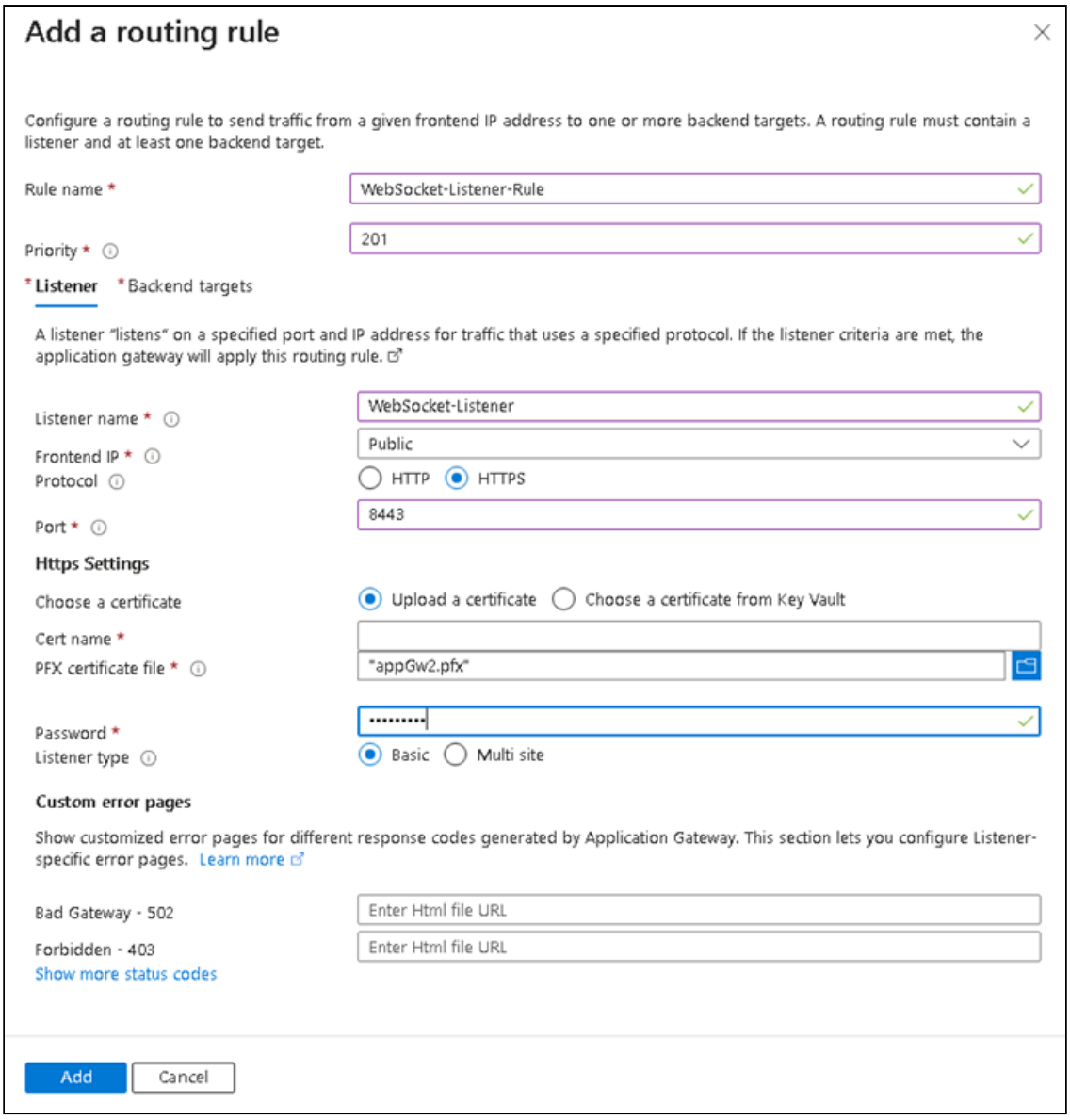


Custom Probe Settings:



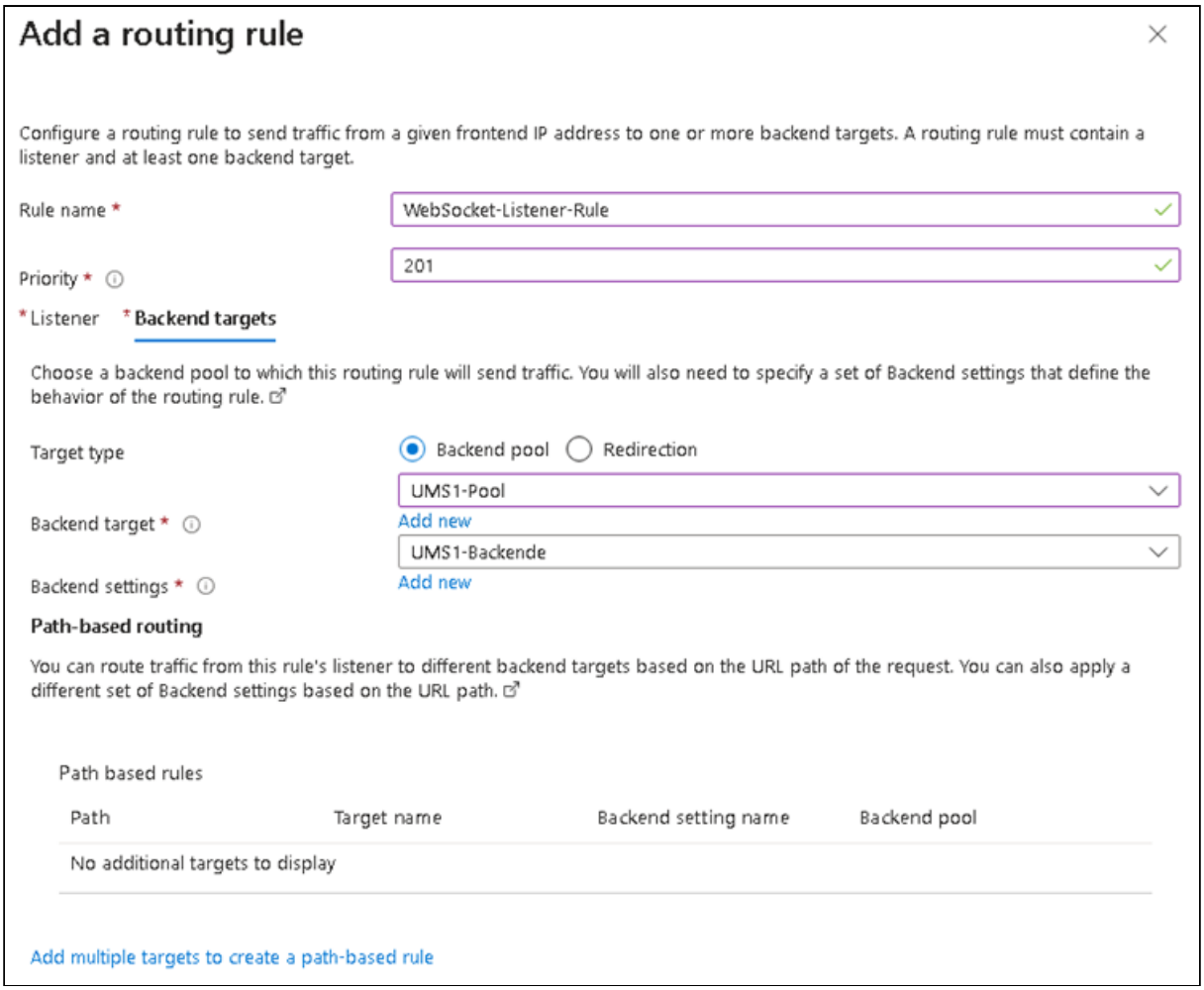
Add a Routing Rule for the Websocket Connection

1. Configure a listener:
    - Set the **Protocol** to **HTTPS**.
    - Set the **Public** IP address.
    - The recommended **Port** value is **8443**.



2. Select the `PFX` file created in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277), and enter the appropriate password.

3. Add the same Backend Settings as for the Onboarding connection.



Check Network Security Group

1. Open the Network Security Group used for the Gateway Network and verify if the used Ports are listed

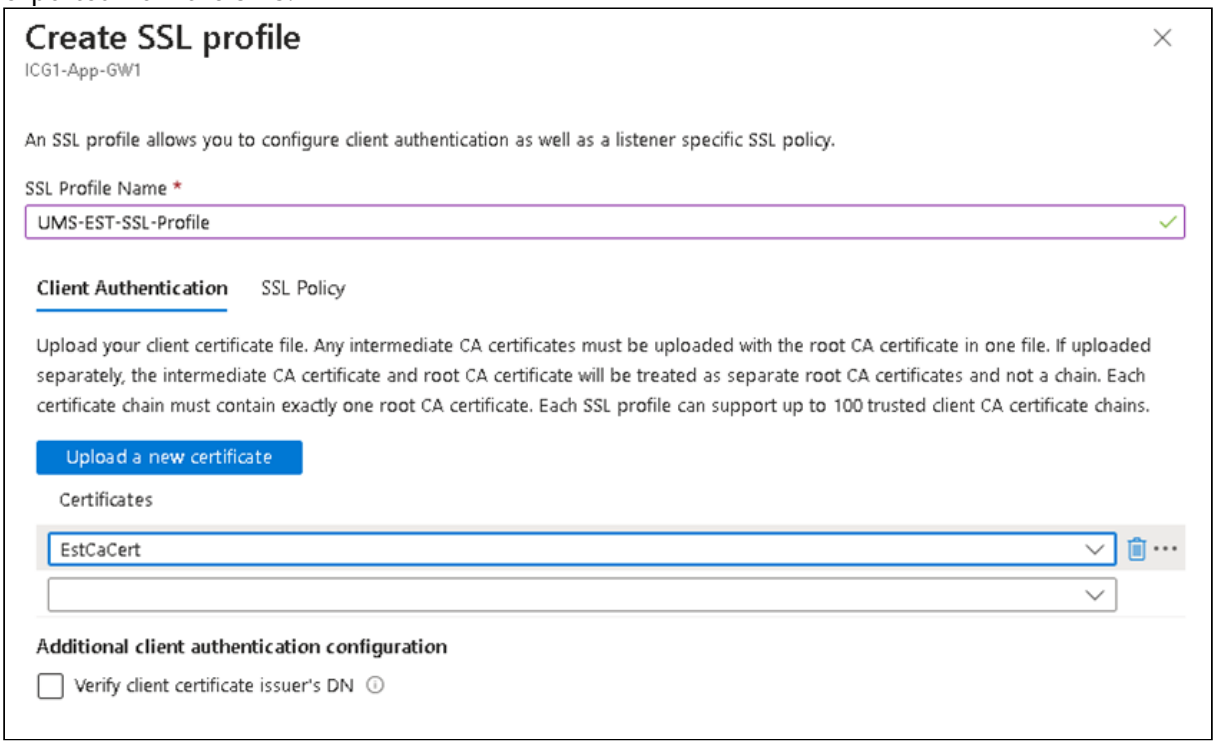
2. If they are not listed, add them.

Set Mutual Authentication for WebSocket Connection

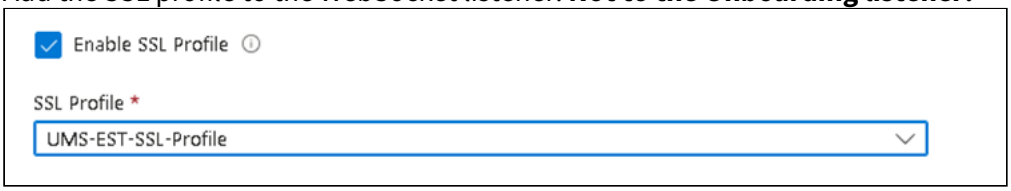
The mutual authentication can be set in Azure Application Gateway with SSL Profiles:

1. Add an SSL Profile under SSL settings.

2. In the **Client Authentication** part of the Dialog the EST CA Certificate is required, that was exported from the UMS.



3. Add the SSL profile to the WebSocket listener. **Not to the Onboarding listener!**

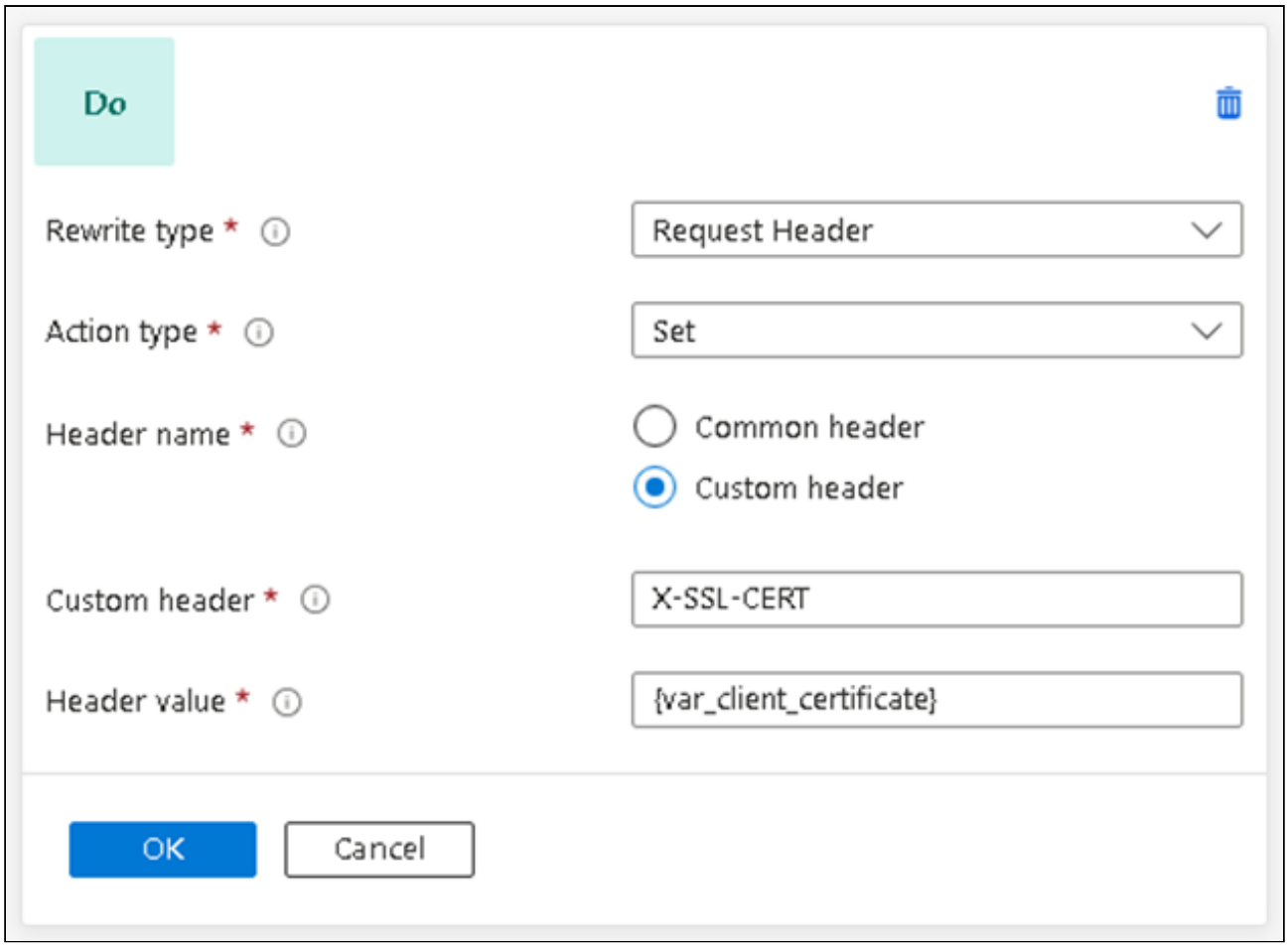


Add a Rewrite for Client Certificate Forwarding

The client certificate must be forwarded to the UMS. The Application Gateway can be configured to forward it by a rewrite definition.

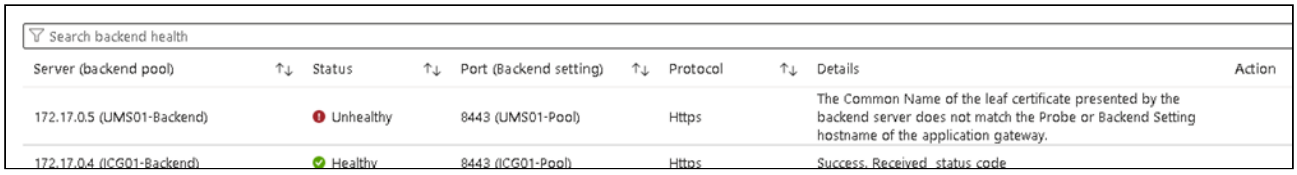
1. Create a rewrite set and assign it to the appropriate rule.

2. Add the following rewrite rule:

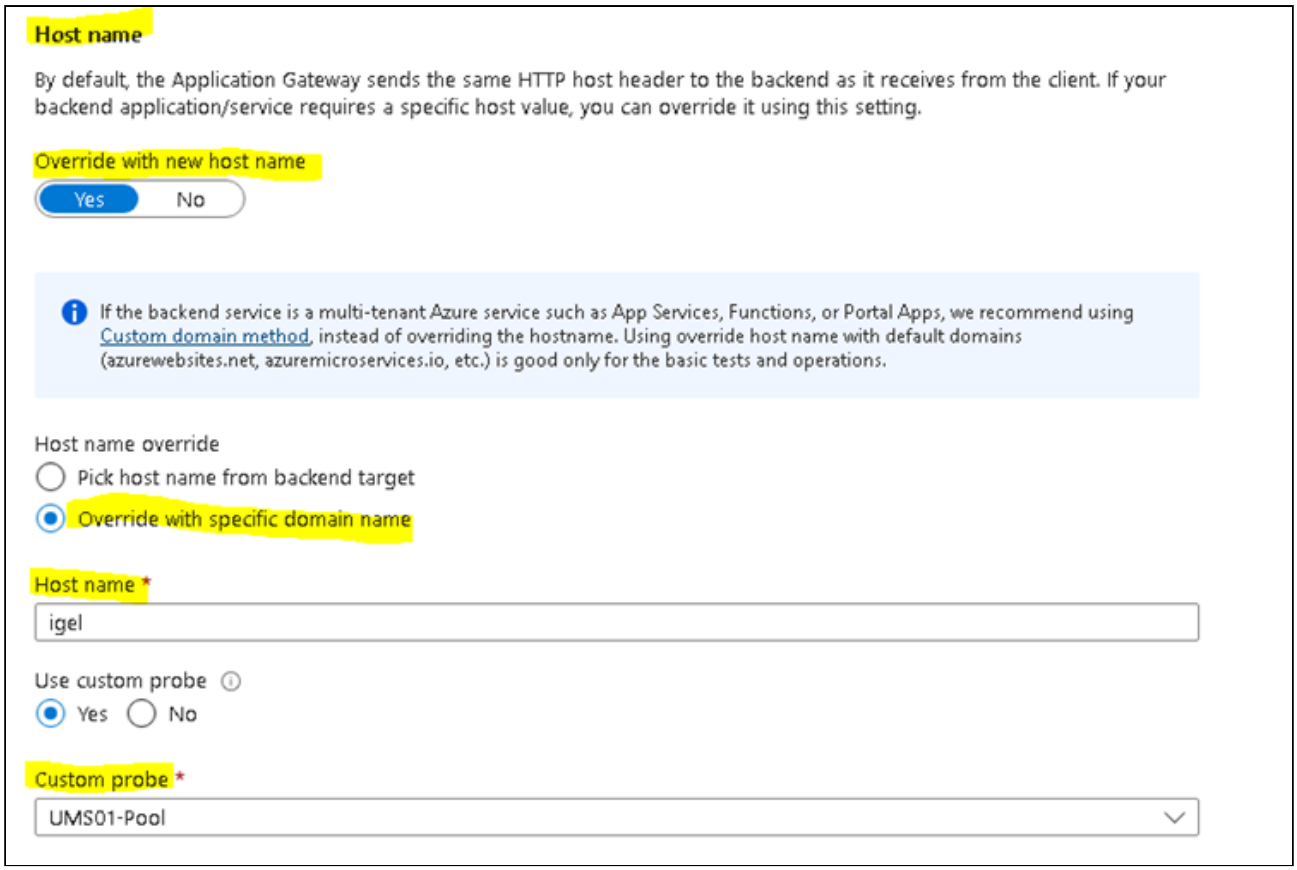


Troubleshooting Certificate Error: Common Name Does Not Match

The UMS or ICG certificate must contain the FQDN of the Backend Server as the Common Name. This value is mandatory for the Azure Application Gateway connection to the Backend. The following error occurs if the certificate is wrong.



In case the Common name cannot be adjusted, it is possible to adopt the Hostname of the UMS / ICG in the Backend Settings. In this case a custom probe must be defined with the **given Host name value**.


Host name
By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.
Override with new host name
Yes
No
If the backend service is a multi-tenant Azure service such as App Services, Functions, or Portal Apps, we recommend using Custom domain method, instead of overriding the hostname. Using override host name with default domains (azurewebsites.net, azuremicroservices.io, etc.) is good only for the basic tests and operations.
Host name override
Pick host name from backend target
Override with specific domain name
Host name *
igel
Use custom probe
Yes
No
Custom probe *
UMS01-Pool

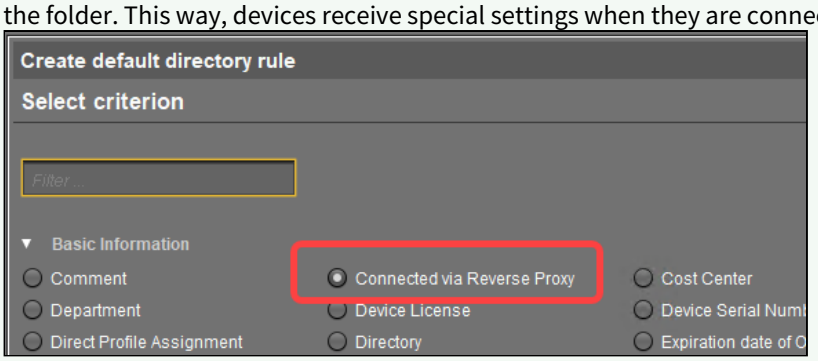
Citrix Netscaler Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

This article describes a possible configuration of the IGEL Universal Management Suite (UMS) and Citrix Netscaler for SSL offloading.

General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
As the reverse proxy is an external software we cannot provide full support for each version.

Default Directory Rules for Devices Connected via Reverse Proxy

If you integrate a reverse proxy, you can create a default directory rule to sort devices connected through the reverse proxy into a dedicated folder. You can do this by using the **Connected via Reverse Proxy** criterion. You can use the dedicated folder to assign objects (files, profiles, etc.) to the devices included in the folder. This way, devices receive special settings when they are connected through a reverse proxy.



For more on default directory rules, see How to Create a Default Directory Rule[89].

Requirements

Requirements for UMS and certificate configuration for reverse proxy are summarized in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).

Process Overview

The configuration tasks of the reverse proxy are:

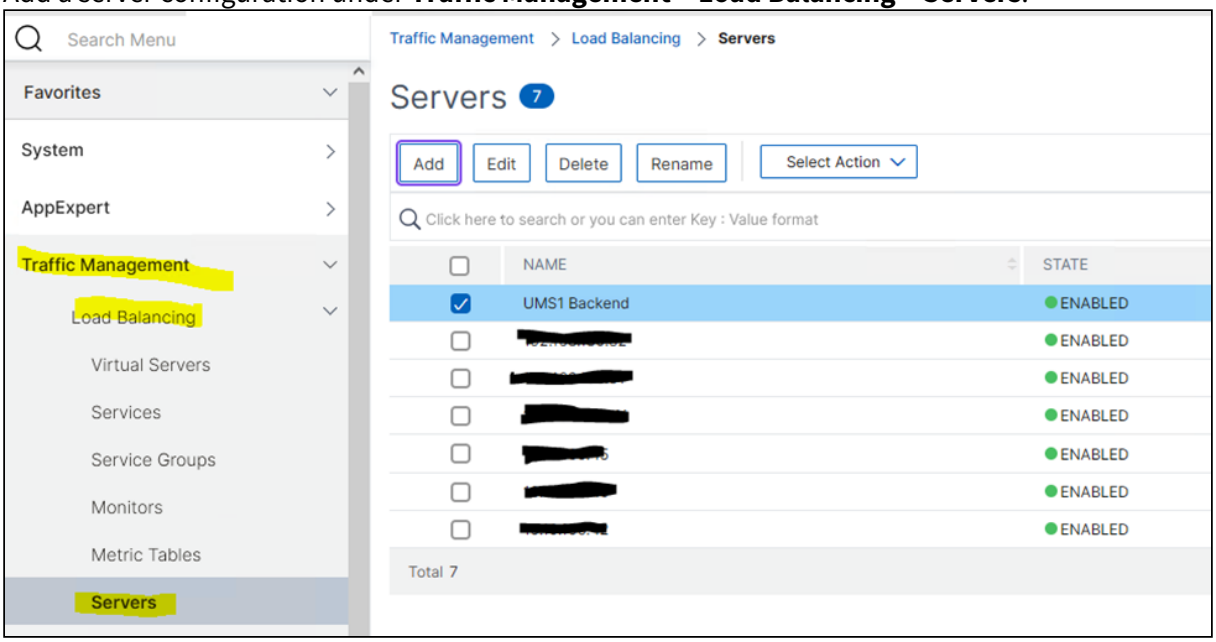
- UMS / ICG configuration and certificate export as described in Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).
- UMS server backend configuration
- Virtual Server configuration
- SSL policy configuration for client certificate forwarding

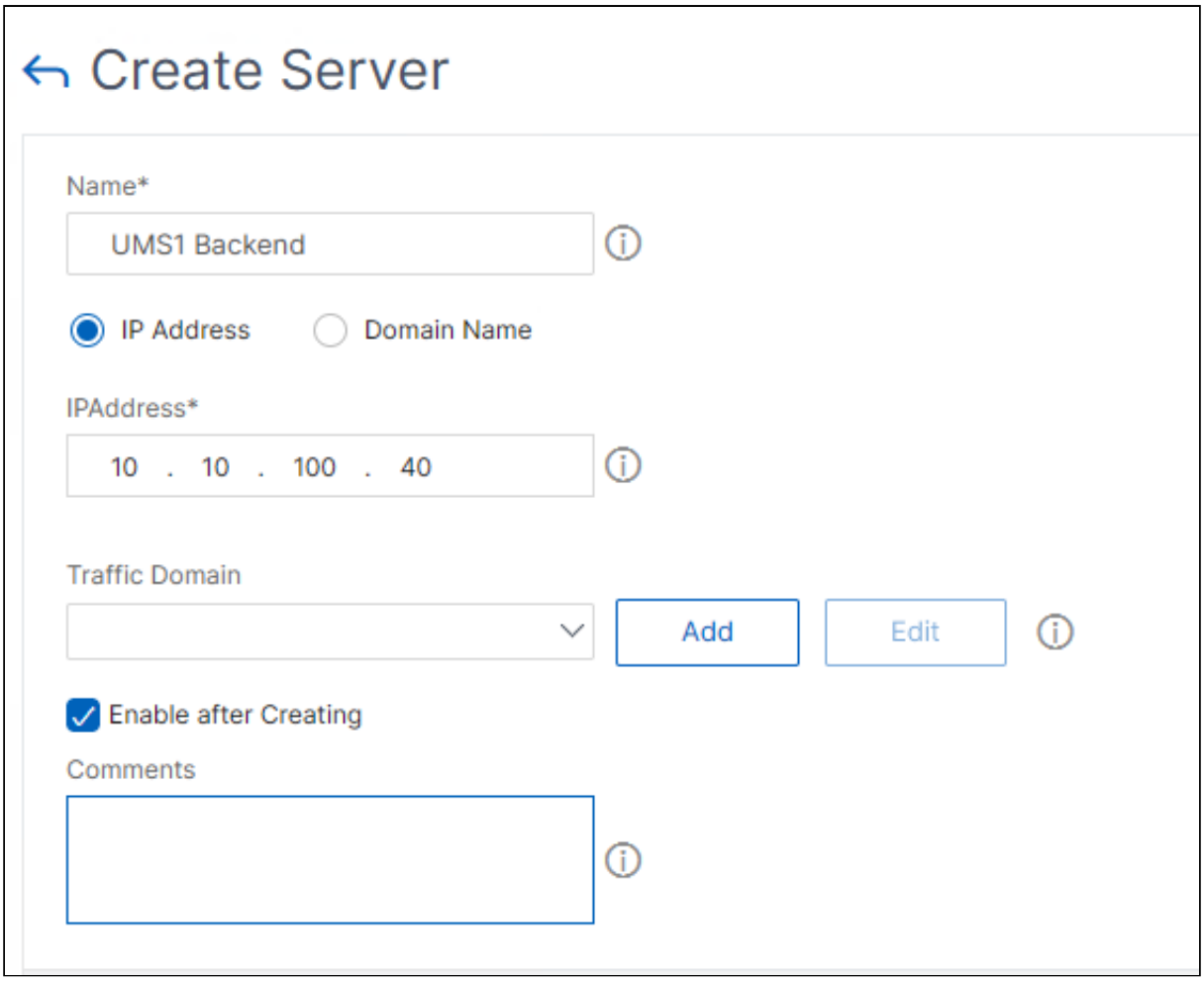
89. https://kb.igel.com/en/universal-management-suite/current/how-to-create-a-default-directory-rule

UMS Server Backend Configuration (SSL)

Create Server

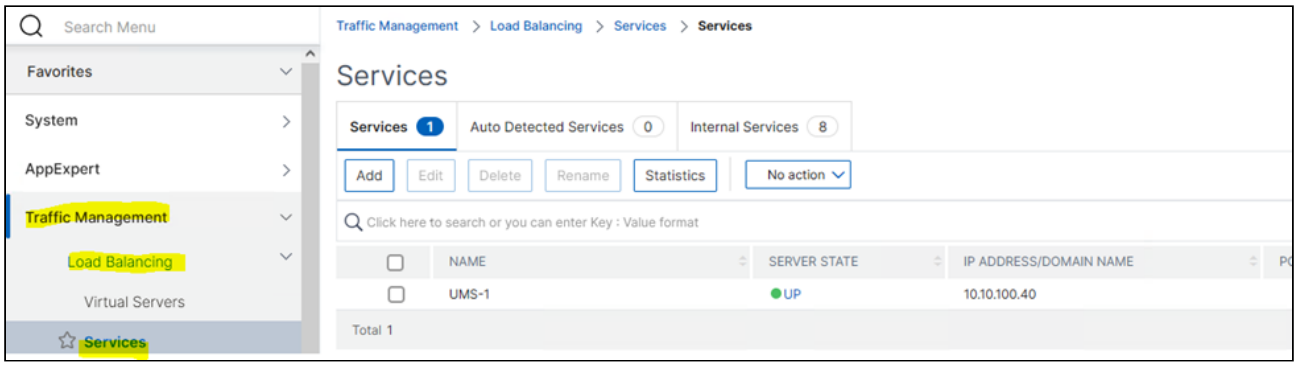
1. Add a server configuration under **Traffic Management > Load Balancing > Servers**.



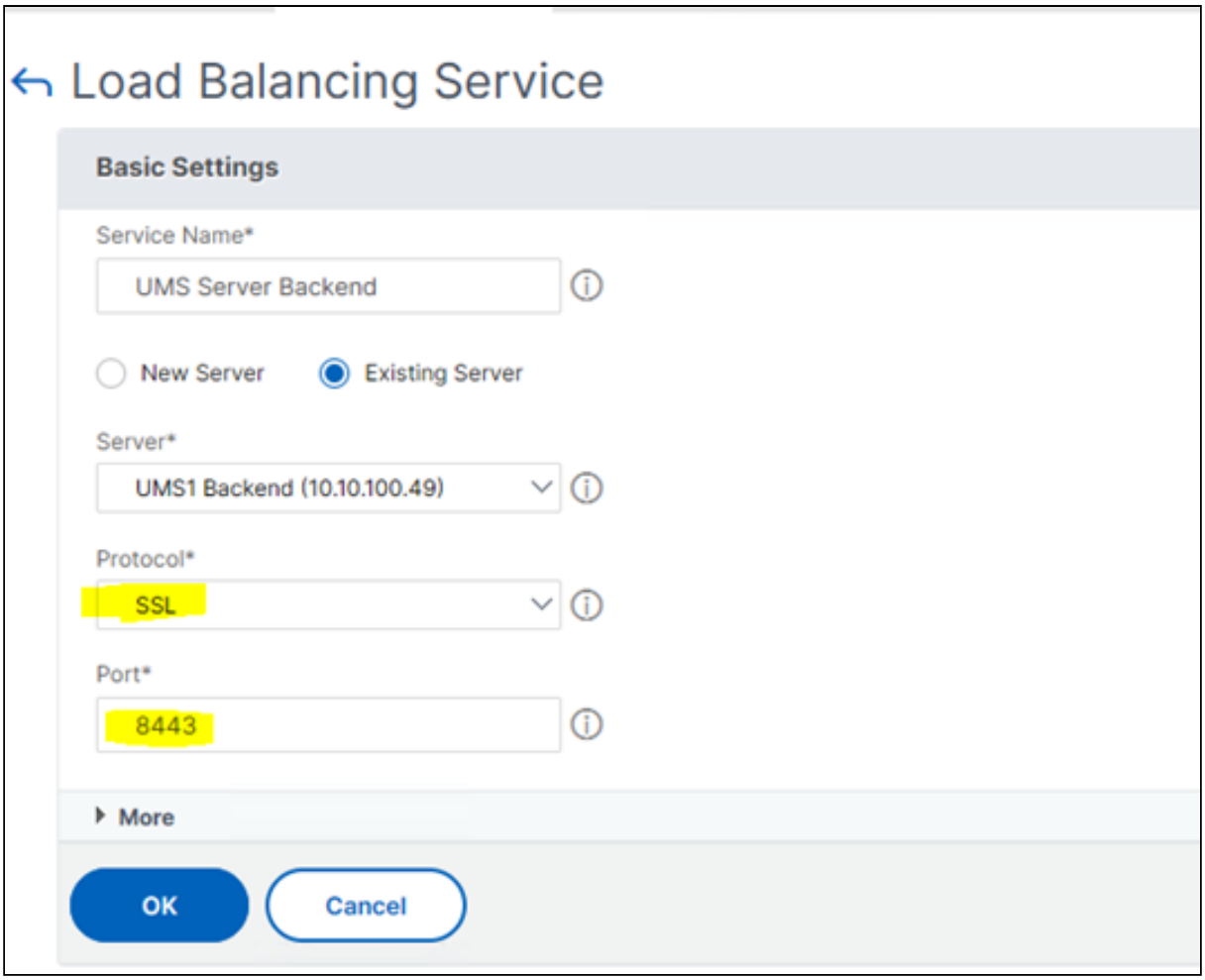


Add Load Balancing Service and Monitor

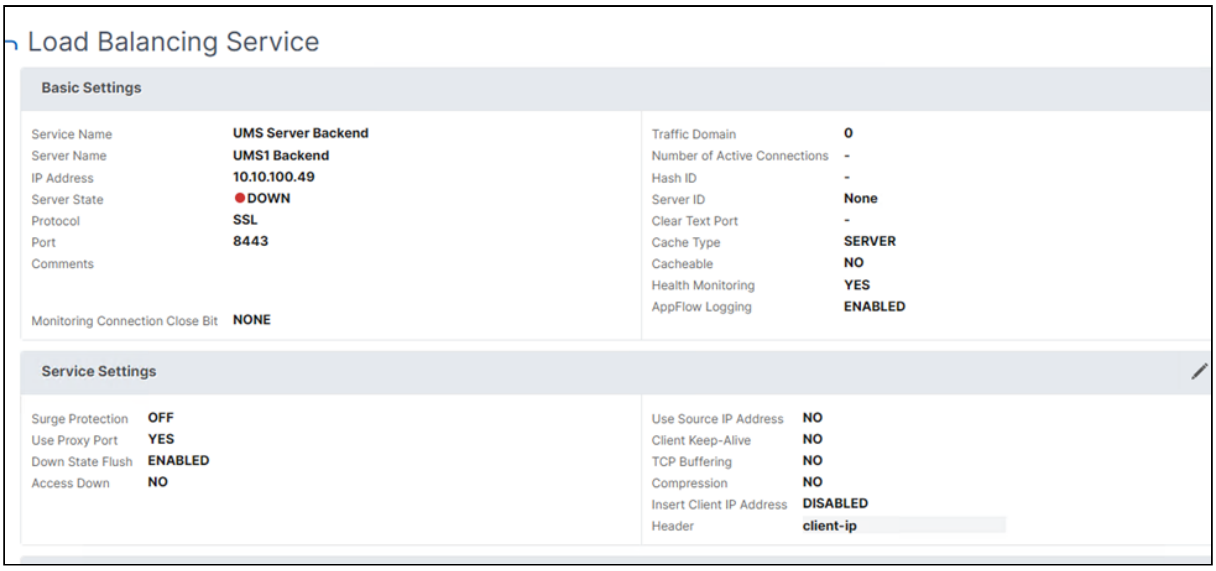
The UMS server backend must be configured as Service under **Traffic Management > Load Balancing > Services**.



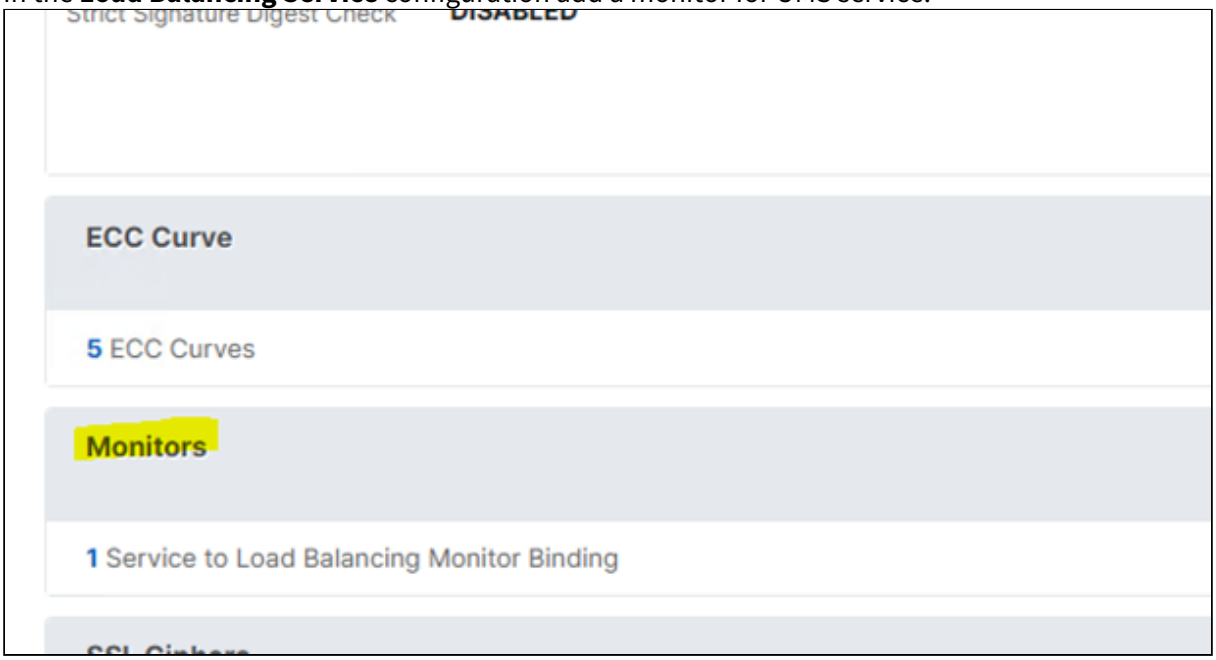
1. Click **Add**.



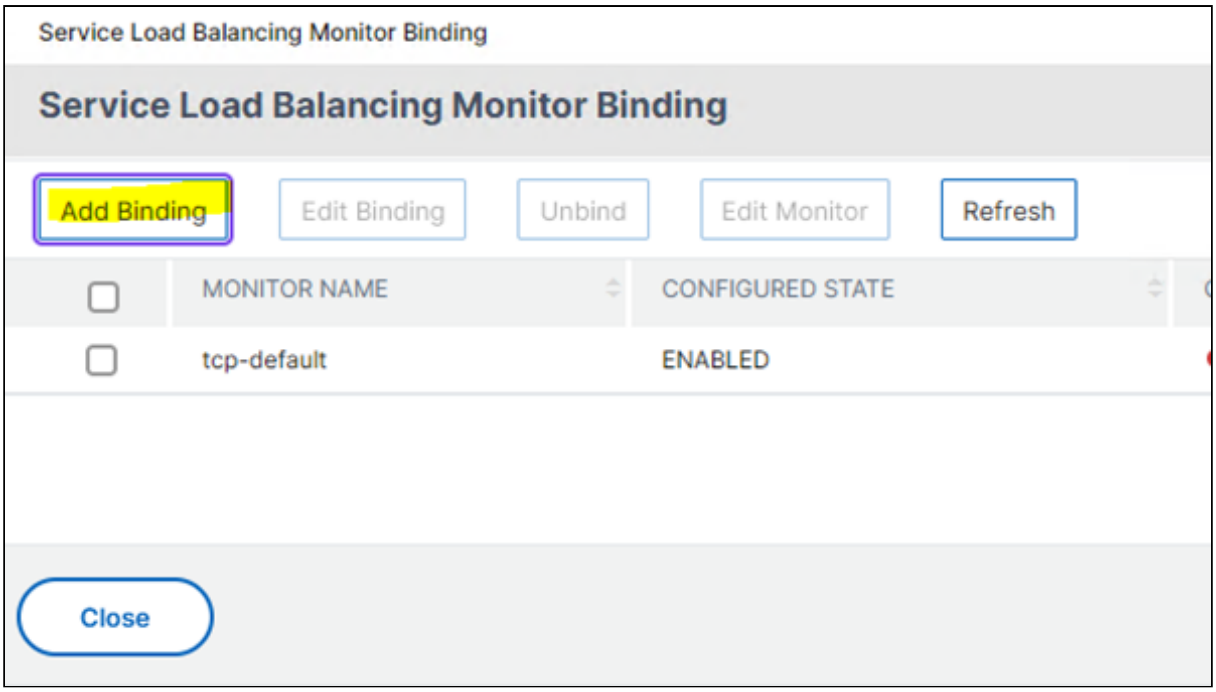
2. Set the following:
    - Select the previously created **Server** definition.
    - Set **Protocol** to **SSL**.
    - Set **Port** to UMS Web Port (**8443**).
3. Click **OK** and check the settings in the **Load Balancing Service** details dialog.



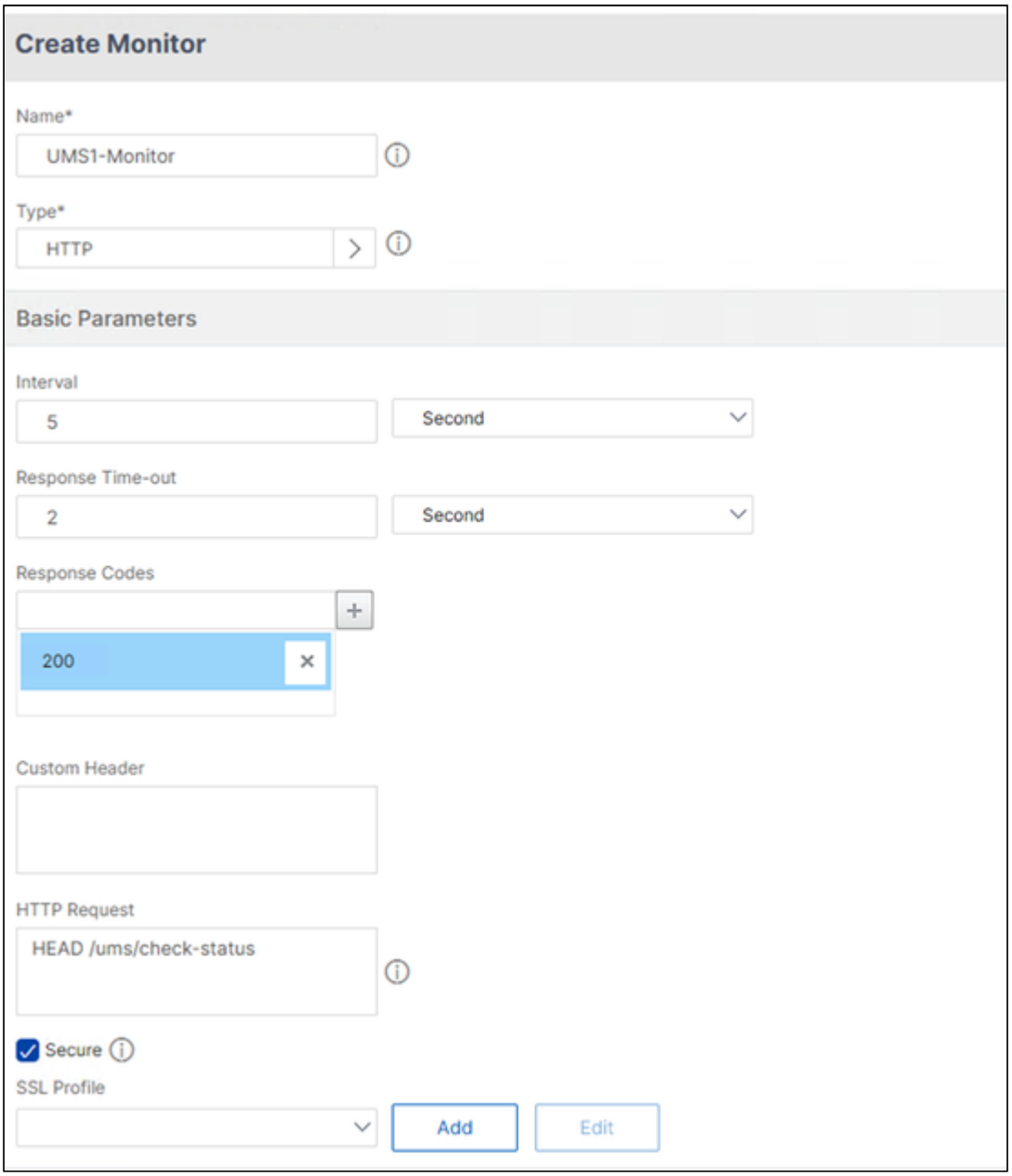
4. In the **Load Balancing Service** configuration add a monitor for UMS service.



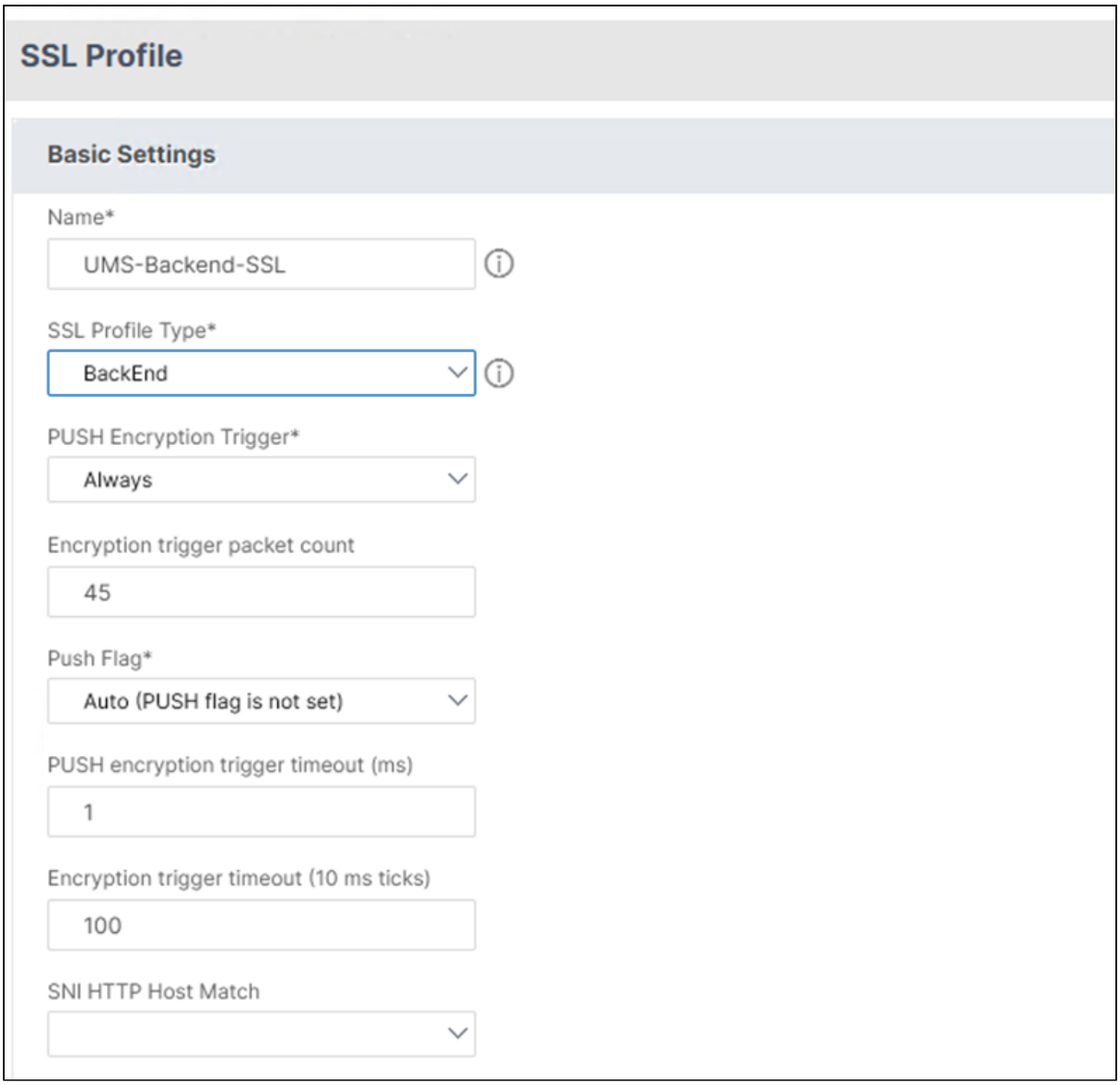
5. Click **Add Binding**.



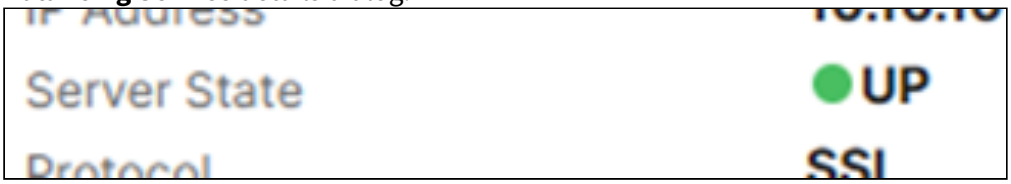
6. Set the following monitor settings:
   - **Type** to **HTTP**.
   - **Response Code** to **200**.
   - **HTTP Request**: `HEAD /ums/check-status`.
   - Enable **Secure**.



7. Under **SSL Profile** click **Add**.
   The **SSL Profile** configuration dialog opens.



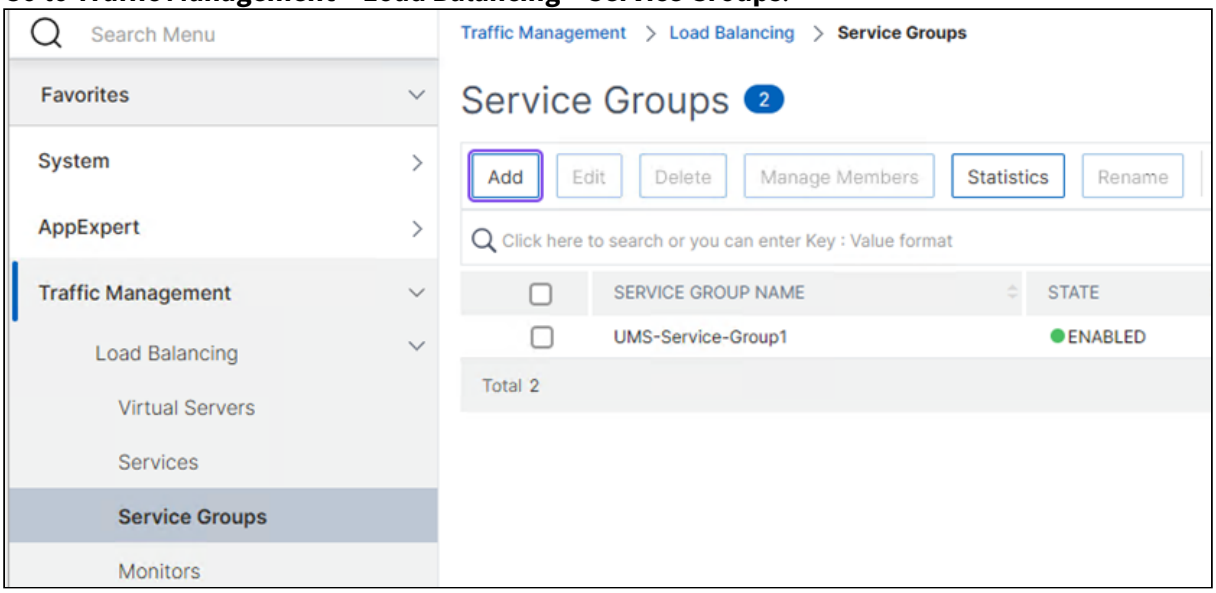
8. Set **SSL Profile Type** to **BackEnd**.
   When the backend configuration is successful the Server State is listed as up in the **Load Balancing Service** details dialog.



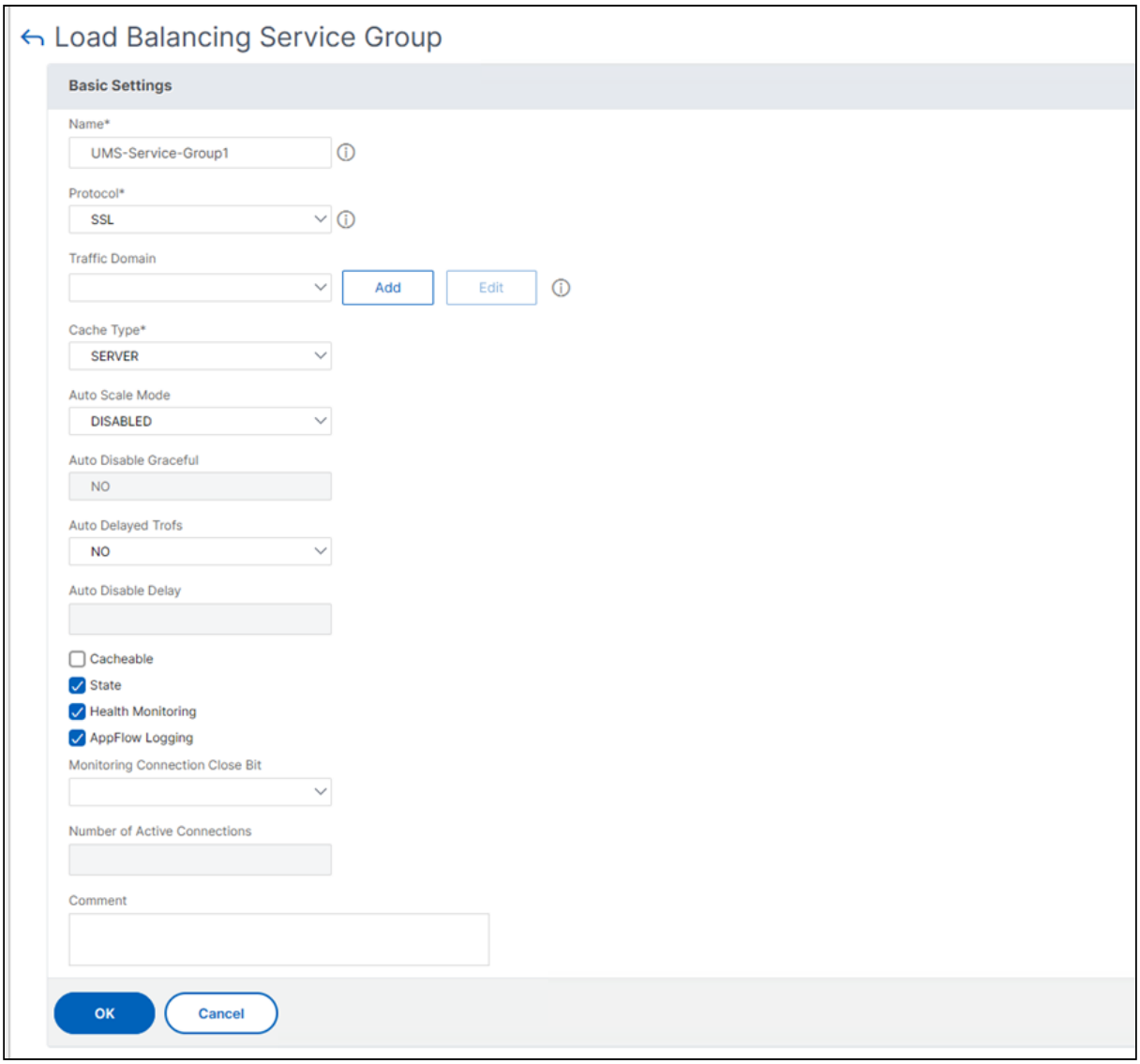
Add a Service Group

The backend server can be grouped to Service Groups.

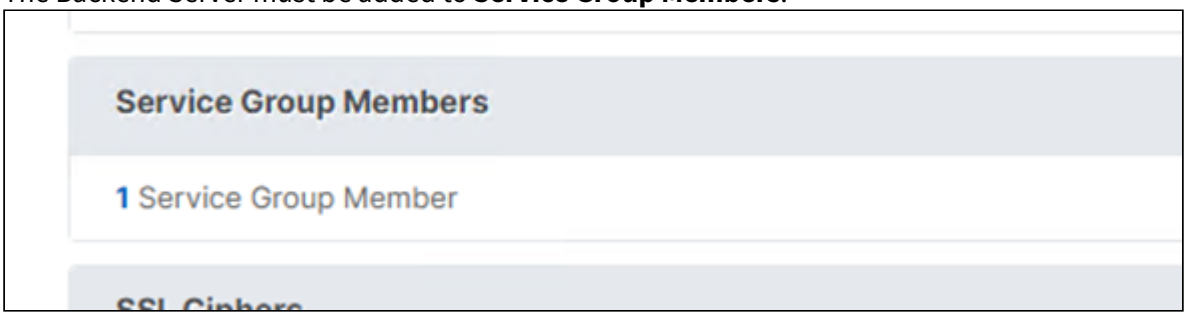
1. Go to **Traffic Management > Load Balancing > Service Groups**.



2. Click **Add**.

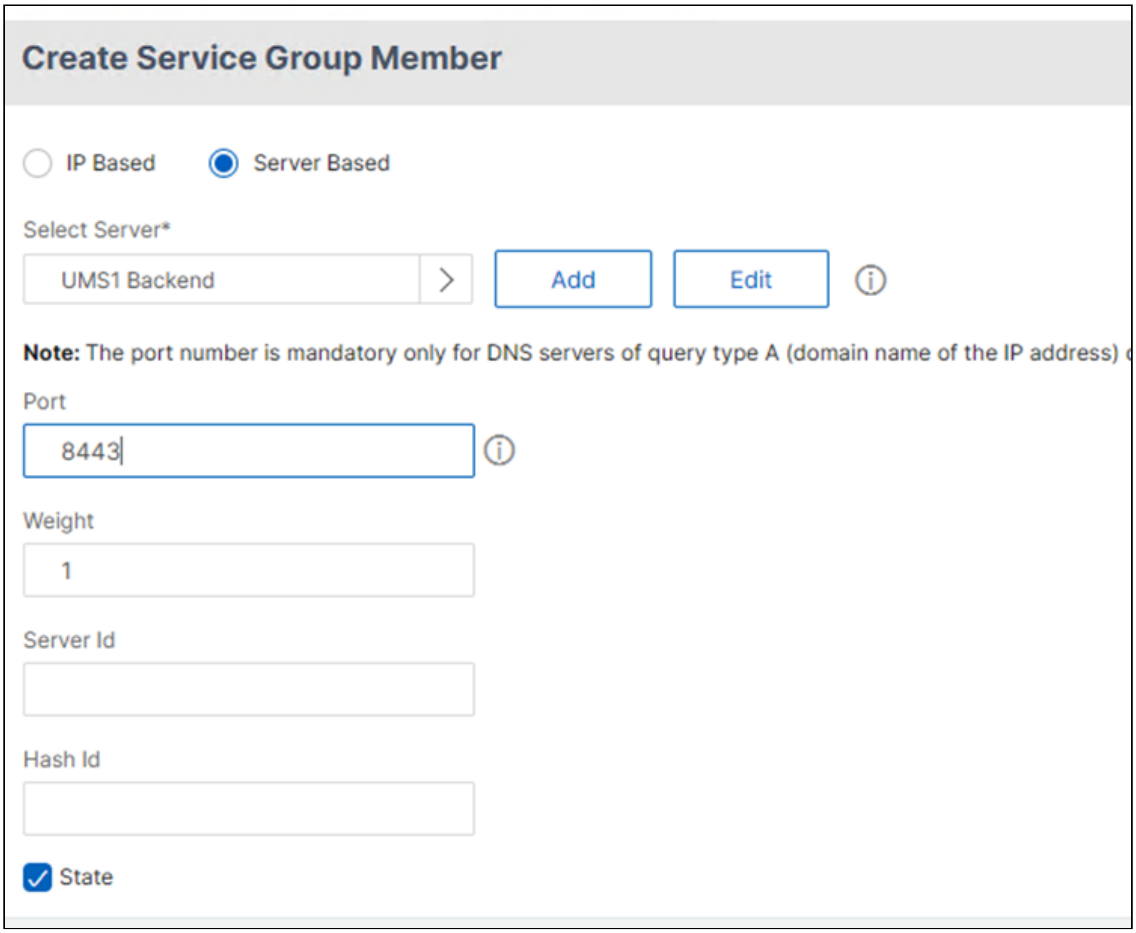


3. Set the **Protocol** to **SSL** and click **OK**.
4. The Backend Server must be added to **Service Group Members**.



5. In the Create Service Group Member dialog, set the following:
   - Select the radio button **Server Based.**

- Under **Select Server**, select the created service (UMS server) definition.
- Add **8443** under **Port**.

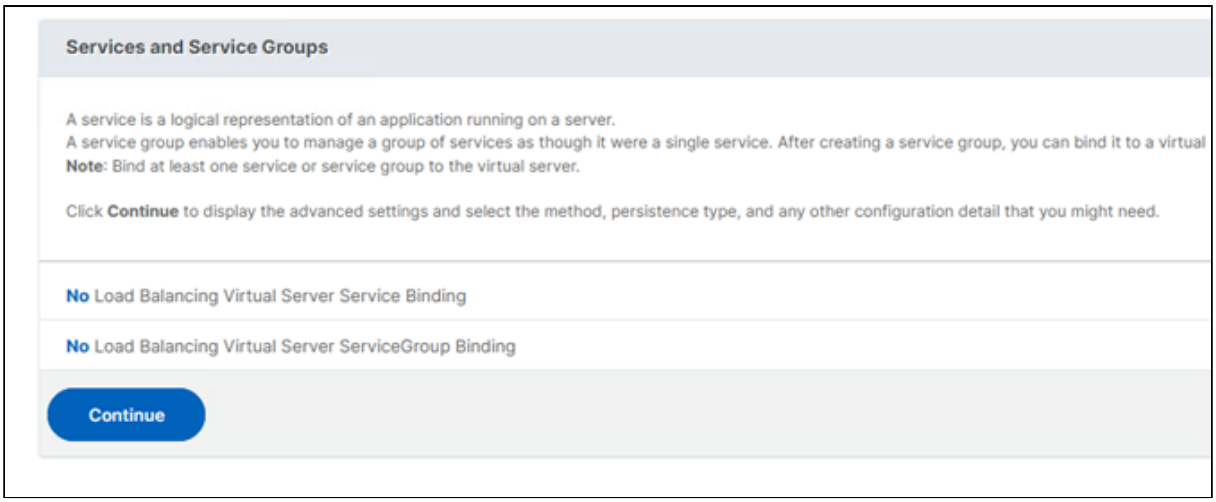


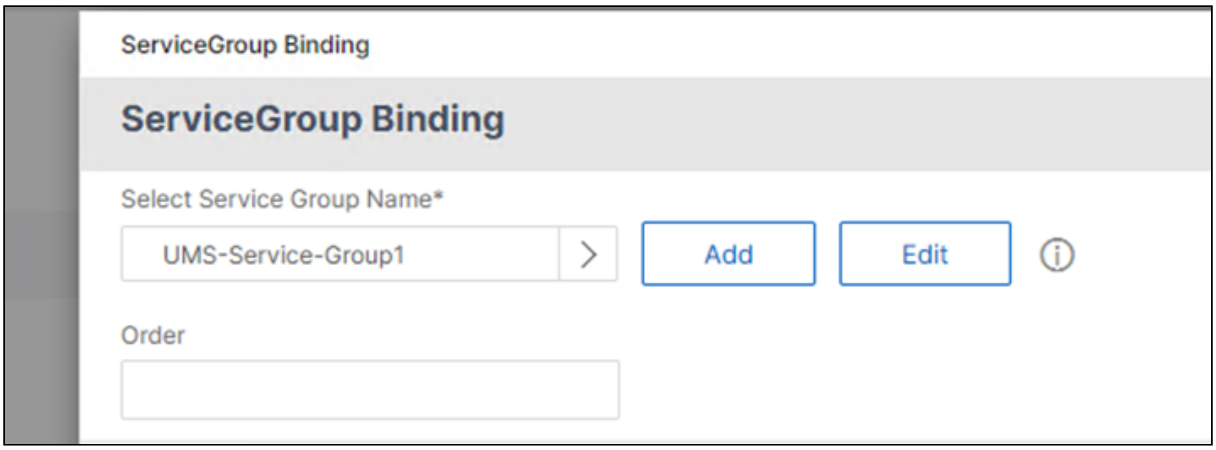
Virtual Server Configuration

The Netscaler Listener is called a Virtual Server and can be configured under **Traffic Management > Load Balancing > Virtual Servers**.

1. Add a Virtual Server.
2. Set the following:
   - **Protocol** to **SSL**
   - **IP Address**
   - **Port** to **443**

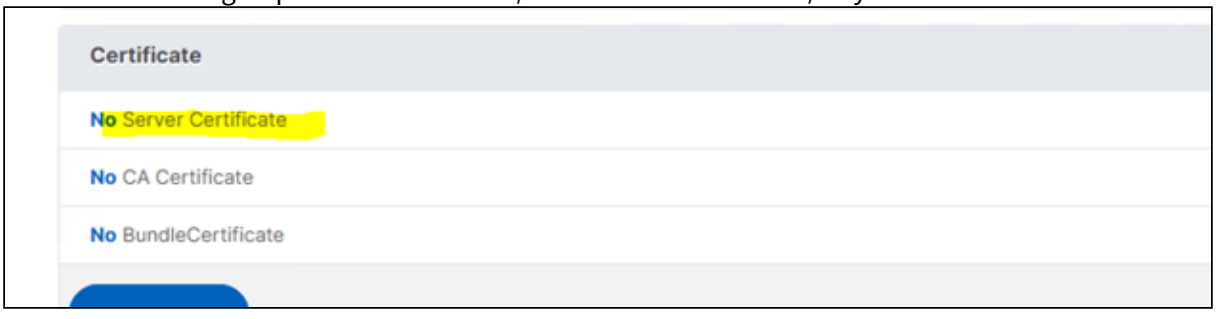
   
3. Under **Services and Service Groups** add the previously created Service Group.



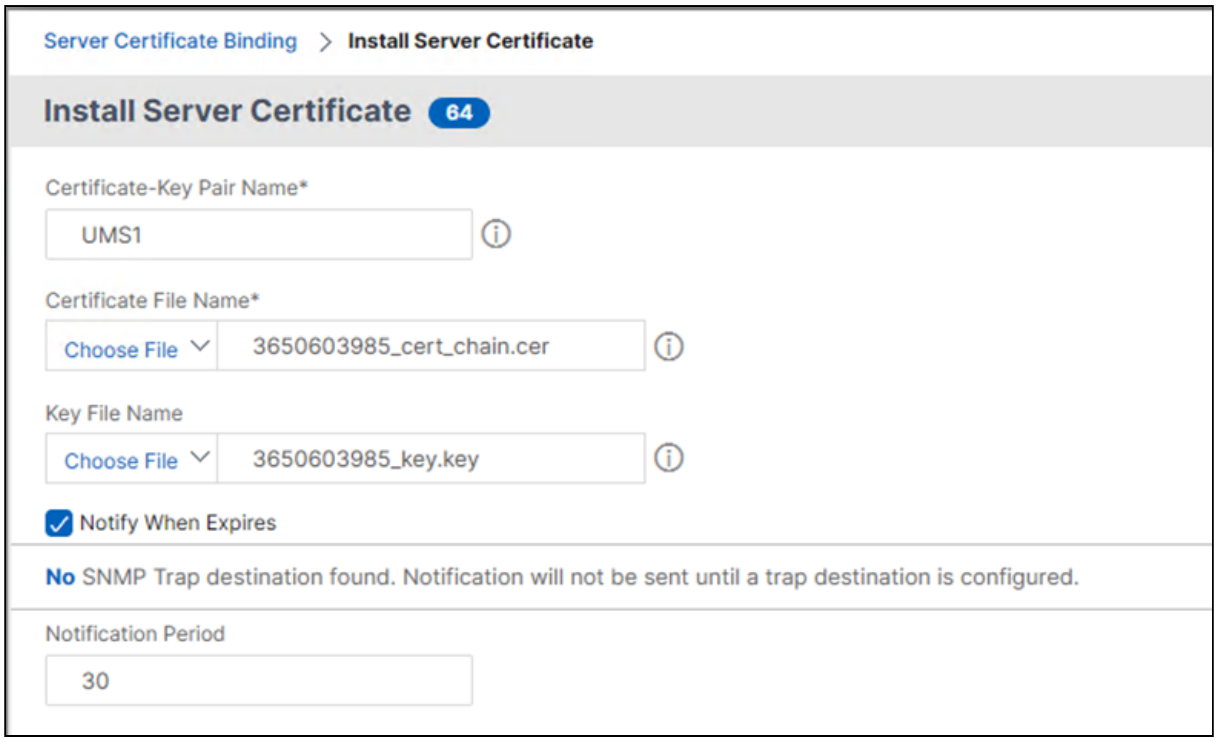


Add Certificates

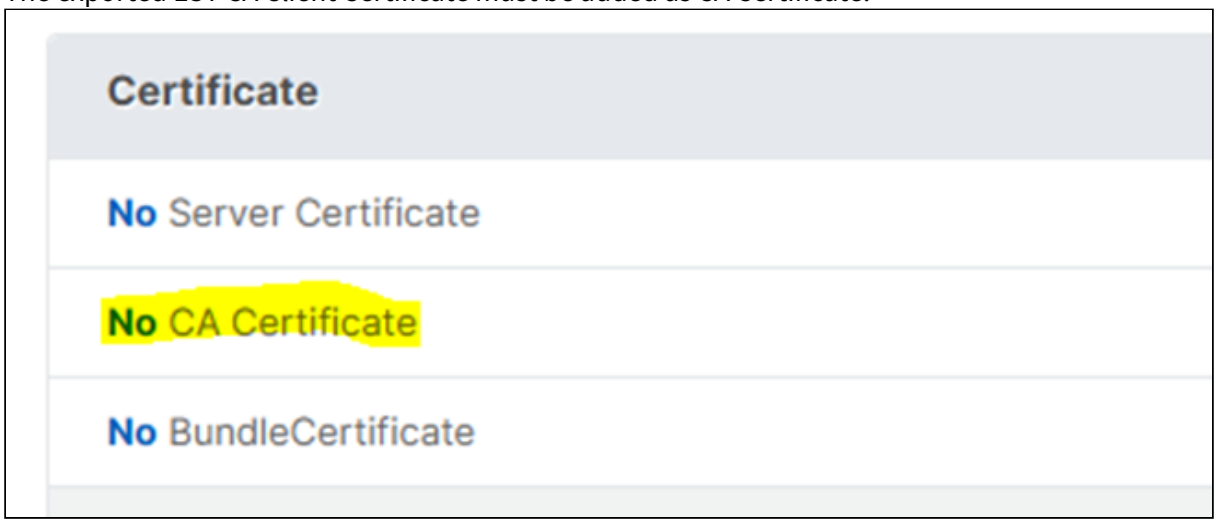
1. Under **Certificate** add a Server Certificate. For details on how to get the certificate chain and key, see Configure the UMS to Integrate Reverse Proxy with SSL Offloading (see page 277).
   The SSL Offloading requires the UMS Web / ICG Server certificates / keys for the SSL termination.

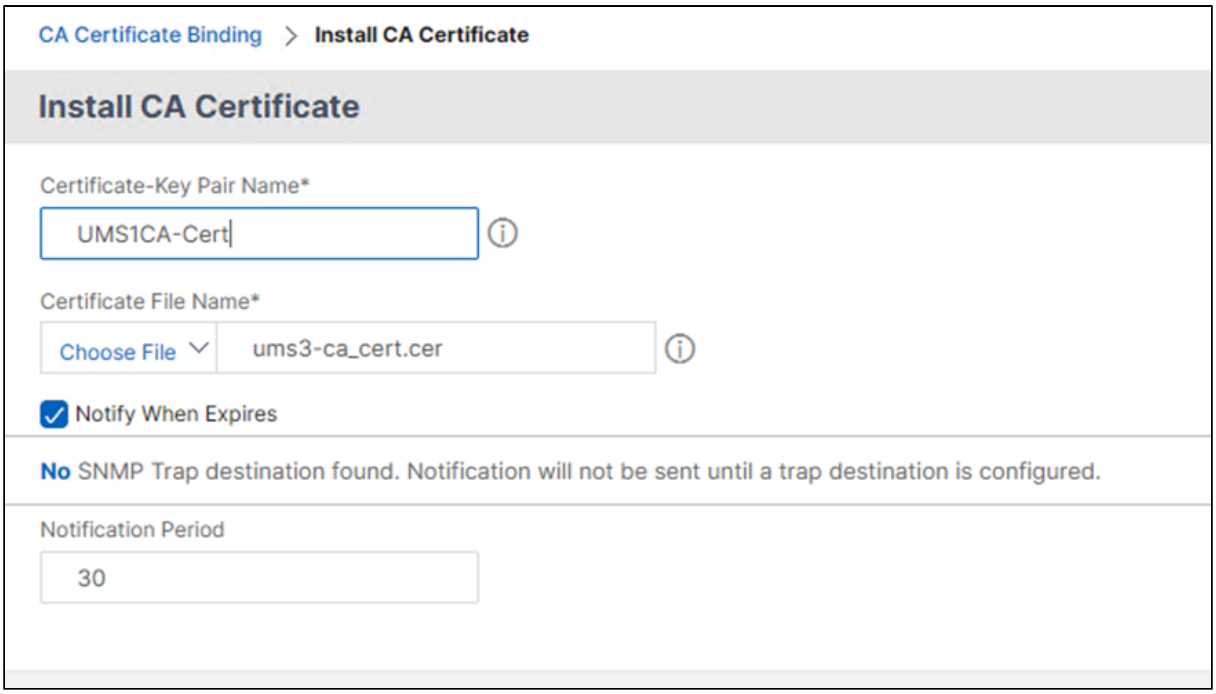


2. Select first the Web/ICG Certificate Chain file and add the Web/ICG key file.

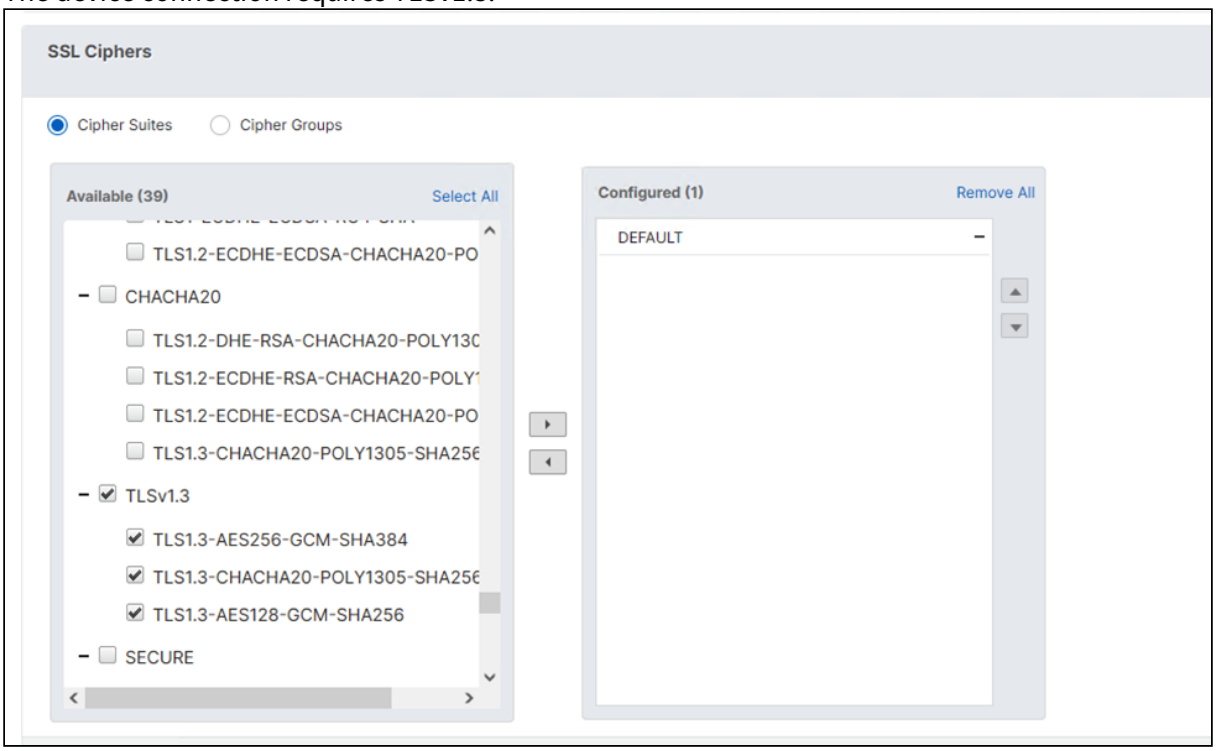


3. Add the Client Certificate Chain.
4. The exported EST CA Client Certificate must be added as CA Certificate.



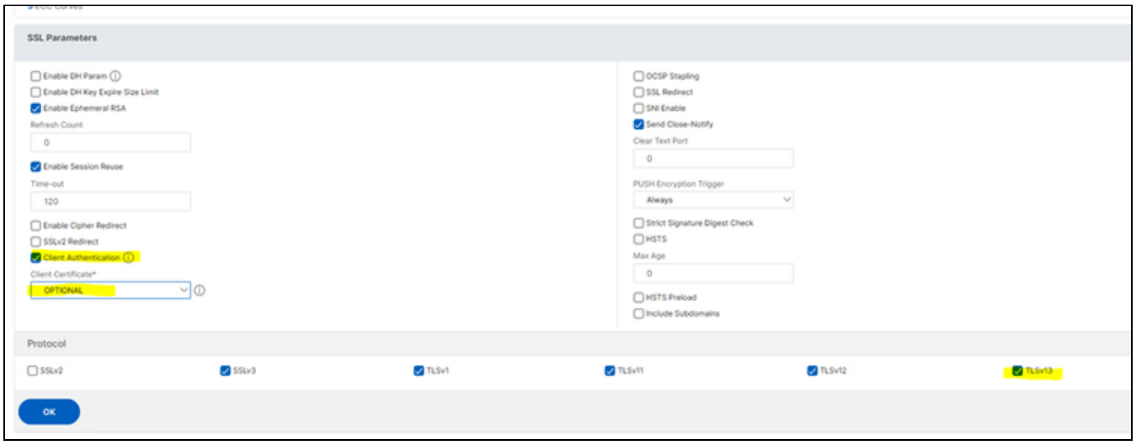


5. Under **SSL Ciphers**, add TLSv1.3
   The device connection requires TLSv1.3.



6. Under SSL Parameters, set the following:

- Enable **Client Authentication**
- Set **Client Certificate** to **Optional**
- Activate **TLSv13** under **Protocol**

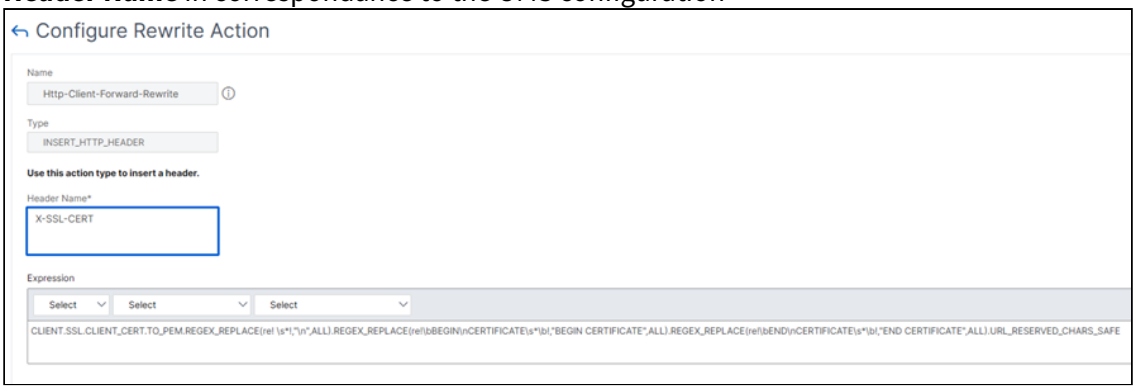


Configure SSL Policy for Client Certificate Forwarding

Add a Rewrite Action and Policy under **AppExpert > Rewrite**:

1. Add a **Rewrite Action**.

2. Set the following parameters:
   - **Type** to **INSERT_HTTP_HEADER**
   - **Header Name** in correspondance to the UMS configuration

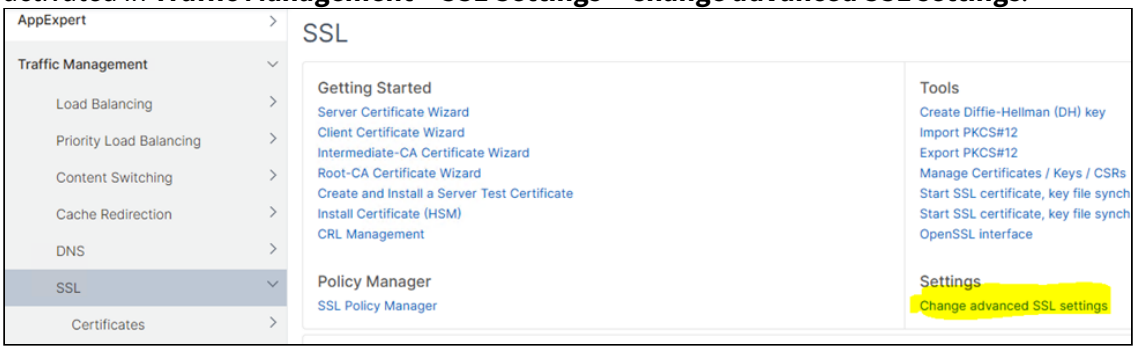


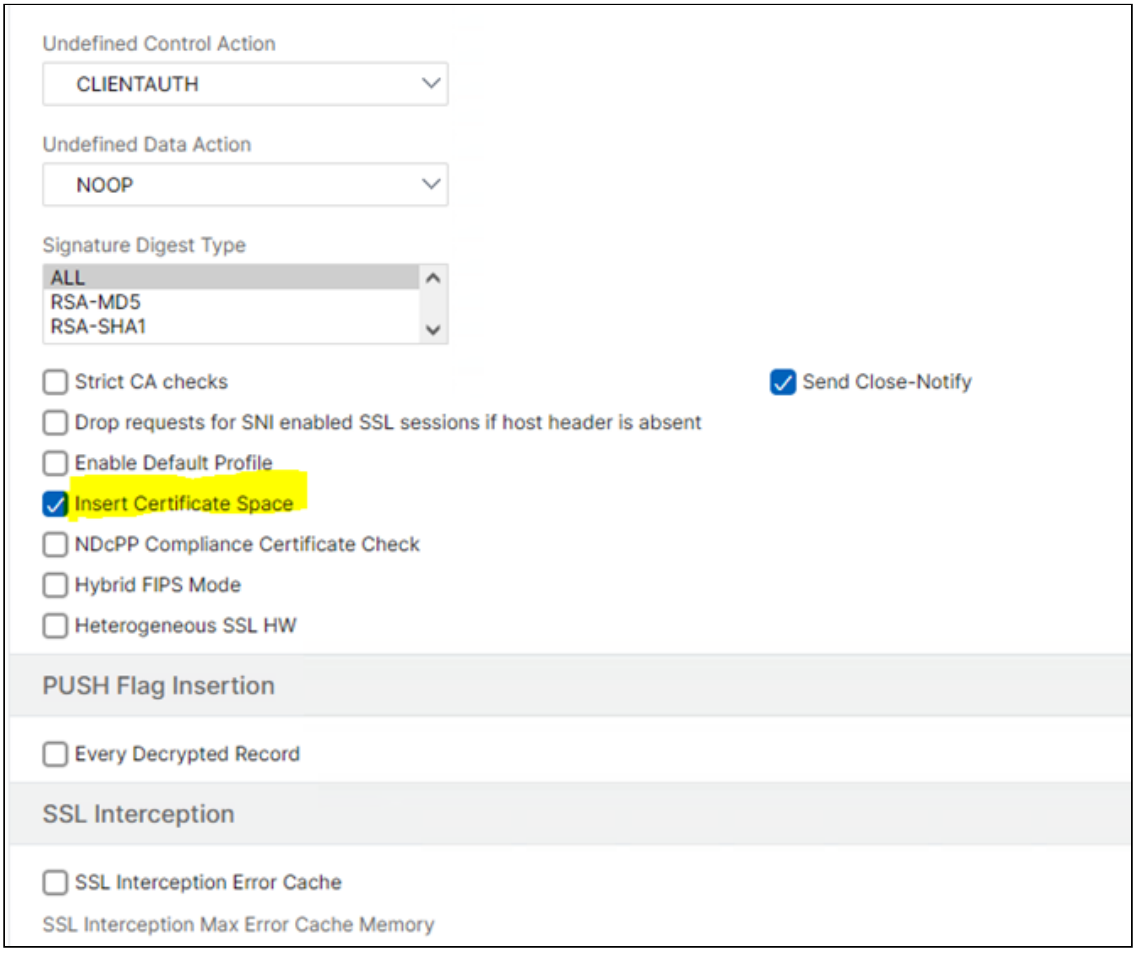
- The expression for the action is used to set the correct Client Certificate value. The forwarded certificate must be URL encoded and contain correct line break information:

```
CLIENT.SSL.CLIENT_CERT.TO_PEM.REGEX_REPLACE(re!
\s*!,"\n",ALL).REGEX_REPLACE(re!
\bBEGIN\nCERTIFICATE\s*\b!,"BEGIN
CERTIFICATE",ALL).REGEX_REPLACE(re!
\bEND\nCERTIFICATE\s*\b!,"END
```

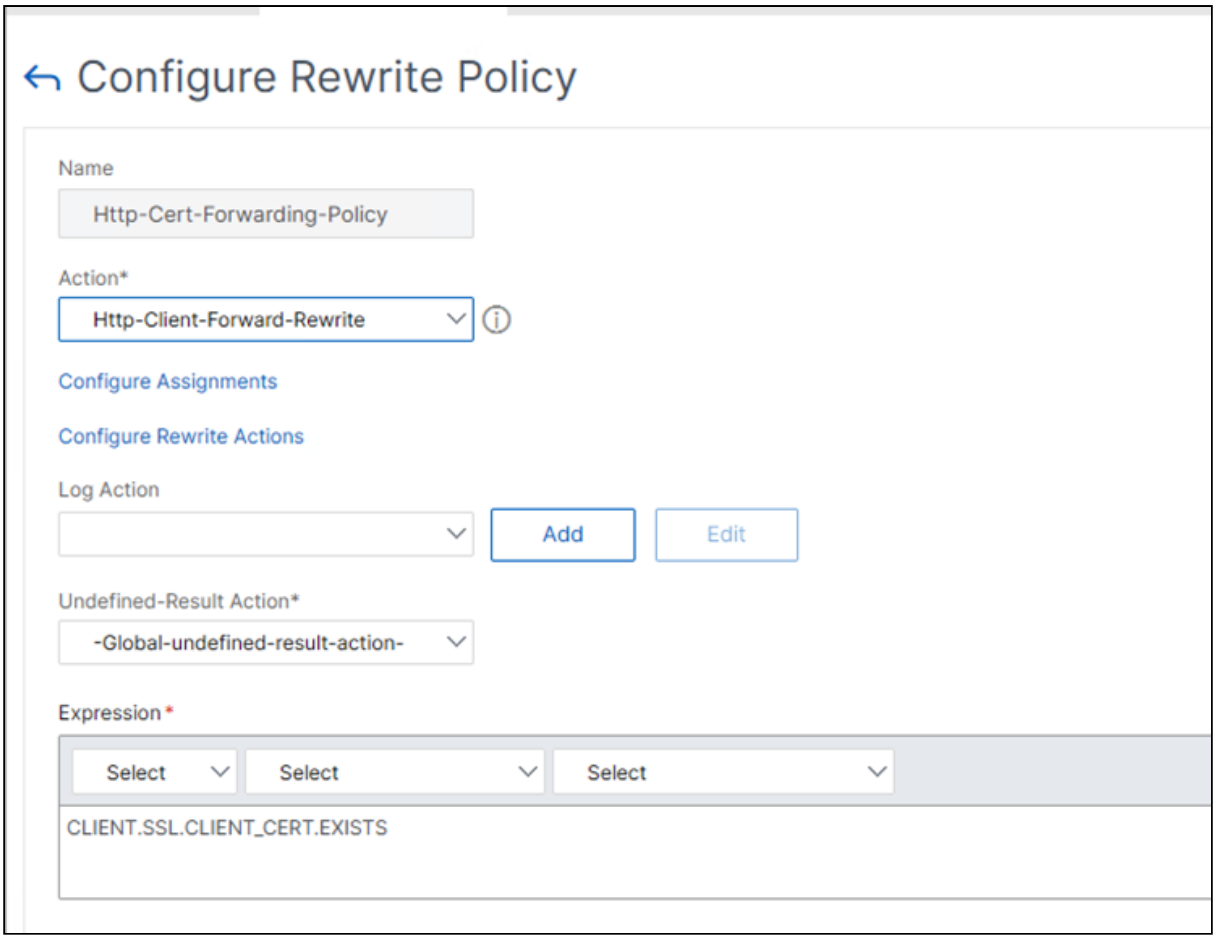
```
CERTIFICATE",ALL).URL_RESERVED_CHARS_SAFE
```

This expression is an example and requires the **Insert Certificate Space** parameter to be activated in **Traffic Management > SSL Settings > Change advanced SSL settings**.

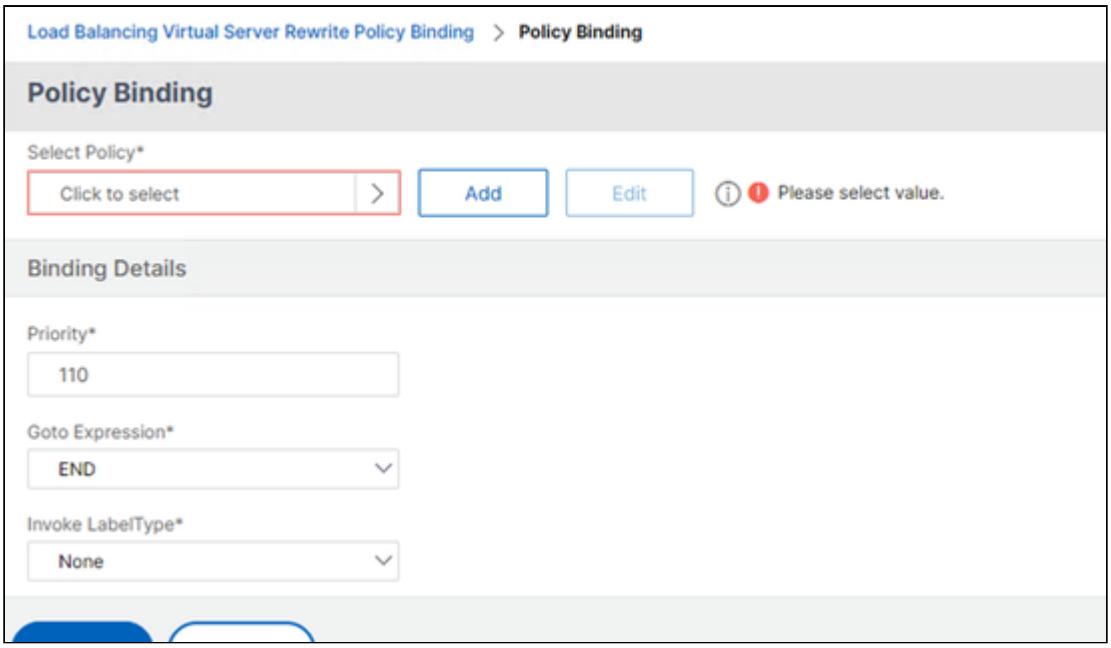




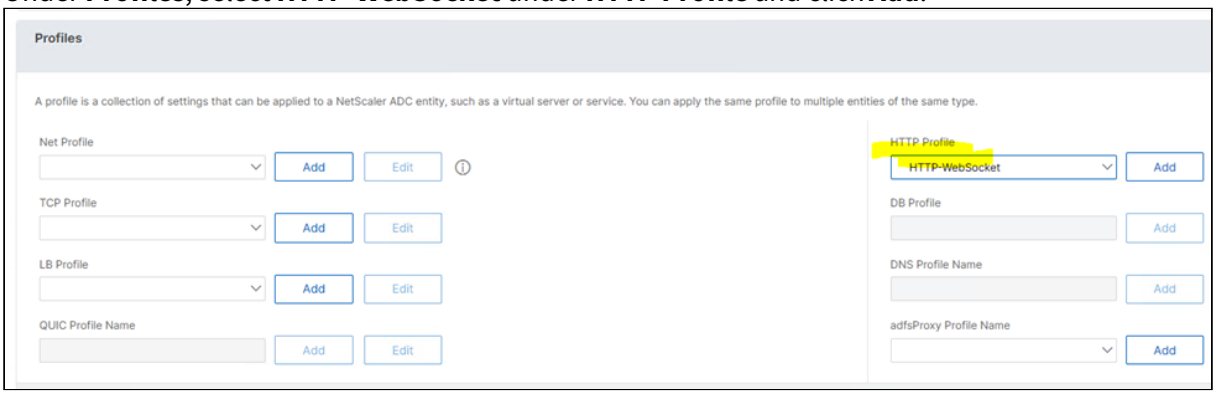
3. Add a **Rewrite Policy**.
4. Under **Action** select the previously configured action to bind it to the policy.



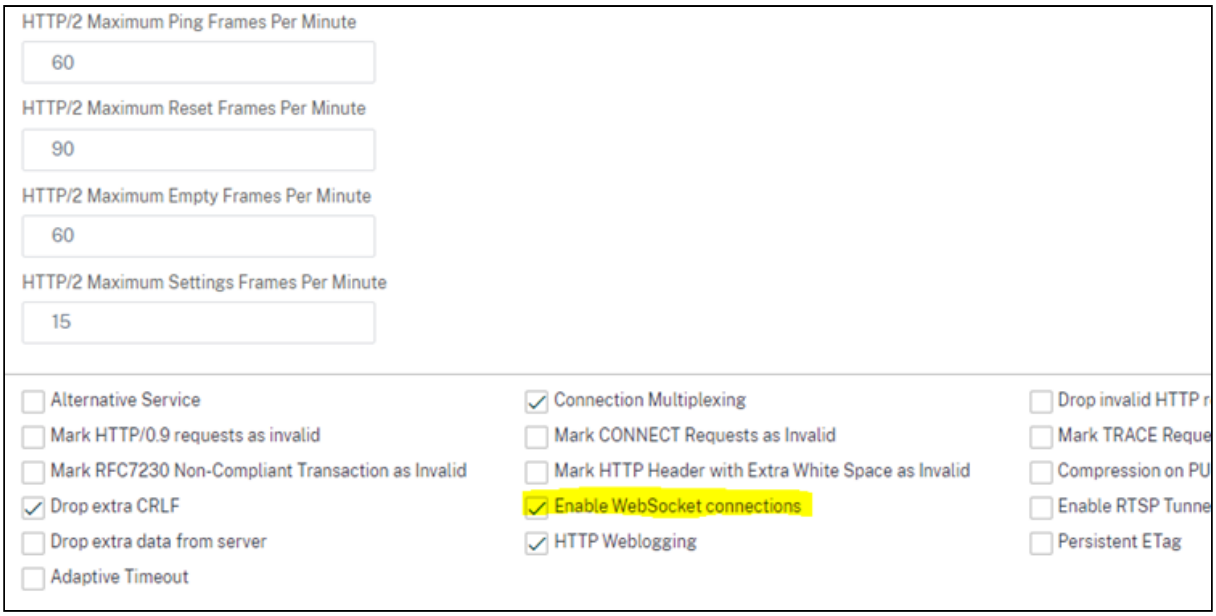
5. Set the expression to:
   CLIENT.SSL.CLIENT_CERT.EXISTS
   The policy expression checks if the Client Certificate is available.
6. Add the Rewrite Policy to the Load Balancing Virtual Server under **Policy Binding.**



7. Under **Profiles**, select **HTTP-WebSocket** under **HTTP Profile** and click **Add**.



8. Activate **Enable WebSocket connections**.


HTTP/2 Maximum Ping Frames Per Minute
60
HTTP/2 Maximum Reset Frames Per Minute
90
HTTP/2 Maximum Empty Frames Per Minute
60
HTTP/2 Maximum Settings Frames Per Minute
15
Alternative Service
Mark HTTP/0.9 requests as invalid
Mark RFC7230 Non-Compliant Transaction as Invalid
Drop extra CRLF
Drop extra data from server
Adaptive Timeout
Connection Multiplexing
Mark CONNECT Requests as Invalid
Mark HTTP Header with Extra White Space as Invalid
Enable WebSocket connections
HTTP Weblogging
Drop invalid HTTP r
Mark TRACE Reque
Compression on PU
Enable RTSP Tunne
Persistent ETag

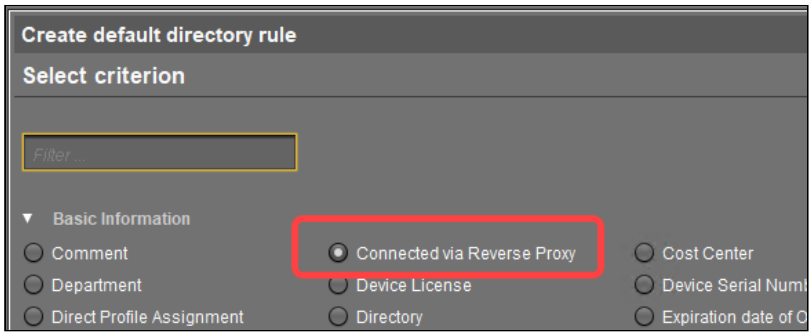
Useful IGEL UMS Features for Managing Reverse Proxy Connected Devices

This article describes IGEL Universal Management Suite (UMS) features that support the management of devices connected through a reverse proxy.

Default Directory Rules for Devices Connected via Reverse Proxy

You can create a default directory rule to sort devices connected through the reverse proxy into a dedicated folder.

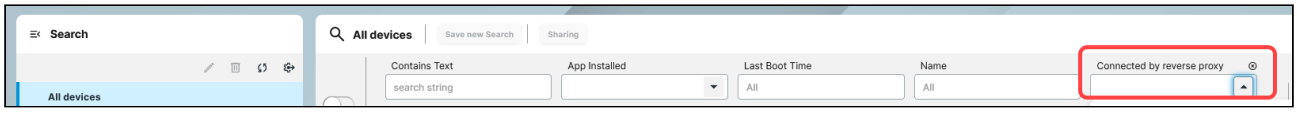
You can do this by using the **Connected via Reverse Proxy** criterion. You can use the dedicated folder to assign objects (files, profiles, etc.) to the devices included in the folder. This way, devices receive special settings when they are connected through a reverse proxy.



For more on default directory rules, see How to Create a Default Directory Rule[90].

Search for Devices Connected via Reverse Proxy in the UMS Web App

In the UMS Web App Search area[91], you can use the **Connected by reverse proxy** search criterion to list devices that are connected through a reverse proxy.



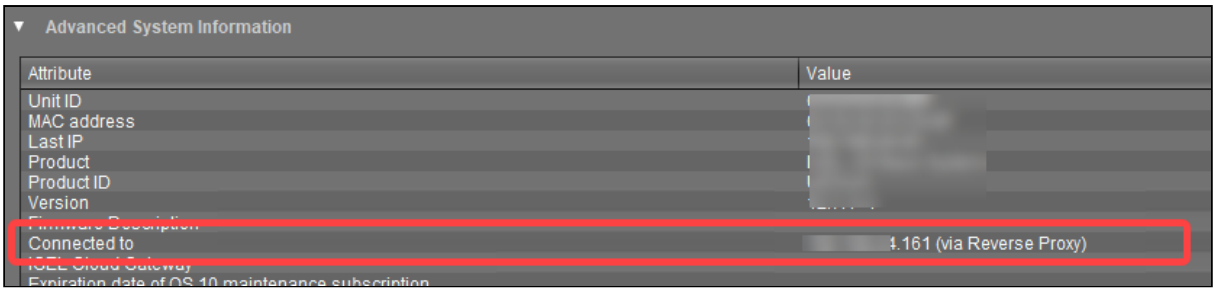
If you save the list as advanced search, you can use it in jobs and administrative tasks, see How to Use Advanced Search in the IGEL UMS Web App[92].

Device Information

You can quickly check whether a specific IGEL OS 12 device is connected via a reverse proxy by navigating to the device in the UMS Console or in the UMS Web App:

- IGEL UMS Web App: **Devices > [name of the device]** > **System Information** > **Connected to**.
- IGEL UMS Console: **Devices > [name of the device]** > **Advanced System Information** > **Connected to**.

90. https://kb.igel.com/en/universal-management-suite/current/how-to-create-a-default-directory-rule
91. https://kb.igel.com/en/universal-management-suite/current/search-for-devices-in-the-igel-ums-web-app
92. https://kb.igel.com/en/universal-management-suite/current/how-to-use-advanced-search-in-the-igel-ums-web-app



IMI

The responses to the following IGEL Management Interface (IMI)[93] requests contain a field `connectedViaReverseProxy` that indicates whether the device is currently routed through a reverse proxy connector:

- GET /v3/thinclients?facets=details[94]
- GET /v3/thinclients/{tcId}?facets=details[95]

93. https://kb.igel.com/en/igel-management-interface/current/imi-manual
94. https://kb.igel.com/en/igel-management-interface/current/get-v3-thinclients-facets-details
95. https://kb.igel.com/en/igel-management-interface/current/get-v3-thinclients-tcid-facets-details

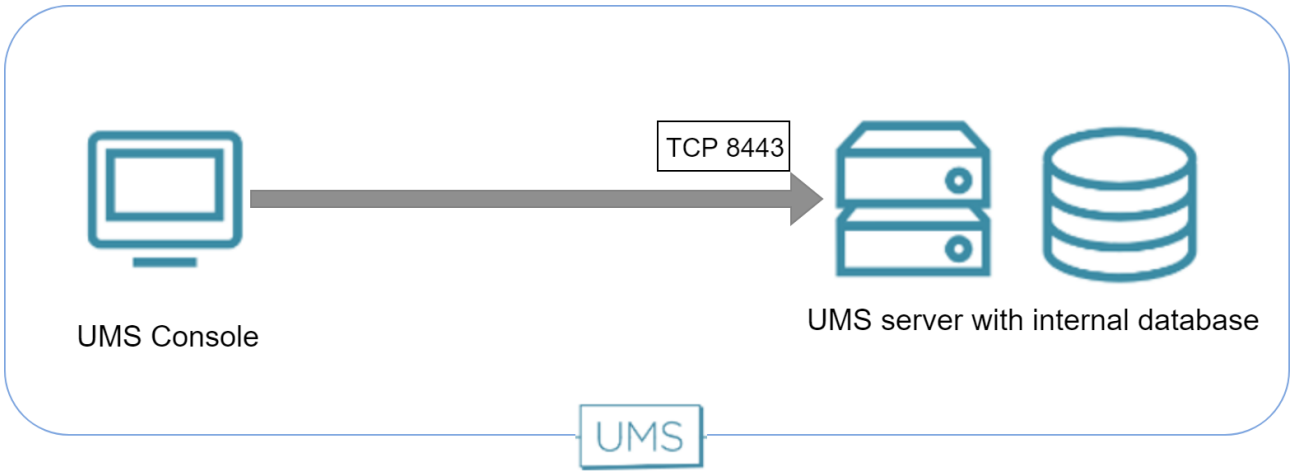
IGEL UMS Internal Communication

UMS with Internal Database

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

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

The following figure illustrates the communication between the UMS components:



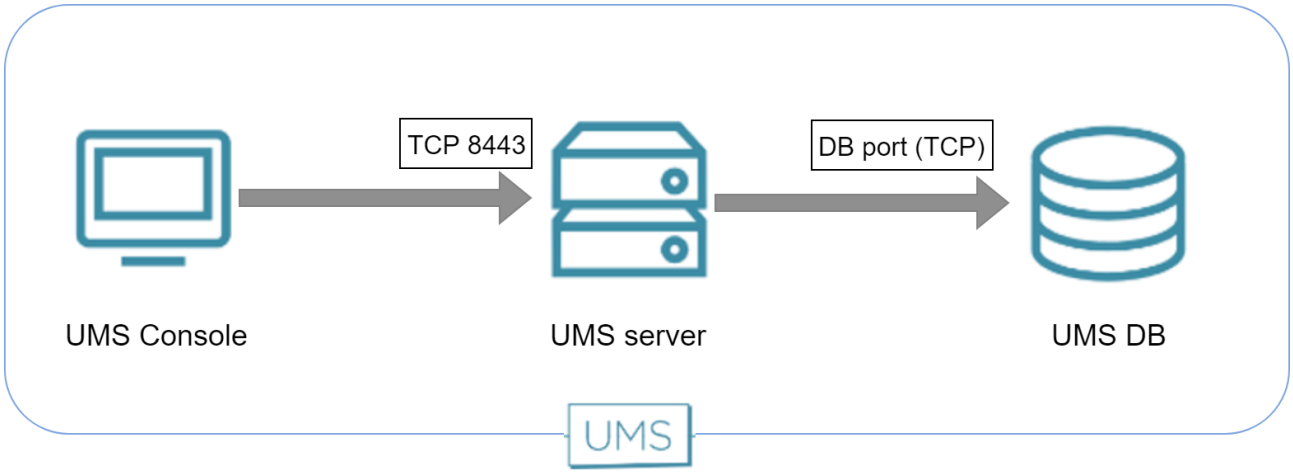
UMS with External Database

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

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

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

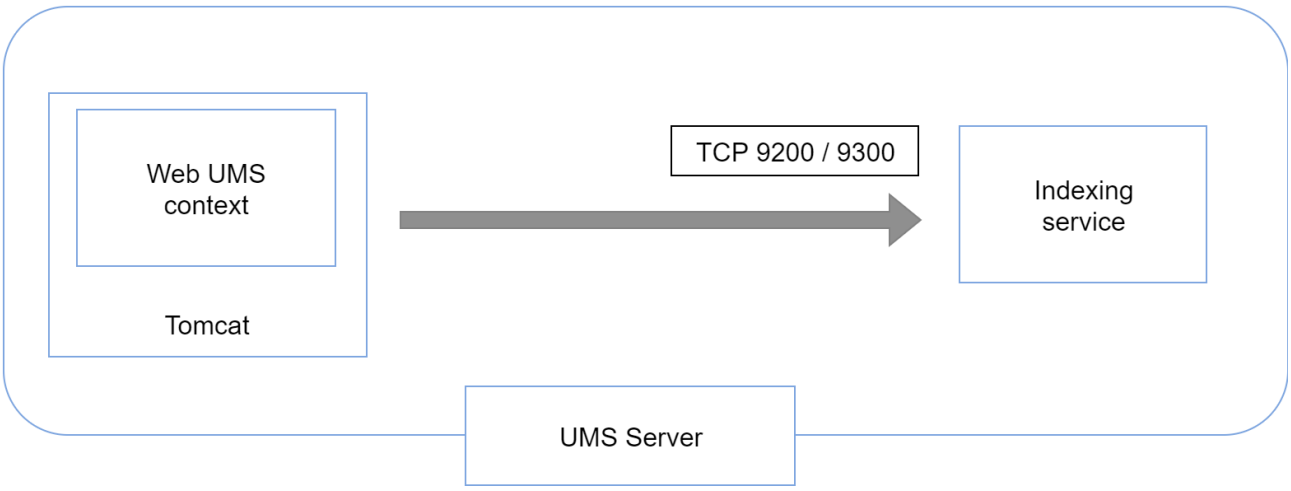
The following figure illustrates the communication between the UMS components:



Indexing for UMS Web App Search

The indexing service that is used by the search function of the UMS Web App is listening on ports 9200 and 9300. The Web UMS context reads and writes data via these ports. The ports are open internally, but cannot be reached from outside the UMS Server.

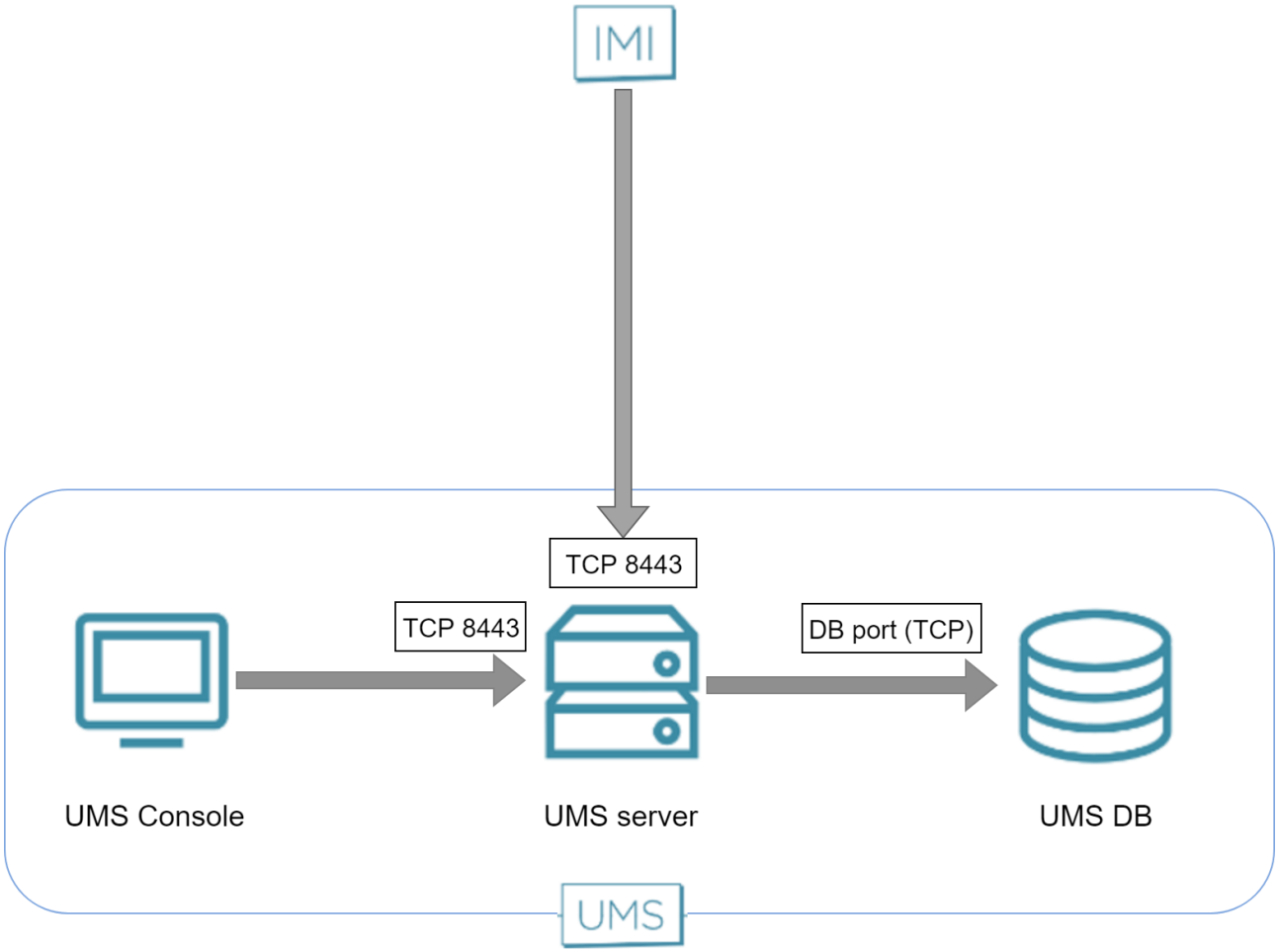
The following figure illustrates the communication within the UMS Server:



IGEL UMS and IGEL Management Interface (IMI) Communication

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

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



IGEL UMS and Devices: Settings and Control

Devices and UMS Server Contacting Each Other via ICG

To communicate with the UMS, the devices initiate a TCP connection to the ICG.

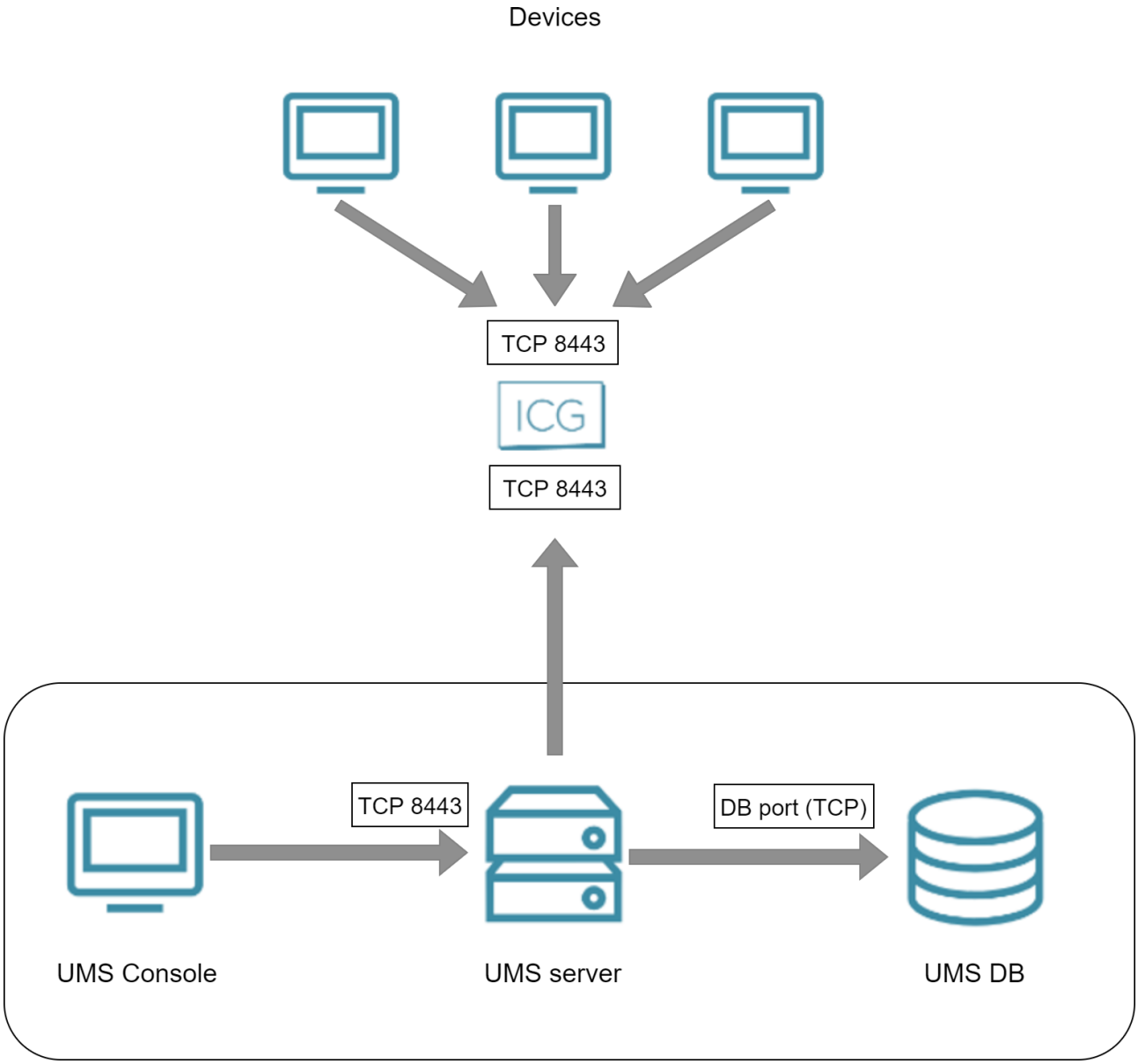
To communicate with the devices, the UMS initiates a TCP connection to the ICG.

The default port on which the ICG is listening is port 8443. It can be changed during the installation of the ICG. With ICG 2.02 or higher, a privileged port can be used, e.g. port 443. When the installation is completed, the port is fixed.

With ICG version 2.x or 12.01.x and UMS version 6.x or 12.01.x, it is not possible to inspect the TLS traffic between any of the components. The inspection would break TLS and interrupt communication between the products.
As of UMS version 12.02, you can inspect the TLS traffic, see IGEL Universal Management Suite Network Configuration (see page 265) .

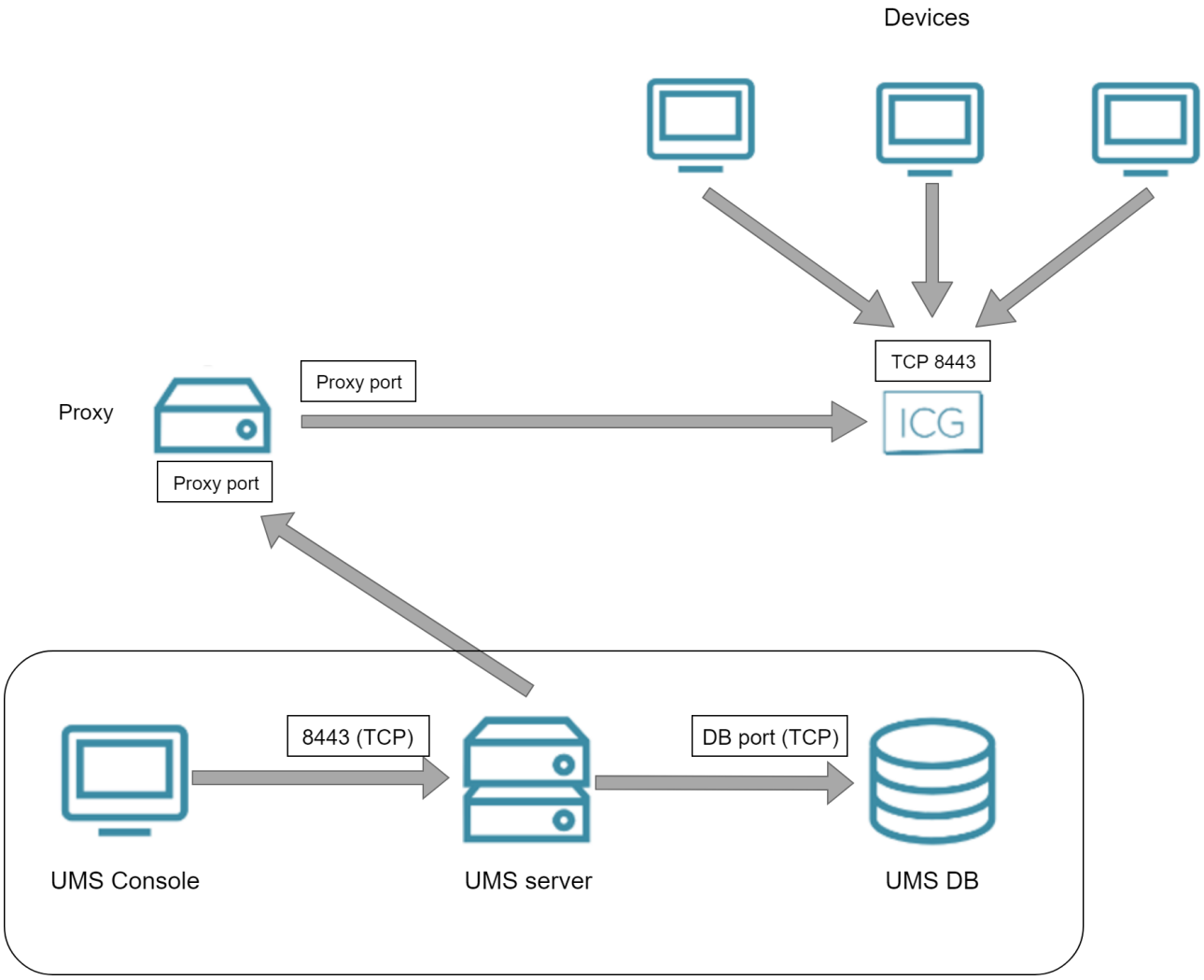
Direct Connection

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



Via Proxy

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

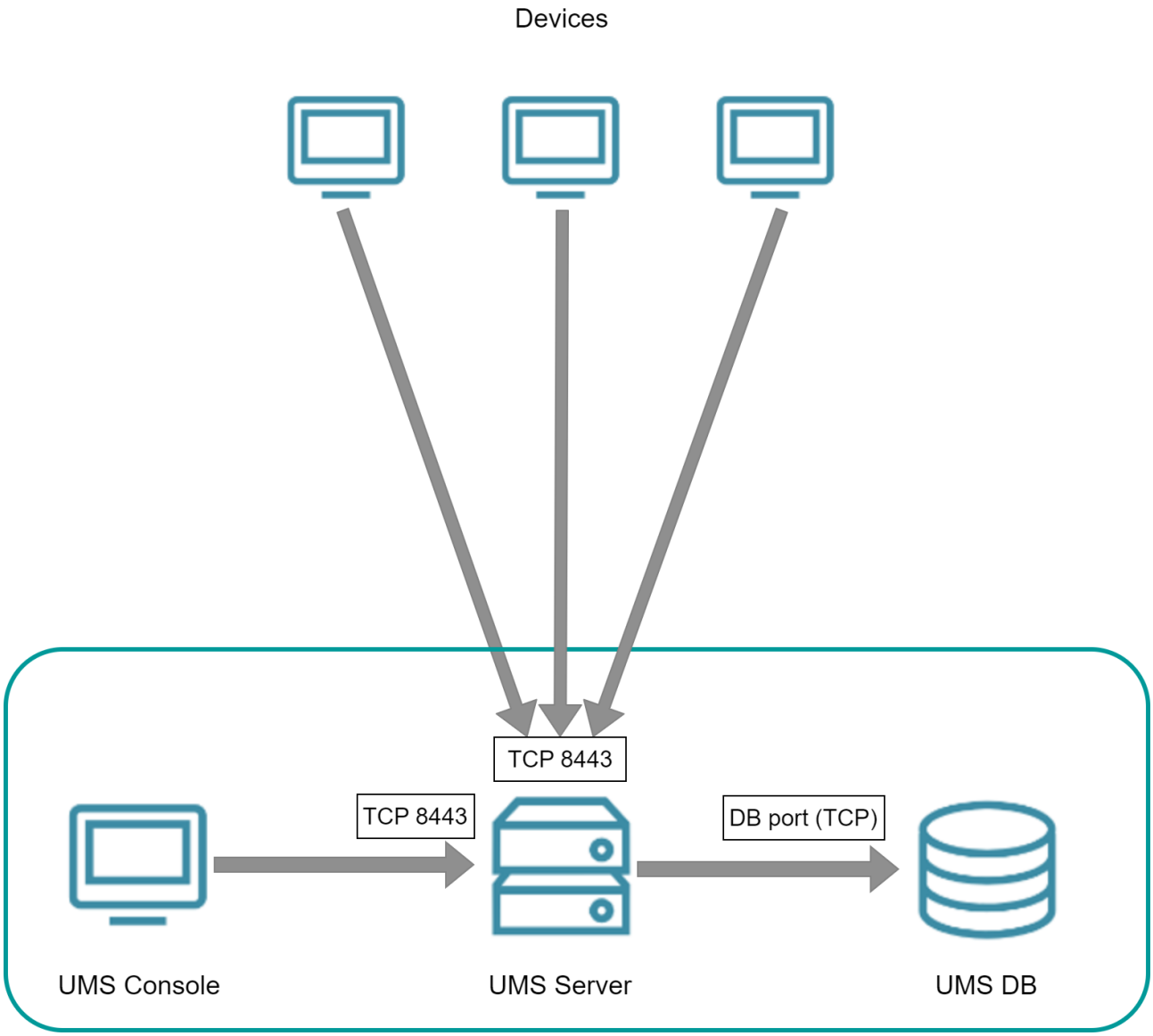

Devices
TCP 8443
ICG
Proxy
Proxy port
Proxy port
8443 (TCP)
DB port (TCP)
UMS Console
UMS server
UMS DB

Devices Contacting UMS

The following figures illustrate the communication between the endpoint devices and the UMS.

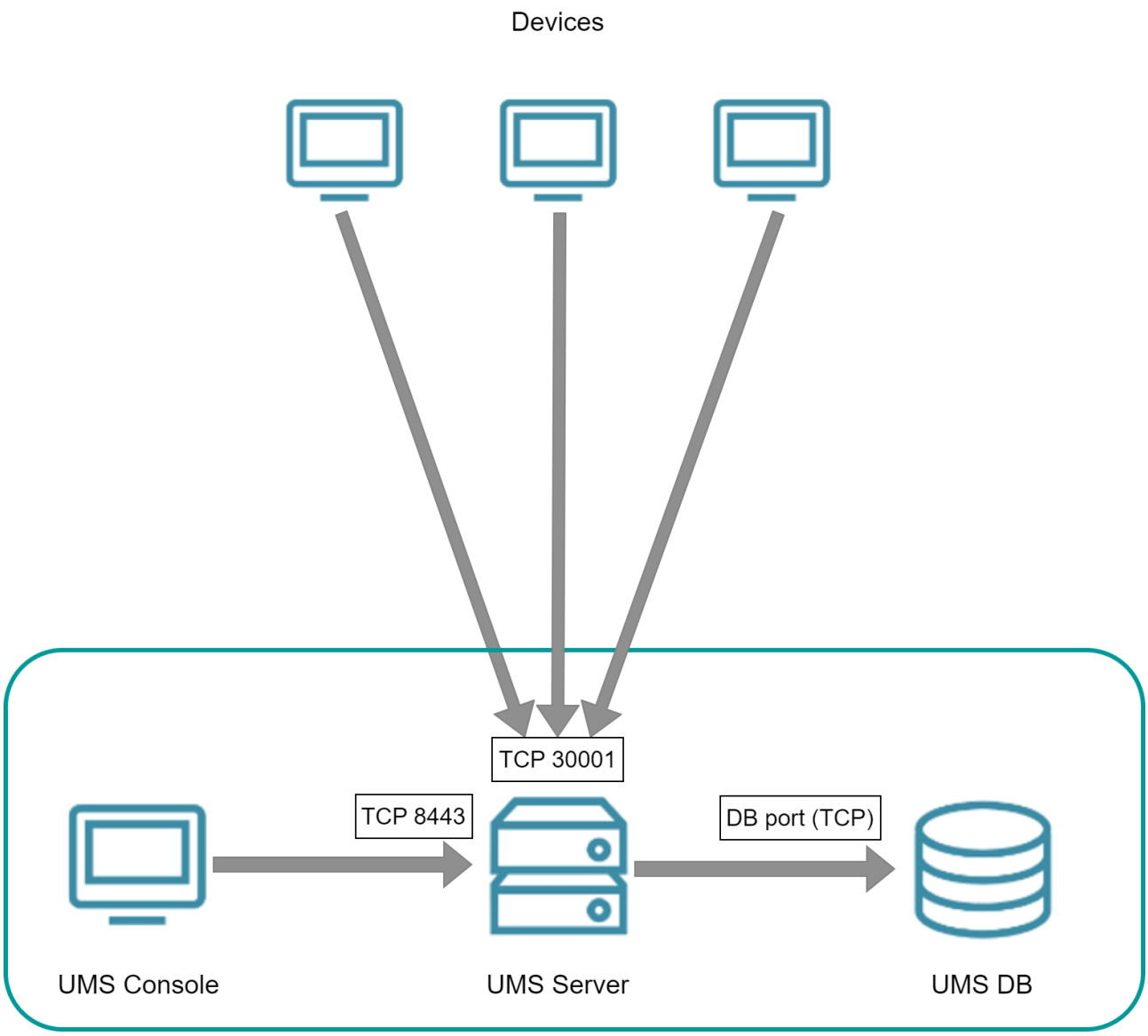
IGEL OS 12

To communicate with the UMS, the devices initiate a TCP connection to the UMS Server using port 8443.



IGEL OS 11 or Earlier

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


Devices
TCP 30001
TCP 8443
DB port (TCP)
UMS Console
UMS Server
UMS DB

UMS Contacting Devices

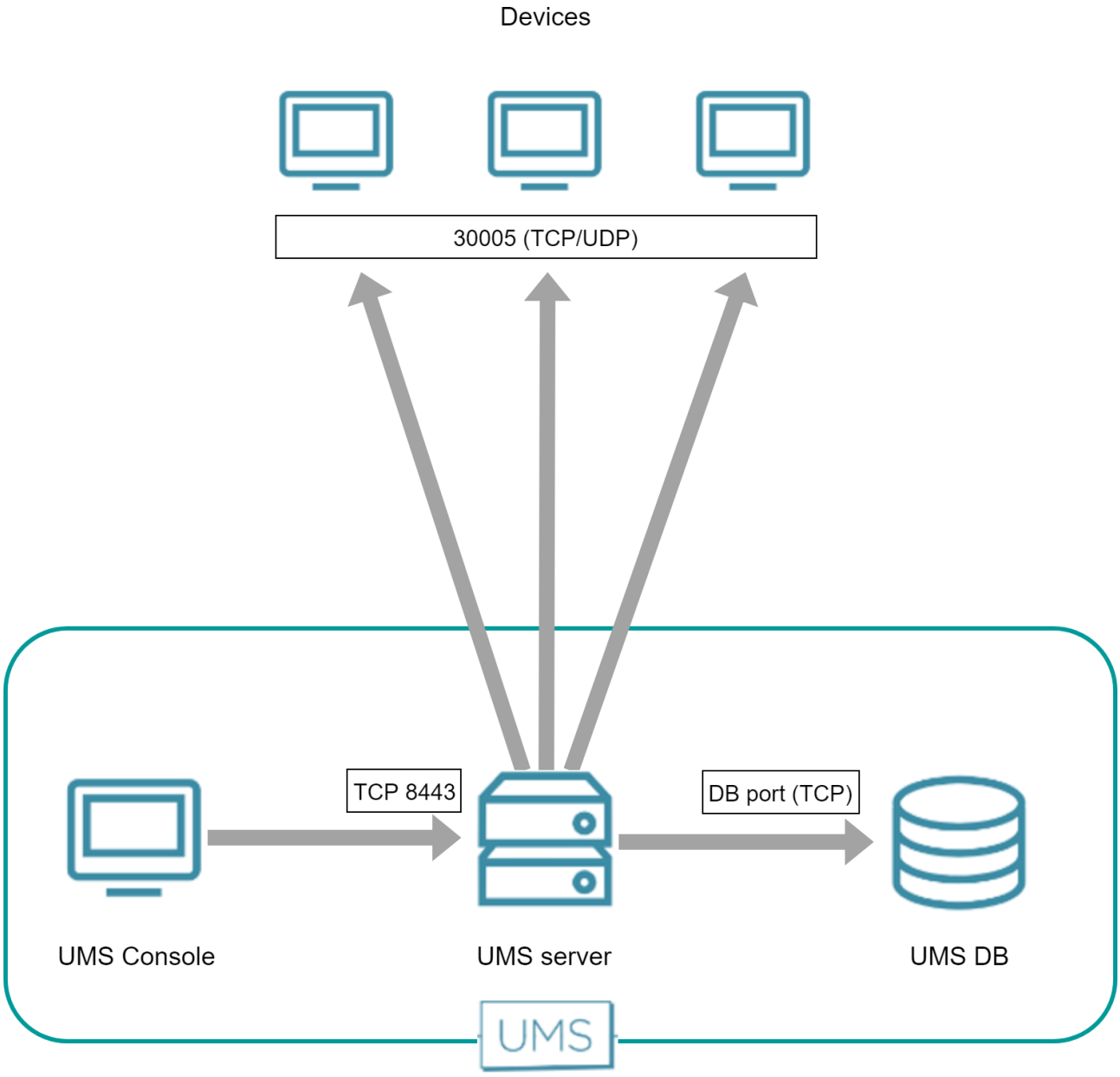
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

To communicate with IGEL OS 11 devices, the UMS initiates a TCP connection to the device's UMS agent using port 30005.

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


Devices
30005 (TCP/UDP)
TCP 8443
DB port (TCP)
UMS Console
UMS server
UMS DB
UMS

IGEL UMS and Devices: Shadowing Communication Flow

IGEL OS 12

Shadowing of IGEL OS 12 devices is always secure, i.e. via the Unified Protocol. The communication is always encrypted. See IGEL UMS and Devices Secure Shadowing Communication Flow[96].

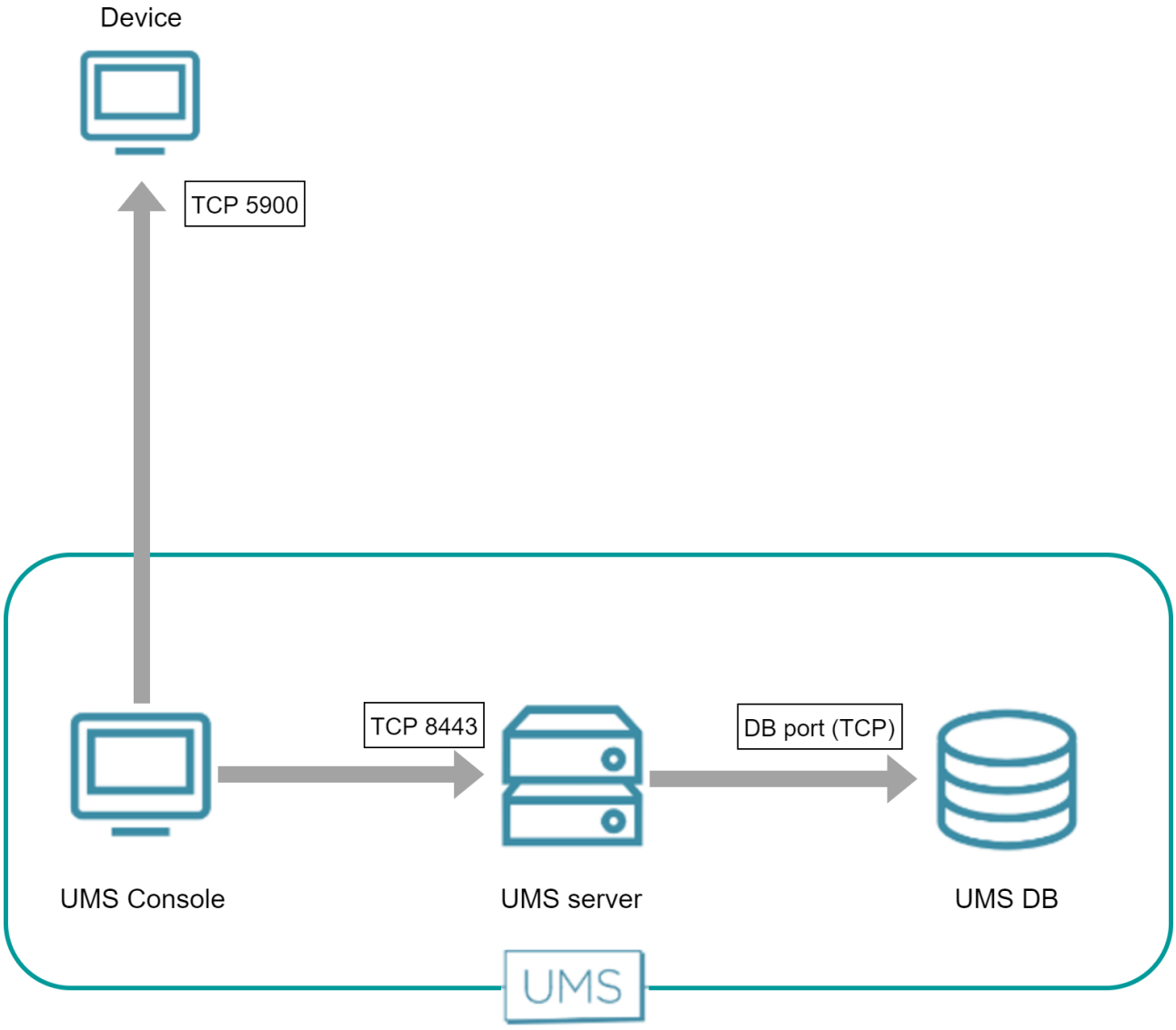
IGEL OS 11 or Earlier

UMS Console

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

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

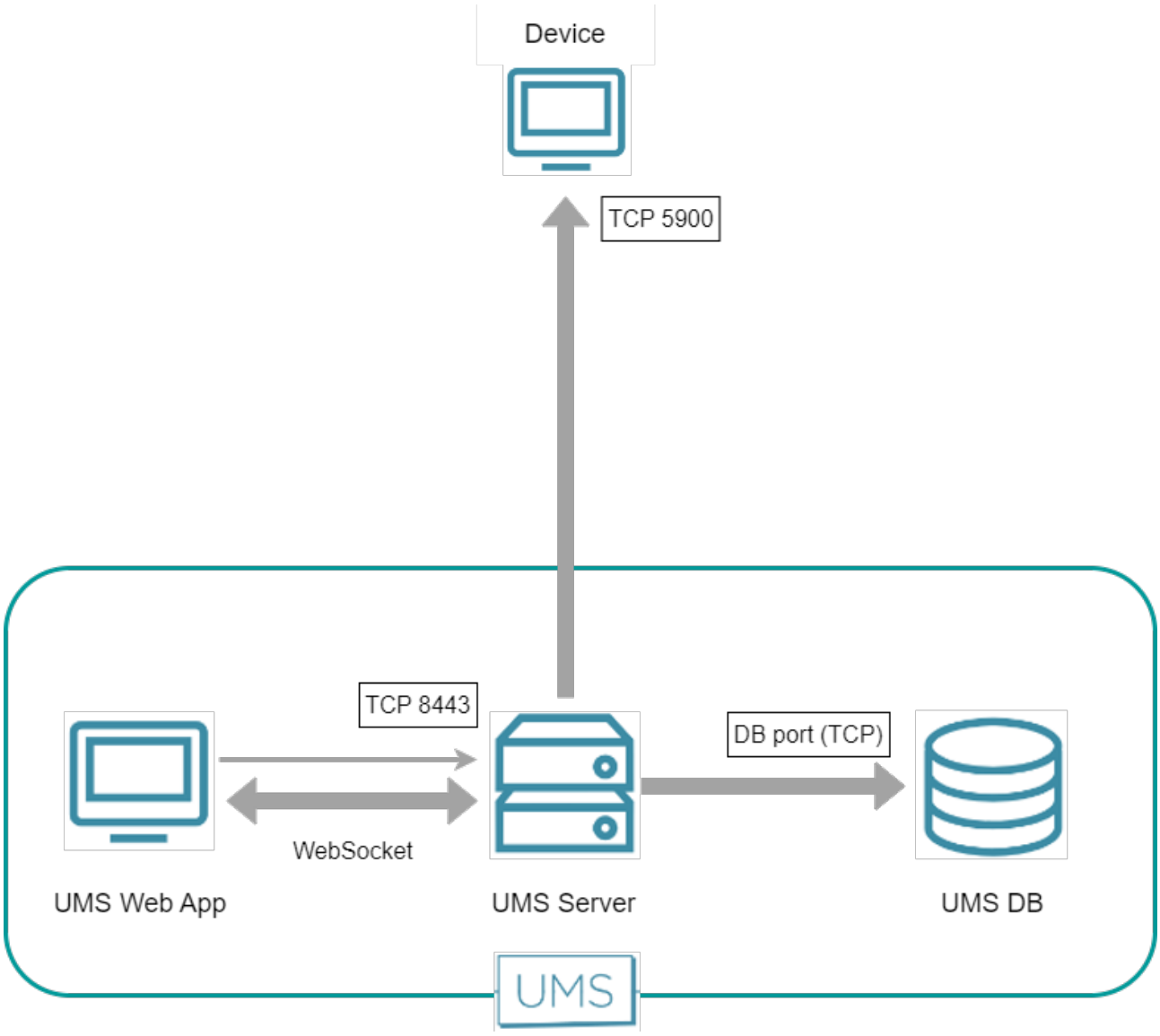
96. https://kb.igel.com/en/universal-management-suite/current/igel-ums-and-devices-secure-shadowing-communicatio



UMS Web App

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; between the UMS Web App and the UMS Server, the data is transferred via WebSocket. The default port for the communication between the UMS Server and the devices is 5900 (TCP).

The following figure illustrates the communication between the UMS Web App, the UMS Server, and a device:


Device
TCP 5900
TCP 8443
DB port (TCP)
WebSocket
UMS Web App
UMS Server
UMS DB
UMS

IGEL UMS and Devices Secure Shadowing Communication Flow

This article describes the communication flow of a secure shadowing session in the IGEL Universal Management Suite (UMS) environment.

IGEL OS 12

Shadowing of IGEL OS 12 devices is always secure, i.e. via the Unified Protocol. The communication is always encrypted.

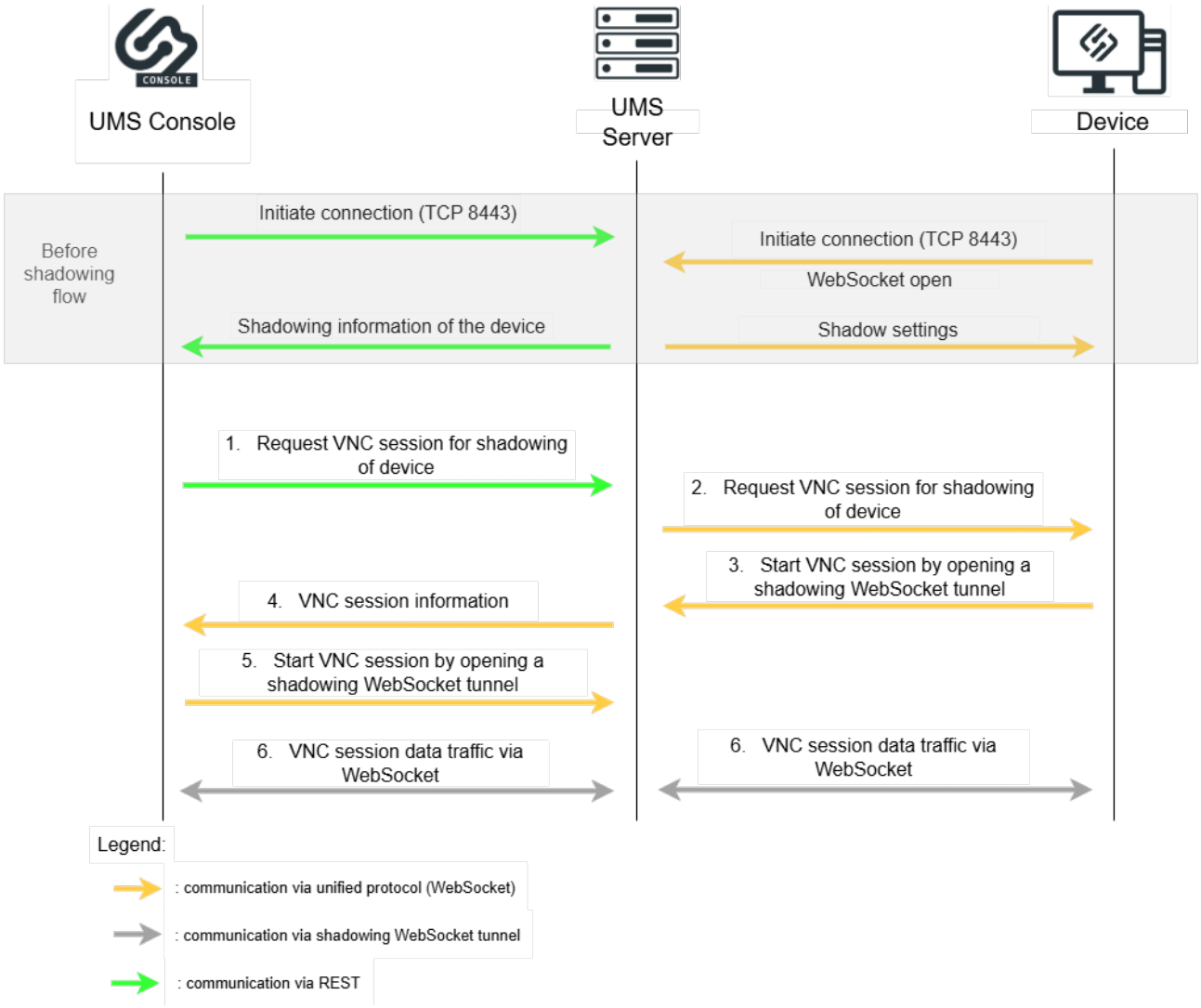
Direct Connection - UMS Console (Internal / External VNC Viewer)

Before the shadowing communication flow:

- REST connection is initiated between the Console and the UMS Server
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Shadow settings and information are forwarded

Shadowing flow:

1. The UMS Console requests the UMS Server to initiate a VNC session for shadowing.
2. The UMS Server requests the device to open a VNC session for shadowing.
3. The device opens the shadowing WebSocket tunnel to the UMS Server and starts the VNC session.
4. The UMS Server forwards the VNC session information to the UMS Console.
5. The UMS Console opens the shadowing WebSocket tunnel and starts the VNC session.
6. The VNC data is sent through the opened WebSocket tunnels between the UMS Console and the UMS Server and between the UMS Server and the Device.



Direct Connection - UMS Web App

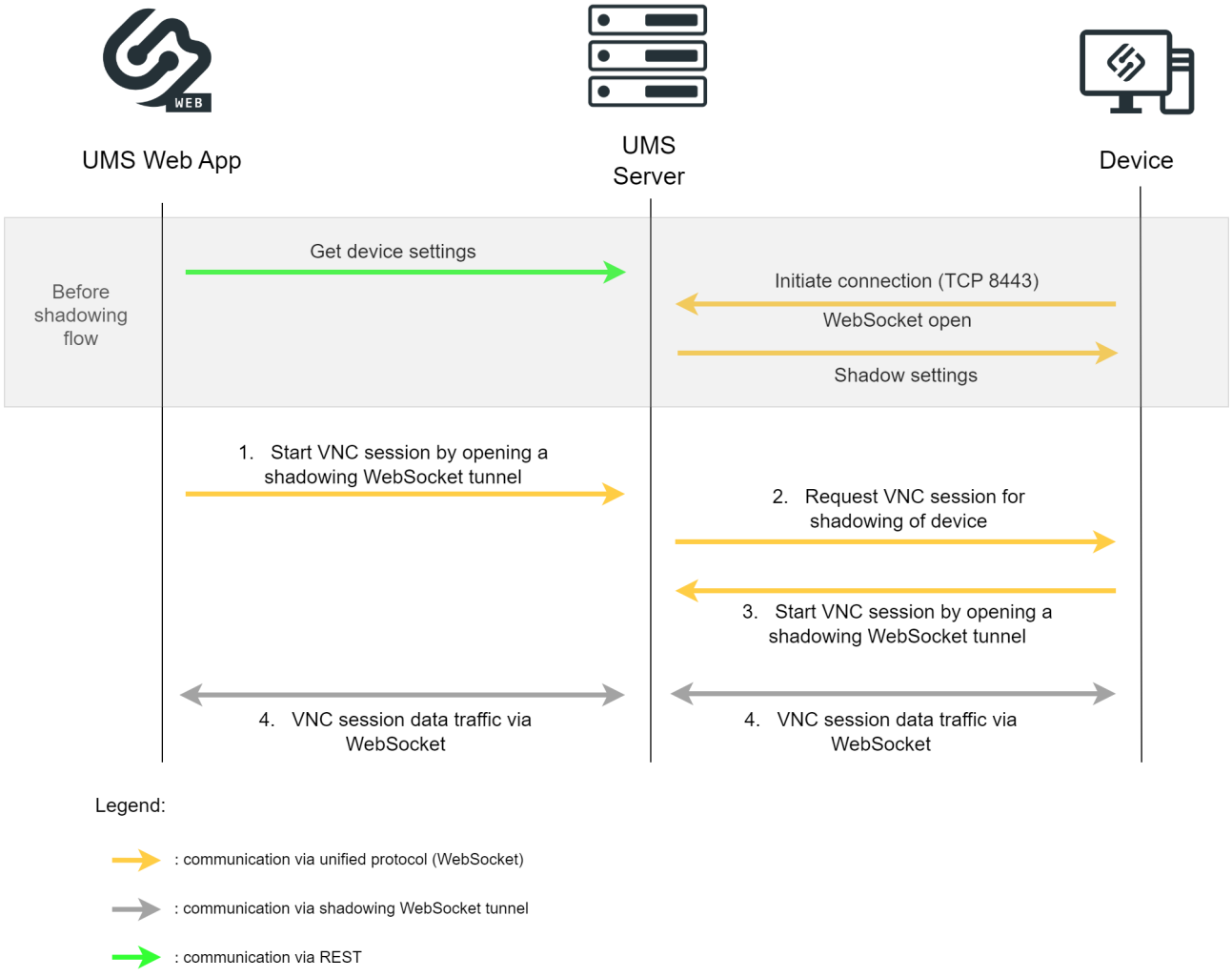
Before the shadowing communication flow:

- Device settings are sent to the UMS Server through REST
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Shadow settings are forwarded

Shadowing flow:

1. The UMS Web App starts the VNC session by opening the shadowing WebSocket tunnel to the UMS Server with information on the device to be shadowed.
2. The UMS Server requests the device via the Unified Protocol WebSocket to open a VNC session for shadowing.
3. The device opens the shadowing WebSocket tunnel to the UMS Server and starts the VNC session.

4. The VNC data is sent through the opened WebSocket tunnels.



Over ICG - UMS Console (Internal / External VNC Viewer)

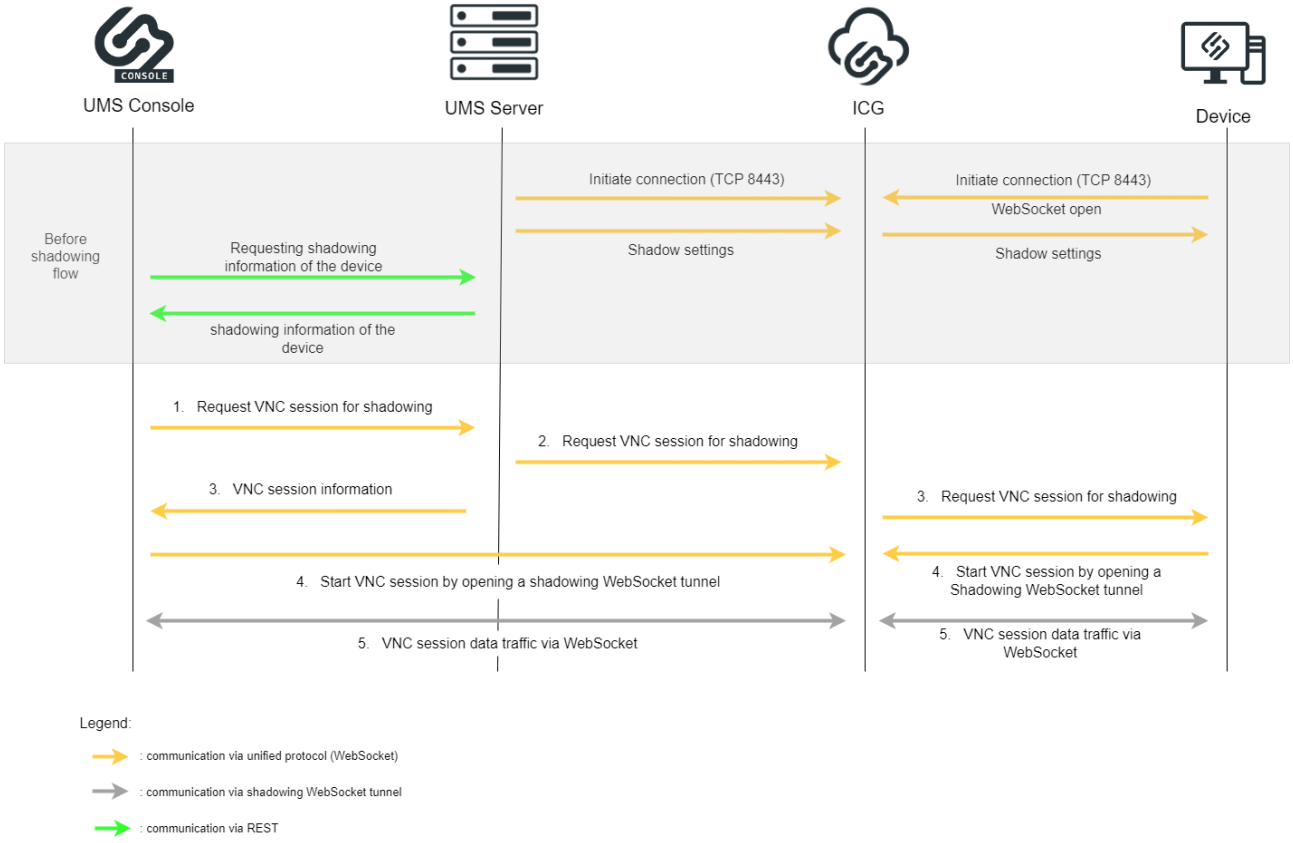
Before the shadowing communication flow:

- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Shadow settings are forwarded
- UMS Server sends shadowing information through REST to the UMS Console

Shadowing flow:

1. The UMS Console requests the UMS Server to initiate a VNC session for shadowing.
2. The UMS Server requests the ICG to open a VNC session for shadowing.
3. The UMS Server sends the VNC information to the UMS Console and the ICG requests the device to open a VNC session for shadowing.

4. The device opens the shadowing WebSocket tunnel to the ICG and starts the VNC session and the UMS Console opens the shadowing WebSocket tunnel to the ICG and starts the VNC session.
5. The VNC data is sent through the opened WebSocket tunnels.



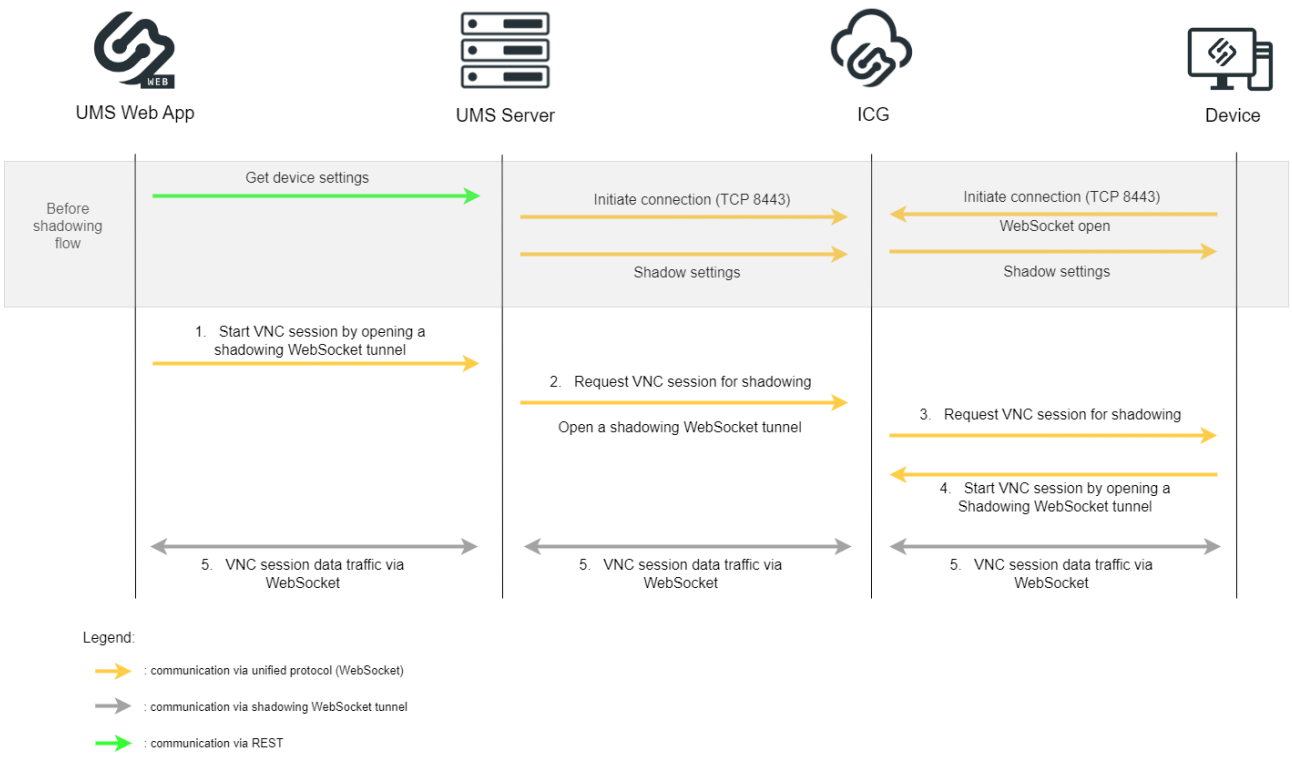
Over ICG - UMS Web App

Before the shadowing communication flow:

- Device settings are sent to the UMS Server through REST
- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Shadow settings are forwarded

Shadowing flow:

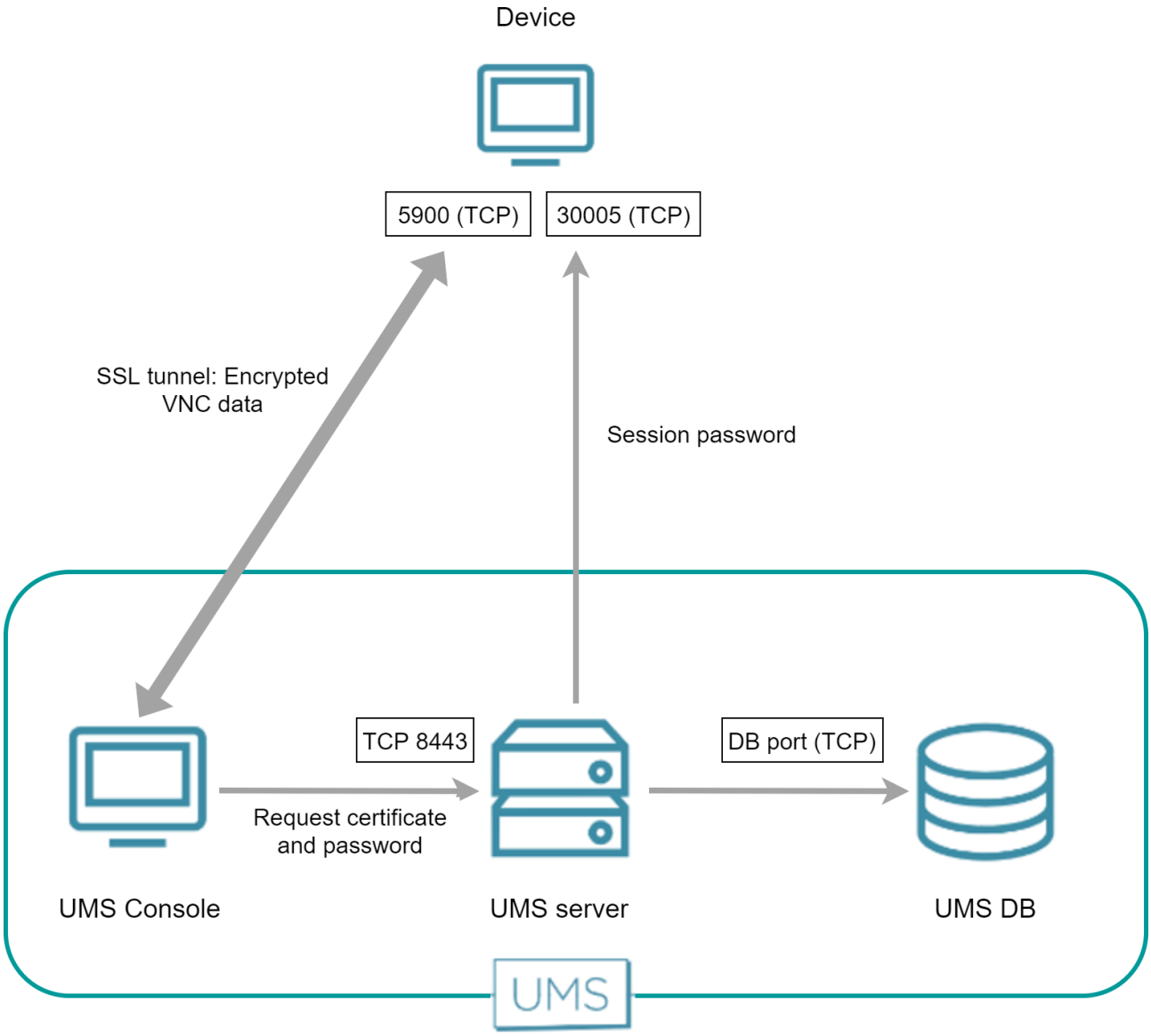
1. The UMS Web App starts the VNC session by opening the shadowing WebSocket tunnel to the UMS Server with information on the device to be shadowed.
2. The UMS Server requests the ICG to open a VNC session for shadowing and opens a WebSocket tunnel for the shadowing.
3. The ICG requests the device to open a VNC session for shadowing.
4. The device opens the Shadowing WebSocket to the ICG and starts the VNC session.
5. The VNC data is sent through these WebSockets.



IGEL OS 11 or Earlier

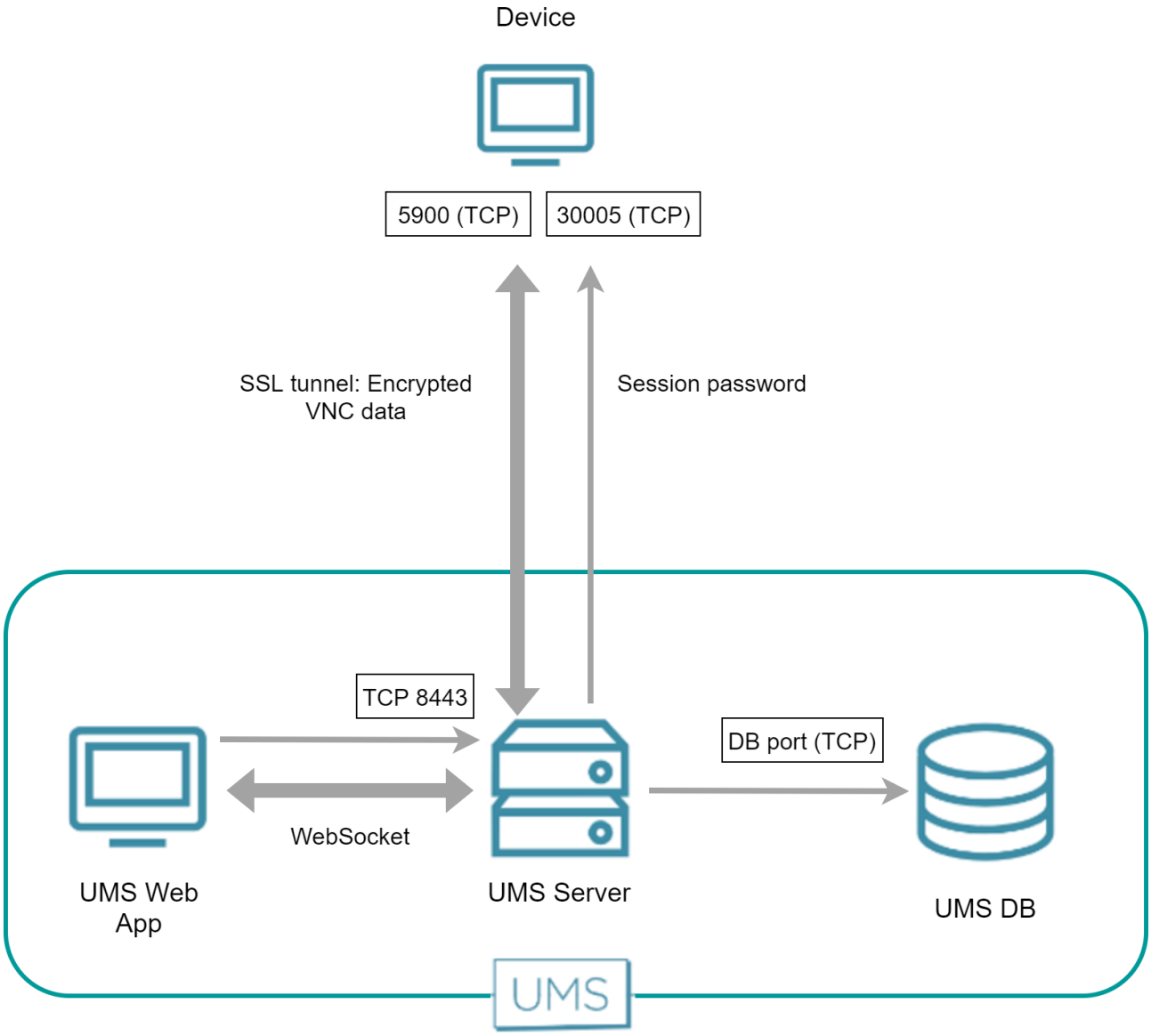
Direct Connection - Internal VNC Viewer

The UMS Console requests the device's certificate and the session password from the UMS Server. The UMS Console then establishes an SSL tunnel with the device using the session password. The device sends the certificate to the UMS Console; the UMS Console checks the certificate against the certificate it has received from the UMS Server. In return, the UMS Console sends the session password to the device. After that, the SSL tunnel between the UMS Console and device is established and can be used for exchanging VNC data.



Direct Connection - UMS Web App

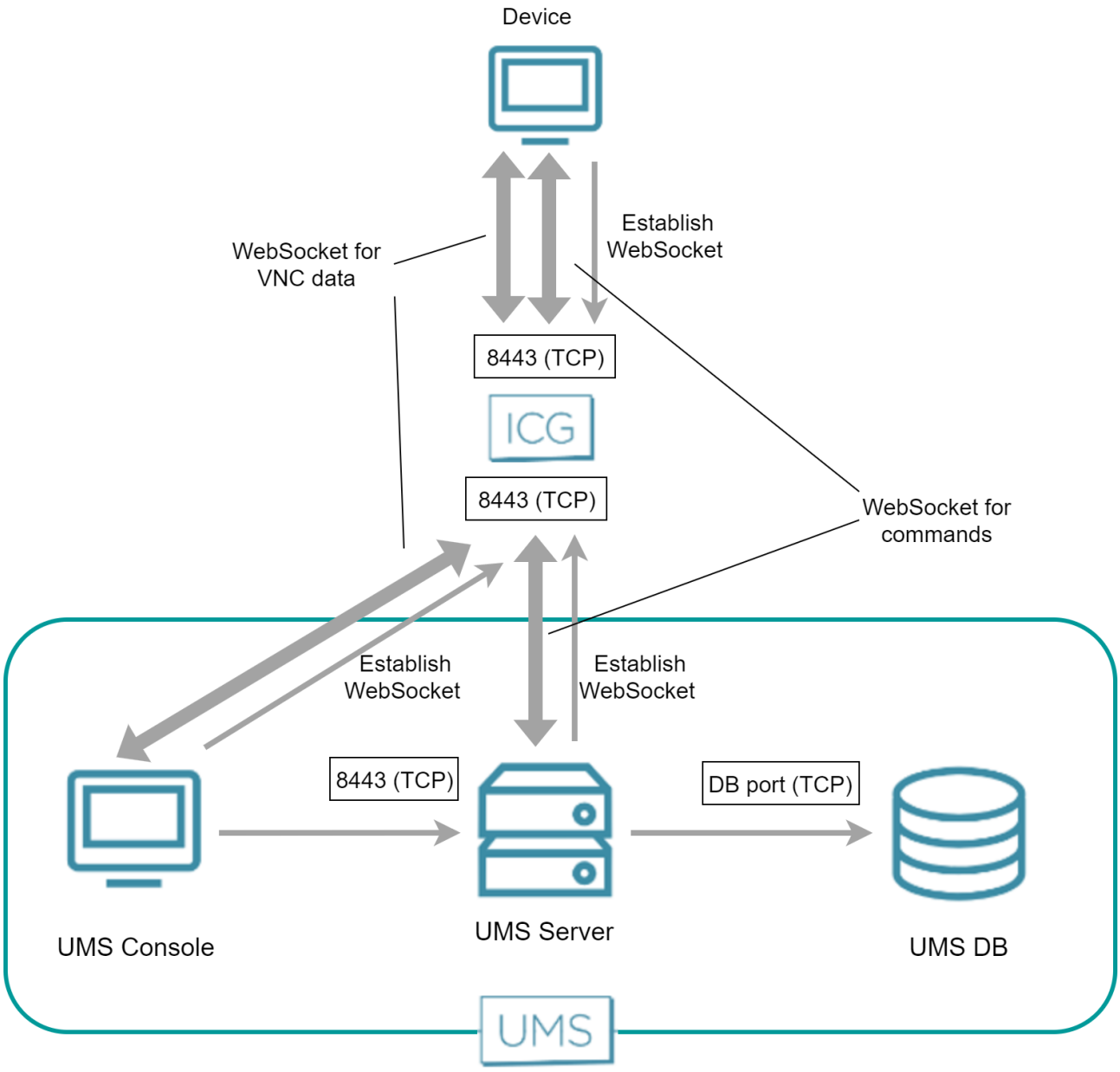
The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server establishes an SSL tunnel with the device using a session password and the device's certificate. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



Over ICG - Internal VNC Viewer

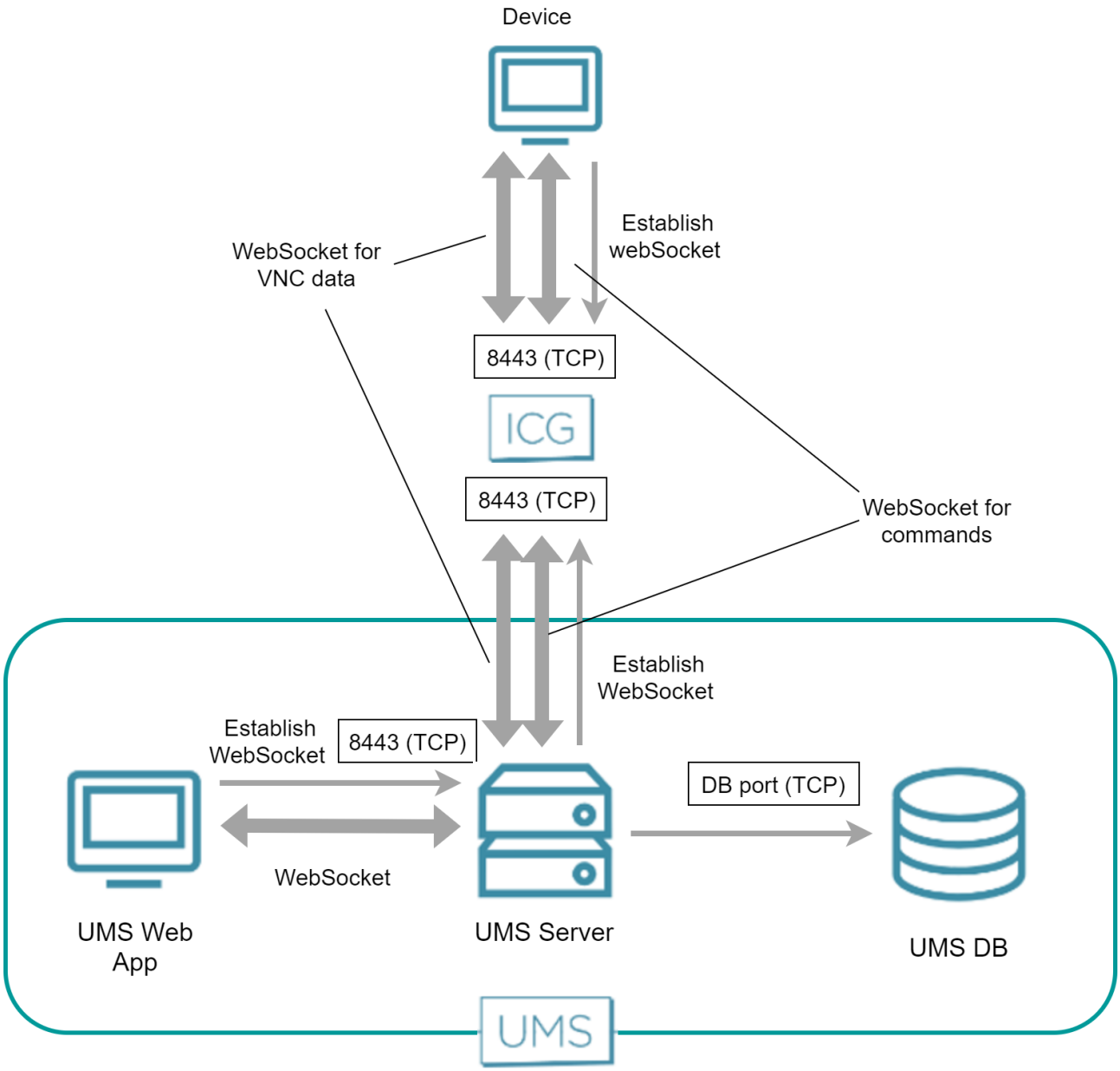
Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

The UMS Console and the device establish a dedicated WebSocket for secure shadowing with the ICG.



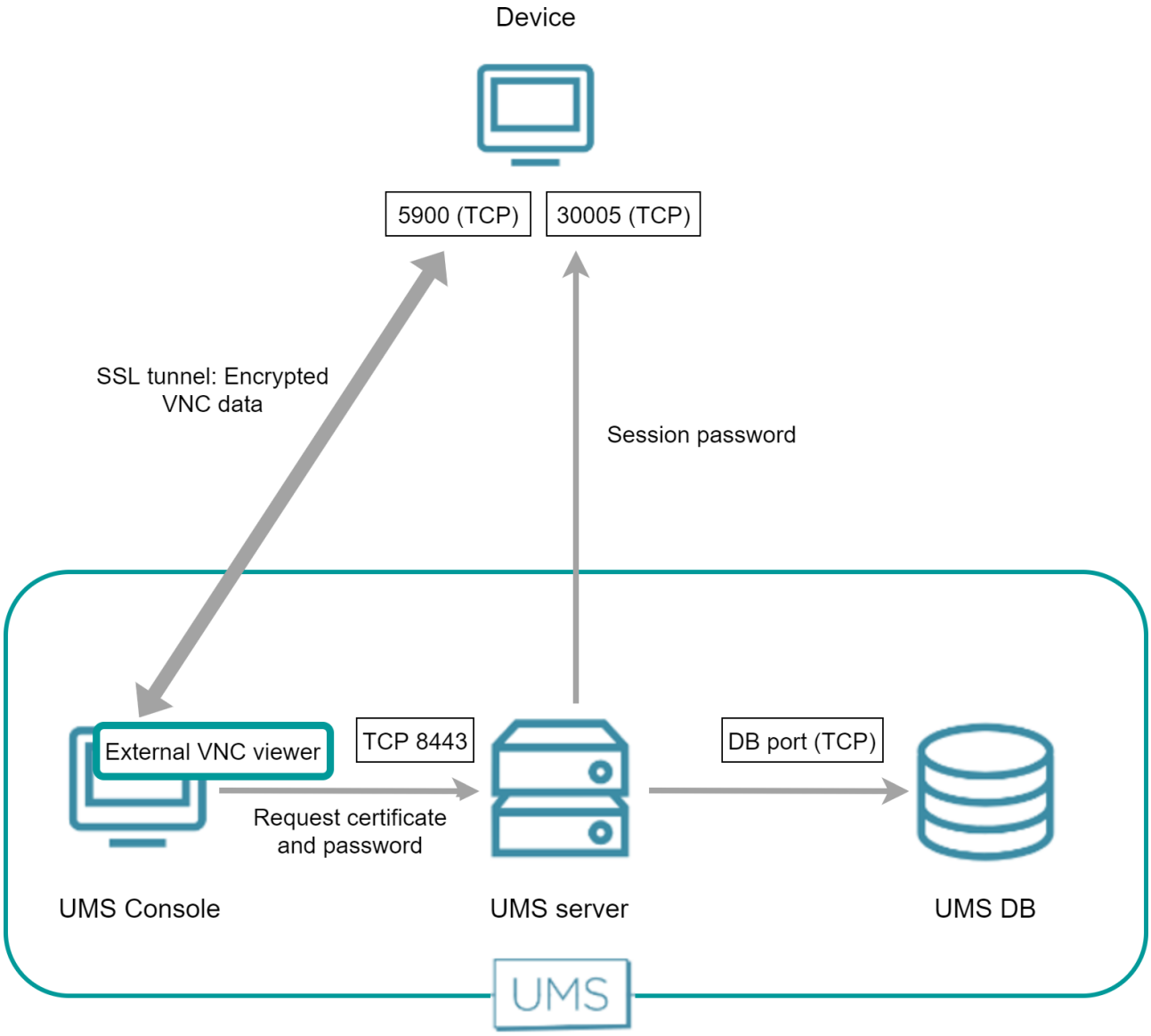
Over ICG - UMS Web App

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server creates an additional WebSocket connection for exchanging the VNC data. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



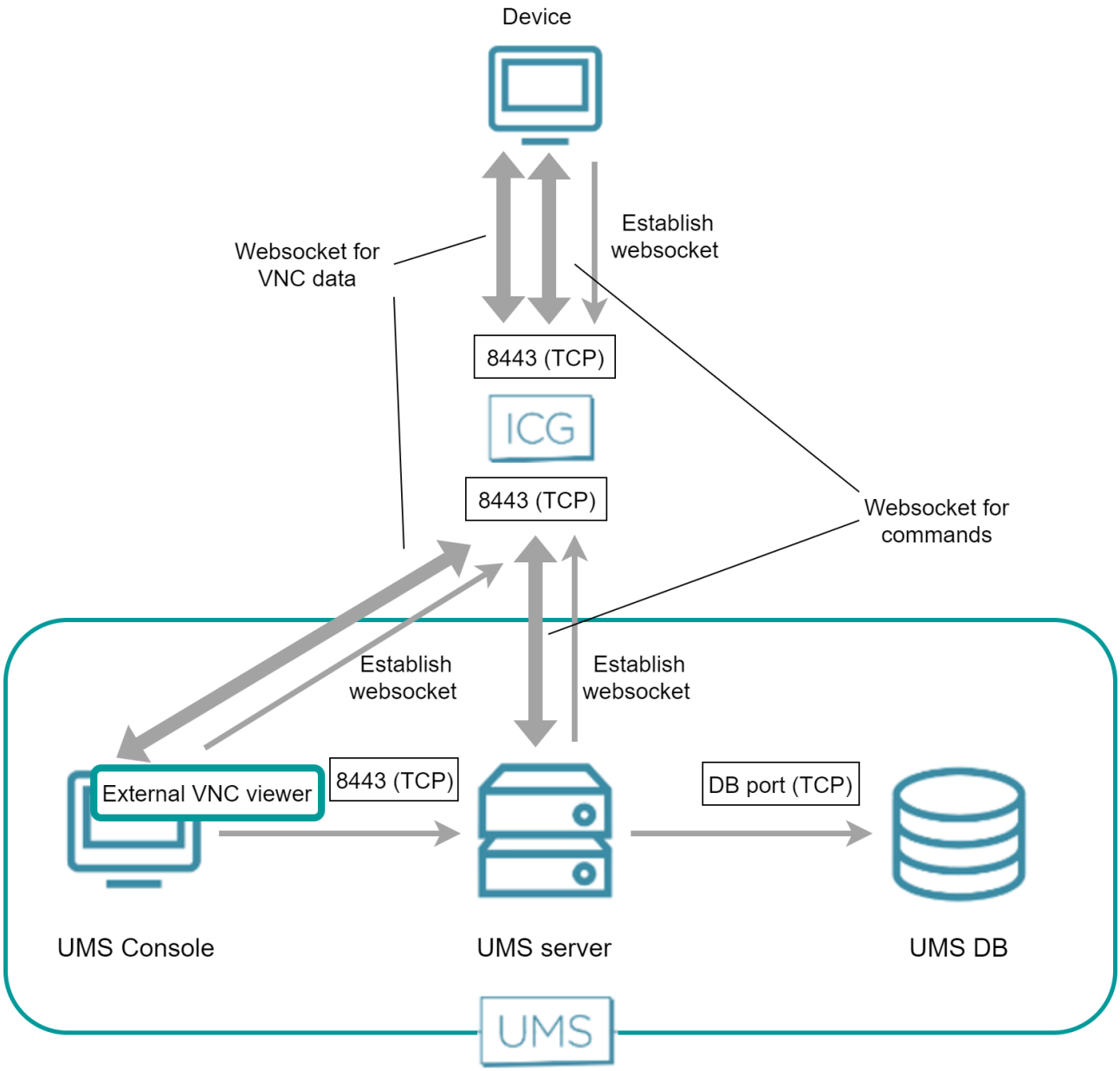
Direct Connection - External VNC Viewer

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the device and the external VNC viewer.



Over ICG - External VNC Viewer

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the ICG and the external VNC viewer.


Device
Websocket for
VNC data
Establish
websocket
8443 (TCP)
ICG
8443 (TCP)
Websocket for
commands
Establish
websocket
Establish
websocket
External VNC viewer
8443 (TCP)
DB port (TCP)
UMS Console
UMS server
UMS DB
UMS

IGEL UMS and Devices: Secure Terminal Communication Flow

This article describes the communication flow of a secure terminal session in the IGEL Universal Management Suite (UMS) environment.

IGEL OS 12

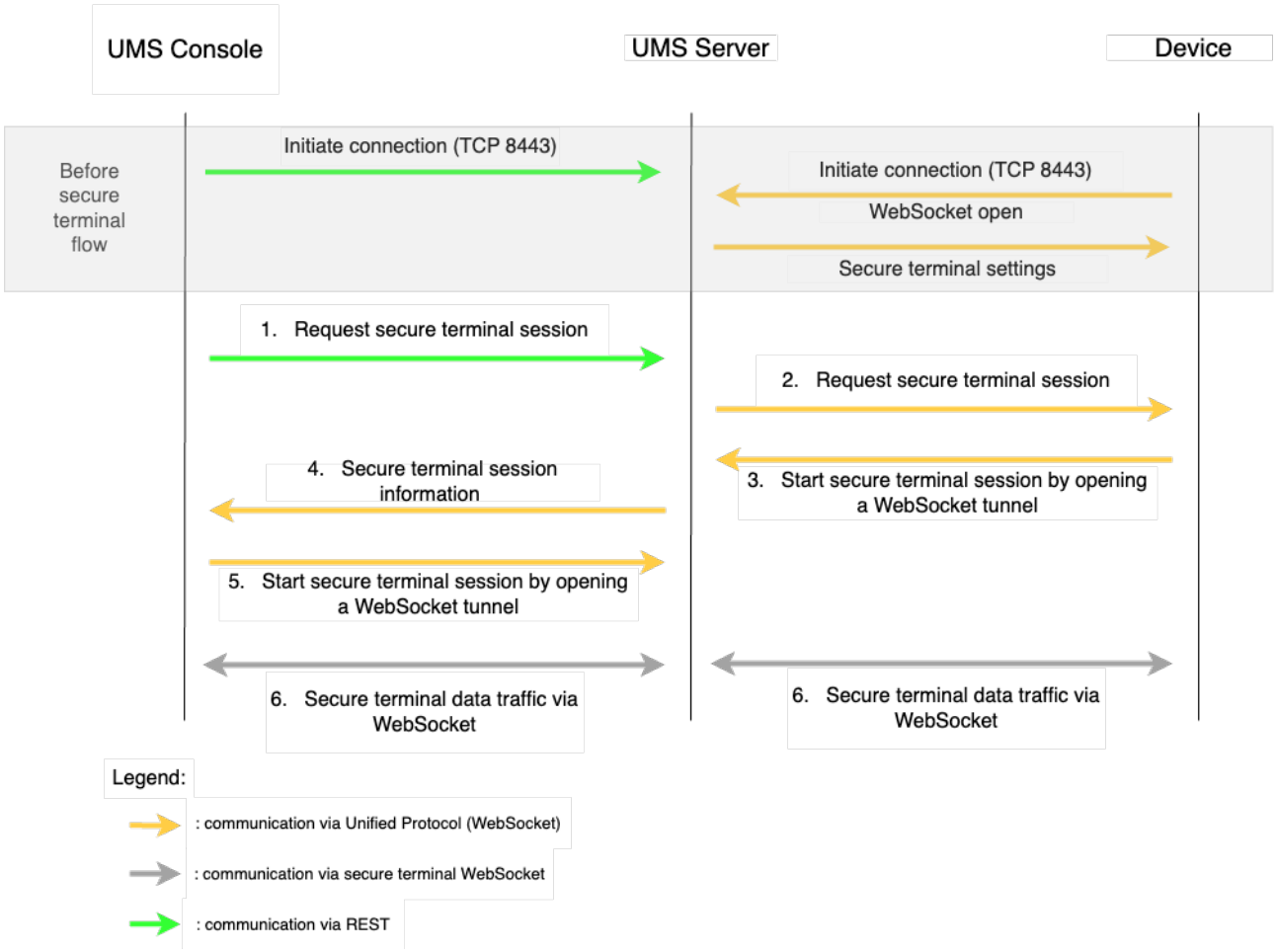
Direct Connection

Before the secure terminal flow:

- REST connection is initiated between the Console and the UMS Server
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Secure terminal settings are forwarded

Secure terminal communication flow:

1. The UMS Console requests the UMS Server to initiate a secure terminal session.
2. The UMS Server requests the device via the Unified Protocol WebSocket to open the secure terminal session.
3. The device opens the WebSocket tunnel for secure terminal data to the UMS Server and starts the secure terminal session.
4. The UMS Server forwards the secure terminal session information to the UMS Console.
5. The UMS Console opens the WebSocket tunnel for secure terminal data to the UMS Server and starts the secure terminal session.
6. The terminal data is sent through the opened WebSockets.



Over ICG

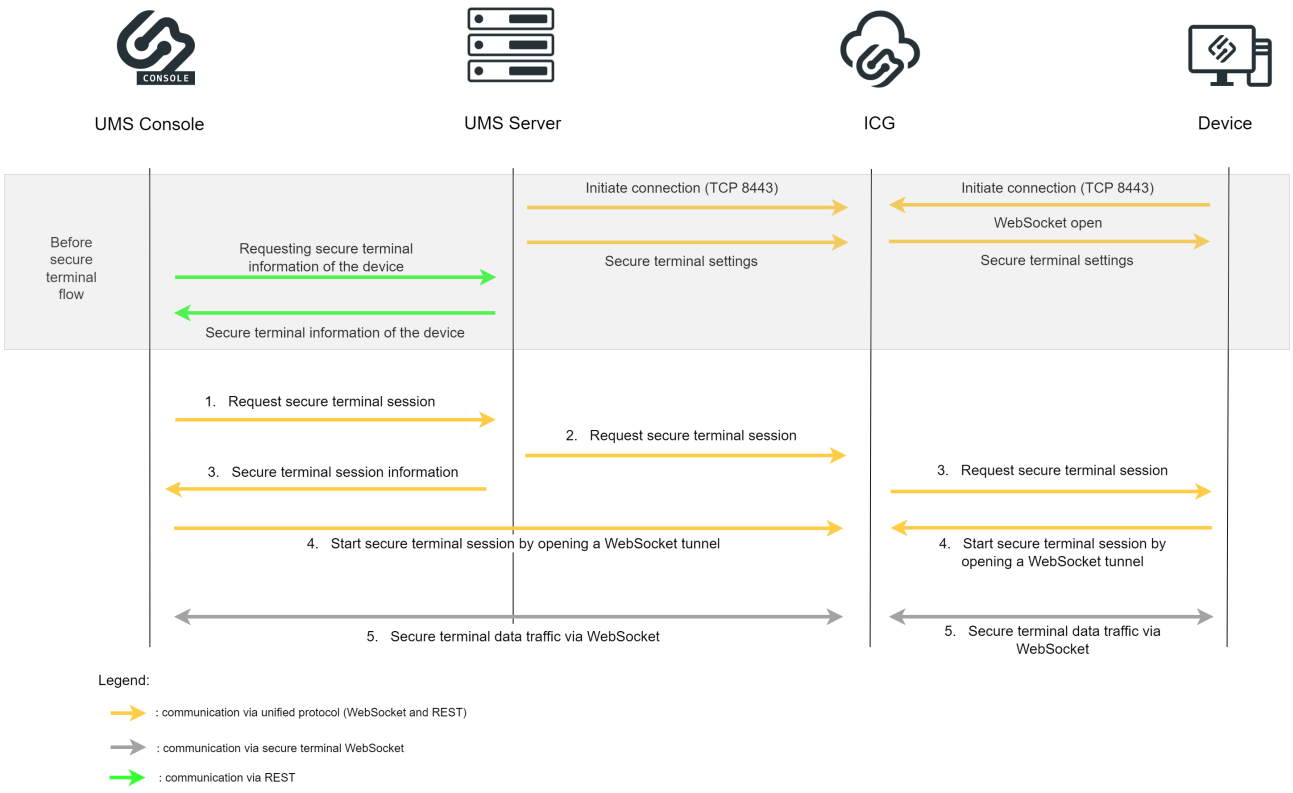
Before the secure terminal flow:

- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Secure terminal settings are forwarded
- UMS Server sends the secure terminal information of the device through REST to the UMS Console

Secure terminal communication flow:

1. The UMS Console requests the UMS Server to initiate a secure terminal session.
2. The UMS Server requests the ICG to open a secure terminal session.
3. The ICG requests the device via the Unified Protocol WebSocket to open a secure terminal session and the UMS Server forwards the secure terminal session information to the UMS Console.

4. The device opens the WebSocket tunnel for secure terminal data to the ICG and starts the secure terminal session and the UMS Console opens the WebSocket tunnel for secure terminal data to the ICG and starts the secure terminal session.
5. The terminal data is sent through the opened WebSockets.

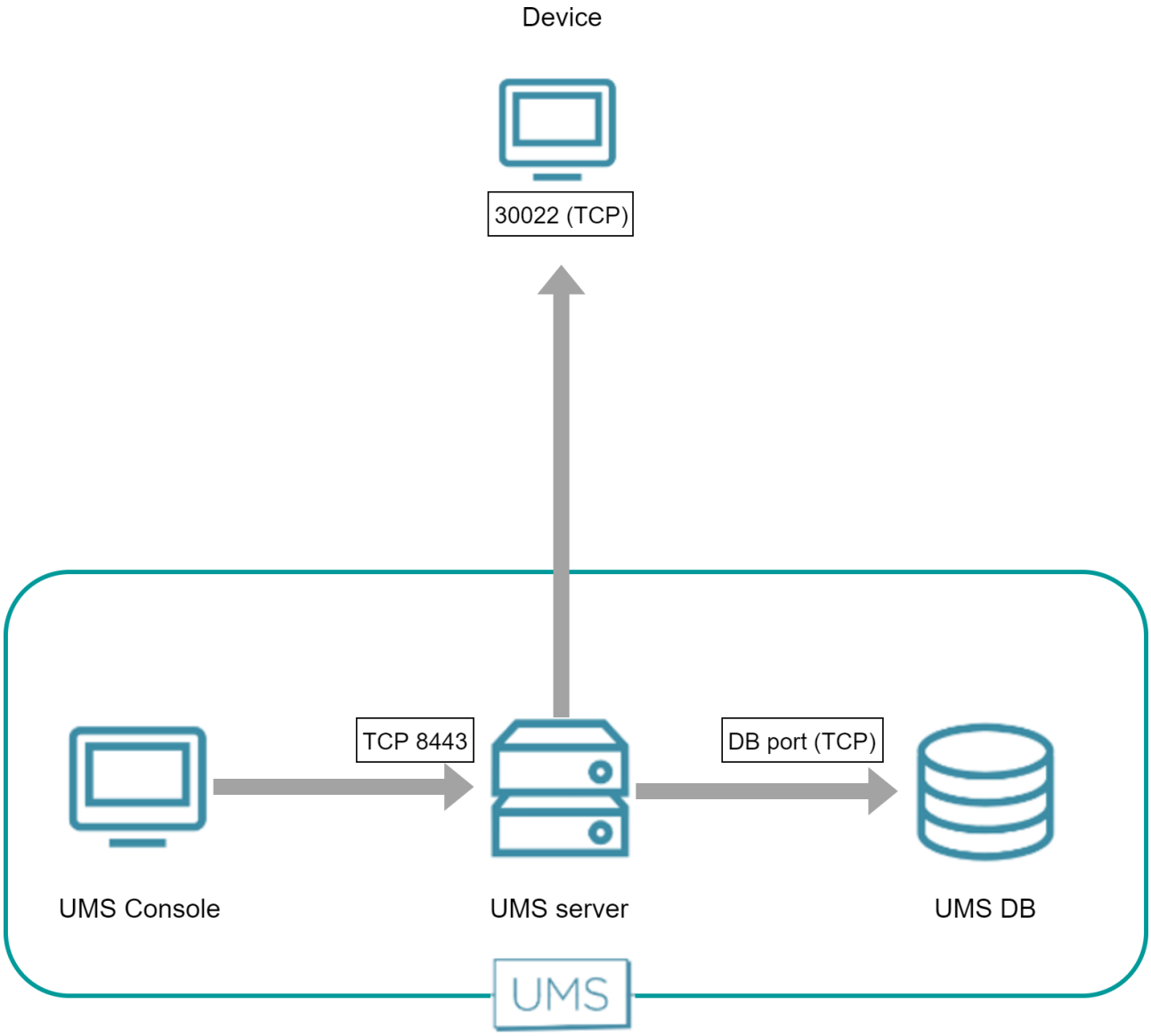


IGEL OS 11 or Earlier

Direct Connection

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

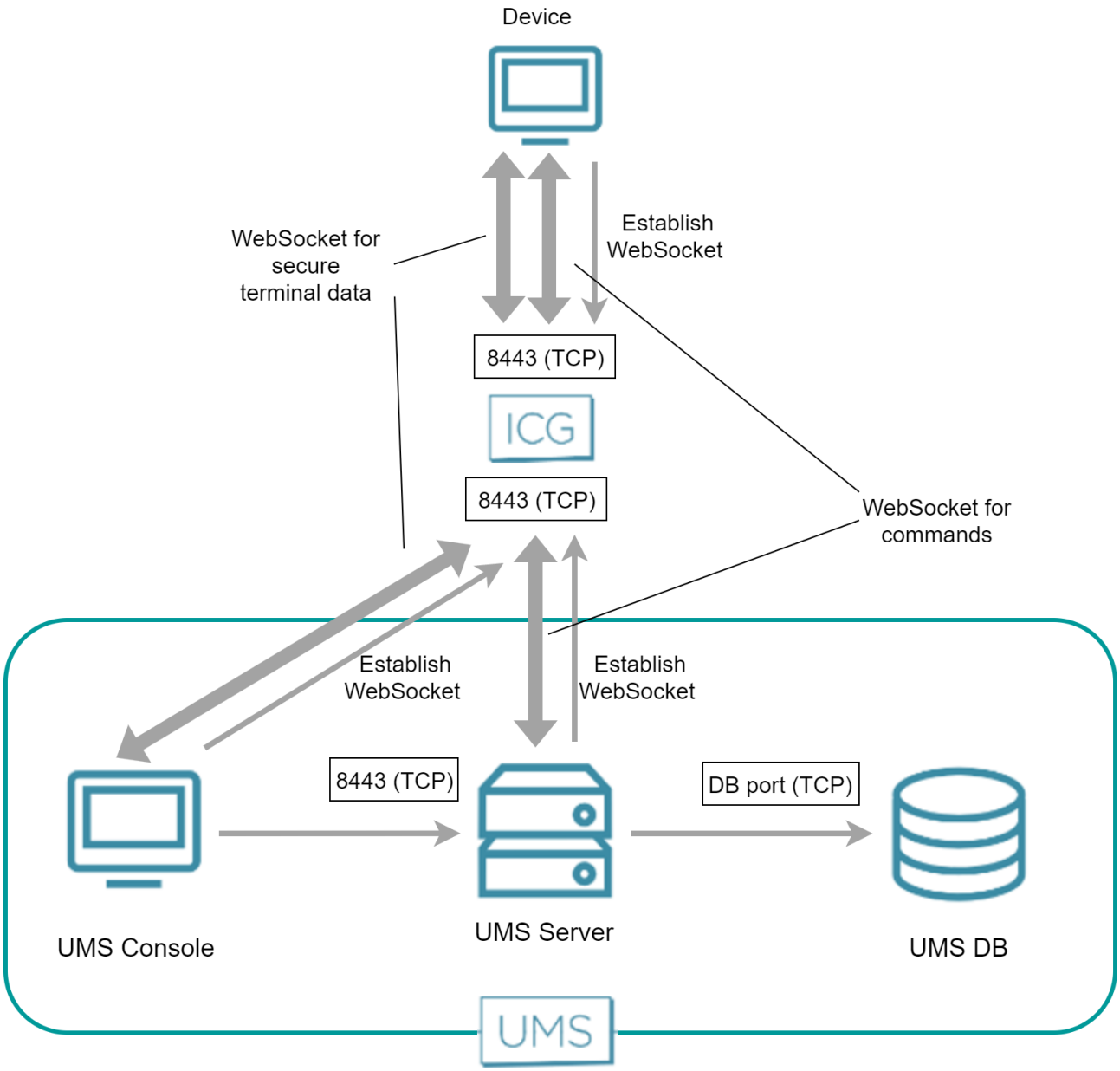
The following figure illustrates the communication between the UMS Console, the UMS Server and a device:



Over ICG

Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

The UMS Console and the device establish a dedicated WebSocket for the secure terminal with the ICG.


Device
WebSocket for secure terminal data
Establish WebSocket
8443 (TCP)
ICG
8443 (TCP)
WebSocket for commands
Establish WebSocket
Establish WebSocket
8443 (TCP)
DB port (TCP)
UMS Console
UMS Server
UMS DB
UMS

IGEL UMS and Devices: File Transfer Communication Flow

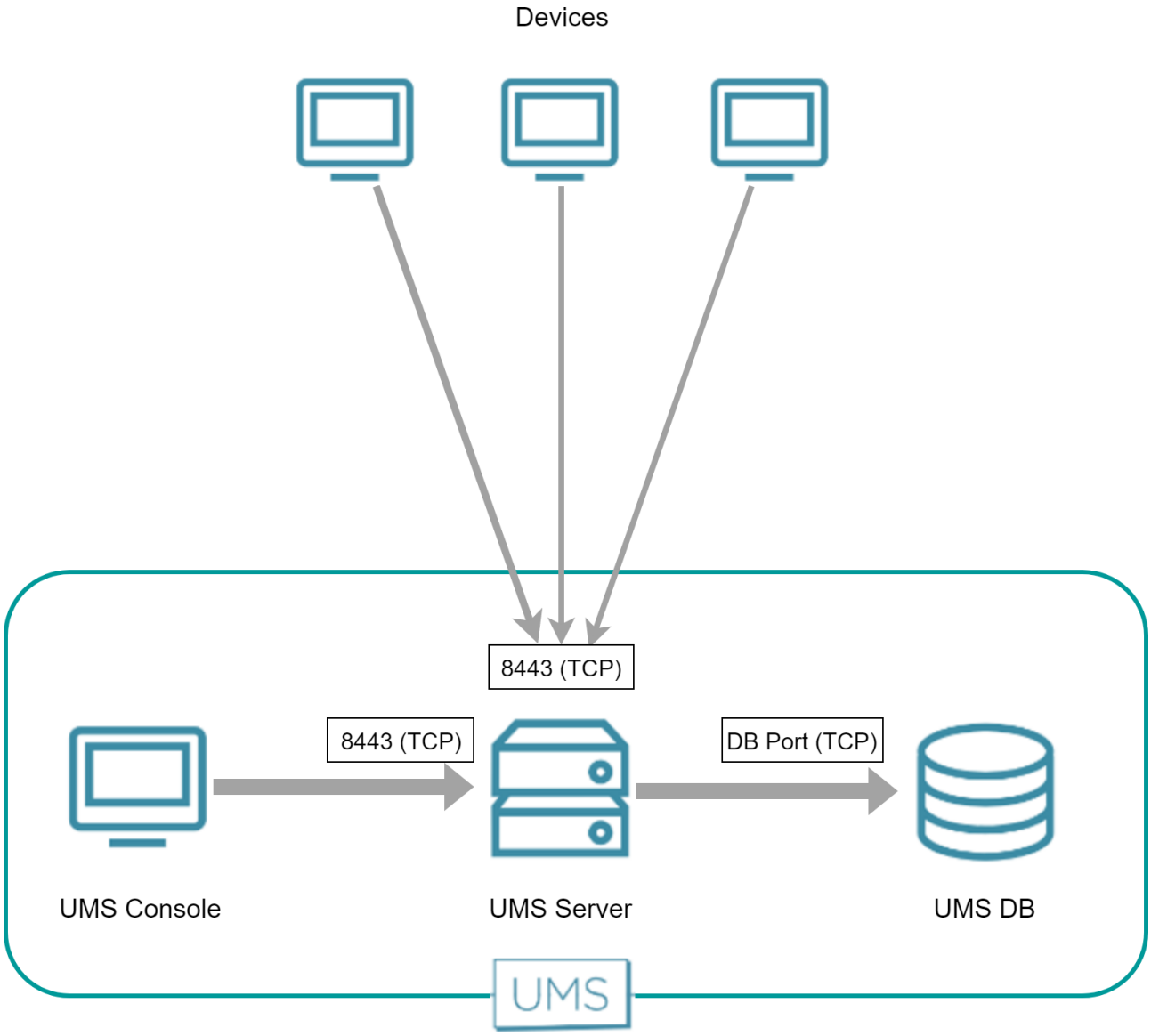
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened for the file transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

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

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


Devices
8443 (TCP)
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

Universal Firmware Update

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

For more information about this feature, see Universal Firmware Update - Distributing Firmware in the IGEL UMS (see page 979).

> The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

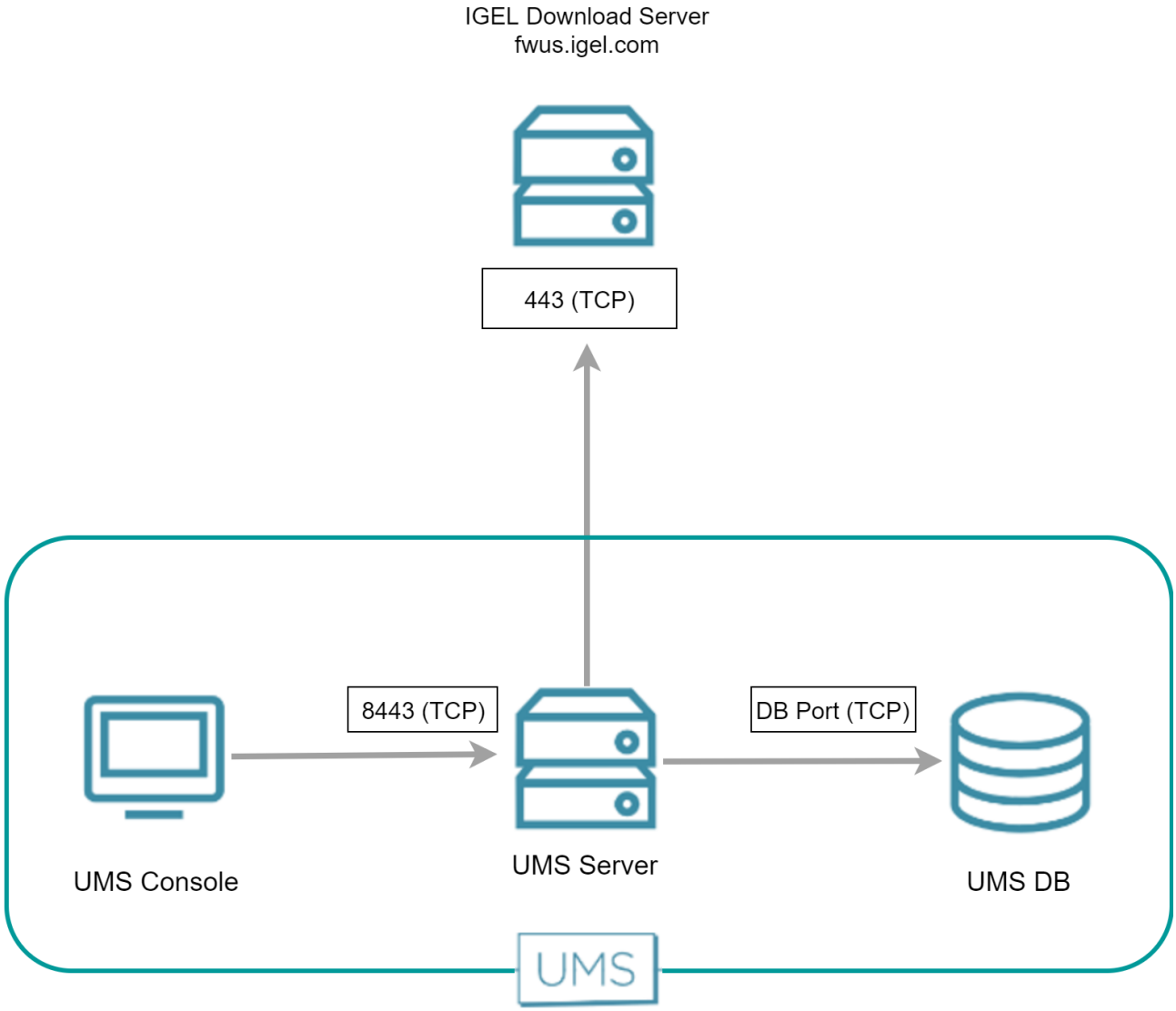
UMS Contacting the Download Server to Check for New Updates

> The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

The UMS initiates a TCP connection to port 443 at fwus.igel.com. The IGEL download server will send an answer containing a list of download links that enable the UMS to download the desired firmware.

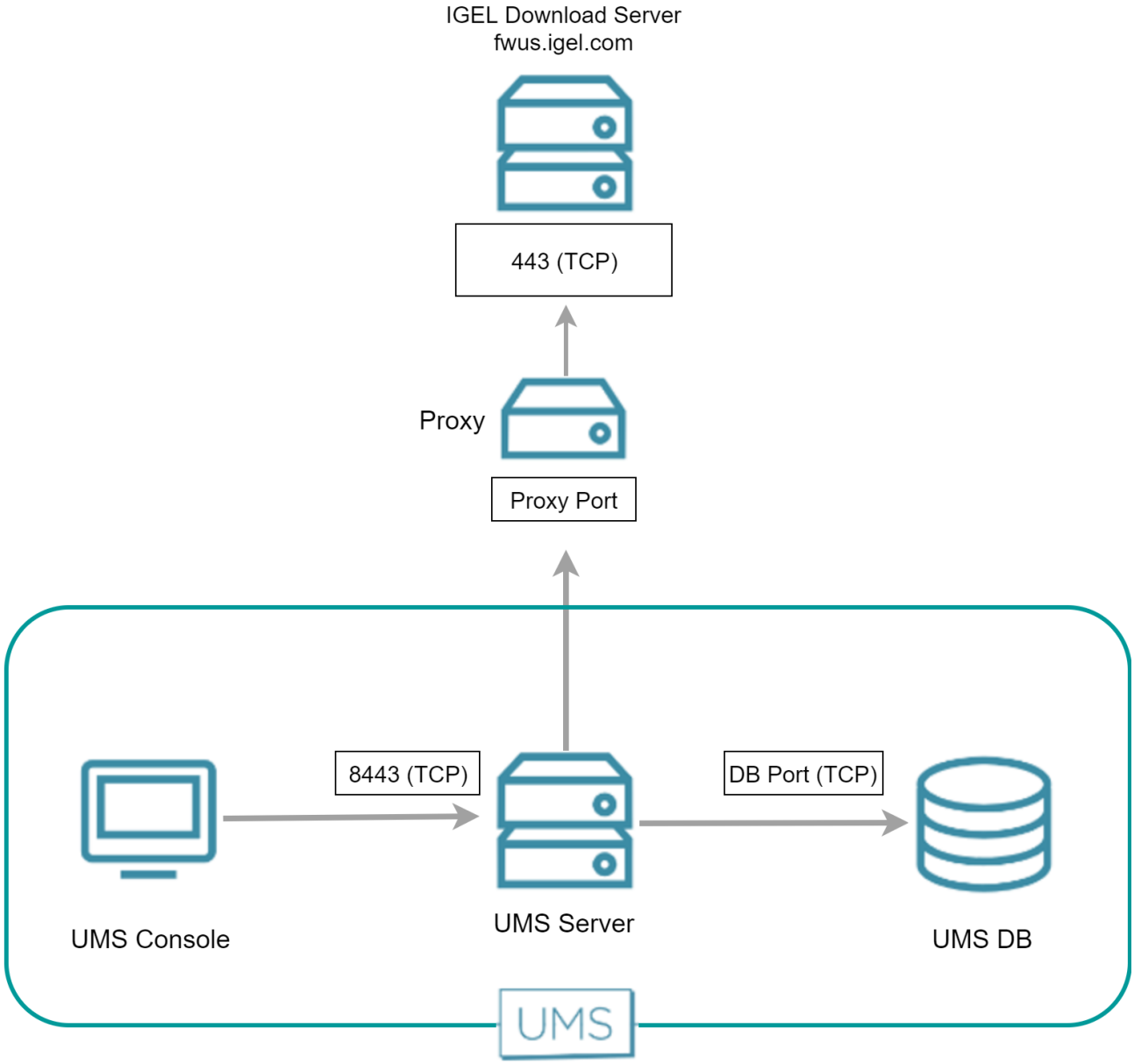
Direct Connection

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



Via Proxy

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



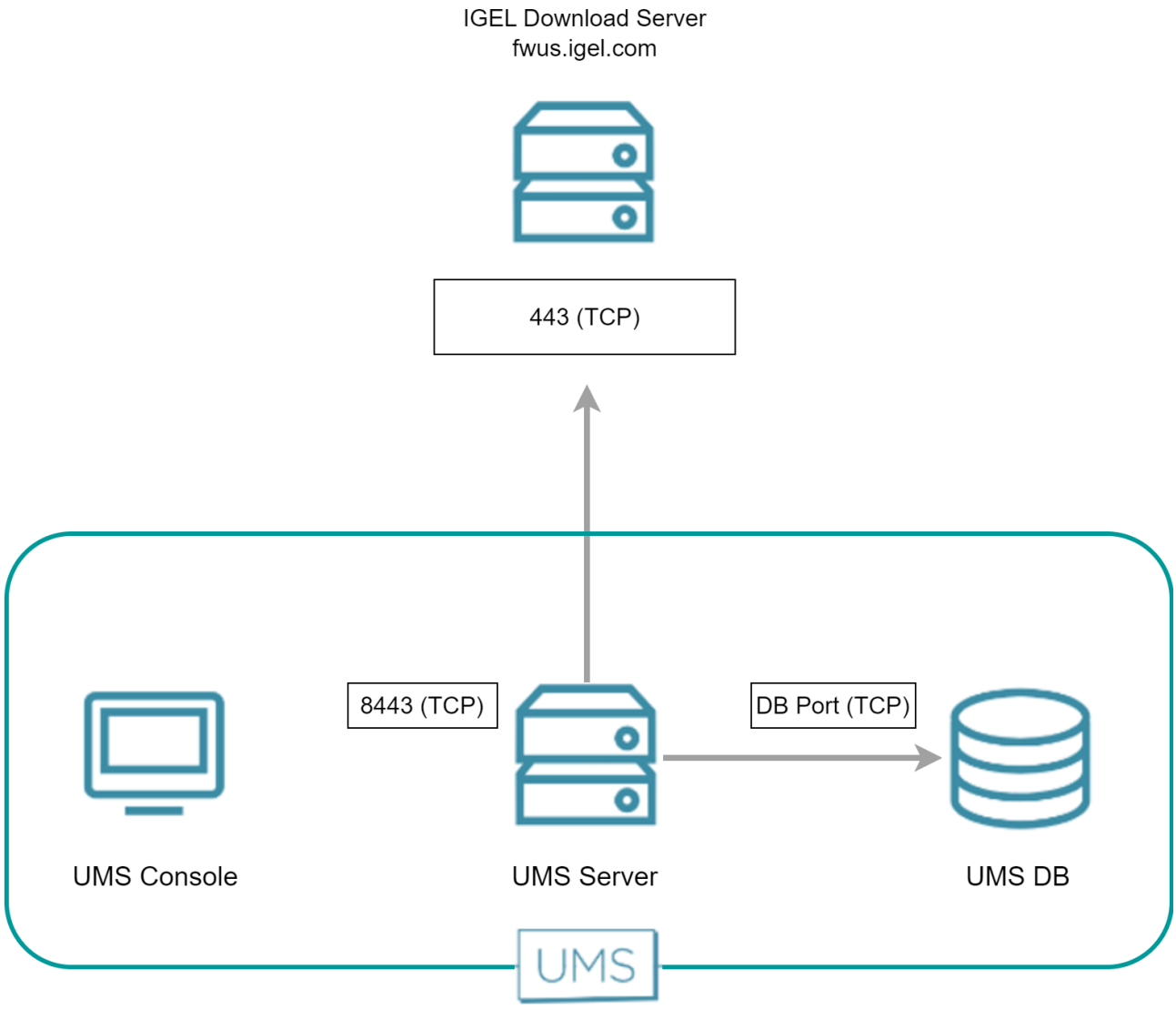
UMS Downloading the Firmware

> The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

The UMS downloads the desired firmware using the URLs it received from the download server. The UMS uses port 443 for fwus.igel.com.

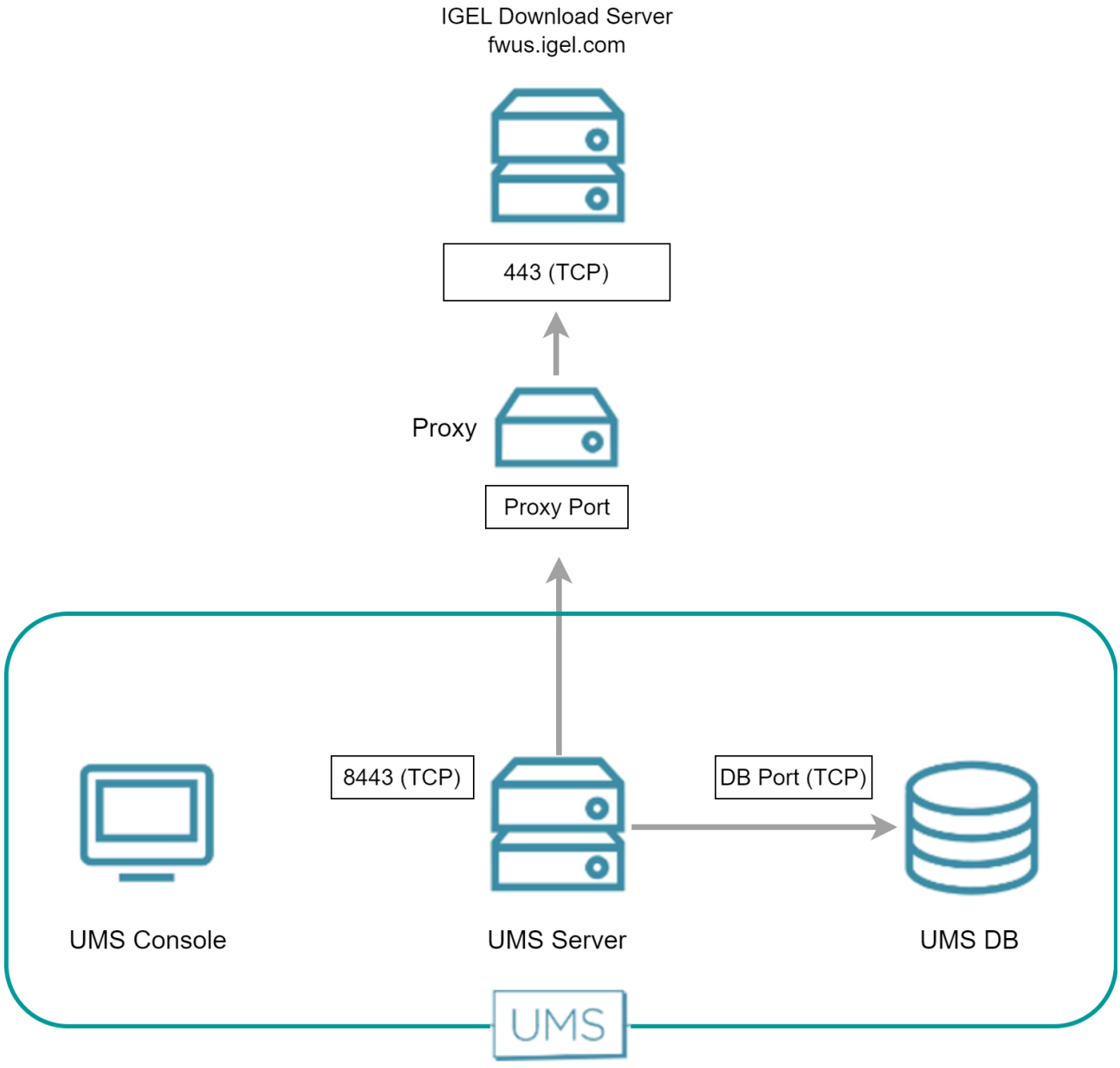
Direct Connection

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



Via Proxy Server

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



Automatic License Deployment (ALD) Communication Flow in IGEL

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

For more information about this feature, see *IGEL Subscription and More > Setting up Automatic License Deployment (ALD).*

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

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

UMS Contacting the Licensing Server

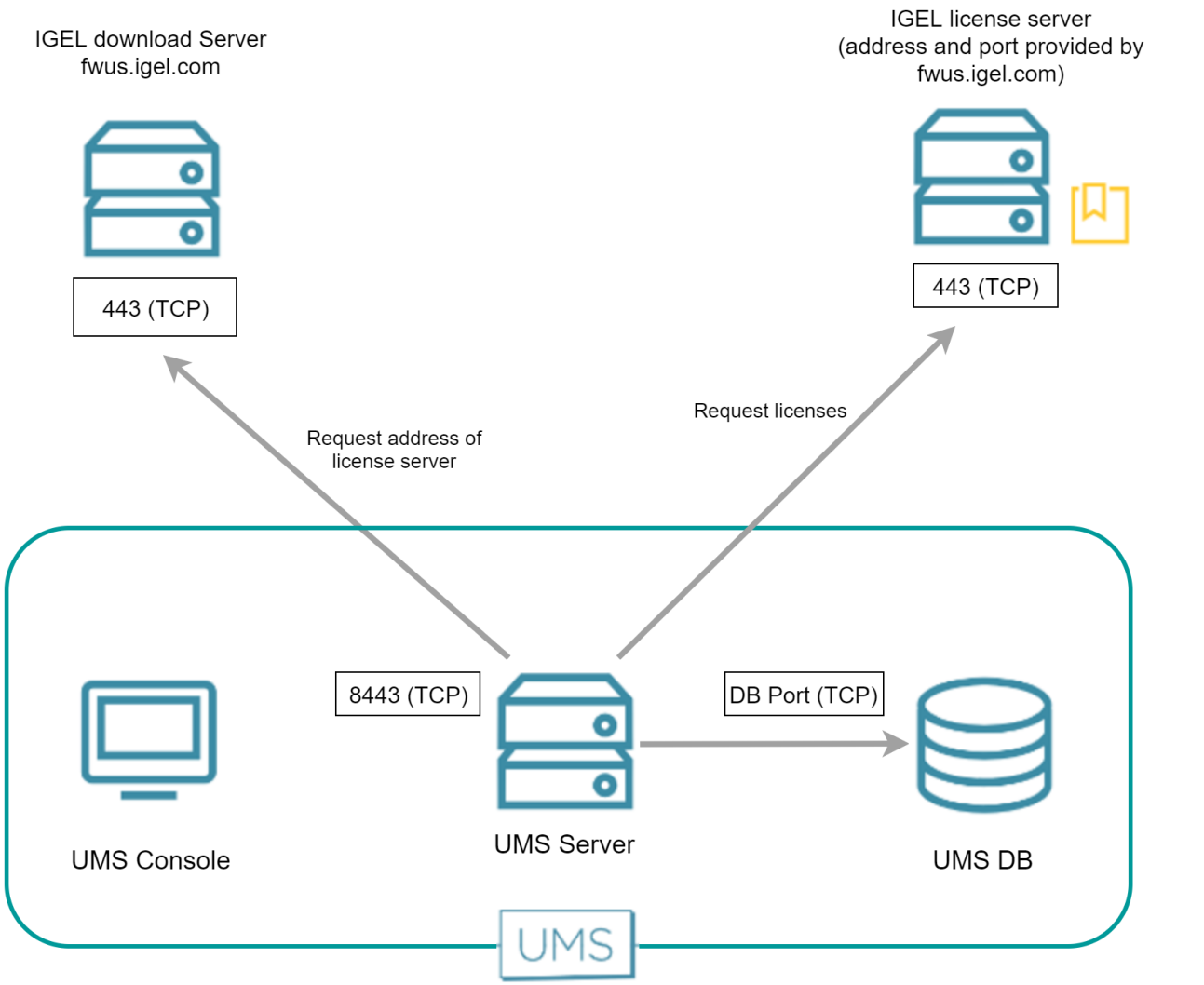
The UMS requests the connection details (URL and port) from the IGEL download server at fwus.igel.com and then contacts the IGEL licensing server. Currently, the connection details are as follows:

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

> The connection details may be changed in the future.

Direct Connection

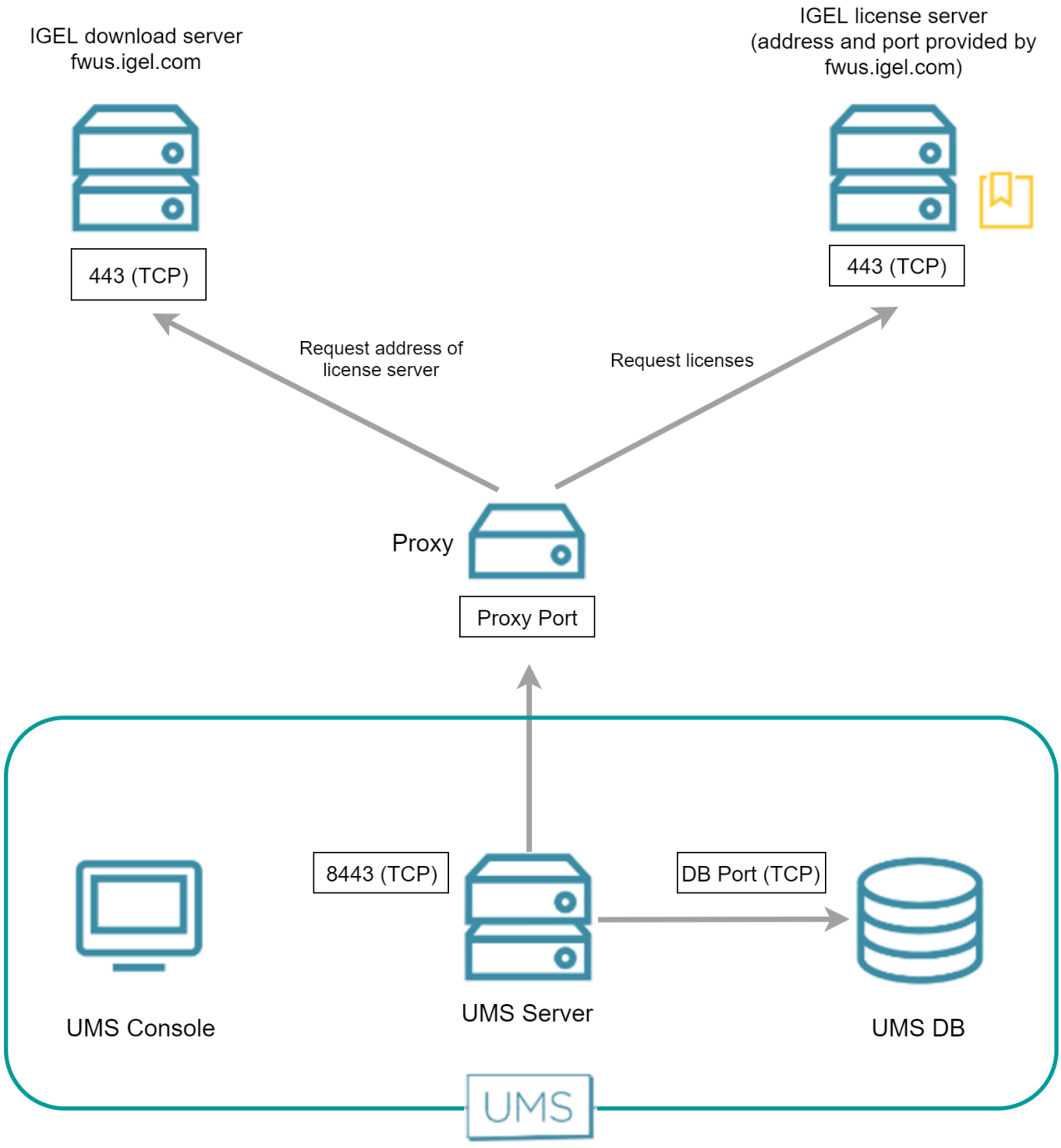
The following figure illustrates the communication between the UMS Server and the IGEL licensing server:



Via Proxy Server

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

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


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

UMS Sending New Settings to the Devices

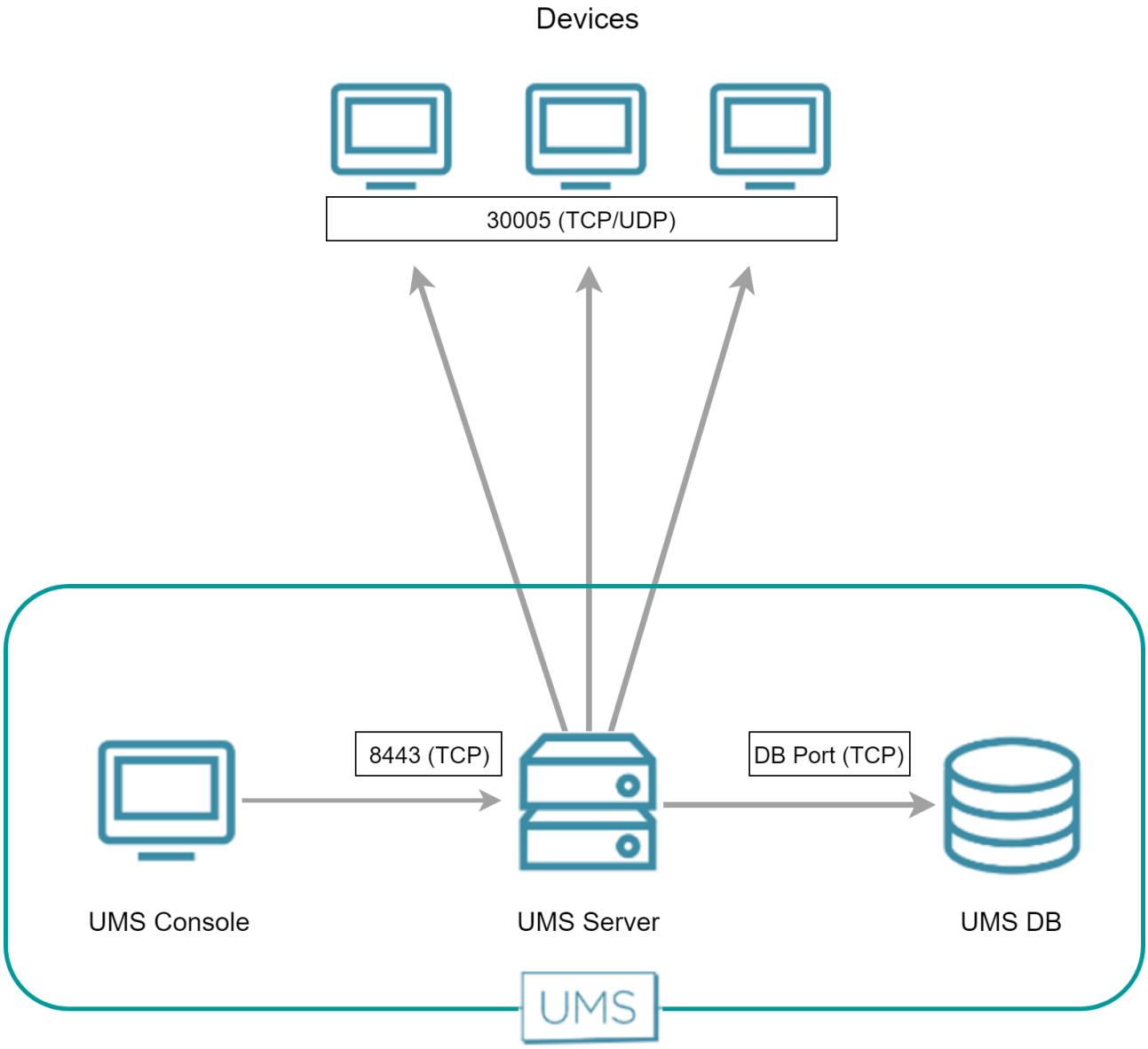
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened for the license transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

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

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



Devices Contacting the UMS to Download License Files

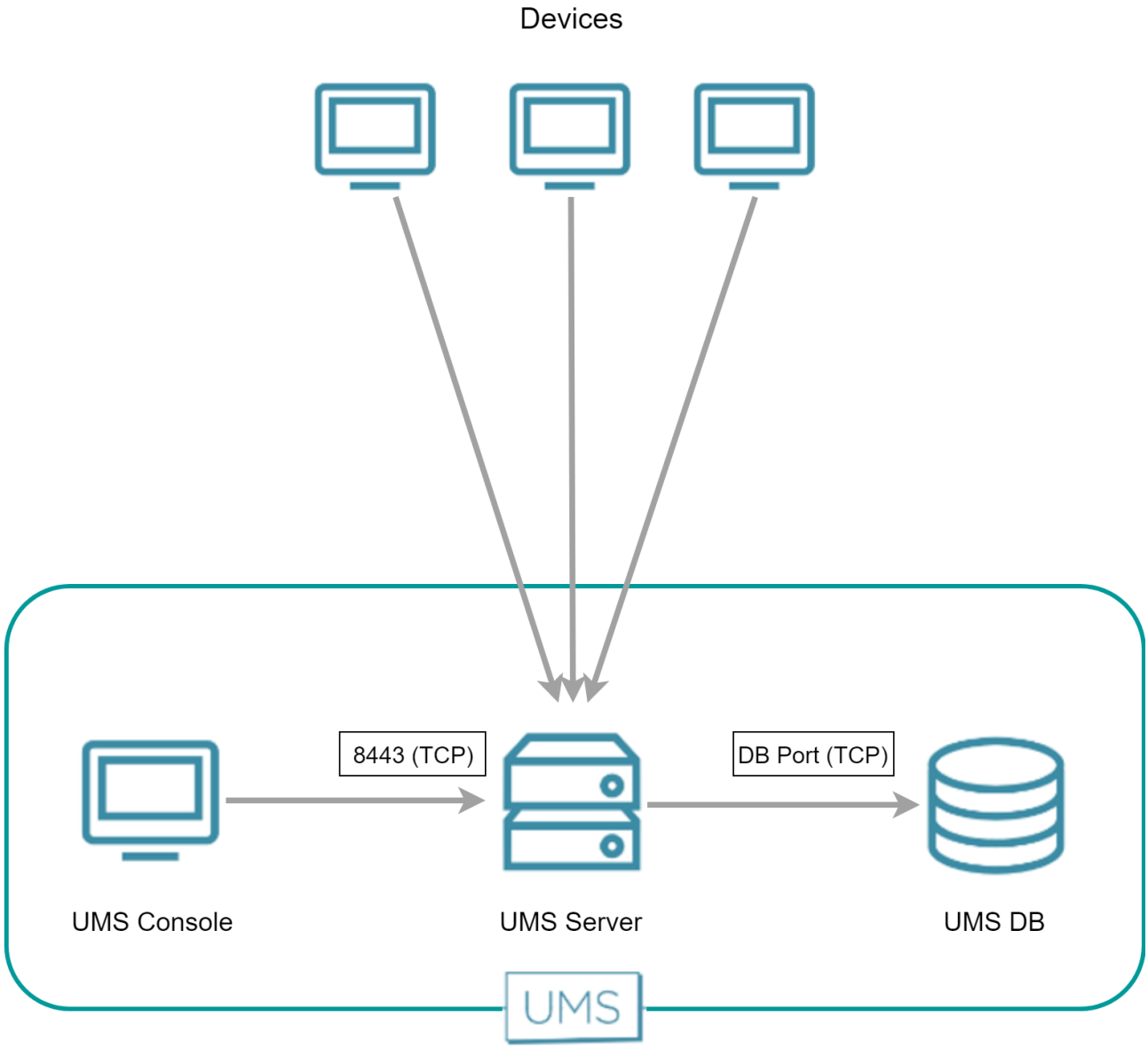
IGEL OS 12

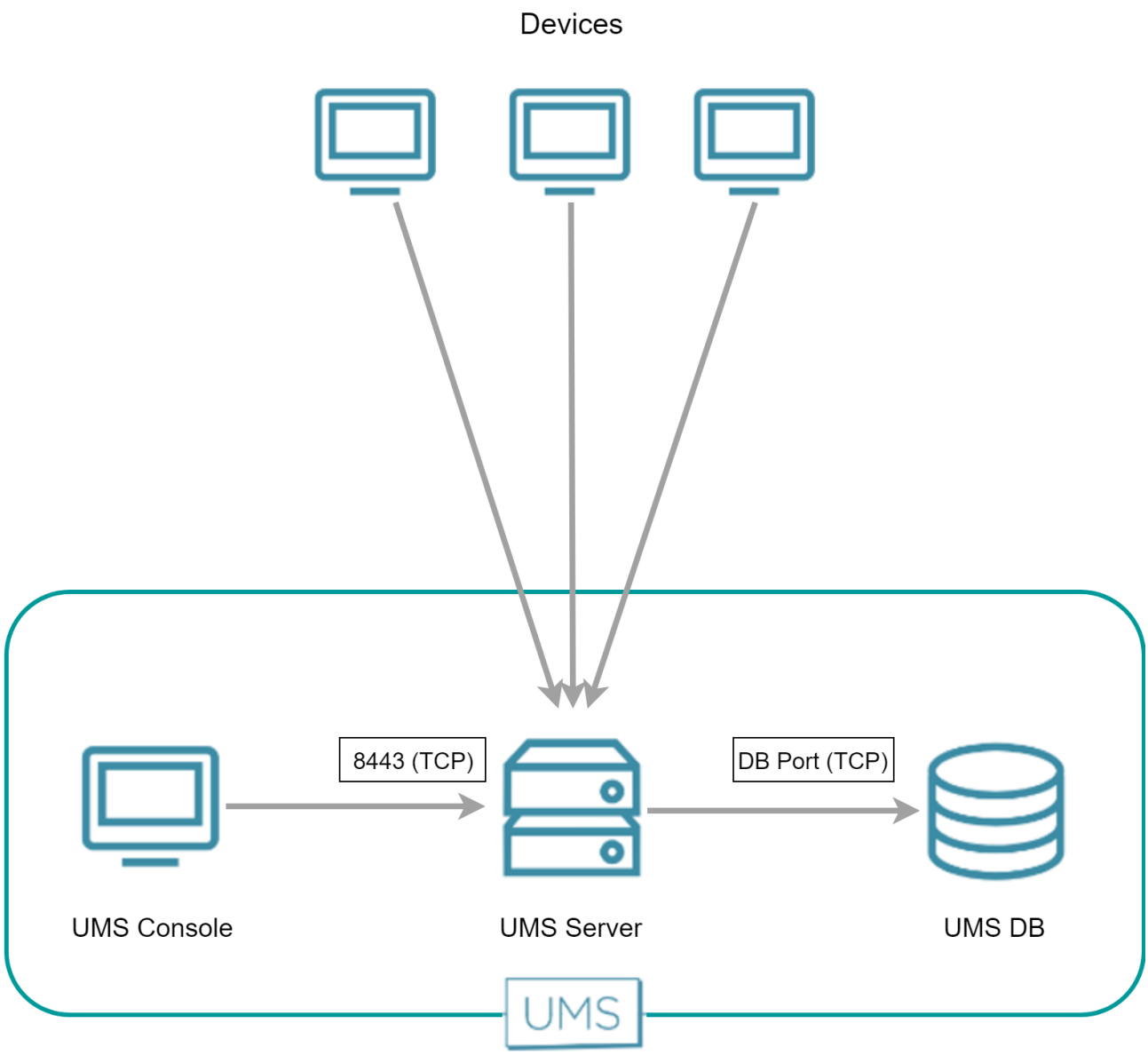
For IGEL OS 12 devices, no additional channel is opened for the license transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

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

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



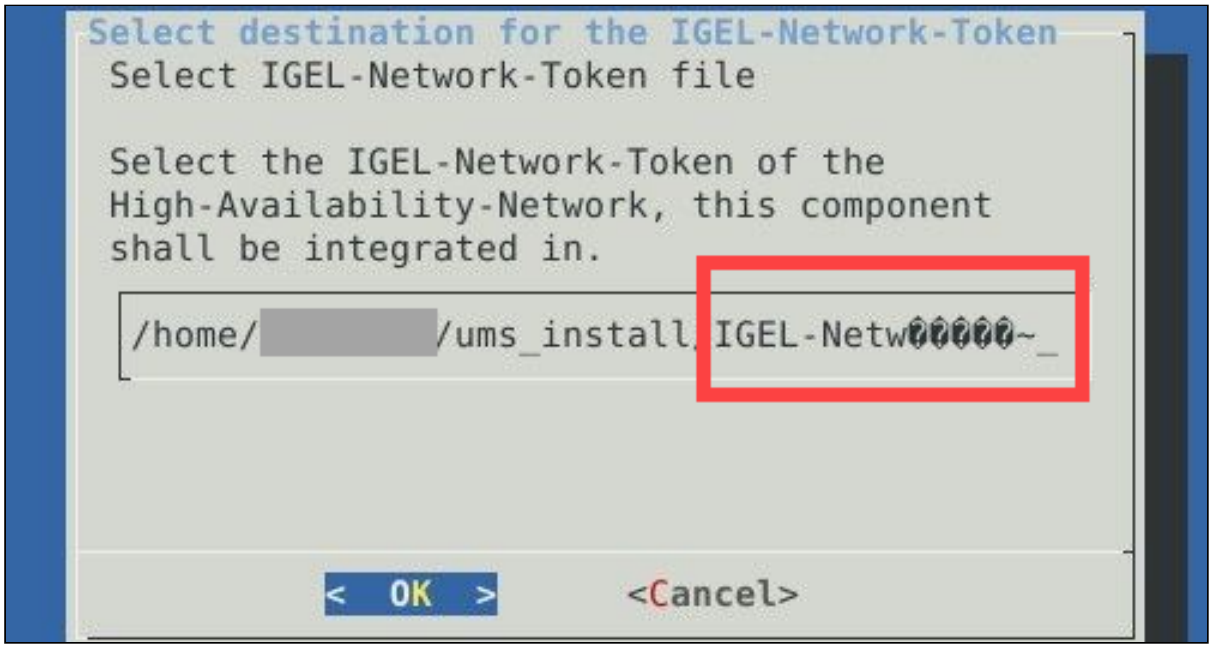

Devices
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

UMS Installation

Using Special Characters during the UMS Installation on Linux

Question

Why do I see strange symbols in the UMS installer on Linux, e.g. when saving / loading the IGEL network token?



Answer

When you want to use language-specific characters, e.g. umlauts (`ä` , `ö` , etc.), for the UMS installation on Linux:

- the correct locale for the language must be set
- the system locale must also be correctly set

→ Run the following command to list the available locales: `locale -a`

→ If the necessary locale is not listed, you can generate and set it as the default locale for your system as follows (example for German):

```
sudo locale-gen de_DE.UTF-8
sudo update-locale LANG=de_DE.UTF-8
```

UMS Installation on 64-Bit Systems

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

Question

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

Answer

Since UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. For information on UMS installation, see IGEL UMS Installation (see page 13) .

Since UMS 5.07.100

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

Before UMS 5.07.100

- Windows: Use the 32-bit compatibility mode (which is activated by default) before installing IGEL UMS (e.g. on Windows Server 2008 R2).
  See also MSDN: "Running 32-bit Applications"[97]

- Linux (amd64/x86_64): Install the 32-bit compatibility packages before installing IGEL UMS. Examples with Ubuntu follow below, apart from that see:
  - Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3 (see page 26)
  - Installing UMS on Oracle Linux Server (see page 28)

Example with Ubuntu 14.04 LTS 64-bit:

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

Example with Ubuntu 16.04 LTS 64-bit:

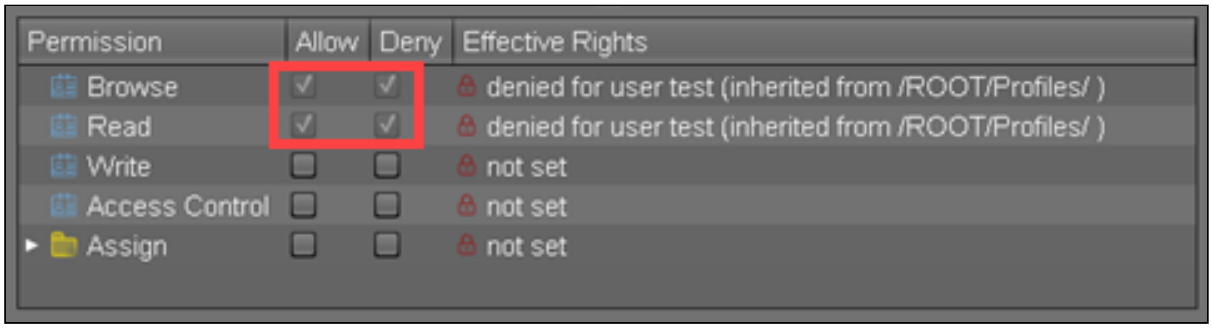
97. https://msdn.microsoft.com/en-us/library/aa384249%28VS.85%29.aspx

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

Troubleshooting Missing Permissions after the UMS Update

Symptom

You have updated the UMS to version 6.05.100 or higher and have no permissions for an object/tree node in the UMS anymore. In the **Access Control** dialog, both checkboxes **Allow** and **Deny** are enabled but not editable:

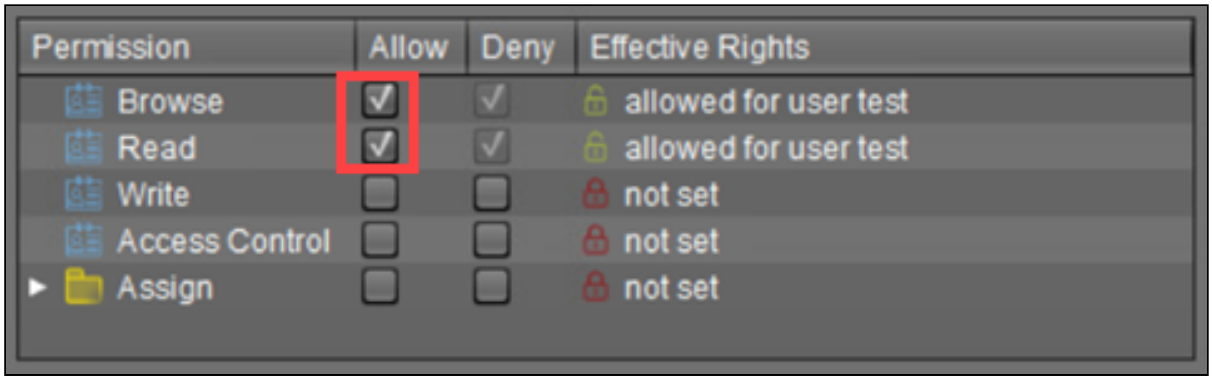


Environment

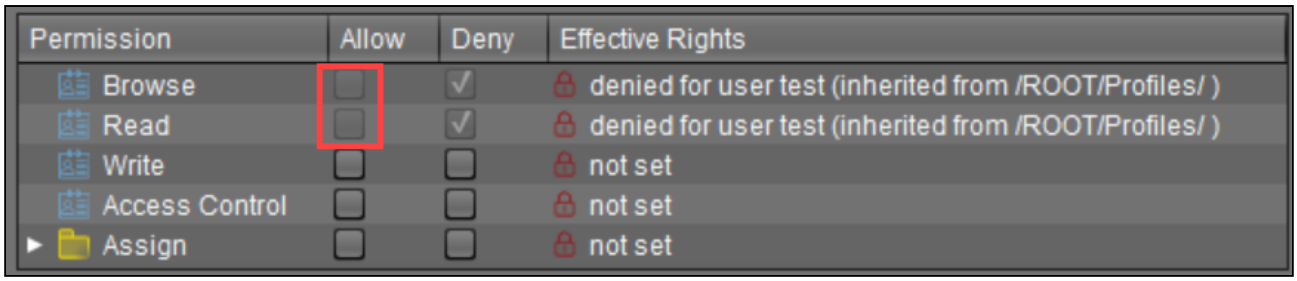
- UMS 6.05.100 or higher

Problem

Before UMS 6.05.100, permissions could be granted for a subnode even if they were denied for a node.



With UMS version 6.05.100, the evaluation of UMS permissions has changed: If you set **Deny** on a node, you cannot set **Allow** permission on a subnode. The **Allow** checkbox is not editable.



Solution

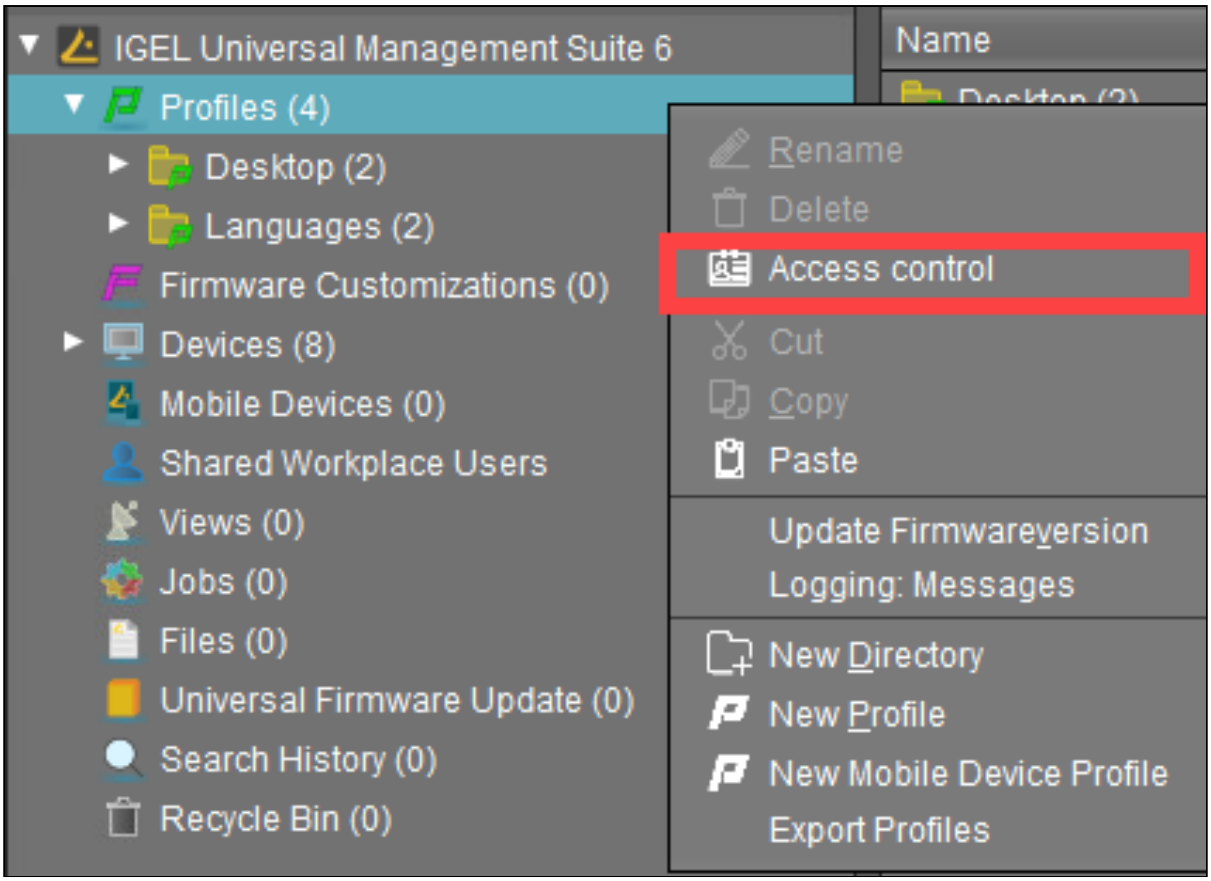
→ Check the permissions in the **Access Control** dialog. If the **Allow** permissions should be given for a subnode, do not set any permissions for the node.

If the permissions are not set, the behavior is like by **Deny**. Therefore, the user will not have access rights on the node but can browse up to the subnode.

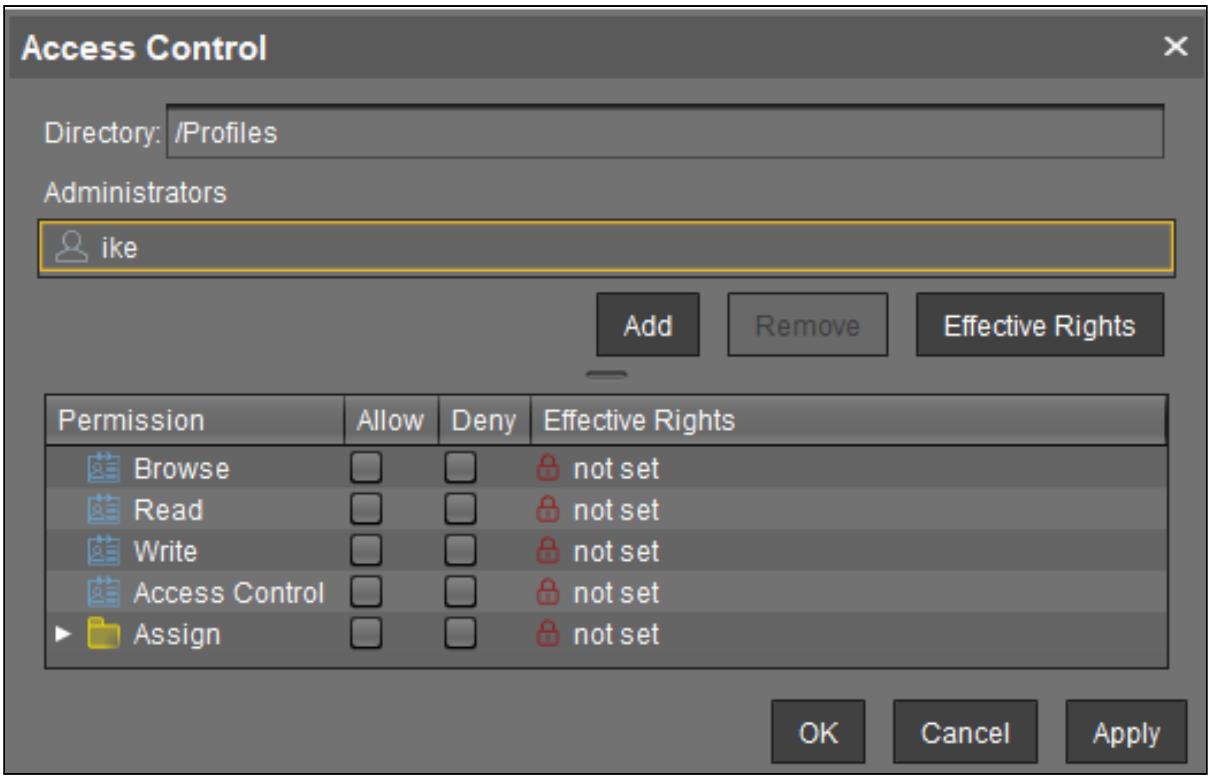
Example:

The user should have access rights only to the profile folder "Languages" and its contents:

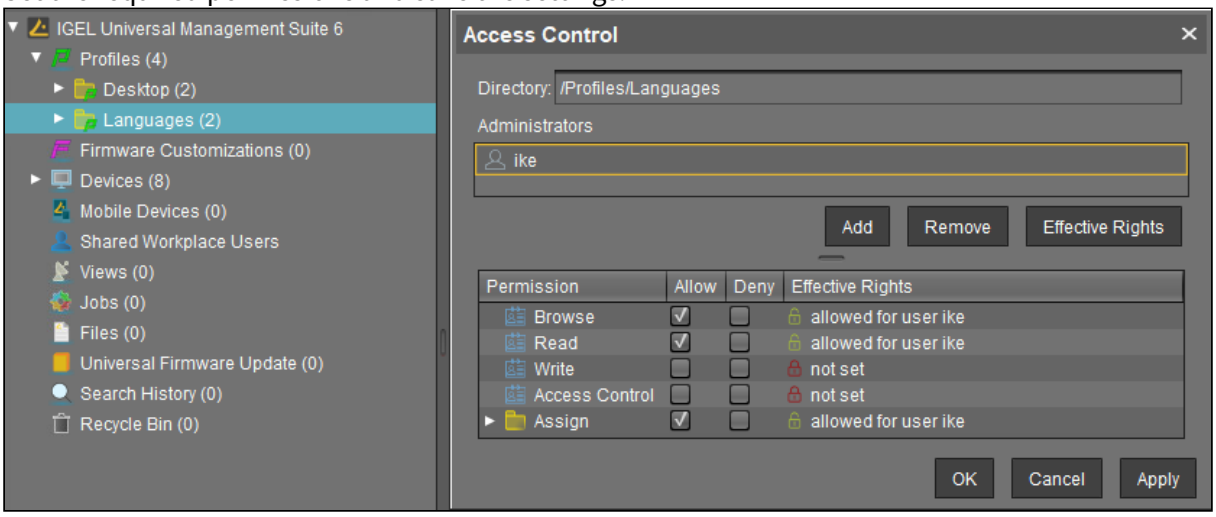
1. Open the **Access Control** dialog for a node, **Profiles** in this case.



2. Disable checkboxes **Allow** and **Deny**.
   The **Effective Rights** read now "not set".



3. Open the **Access Control** dialog for a subnode, for which premissions should be granted. In our case, it is the folder "Languages".
4. Set the required permissions and save the settings.



The user can only browse up to the subnode "Languages", for which the access rights have been given.

Troubleshooting Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux

You have just installed IGEL Universal Management Suite (UMS) 12 or updated your existing UMS installation to UMS 12 on Linux and face now various issues, e.g. with the scanning and registration of IGEL OS 12 devices.

Symptom

After the installation of UMS 12 on Linux, you have problems with automatic or manual device registration, logging in to the UMS Web App, etc.

On the device side, you get the following error (e.g. when running the command `journalctl -f` when trying to register the device):

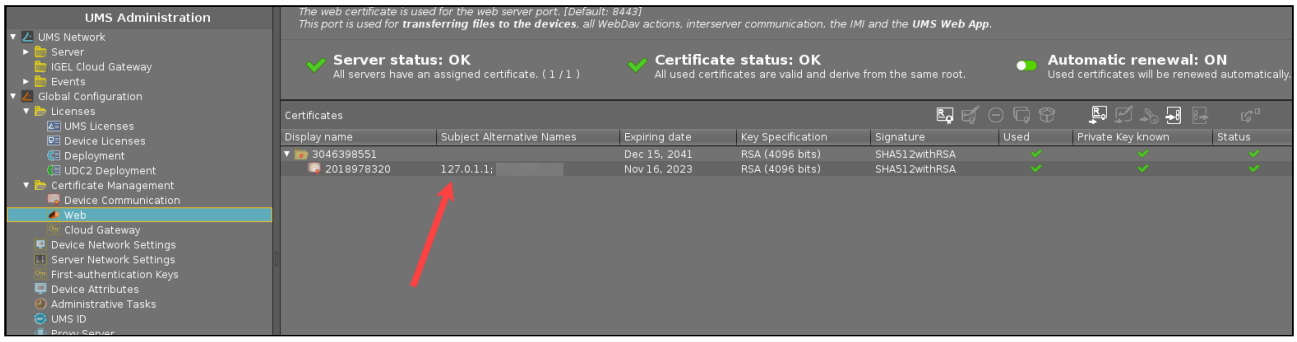
```
ERROR: Failed to verify certificate... IP address mismatch
```

Environment

- IGEL UMS 12 on Linux

Problem

For new or update installations on a Linux host, the IP address determined by the JRE can be often wrong (e.g. default IP: 127.0.1.1). If the correct IP of the UMS Server was not specified in the UMS installer during the installation / update, this will lead to invalid UMS certificates.

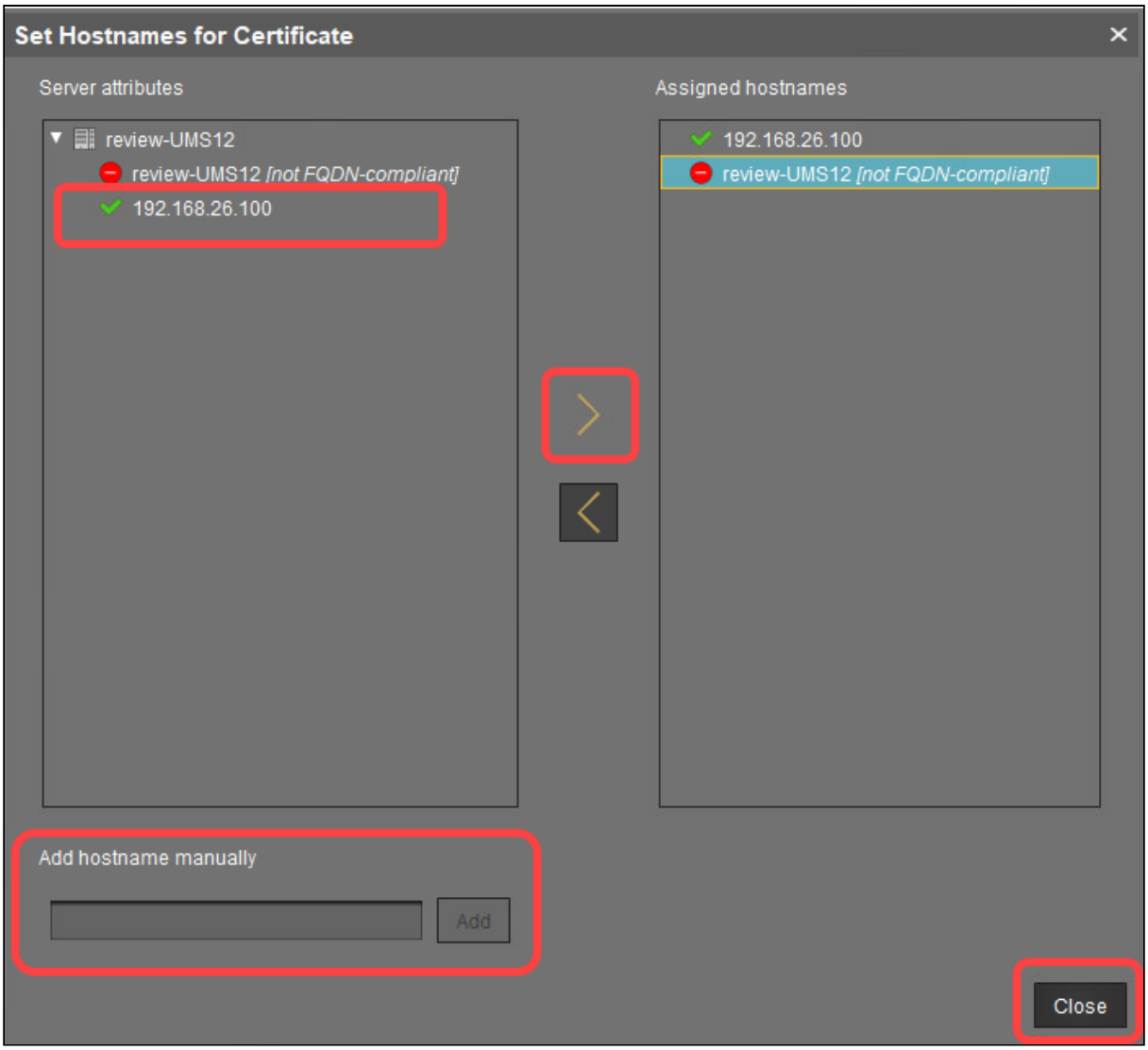


Solution

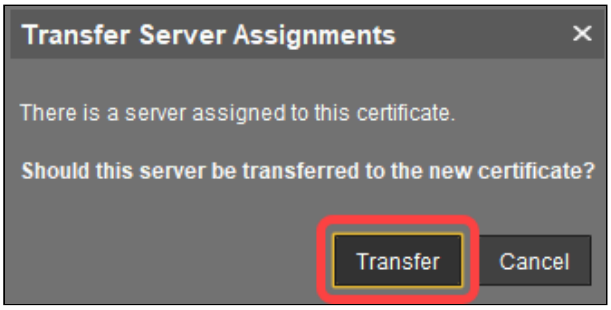
You have to generate a new certificate:

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Select the existing certificate and click **Renew certificate**  .

3. In the dialog **Create Signed Certificate**, fill in the empty fields (if there are any); all other settings can be left unchanged. Click **Manage hostnames**.
4. In the dialog **Set Hostnames for Certificate**, check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.
   Note: Under **Assigned hostnames**, there must be only FQDN-compliant names. Remove all not FQDN-compliant names, if there are any, using an arrow button.



5. Click **Ok**.
6. In the dialog **Transfer Server Assignments**, click **Transfer**.
   Note: If you are not sure, you can click **Cancel** and assign the created certificate later via **Assign server** in the context menu.



A new certificate will be created and used for the server.

It is also recommended to check the Linux OS file `/etc/hosts` and, if there are wrong entries there like 127.0.1.1, change them to the correct IP of your UMS Server and the correct server name.

Best Practices for User Access to IGEL UMS Server

Starting from IGEL Universal Management Suite (UMS) version 12.07.100, you can define the user under which the UMS Tomcat services should run. Using a non-root user allows you to meet security standards with greater flexibility. In this article, you will find how to define user access and why it is not recommended to start the UMS Tomcat services as root user or admin user.

The service user can only be set during an initial UMS installation, not during an update installation.

The installation of the IGEL UMS itself must be performed under a root/admin user but for security reasons, it is not recommended to run the UMS Tomcat services as a root/admin user. Using a dedicated user with the minimum necessary authorizations for the operating system significantly reduces security risks.

We strongly recommend using a user with minimal authorizations in order to follow the principle of least privilege and increase system security.

How to Specify the User in Windows Installation

1. Create a user that can be used to start the UMS Tomcat services before the UMS installation is started.
    - The service user should not have root rights.
    - The user must have a valid password.
    - No additional permissions are required, as all necessary permissions are granted during the installation process.

2. Select the service user during the UMS installation. For details, see IGEL UMS Installation under Windows (see page 48) .

3. Authenticate the user through password verification.
   All UMS Tomcat services will now be started with this user.

How to Specify the User in Linux Installation

1. Create a user that can be used to start the services before the UMS installation is started.
    - The service user should not have root rights.
    - The user must have a valid password.
    - No additional permissions are required, as all necessary permissions are granted during the installation process.

2. Select the service user during the UMS installation. For details, see IGEL UMS Installation under Linux (see page 17) .

The watchdog service (used in UMS High Availability) needs root user privileges on Linux. Therefore, this service will be started as root on Linux.

3. Authenticate the user through password verification.
   All UMS Tomcat services will now be started with this user.

For password verification, the module “pamtester” is required on your system. This module will be automatically downloaded as part of the installation process. If you choose not to install it, the installation will only be functional for the root user.

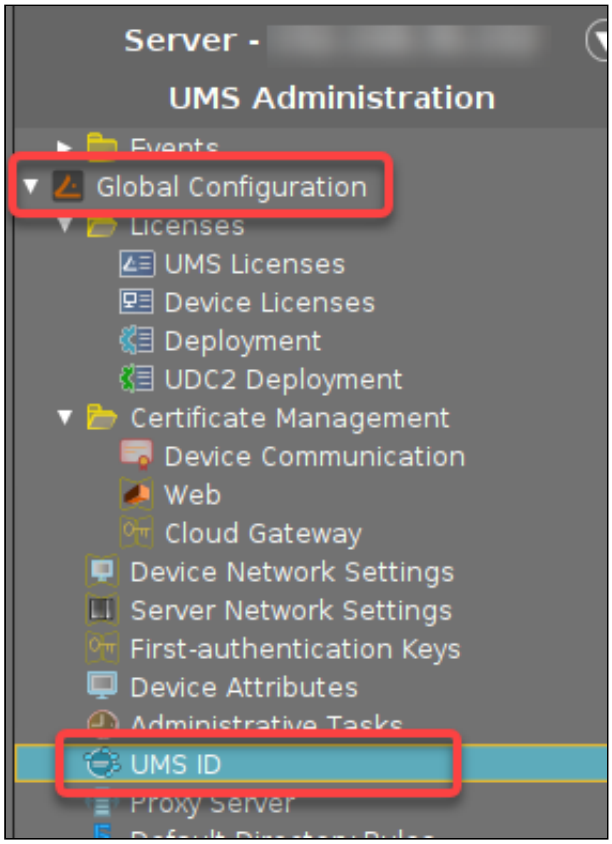
How to Export the UMS ID

The IGEL Universal Management Suite (UMS) ID[98] is used, for example, for the communication of your UMS with the IGEL Cloud Services. The UMS ID also enables communication between the UMS and the IGEL License Portal (ILP). Follow the steps below to export the UMS ID to a certificate file from the UMS Console or the UMS Administrator.

Exporting the UMS ID from UMS Console

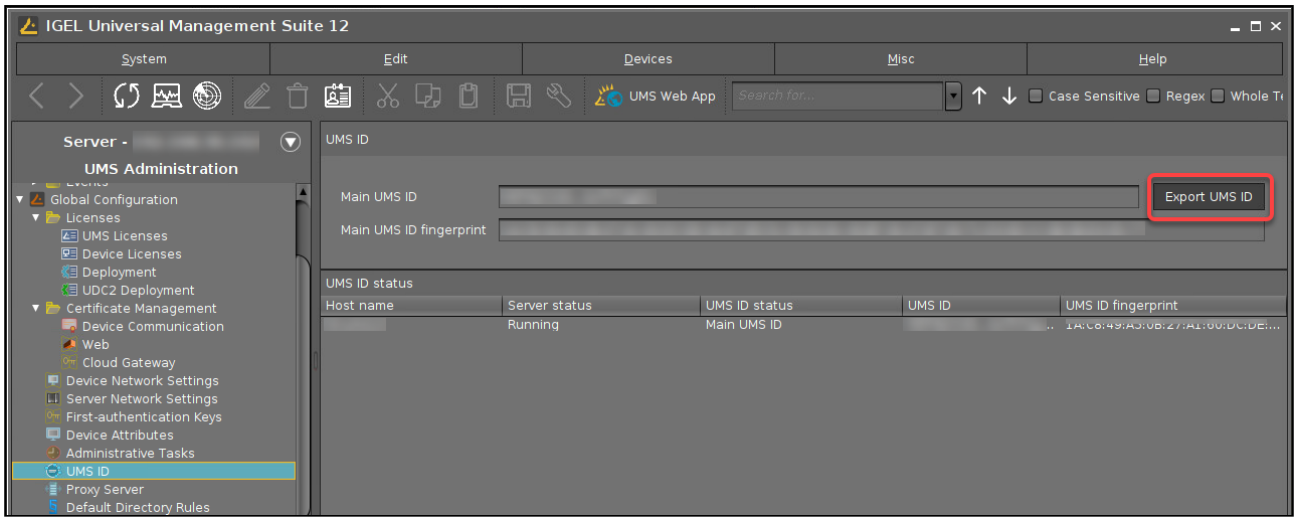
The UMS ID can be exported from the UMS Console:

1. Open your UMS Console, go to **UMS Administration > Global Configuration > UMS ID**.

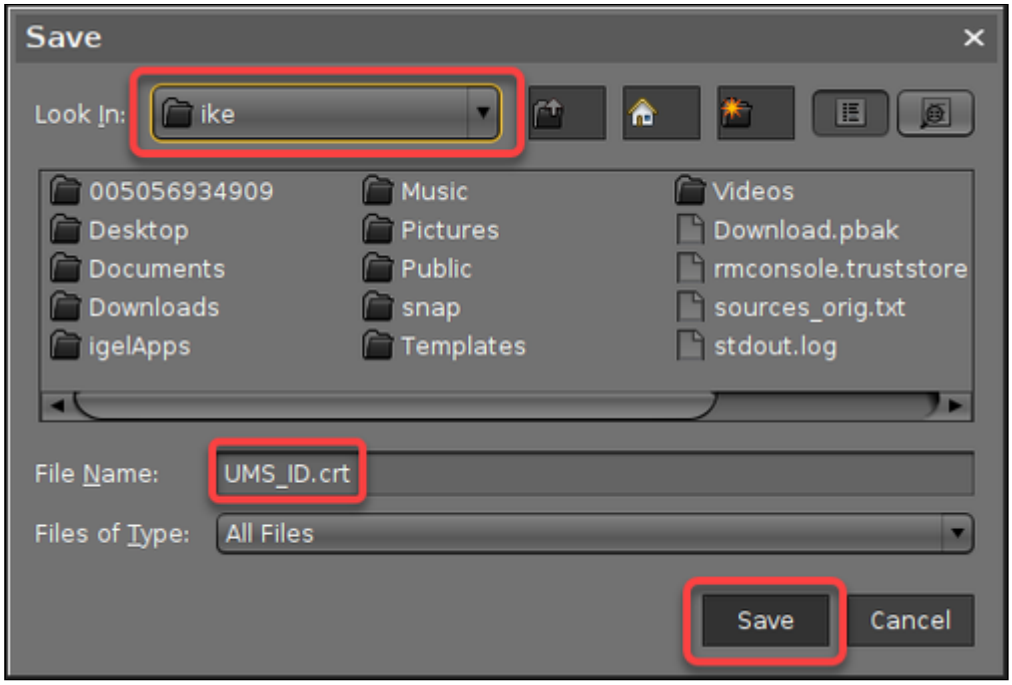


2. Click **Export UMS ID**.

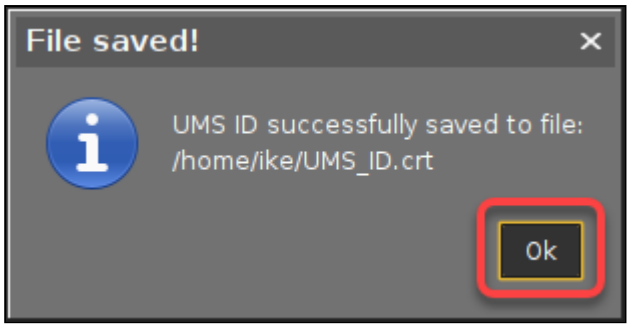
98. https://kb.igel.com/en/universal-management-suite/current/ums-id



3. Select a storage location to save the certificate file (`UMS_ID.crt`) and click **Save**.



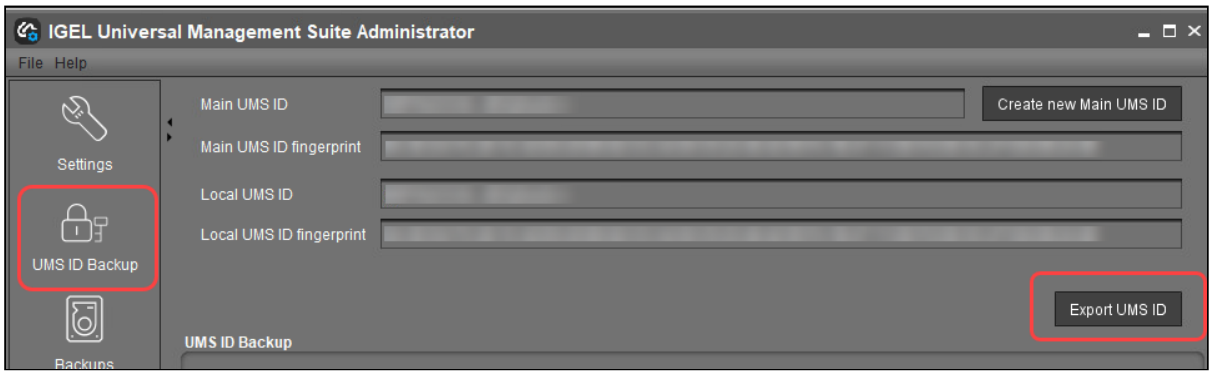
4. Close the confirmation dialog.



Exporting the UMS ID from UMS Administrator

To export from the UMS Administrator:

1. Open the UMS Administrator and go to **UMS ID Backup**.



2. Click **Export UMS ID** and save the certificate file (`UMS_ID.crt`).

Customization

User Authorization Rules

Problem

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

Reason

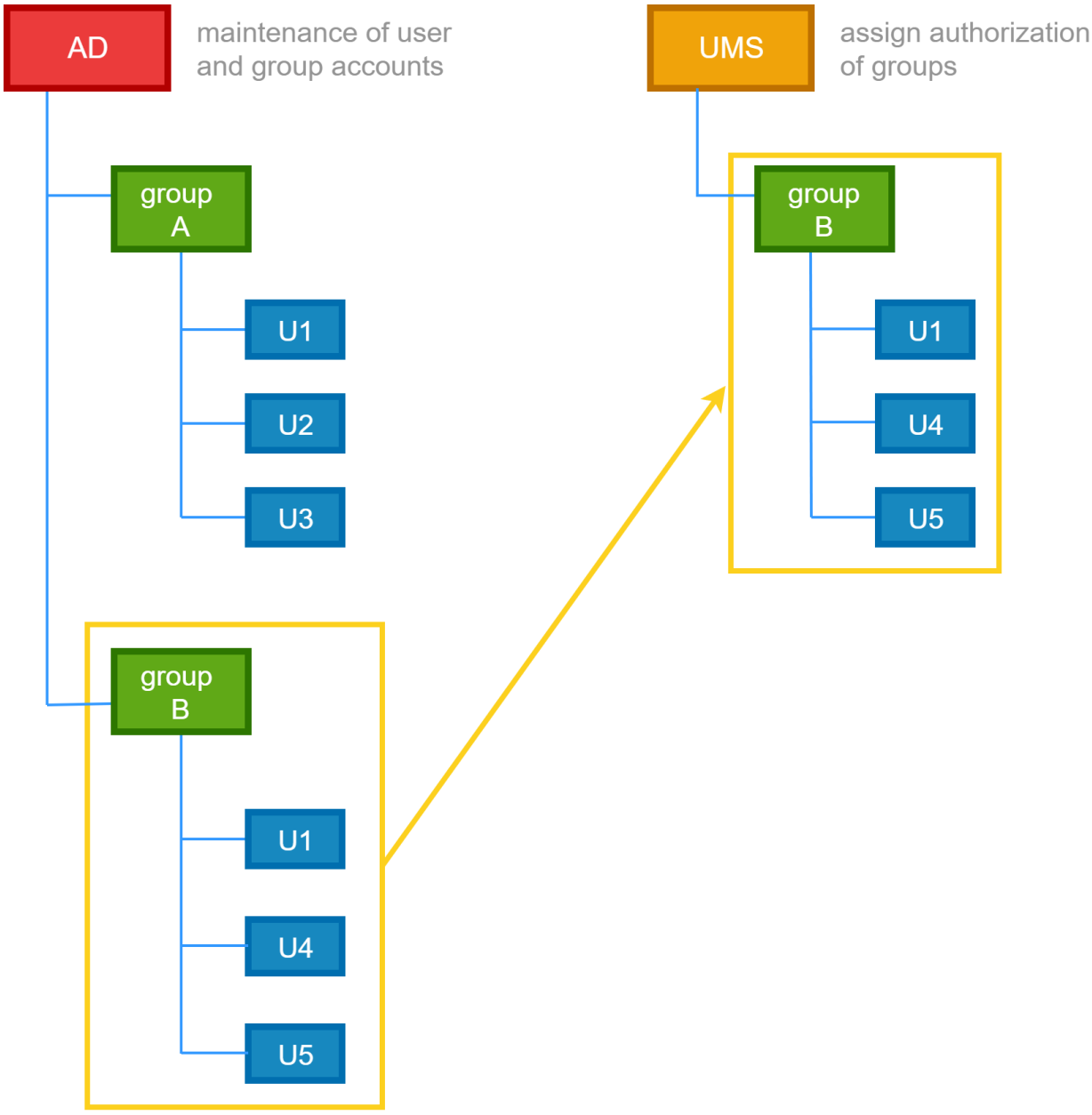
In the IGEL UMS, you can create user or administrator accounts, and you can assign rules to them, but it is not possible to assign roles.

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

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

Solution

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



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

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

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

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

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

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

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

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

Please note:

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

How to Manage User Permissions via IGEL UMS

Purpose

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

Solution

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

Additional Information

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

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

Defining end user permissions:

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

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

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

For further details about authorization rules see our How-To User Authorization Rules (see page 414) .

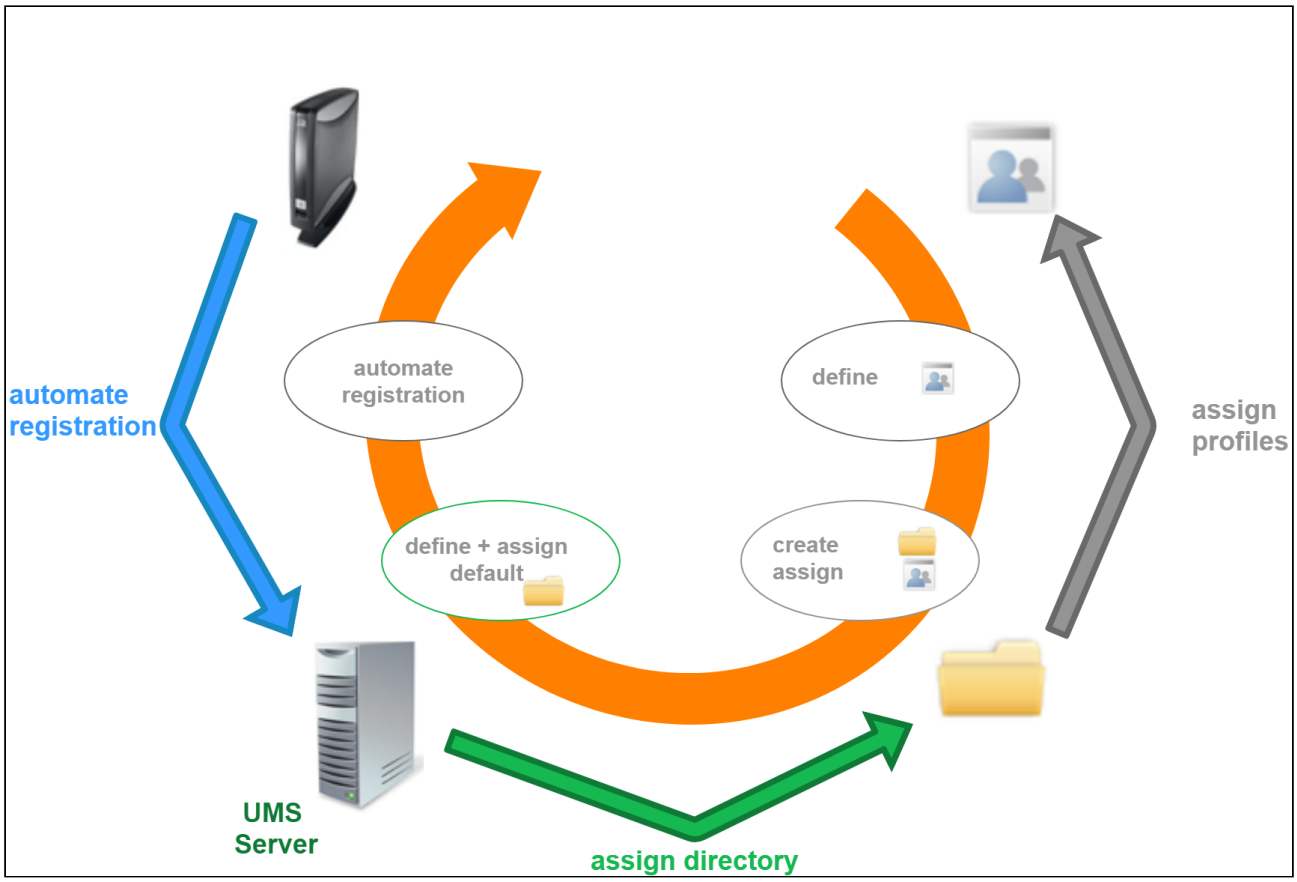
Access rights to objects or actions within the *IGEL* UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

How to Automate the Rollout Process in the IGEL UMS

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

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

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



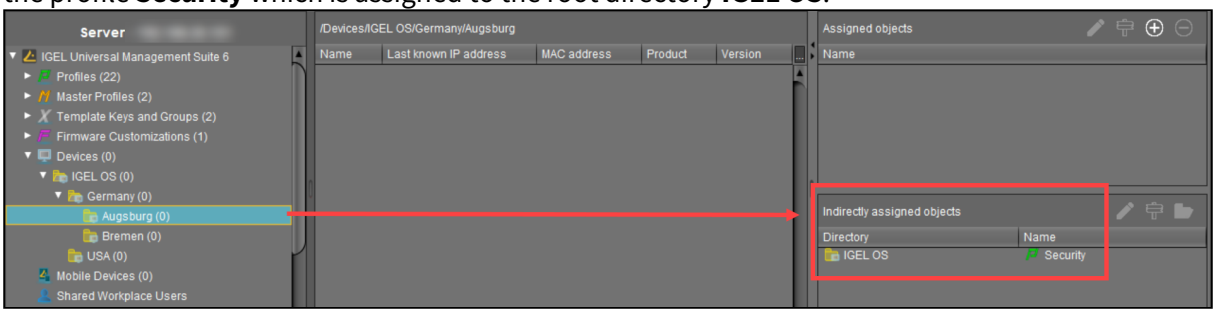
Preparing Automatic Rollout

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

1. Create a new root directory, e.g. **IGEL OS**.
   For how to create a device directory, see Creating a Directory in the IGEL UMS (see page 787).
2. Assign certain profiles to this root directory, e.g. **Security**.
   For how to assign profiles, see How to Allocate IGEL UMS Profiles (see page 707). See also Prioritizatio

n of Profiles in the IGEL UMS (see page 728).
For detailed information on profiles, see Profiles in the IGEL UMS (see page 695).

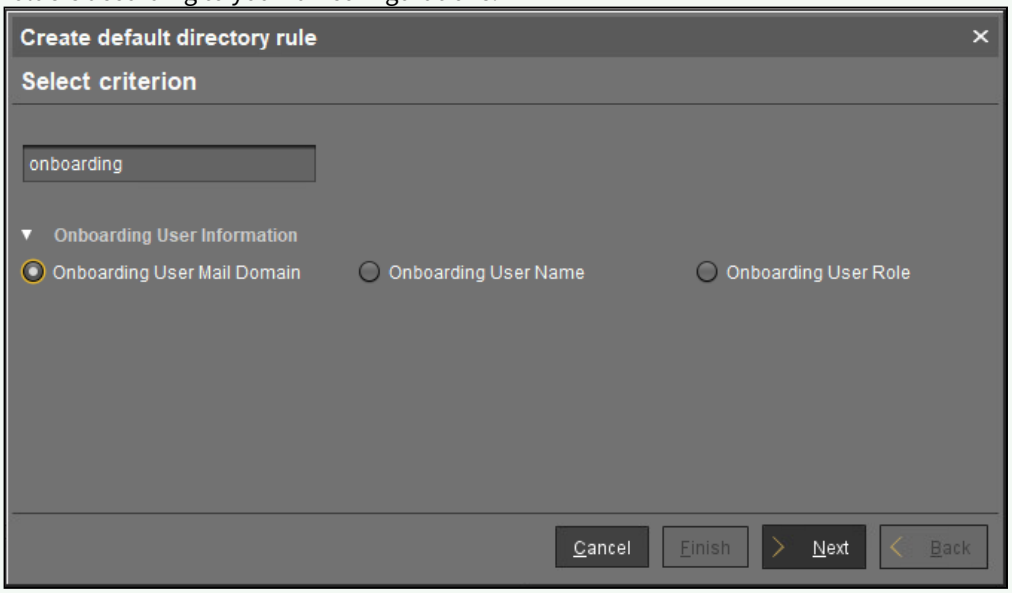
3. Move your devices or your directories containing devices to this root directory.
   These devices will inherit the profiles assigned to the root directory.
   Example: Devices that will be placed to the directory **Augsburg** during the registration will inherit the profile **Security** which is assigned to the root directory **IGEL OS**:



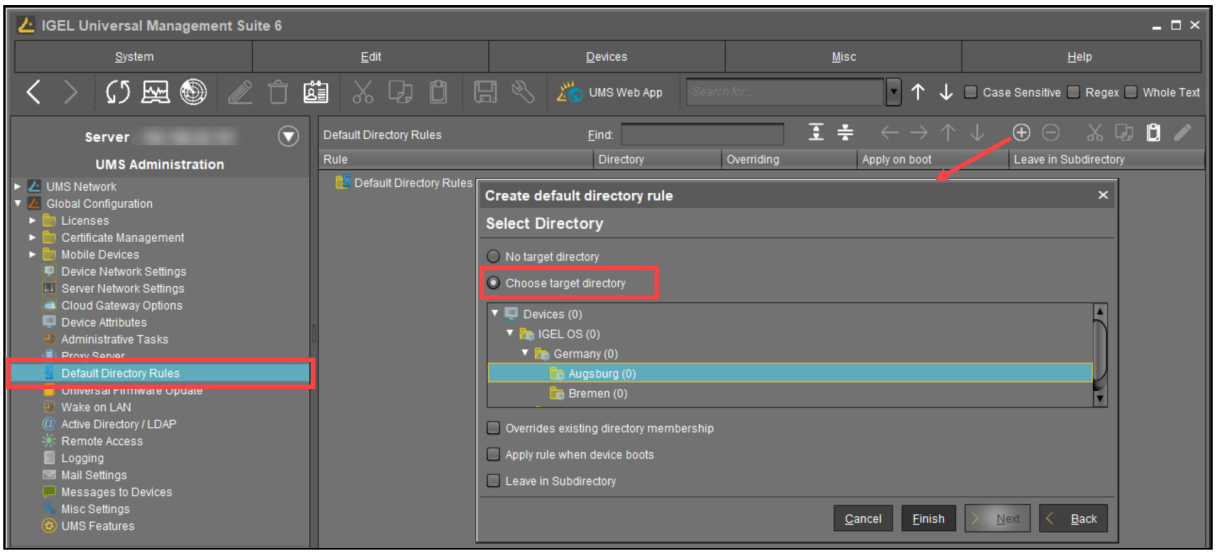
Automating the Rollout

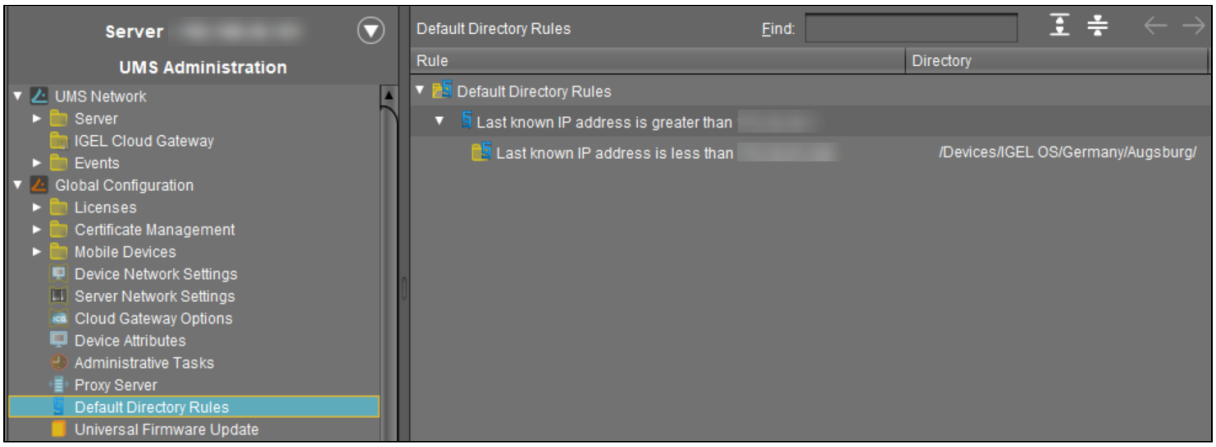
1. Click **UMS Administration > Global Configuration > Default directory rules** to create a new default directory rule.
   For detailed information on default directory rules, see Default Directory Rules (see page 969).

If you use the IGEL Onboarding Service (OBS) to onboard devices, you have an Identity Provider (IdP) configured for the authentication. You can also use the user mail domains, user names, or user roles of the configured IdP as default directory rule criterion, so that you can automatically assign devices to device folders according to your IdP configurations.



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

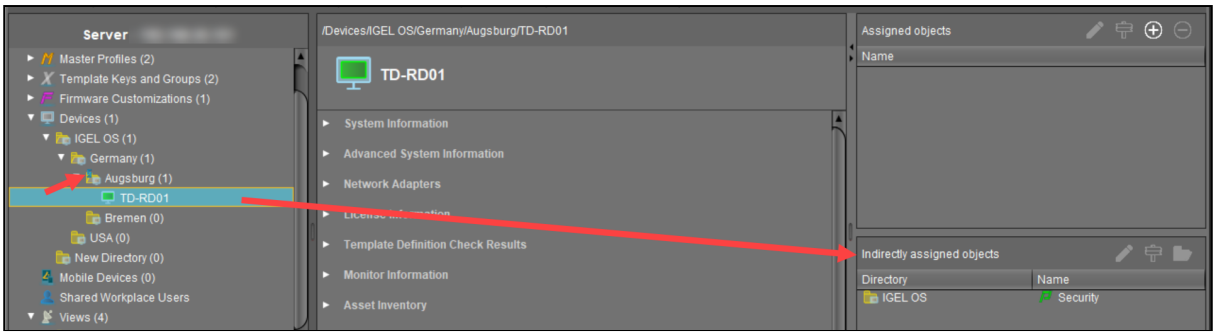




3. Configure your DNS or DHCP server and activate the automatic registration of devices as described under Registering Devices Automatically on the IGEL UMS (see page 1151).

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

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



Related Topics

If you want to use structure tags for automating the rollout: Using Structure Tags with IGEL OS 11 Devices (see page 422)

If you have problems with the device registration: Troubleshooting: Registration of a Device via Scanning for Devices Fails (see page 533)

Using Structure Tags with IGEL OS Devices

When rolling out devices automatically it can be difficult to assign each to the desired folder in the IGEL Universal Management Suite (UMS). Using structure tags, newly registered devices will automatically have the information where they are to be placed in the structure tree of the UMS. The UMS has flexible rules to place a newly registered device into a folder of the structure tree.

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

To use structure tags:

1. Define a structure tag in your Default Directory Rules under **UMS Administration > Global Configuration > Default Directory Rules**.
   Learn more in the UMS manual: Default Directory Rules (see page 969) .
2. Assign a structure tag to a device manually, through onboarding, or via DHCP.

Manual Assignment

In OS 11 you can assign the structure tag value manually on the endpoint or through a profile. To assign the value, enter the value in **System > Remote Management** > **Structure tag**.

In OS 12, you can assign structure tags starting from IGEL OS 12.5.0. To assign the value, use the command tool `/sbin/rmagent-set-structure-tag -t <TAG>` .

⚠ Setting the structure tag via a profile should be avoided as it can cause unwanted side-effects.
Example scenario:
There is a default directory rule in place that moves the device to a target UMS folder based on the structure tag value. As the structure tag value is set by the profile, the default directory rule gets activated, and the device is moved to the target UMS folder. As soon as the device is moved to the target folder, it receives the profiles assigned to this folder. If the target folder doesn't contain the profile value of the structure tag, the device loses the structure tag value. As a result, the device will be moved back to the original folder because the structure tag default directory rule isn't fulfilled anymore.

ℹ Use the command `/sbin/rmagent-get-structure-tag` for getting the currently used structure tag value. If the structure tag was already set via Setup Assistant or via DHCP tag the tool will retrieve the value.

✓ The command line tool `/sbin/rmagent-register` provides also a possibility to set the structure tag using the option `-u <TAG>` . This tool is used for some scenarios of automatic registration with custom scripts.

Assignment During Onboarding Using Setup Assistant

The structure tag can be entered during the onboarding of the IGEL OS 12 devices. For details, see Onboarding IGEL OS 12 Devices[99].

DHCP Assignment

To assigning a structure tag via DHCP Server:

Use the appropriate DHCP option, depending on the IGEL OS version of your endpoint devices:

- IGEL OS 11.03.500 or lower: Use DHCP option 226 to distribute the tag value to the devices. Set the DHCP option 226 as a string - not as a DWORD.
- IGEL OS 11.04.100 or higher: As an alternative, you can use the DHCP option 43 (encapsulated vendor-specific options) to send the DHCP option 226 (name: "umsstructuretag") to the right endpoint devices. An endpoint device with IGEL OS 11.04.100 or higher sends option 60 (vendor class identifier) with `igel-dhcp-1` as the 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 226 that has been sent in the global namespace from being interpreted. To achieve this, you must add option 1 (name "exclusive", type Byte, value 1) to DHCP option 43.

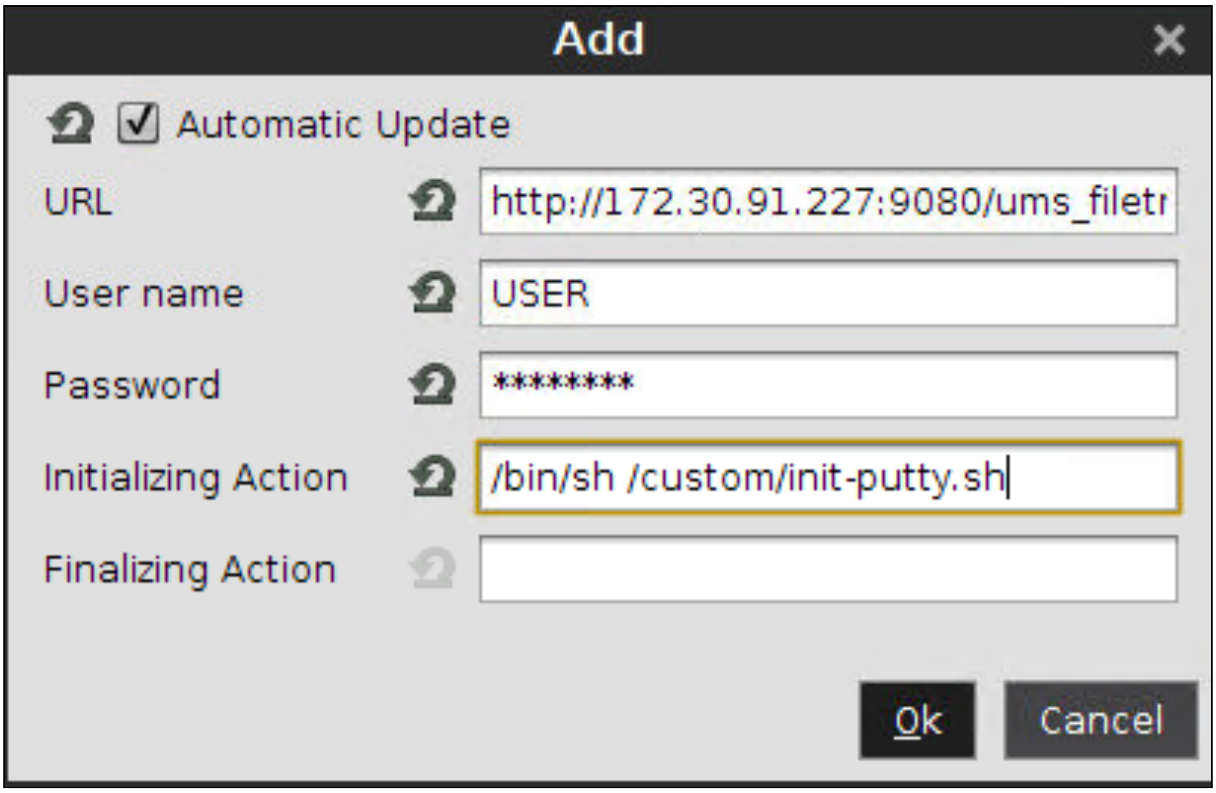
99. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices

How to Deploy an IGEL Custom Partition via UMS

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

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

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



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

IGEL UMS Environment

How to Use Distributed App Repositories in IGEL UMS

Distributed App Repositories can help to securely distribute apps to locations with no internet connection or low bandwith. You can find more information on the benefits, use cases and best practices in the IGEL Blog post https://www.igel.com/blog/the-power-of-a-distributed-app-repository-enabling-access-for-offline-and-low-bandwidth-environments/ .

By enabling and configuring this feature, binaries of apps will be stored on a self-hosted WebDAV server. Devices can then download the binaries of those apps from the WebDAV server, but the metadata will still be downloaded from the UMS Integrated App Repository or the IGEL App Repository.

> The feature is offered as an enterprise feature in the IGEL OS Editions licensing model. For details, see IGEL OS Editions.

Prerequisites

- You have the following UMS permissions :
  - App management; see General Administrator Rights in IGEL UMS (see page 1013)
  - Write access for **UMS Administration > UMS Network > Server**; for details on access rights, see Object-Related Access Rights (see page 1016)
- The devices must run IGEL OS 12.5.0 or higher.
- At least one self-hosted WebDAV server must exist. This server will act as the Distributed App Repository, therefore it needs to fulfill the following requirements:
  - Enough disk space to store binaries
  - A user with write permission to update and add new files
  - A user with read permissions used by the devices to download the app binaries
  - Digest login enabled
  - It is recommended to use a secured connection:
    - The UMS needs a certificate for the Webdav server to be used for file uploads if SSL is used. This certificate is also forwarded to the devices to be used to download the files.
    - To make the certificate visible, the public key has to be imported into the UMS. Use **Import root certificate** for this. For details, see Web Certificates in the IGEL UMS (see page 899) .
    - The certificate must contain Subject Alternative Names (SANs) to be imported into the UMS.

Setup Distributed App Repositories in UMS

After enabling the feature manually, you can perform the following steps to set up one or multiple repositories in UMS Web App:

1. Navigate to the **Apps** area.
2. Open **Settings**.
3. If not yet done, enable **UMS as update proxy**. For more information, see Configuring Global Settings for the Update of IGEL OS Apps (see page 1342).

You can also use the app repository without the UMS as an update proxy. In this case, the repository gets the binaries directly from the IGEL App Portal.

4. On the same tab, open **Manage Binary App Repositories**.
5. By clicking **+** you can add a new repository with the following parameters:
    - **Name**
      Name of the repository to add.
    - **WebDAV URL**
      URL of an existing WebDAV server. This URL is used by the UMS to upload binaries. If no **Load Balancer URL** is given, devices will use it to download the binaries.
    - **Load Balancer URL**
      URL of the load balancer, if the WebDAV server is balanced by one. Devices will use it to download the binaries.
    - **Download User**
      Username that is used to download binaries from the WebDAV server.
    - **Download User Password**
      Password that is used to download binaries from the WebDAV server.
    - **Upload User**
      Username that is used to upload binaries from the WebDAV server.
    - **Upload User Password**
      Password that is used to upload binaries from the WebDAV server.
    - **Priority**
      Priority that this repository will be handled by. See more details on priority explanation below.
    - **Certificate path**
      File path to the SSL certificate that is used for the HTTPS connection, if the certificate is not handled by UMS administration.
      It is recommended to manage the certificate by UMS administration and import the web certificate through the UMS Console under **UMS Administration > Global Configuration > Certificate Management > Web**. For more information, see Web Certificates in the IGEL UMS (see page 899).

App Upload to Repository

Apps are automatically sent to the configured repository within minutes after the app import into UMS. Apps normally cached by the UMS update proxy are uploaded to the distributed app repositories. If UMS is not set as the update proxy, all apps imported to the UMS Web App are also uploaded to the distributed repositories.
Once an app is cached in the repository, synchronization to the repository is performed at regular intervals. The interval is the same as defined under **Apps > Settings > Automatic Updates** (see page 1342).
For details on importing apps, see How to Import IGEL OS Apps from the IGEL App Portal (see page 1303).

Assign Priorities to Distributed App Repositories

> Be aware that the available repository with the highest priority value will be used by the devices to download binaries. If none is available, download will fall back to the UMS Integrated App Repository or the IGEL App Repository.

It is possible to assign a negative value to a repository. In that case binaries will be synchronized to that server, but devices won't download from them. However, those repositories can be then configured via profiles for some devices with another higher priority.

Example:

1. Set up a Distributed App Repository named "Local Download" with priority "-1".
2. Create a profile named "Local Download" for the base system.
3. Under **System > Update** add the repository with priority "300".
4. Assign the profile to the devices that should download from that repository.

Hints for WebDAV servers

Apache HTTP with WebDAV

The password for the WebDAV users should be created with the command ‘htdigest’ to work properly.

Windows Server IIS with Webdav

Make sure the following features are installed:

- WebDAV publishing
- Digest Authentication

When setting up virtual directories, ensure that:

- The WebDAV users must have access
- Digest Authentication must be enabled
- Directory Browsing must be enabled

As the uploaded files could contain + signs, the IIS WebDAV must be configured to accept them. Add the following to ‘web.config’ of your web site:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <directoryBrowse enabled="true" />
        <security>
            <requestFiltering allowDoubleEscaping="true" />
        </security>
    </system.webServer>
</configuration>
```

How to Migrate a UMS Server

If you want to migrate your IGEL Universal Management Suite (UMS) to a new server, here you find the instructions, recommendations and tips about the migration process.

During the migration, there will be no negative impact on your endpoint devices – they will continue to work autonomously. Exception: login via Shared Workplace (SWP) (see page 1427). For details, see Which Features of IGEL OS Will Be Affected If the UMS Is Down?[100]

Before You Begin the Migration

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

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

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

Instructions for Migration Scenarios

You can find detailed instructions for the following migration scenarios:

- Migrating the UMS server and keeping the same embedded data source: Migrate a UMS Server with the Same Embedded Database (see page 432).
- Migrating the UMS server and keeping the same the external data source: Migrate a UMS Server with the Same External Database (see page 437).
- Migrating the UMS and changing the data source: Migrate a UMS Server with a Different Database (see page 441).

Known issue when migrating to an Oracle Database

It is not possible to migrate from a non-Oracle Database to an Oracle Database via RMAdmin. The initial use of an Oracle Database is possible and is supported. It is also possible to update an Oracle Database to a higher version.

Recommendations

- Keep the migration and the update procedures separate. If you want to move from UMS 12.01 to 12.03, first update the UMS and migrate the server afterward, or vice versa.

100. https://kb.igel.com/en/igel-os/11.10.270/which-features-of-igel-os-will-be-affected-if-the-

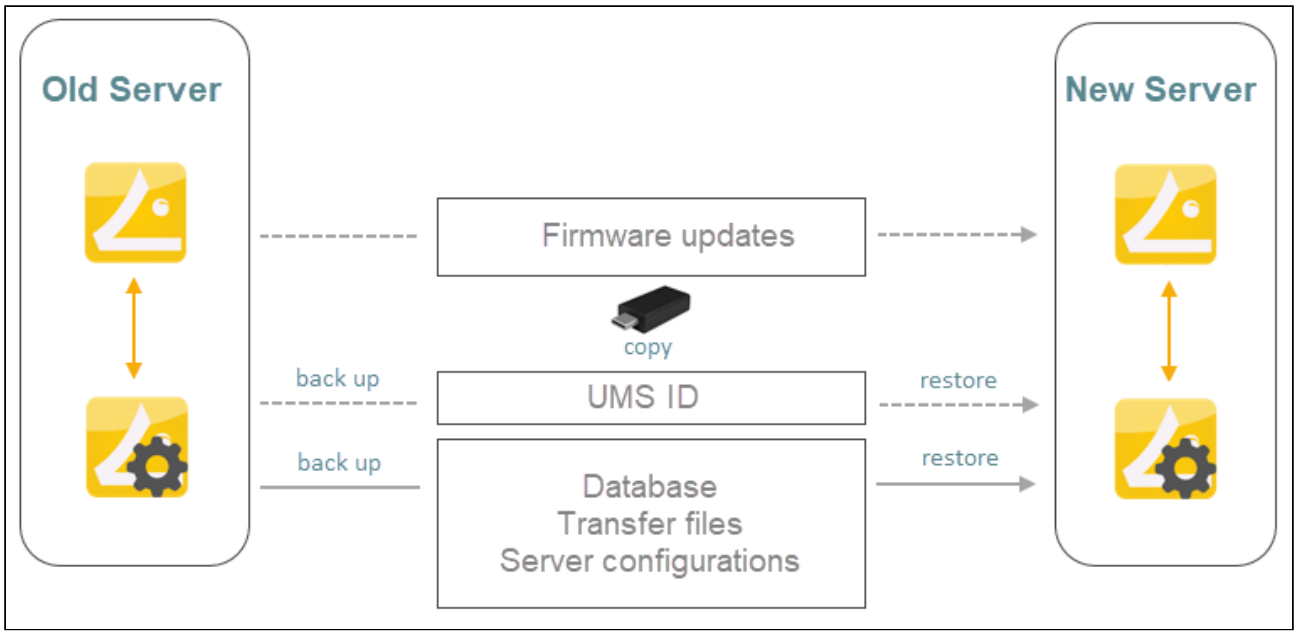
- Use the same UMS ID.
  The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.
- Use the same certificate chain.
  If it must be changed, use the old chain for migration and change it after the migration successfully worked or change it before migrating.

Migrate a UMS Server with the Same Embedded Database

Use Case

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

General Overview of the Migration Procedure



The migration procedure generally involves the following steps:

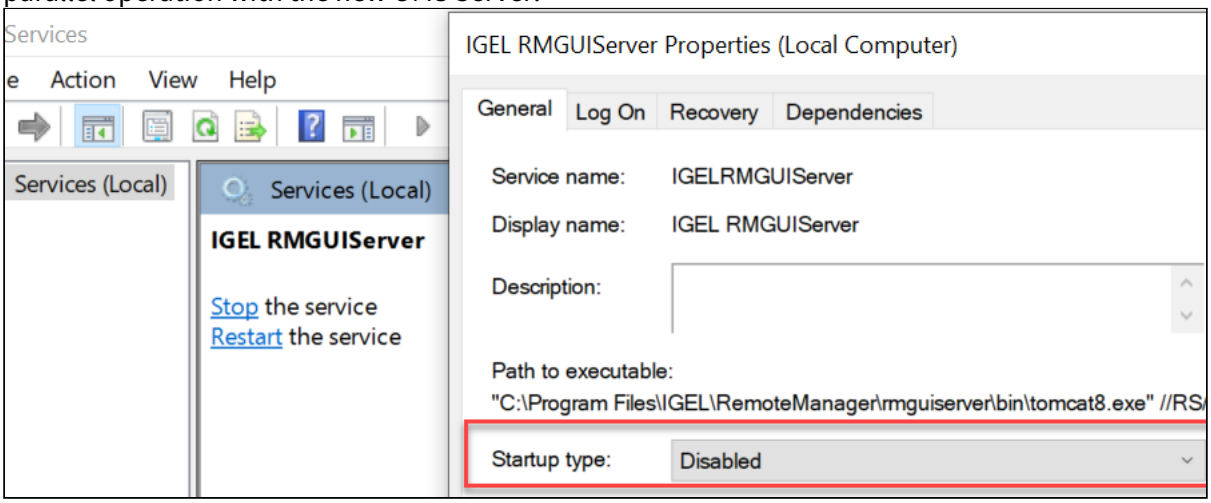
1. Setting the IP address of the new server through profiles (only necessary, if devices find the UMS via IP)
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Backing up the old server. Checklist for the backups:
   - **Database**
   - **Transfer files**
   - **Server configurations** (host-specific server configurations that differ from the defaults are noted down separately)
   - **Firmware updates**
   - **UMS ID**
4. Transferring the created backups to the new server
5. Uploading OS 12 Apps to the new server
6. Adjusting DHCP tag and DNS alias on the new server (only necessary, if devices find the UMS via DNS/DHCP)

Instructions

On the Old Server

1. If the devices find the UMS via the IP address, they can only connect to the new server if the IP address of the new server is set before the migration. To set the IP address:
   a. Create an OS 11 and an OS 12 profile with the new UMS server IP. The new server needs to get listed under **System > Remote Management**. For more information, see Remote Management in OS 12[101] and Remote Management in IGEL OS 11[102].
   b. Assign the profiles.
   c. Check that all devices got their settings by creating a view with the **Last Boot Time** criterion under **Views**. For more information, see How to Create a New View in the IGEL UMS (see page 820).

2. Stop the service `IGEL RMGUIServer` (for instructions, see IGEL UMS HA Services and Processes (see page 1425)) and set the startup type for it to **Disabled** in order to prevent accidental parallel operation with the new UMS Server.



3. Create a backup under **UMS Administrator > Backups** and copy it to a storage medium. Include all options in the backup. For detailed instructions, see the "Embedded Database" section under Creating a Backup of the IGEL UMS (see page 1051).

101. https://kb.igel.com/en/igel-os-base-system/current/remote-management-in-igel-os-12
102. https://kb.igel.com/en/igel-os/11.10.270/remote-management-in-igel-os-11

The backup of **Server configurations** includes most configurations of the **Settings** (see page 1038) 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.

4. Create a backup of the UMS ID in the **UMS Administrator > UMS ID Backup**. For detailed instructions, see Transferring or Registering the UMS ID (see page 442).

5. Create a backup of all the files in the following folder. (You will need to restore them on the new server.)

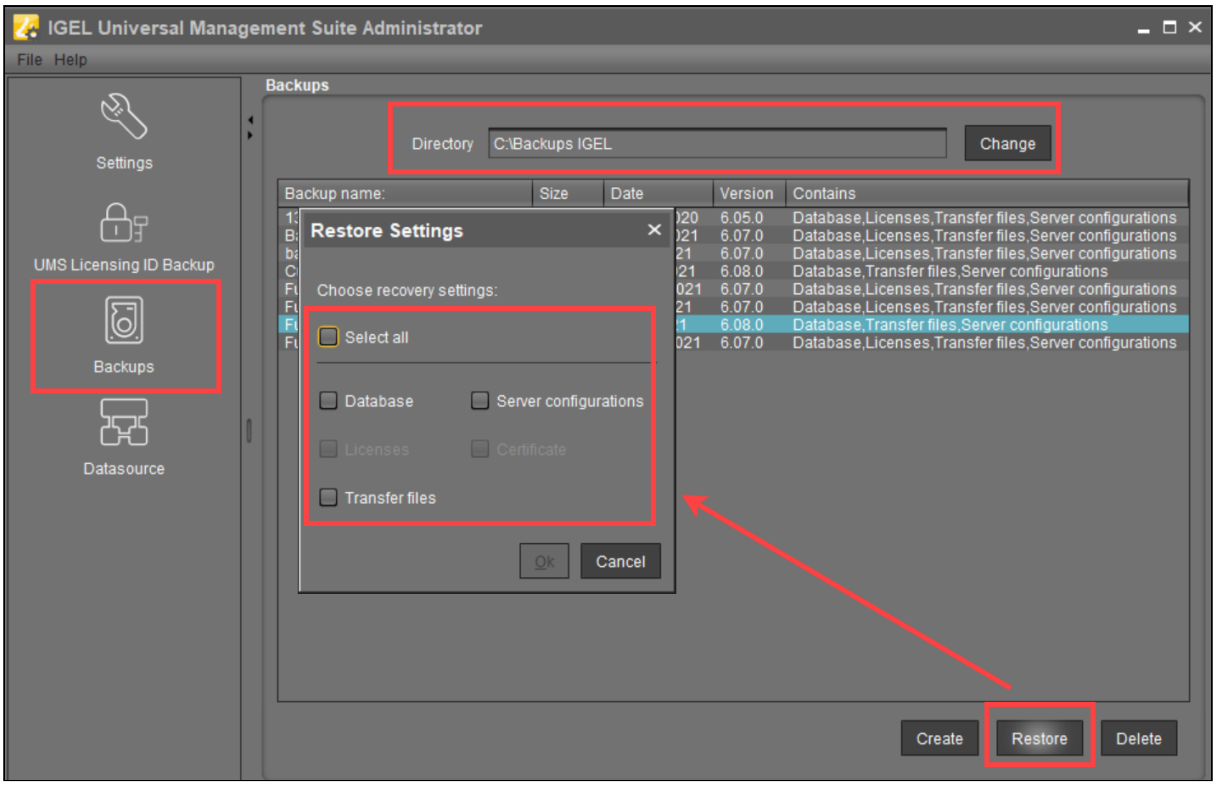
```
[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer
```

6. In the UMS Console, go to **UMS Administration > UMS Network > Server** and note the process ID of the server.

On the New Server

1. Install the UMS on the new server. If possible, use the same database user and password. For the installation instructions, see IGEL UMS Installation (see page 13).

2. Under **UMS Administrator** > **Backups**, select the folder with your backup and restore the respective backup file with all options. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.



3. Transfer the UMS ID of the previous UMS installation to the new server: **UMS Administrator > UMS ID Backup > Restore**. Alternatively, you can register the new UMS ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS ID (see page 442).

⚠ It is recommended to use the same UMS ID. The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.

4. If necessary, transfer host-specific server configurations to the new server.

5. Restore the files to the folder, keeping the folder structure of the old server:

```
[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer
```

6. Upload the app packages for OS 12 devices that were manually uploaded in the old UMS.

ℹ This step is only needed if apps are manually uploaded into the UMS for distribution (for example, in air-gapped scenarios).

If the UMS is connected to the IGEL App Portal and the app binaries were not manually uploaded to the UMS, then the new UMS Server automatically downloads the apps from the IGEL App Portal into the UMS update proxy cache.

7. If the ICG is used: Connect the existing ICGs as described under How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database (see page 457).

8. Restart the service `IGEL RMGUIServer`. If the devices find the UMS via the IP address, they should connect automatically.

9. If the devices find the UMS via DNS/DHCP:
   a. Adjust the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS (see page 1151).
   b. Assign the new server to the old server certificate or create and assign a new certificate with the FQDN of the new server. For more information, see How to Use Your Own Certificates for Communication over the Web Port (Default: 8443) in IGEL UMS[103].

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

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

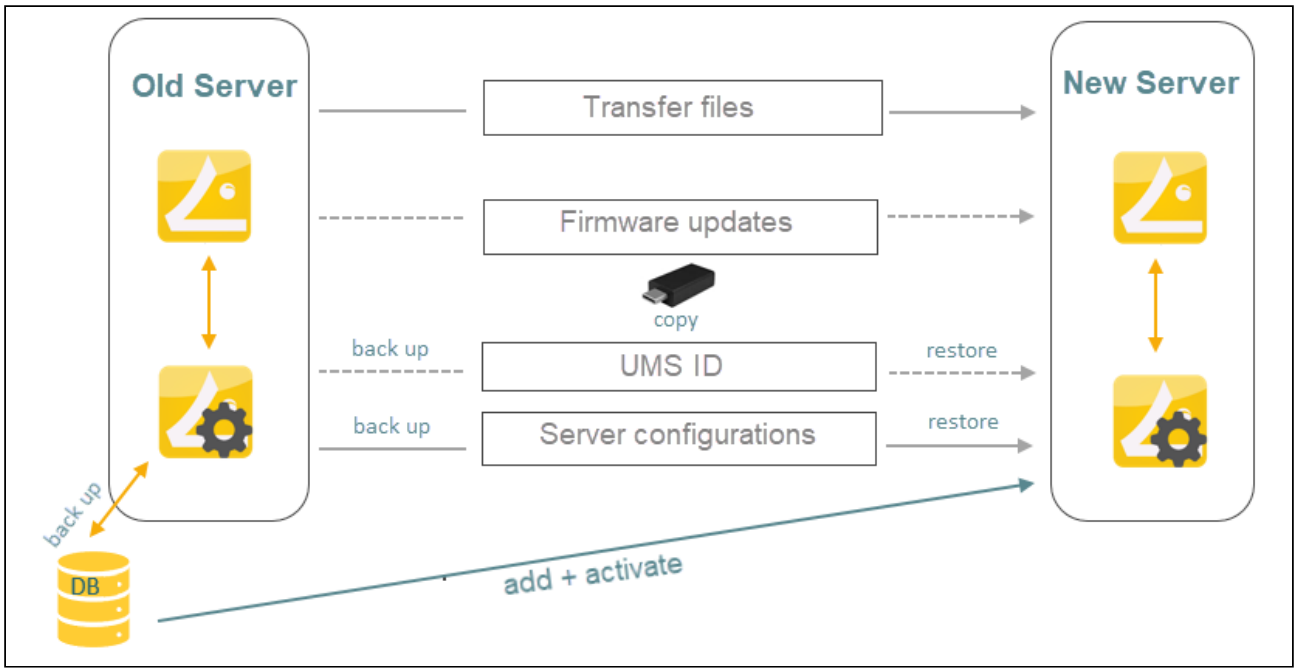
103. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication

Migrate a UMS Server with the Same External Database

Use Case

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

General Overview of the Migration Procedure



The migration procedure generally involves the following steps:

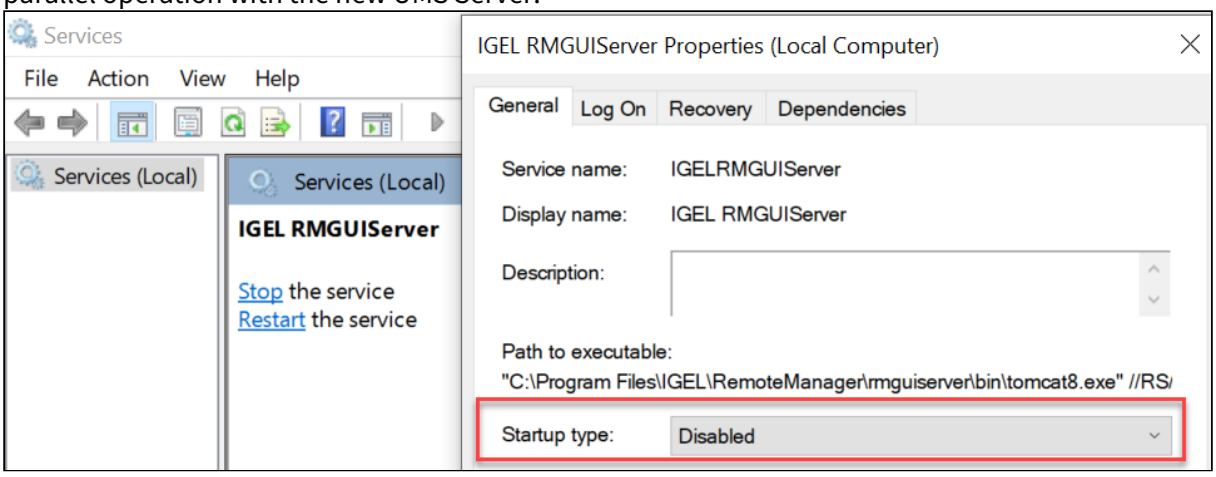
1. Setting the IP address of the new server through profiles (only necessary, if devices find the UMS via IP)
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Backing up the old server. Checklist for the backups:
   - **Database**
   - **Transfer files**
   - **Firmware updates**
   - **Server configurations** (host-specific server configurations (see page 1051) that differ from the defaults are noted down separately)
   - **UMS ID** (see Transferring or Registering the UMS ID (see page 442))
4. Adding the existing external database as the data source for the new server
5. Activating the data source
6. Transferring the backed-up data to the new server
7. Uploading OS 12 apps to the new server

8. Adjusting DHCP tag and DNS alias on the new server (only necessary, if devices find the UMS via DNS/DHCP)

Instructions

On the Old Server

1. If the devices find the UMS via the IP address, they can only connect to the new server if the IP address of the new server is set before the migration. To set the IP address:
   a. Create an OS 11 and an OS 12 profile with the new UMS server IP. The new server needs to get listed under **System > Remote Management**. For more information, see (12.4-en) Remote Management in IGEL OS 12 and (11.10-en) Remote Management in IGEL OS 11 .
   b. Assign the profiles.
   c. Check that all devices got their settings by creating a view with the **Last Boot Time** criterion under **Views**. For more information, see How to Create a New View in the IGEL UMS (see page 820).
2. Stop the service `IGEL RMGUIServer` (for instructions, see IGEL UMS HA Services and Processes (see page 1425)) and set the startup type for it to **Disabled** in order to prevent accidental parallel operation with the new UMS Server.



3. Before the migration, make the backups as described in the "External Database" section under Creating a Backup (see page 1051).
4. Note the values of host-specific server settings (Web server port, JWS server port, and ciphers).
5. Create a backup of the UMS ID in the **UMS Administrator > UMS ID Backup**. For detailed instructions, see Transferring or Registering the UMS ID (see page 442) .
6. Create a backup of all the files in the following folder. (You will need to restore them on the new server.)

`[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

7. In the UMS Console, go to **UMS Administration > UMS Network > Server** and note the process ID of the server.

On the New Server

1. Install the UMS on the new server. For the installation instructions, see IGEL UMS Installation (see page 13).
2. Go to **UMS Administrator > Datasource > Add** and enter the connection properties of the existing database.
3. **Activate** the data source. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.
4. In the **UMS Administrator > Backups**, restore the backup of server configurations. If necessary, transfer host-specific server configurations (see page 1051) to the new server.
5. Transfer the UMS ID of the previous UMS installation to the new server: **UMS Administrator > UMS ID Backup > Restore**. Alternatively, you can register the new UMS ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS ID (see page 442) .

⚠ It is recommended to use the same UMS ID. The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.

6. Restore the files to the folder keeping the folder structure of the old server:

`[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

7. Upload the app packages for OS 12 devices that were manually uploaded in the old UMS.

ℹ This step is only needed if you are using a Standalone UMS and apps are manually uploaded into the UMS for distribution (for example, in air-gapped scenarios).
If the UMS is not Standalone, the servers can sync with each other during migration and share the binaries automatically.
If the UMS is connected to the IGEL App Portal and the app binaries were not manually uploaded to the UMS, the new UMS Server automatically downloads the apps from the IGEL App Portal into the UMS update proxy cache.

8. If the ICG is used: Connect the existing ICGs as described under How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database (see page 457).
9. Restart the service `IGEL RMGUIServer`. If the devices find the UMS via the IP address, they should connect automatically.
10. If the devices find the UMS via DNS/DHCP:
    a. Adjust the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS (see page 1151).

b. Assign the new server to the old server certificate or create and assign a new certificate with the FQDN of the new server. For more information, see How to Use Your Own Certificates for Communication over the Web Port (Default 8443) in IGEL UMS[104] .

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

10. For HA installations only: Update the host assignment for job execution. For the instructions, see Updating Host Assignment for Job Execution (see page 444).

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

104. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication

Migrate a UMS Server with a Different Database

If you want to migrate to a new Universal Management Suite (UMS) server and at the same time transfer your data to a different database, you can find the instructions here.

Data Transfer

Before the migration, you need to transfer the UMS data to the new database using the **Copy** functions of the UMS Administrator as described in Copying a Data Source (see page 1065).

Migration

After the transfer of data, you can begin the migration procedure based on the database:

- If the new data source is an embedded database, follow the instructions in Migrate a UMS Server with the Same Embedded Database (see page 432) .
- If the new data source is an external database, follow the instructions in Migrate a UMS Server with the Same External Database (see page 437) .

Transferring or Registering the UMS ID

There are two different ways to handle the UMS ID (see page 964) if you migrate the UMS Server:

- Transferring the UMS ID (see page 442) (recommended)
  With this method, you make a backup of the old UMS ID and take it with you. The UMS ID, which is automatically created during the installation of the new UMS Server, is overwritten.
  Advantage: You do not have to reassign the license packages in the IGEL License Portal (ILP) and to re-register your UMS.
- Registering a New UMS ID (see page 443)
  With this method, you do not create a backup of the current UMS ID. A new UMS ID is created for the new UMS server.
  Advantage: You do not need to know the UMS ID of the old server.
  Disadvantage: You have to register the UMS ID of the new server in the IGEL License Portal (ILP). To authenticate your UMS to the IGEL Cloud Services, you also have to re-register your UMS in the IGEL Customer Portal using the new UMS ID.

Transferring the UMS ID

On the Old Server: Create a Backup of the UMS ID

1. Open the UMS Administrator on your old server.

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

2. Go to **UMS ID Backup** and create a backup as described under UMS ID Backup in the IGEL Administrator (see page 1043).
3. In your file explorer, go to the folder where you saved the UMS ID backup.
4. Copy the backup (e.g. `UMS ID_backup before migration.ksbak`) to a directory of your new UMS Server environment.

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

1. Open the **UMS Administrator** on the new server.
2. Go to **UMS ID Backup** and restore the backup as described under UMS ID Backup in the IGEL Administrator (see page 1043).
   The UMS ID is now connected to the new UMS server.

Registering a New UMS ID

When you migrate without creating a backup of your UMS ID, a new UMS ID is generated for the new UMS server. This new UMS ID must be registered in the ILP and in the IGEL Customer Portal.

Registering in the ILP

For details, see How to Register the UMS ID in ILP[105].

Registering in the IGEL Customer Portal

For details, see Registering the UMS in the IGEL Customer Portal[106].

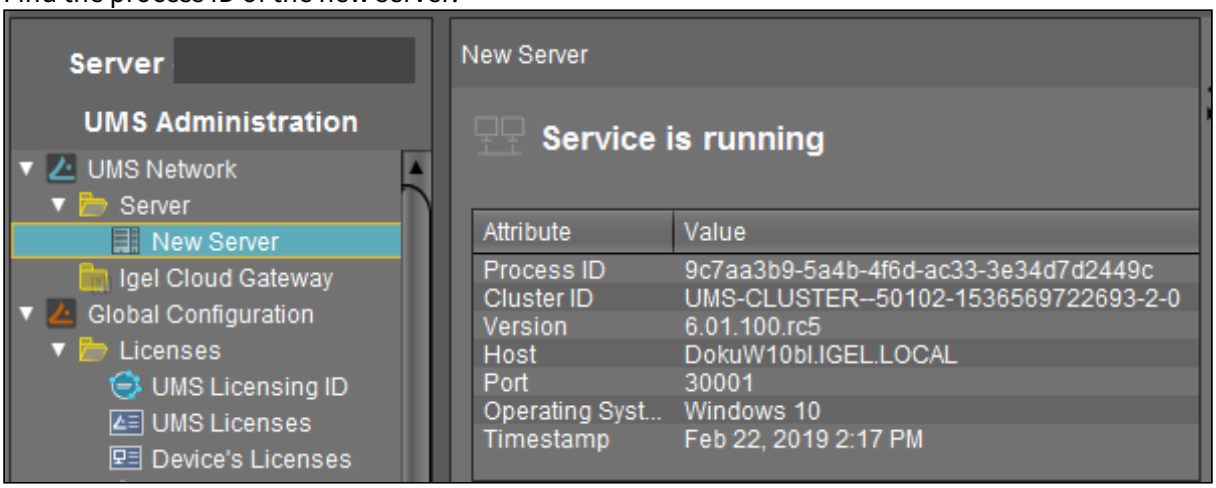
105. https://kb.igel.com/en/igel-subscription-and-more/current/how-to-register-the-ums-id-in-ilp
106. https://kb.igel.com/en/how-to-start-with-igel/current/registering-the-ums

How to Update Host Assignment for Job Execution

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

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

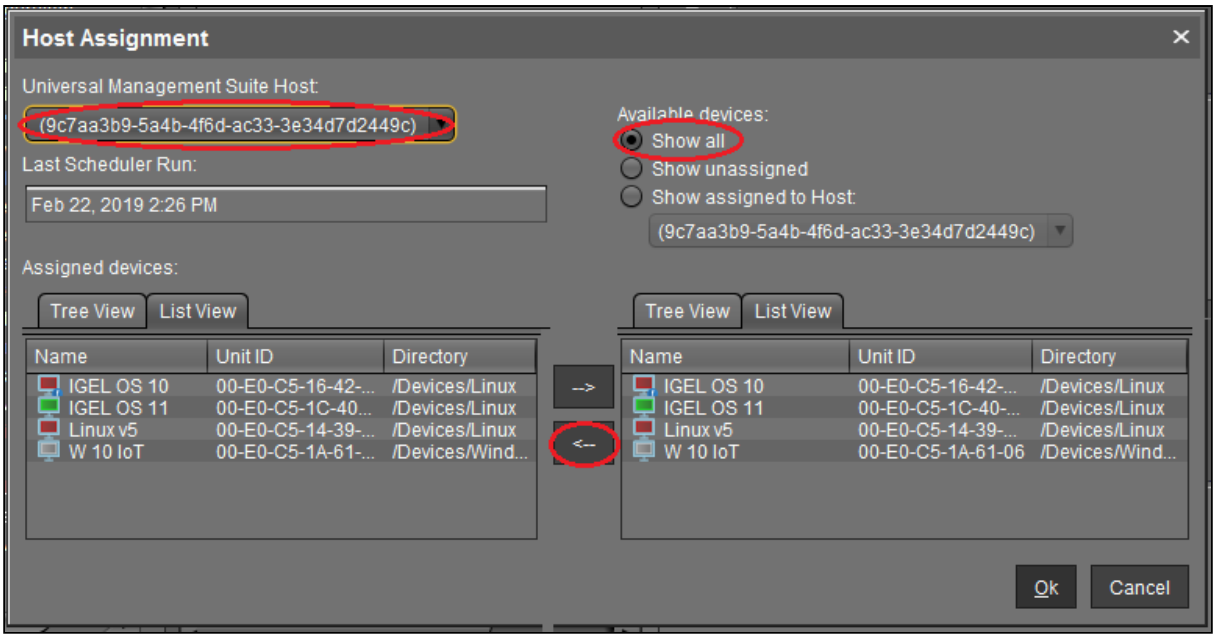
1. In the UMS Console, go to **UMS Administration > UMS Network > Server >** [new server].
2. Find the process ID of the new server.



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

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

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


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

How to Migrate a UMS Database From Embedded DB to Microsoft SQL Server

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

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

IGEL Demos Channel

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

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

Setting Up the SQL Database

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

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

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

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

For detailed instructions, see:

- Microsoft SQL Server/Cluster with Native SQL Authentication (see page 66)
- Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84)
- Microsoft SQL Server/Cluster with Active Directory (AD) Authentication via Kerberos (see page 103)

Copying the Database Contents

1. Start IGEL Universal Management Suite Administrator.

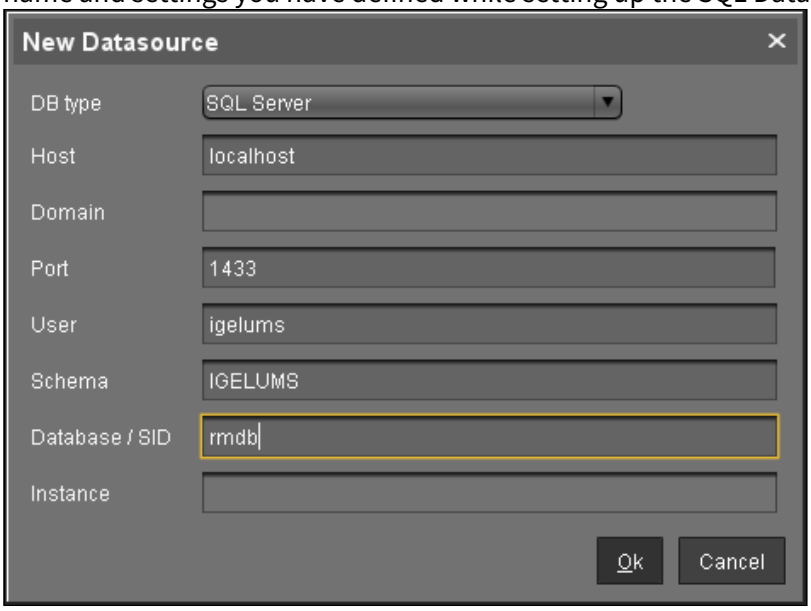
Default path to the UMS Administrator:

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

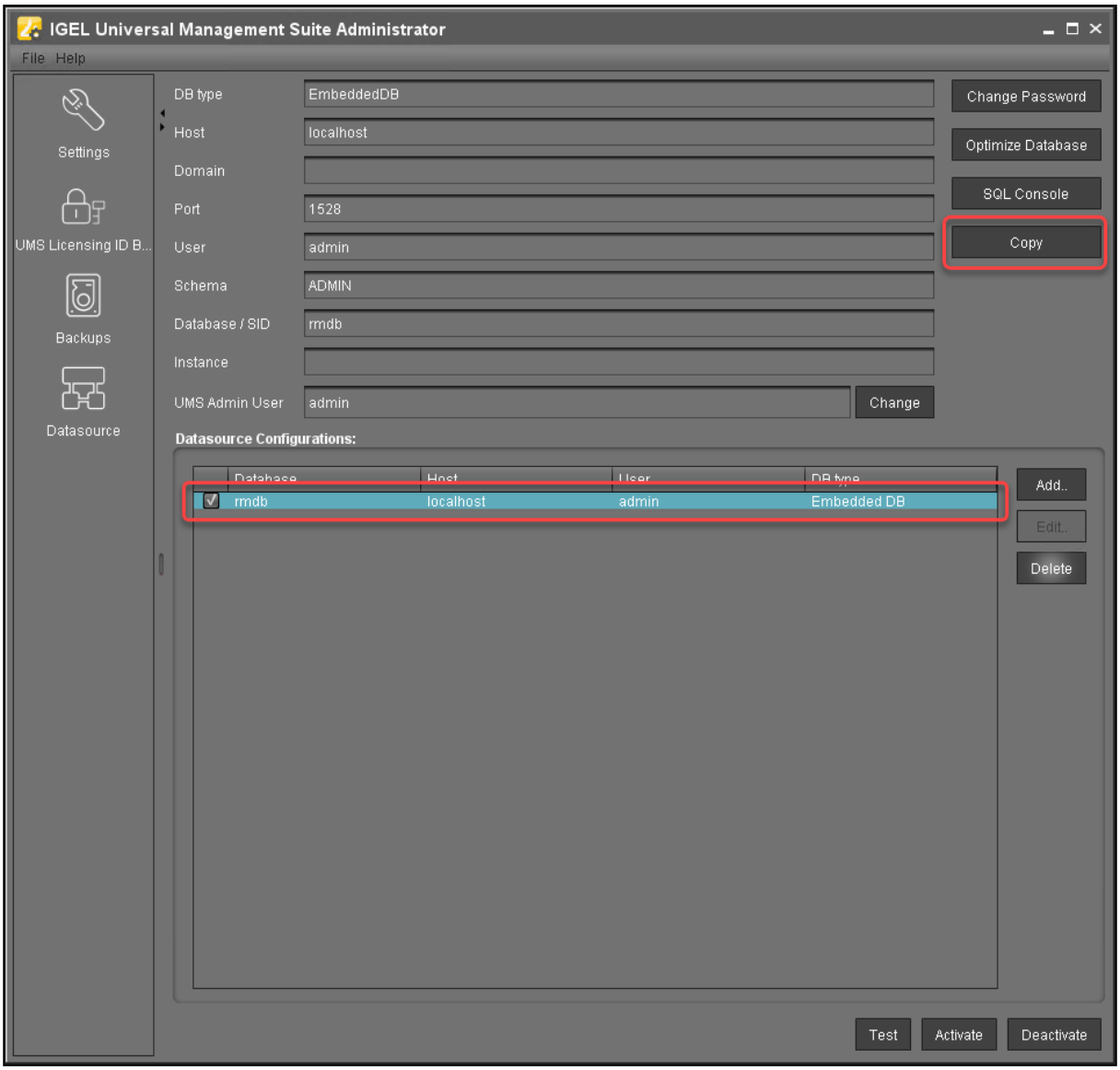
Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

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

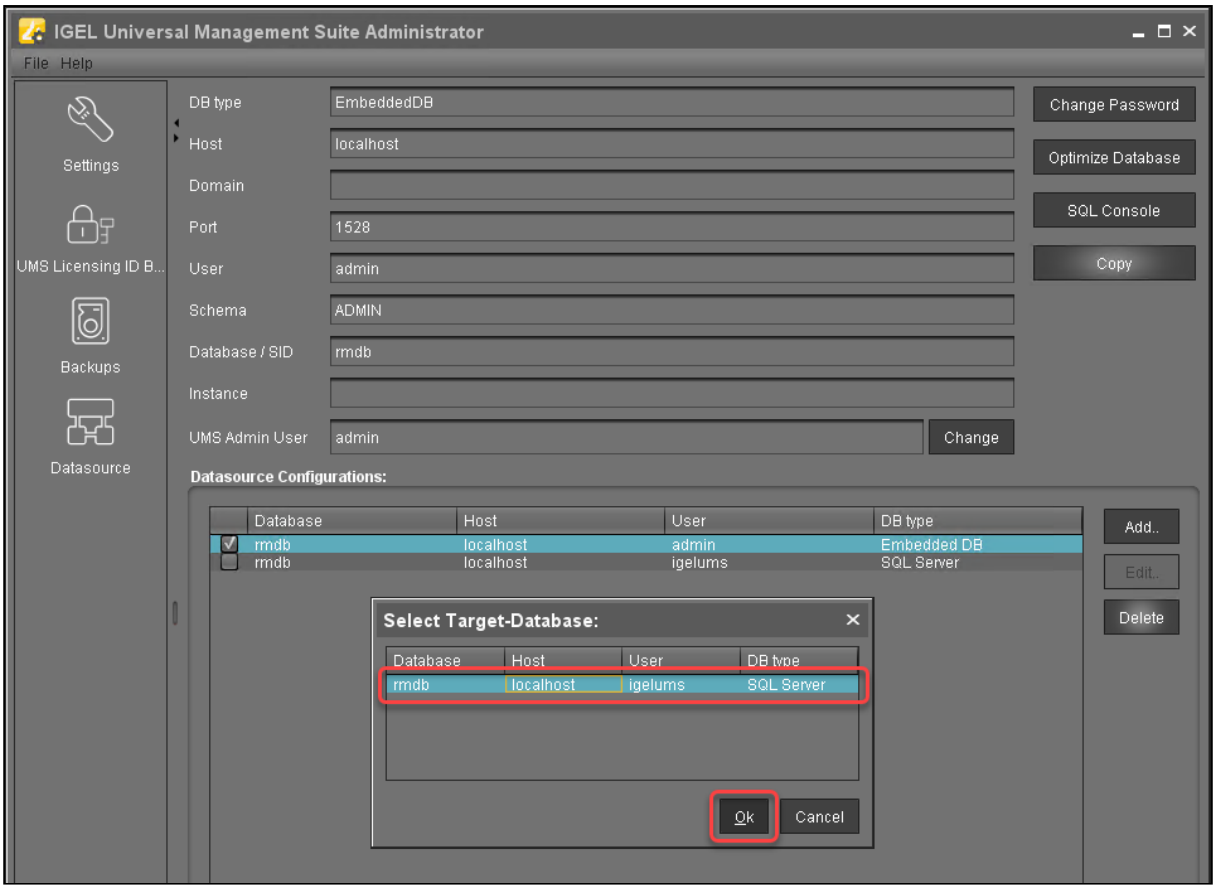
2. Go to **Datasource > Add...** to create a new SQL Server data source; use exactly the same database name and settings you have defined while setting up the SQL Database.



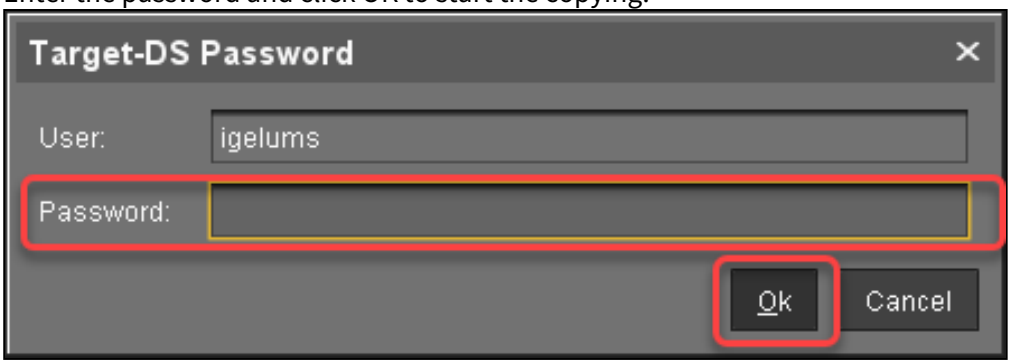
3. Select the **Embedded DB** entry and click **Copy.**



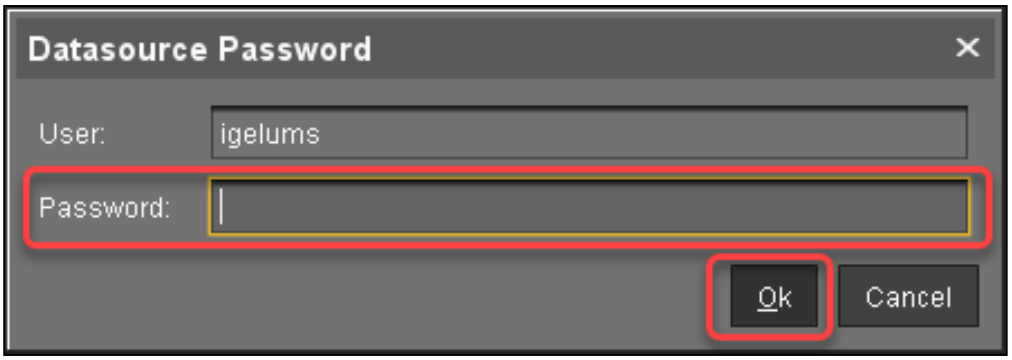
4. Select the newly created SQL Server entry as the target and click **OK.**



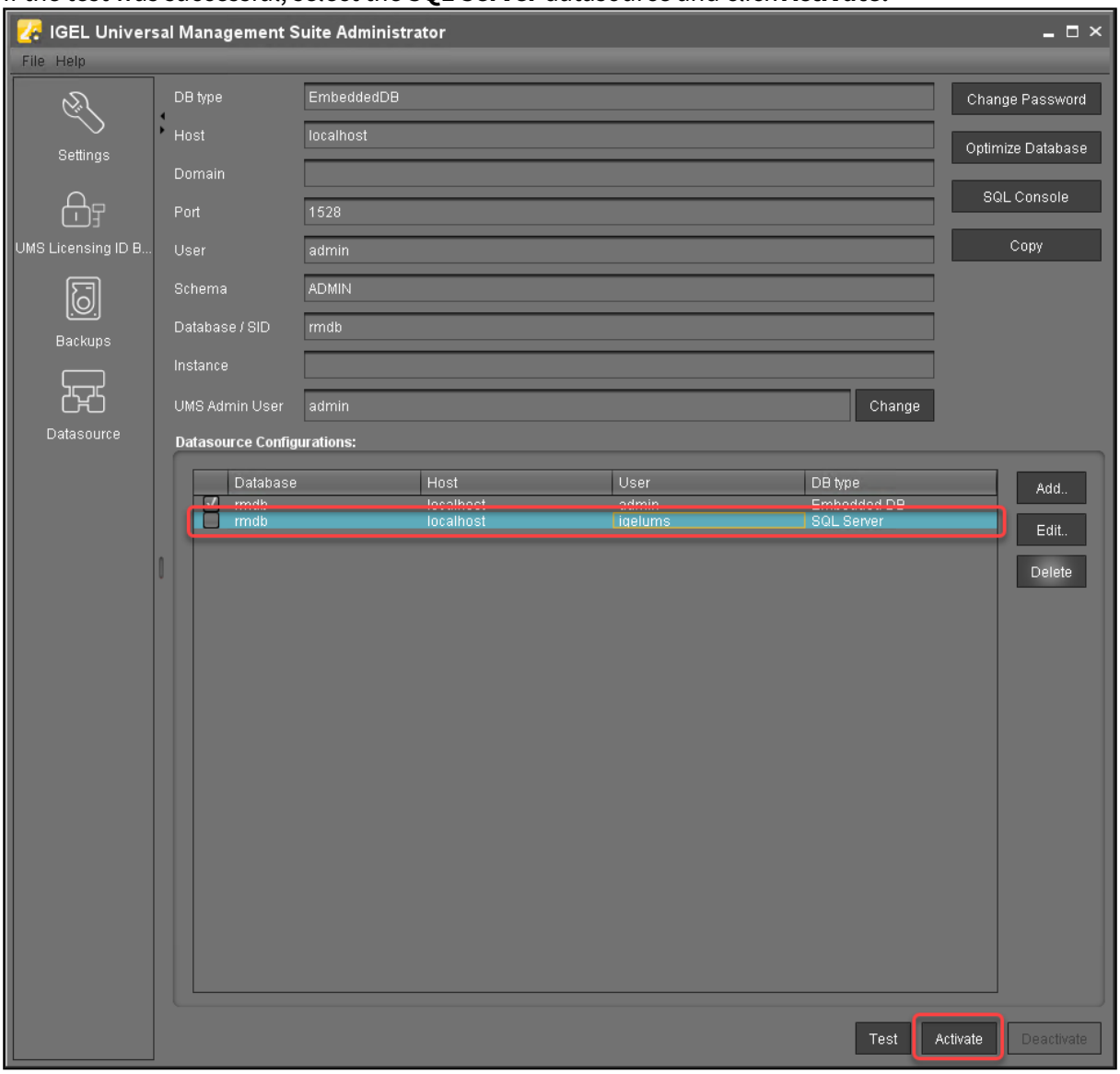
5. Enter the password and click OK to start the copying.



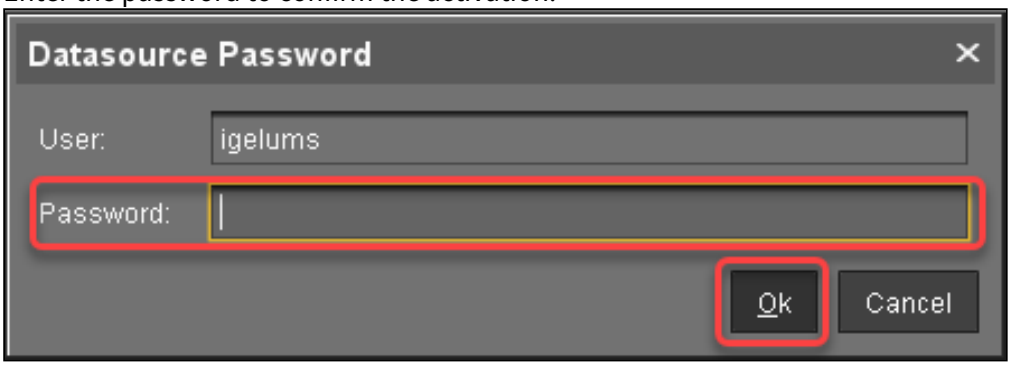
6. When the copying has completed, test the database connection by clicking Test and entering the password.



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



8. Enter the password to confirm the activation.



Now the Microsoft SQL Server is set up as the datasource. From now on, back up the SQL Server in order to back up UMS data.
The same way you can go back to the embedded database, if you need.

How to Restore and Recover a Corrupted UMS Embedded DB

Environment

- UMS 6 on Windows or Linux

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

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

Restoring a Database Backup Made with the UMS Administrator

If a backup of the embedded database is available (see Creating a Backup of the IGEL UMS (see page 1051)), just restore the backup, see Restoring a Backup (see page 1056).

Restoring a File-Based Backup

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

To restore the backup, perform the following steps:

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

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

2. In the **Datasource** area, delete the corrupted Derby DB.
3. Create a new embedded DB with exactly the same user name and password as you used for the deleted DB.
4. Deactivate the newly created DB.
5. Stop the UMS Server service. For details on how you can stop it, see IGEL UMS HA Services and Processes (see page 1425).
6. Erase all files contained in the folder at `RMDB_PATH` .
7. Copy your previously backed-up files to `RMDB_PATH` .
8. Activate the DB with the UMS Administrator under **Datasource**.

9. Wait 1 - 2 minutes, then log in to the UMS Console.

Disaster Recovery: UMS with an External Database

The following instructions require a proper backup of your environment, see the "External Database" section under Creating a Backup of the IGEL UMS (see page 1051) .

Execution Order in Case of the Disaster Recovery

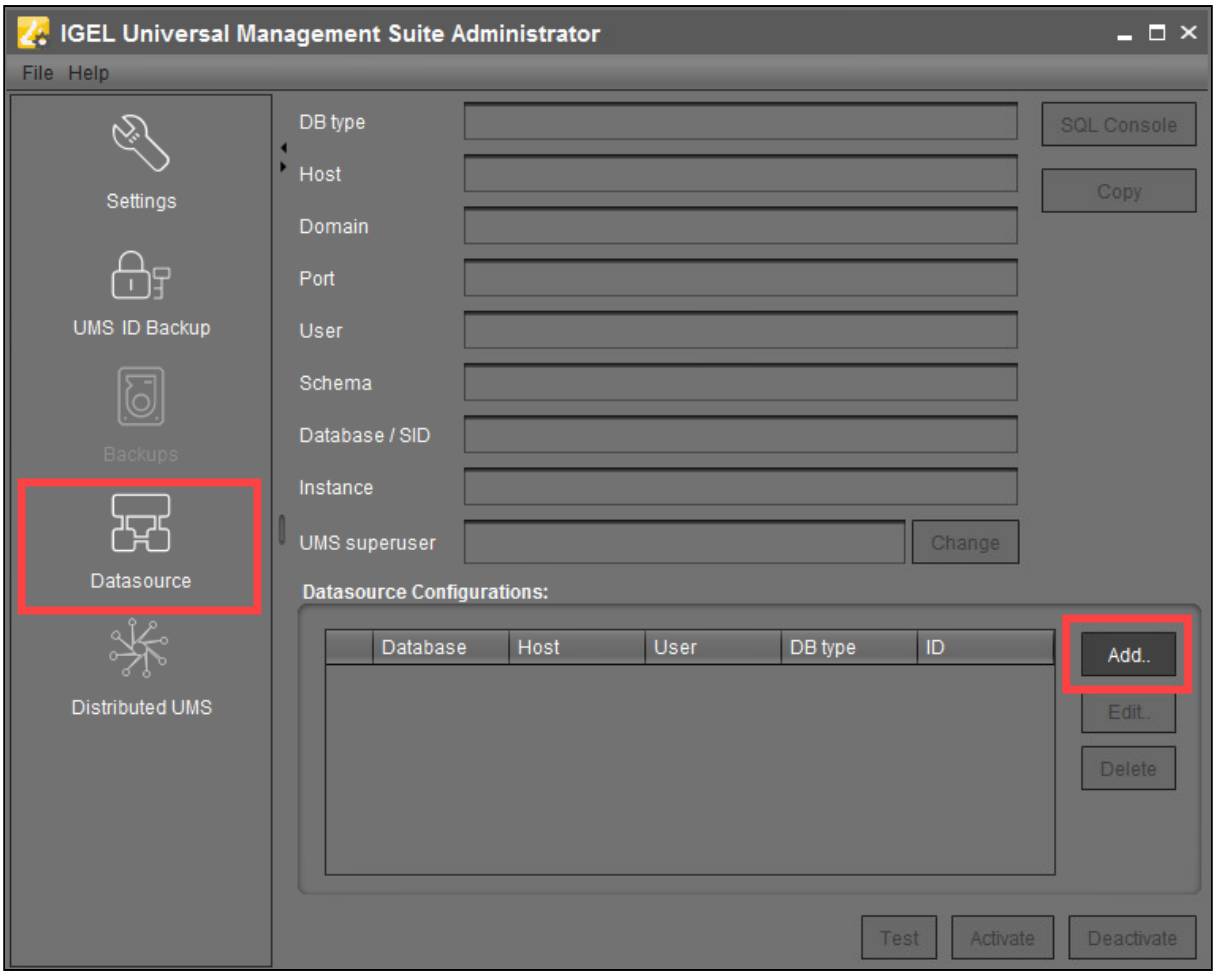
1. Install the UMS on the server, see IGEL UMS Installation (see page 13). All the UMS components must be installed like before:
    a. The same UMS version
    b. The same network configuration of the host (the same IP addresses, ports)
    c. For High Availability (HA) installations only: During the installation, use the backed-up IGEL network token. See the "Starting the Installation" section under Adding Further Servers to the HA Network (see page 1401).
2. Stop the existing UMS Server(s). For the details on how you can do it, see IGEL UMS HA Services and Processes (see page 1425).
3. Copy all the saved files and firmware updates from

`[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

to the new UMS Server(s) – without the `WEB-INF` folder.

If you deploy the HA environment, see also Which Files Are Automatically Synchronized between the IGEL UMS Servers? (see page 514).

4. Restore the database backup using the procedures recommended by the DBMS manufacturer.
5. Add the database connection to your external database on each UMS Server: **UMS Administrator > Datasource > Add**.



6. Click **Activate** to enable the data source.
   The UMS Server will start automatically after that.
7. In the **UMS Administrator > Backups > Restore**, restore the backup of server configurations on each UMS Server. If necessary, transfer host-specific server configurations (see page 1051) to the new server(s).
8. In the **UMS Administrator > UMS ID Backup > Restore**, restore the backup of the UMS ID.

9. For HA and Distributed UMS installations only: Check host assignments for job execution and, if required, adjust them. See Updating Host Assignment for Job Execution (see page 444).

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

In the case of the HA installations, the same must be done for the load balancers: **UMS Administration > UMS Network > Load Balancer**.

If you have a UMS installation with an embedded database, you may find it useful to read: How to Restore and Recover a Corrupted UMS Embedded DB (see page 452) .

How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database

After you have migrated your UMS Server, or newly installed it with the same database, or restored a database backup on this reinstalled server, the server cannot connect to an already existing IGEL Cloud Gateway (ICG). This happens because the ICG credentials are bound to the old process ID.

There are two possibilities to solve the problem:

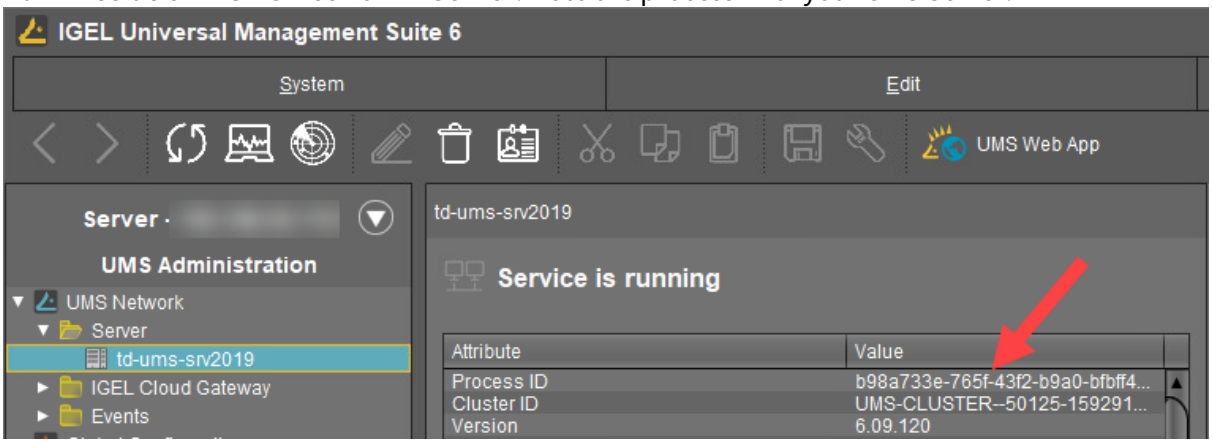
- Keeping the connection to the existing ICG (see page 457): Applicable to UMS version 6.09.100 and higher. With this method, you follow the below instructions exactly in the order given and do NOT restart the UMS Server before performing these steps. Otherwise, you cannot connect to the existing ICG and have to reinstall it.
- ICG reinstallation (see page 458): Applicable to all UMS versions. With this method, you have to uninstall the ICG and then install it again.

With both methods, there will be no negative impact on your endpoint devices – they will continue to work autonomously. Exception: login via Shared Workplace (SWP) (see page 1427).

Keeping the Connection to the Existing ICG

Before UMS 6.09.100, it was always necessary to reinstall the existing ICGs after the migration of the UMS Server or reinstalling the UMS Server with the same database / backup restored. As of UMS 6.09.100, it is possible to keep the connection to the existing ICG. Proceed as follows:

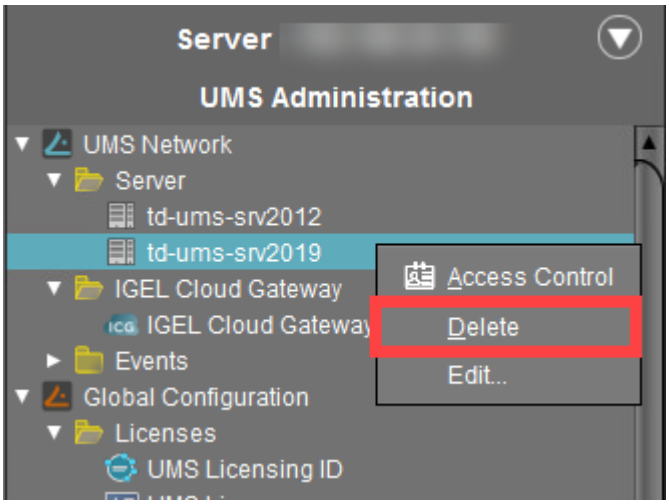
1. On the old server / before the server reinstallation, open the UMS Console and go to **UMS Administration > UMS Network > Server**. Note the process ID of your UMS Server.



2. Install the UMS Server. For how to install the UMS, see IGEL UMS Installation (see page 13) .
3. In the UMS Administrator, restore the backup (see Restoring a Backup (see page 1056)) or, in the case of the external database, connect the existing data source and activate it (see How to Set Up a Data Source in the IGEL UMS Administrator (see page 1073)).
   You will see the entries with the old and the new process ID in the UMS Console under **UMS Administration > UMS Network > Server** and **IGEL Cloud Gateway > [ICG name]**.

4. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway > [ICG name]** and click the **Connect** button.
   If there are several ICGs installed, perform this for each ICG.

5. Go to **UMS Administration > UMS Network > Server** and delete the server with the old process ID.



> After the above steps, you can restart the UMS Server at any time – you will keep the connection to the ICG. If you restart the UMS Server before performing the above steps, you will NOT be able to connect to your existing ICG and will have to reinstall it.

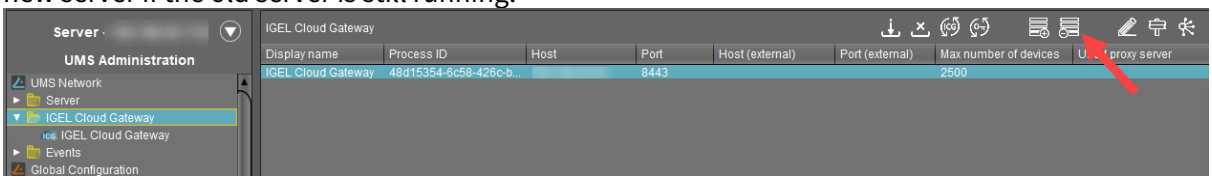
ICG Reinstallation

If you have migrated the UMS Server or reinstalled it with the same database / backup restored and cannot use the above-mentioned method for some reason, you will have to uninstall all the ICGs and install them again.

After you have confirmed that the new / reinstalled UMS Server is running properly, proceed as follows:

1. Log in to the ICG host and uninstall the ICG, see *IGEL Cloud Gateway > ICG How-Tos > How to Uninstall the IGEL Cloud Gateway*.
2. Reboot the ICG server.

3. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway** and click **Remove Gateway from database** button to remove the ICG from the UMS Server.
   In the case of the UMS Server migration, you have to remove the ICG from both the old and the new server if the old server is still running.



4. Install the ICG, and in the case of the UMS Server migration, connect it only to the new UMS Server. See *IGEL Cloud Gateway > ICG Manual >IGEL Cloud Gateway Installation and Setup.*

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

Check preliminarily if ICG updates are available, see IGEL Download Server[107]. It is also recommended to check time and date on all UMS and ICG servers and ports, see IGEL UMS Communication Ports (see page 256).

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

107. https://www.igel.com/software-downloads/enterprise-management-pack/

Troubleshooting: UMS Does Not Connect to ICG: "TrustAnchor ...is not a CA certificate"

Symptom

The UMS fails to connect to the IGEL Cloud Gateway (ICG). The following message appears in the GUI or in the log file:

```
TrustAnchor ...is not a CA certificate
```

```
Caused by: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=UMS-CLUSTER--xxx, O=test, L=test, C=US" is not a CA certificate
at sun.security.validator.PKIXValidator.doValidate(PKIXValidator.java:380)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:273)
at sun.security.validator.Validator.validate(Validator.java:262)
at sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:327)
at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:236)
at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:113)
at de.igel.apps.usg.connection.ssl.TrustedOnlyTrustManager.checkServerTrusted(TrustedOnlyTrustManager.java:74)
at sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:1099)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1622)
... 54 more
```

Environment

- UMS 6.04 or higher

- ICG with older root certificates created with UMS 5.07 or UMS 5.08

Problem

Older ICG root certificates (created with UMS 5.07 or UMS 5.08) do not have the right CA modifier, which was never a problem with previous Java versions. But the Java version used in UMS 6.4.x onwards blocks these certificates.

To check whether you have an old ICG root certificate:

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway** and select your ICG root certificate.
2. Click  to read the certificate content.
   If **Certificate Authority** is set to "false", you have an old ICG root certificate.

Solution

If you do not want to exchange the ICG root certificate (involves installing the ICG anew and re-registering all endpoint devices), you can add a start parameter that tells the UMS Server to ignore the CA flag in the certificate.

> ⚠ This start parameter will be overwritten on each UMS update installation, so you must set it again after the update.

Follow the instructions below, according to your operating system.

For Windows

1. Open the Windows **Services** dialog and stop the service **IGELRMGUIServer**.
2. Navigate to the directory `<UMS installation directory>\RemoteManager\rmguiserver\bin` (example: `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\bin`)
3. Double-click on **editTomcatService**.
4. Confirm the warning dialog.
5. Select the **Java** tab.
6. Under **Java Options**, add the following entry as a new line:
   `-Djdk.security.allowNonCaAnchor=true`
7. Click **Ok** to save the changes.
8. In the Windows **Services** dialog, start the service **IGELRMGUIServer**.

For Linux

1. Stop the service `igelRMserver`
2. Navigate to the directory `/opt/IGEL/RemoteManager/rmguiserver/bin`
3. Open the file `igelRMserver`

4. Find the two entries `-Xmx4096` and add a new line before each entry with the following content: `-Djdk.security.allowNonCaAnchor=true`
5. Save the changes.
6. Start the service `igelRMserver`

How to Use Your Own Certificates for Communication over the Web Port (Default 8443) in IGEL UMS

For all communication that is taking place over the Web Port (default: 8443, see also IGEL UMS Communication Ports (see page 256)), a specific self-signed certificate chain comes with the UMS on installation. Nevertheless, you can use a certificate chain of your own.

See also Web (see page 899) in the UMS Reference Manual (see page 659).

This article describes how to deploy a certificate chain with a corporate CA certificate or a public certificate:

- Deploying a Self-Signed Corporate Certificate Chain (see page 463) (recommended)

  We recommend using a self-signed corporate certificate chain. Of course, a self-signed certificate must be made known to the browsers first, otherwise, the browsers will display warning messages.

- Deploying a Certificate Chain with a Public Root CA (see page 474)

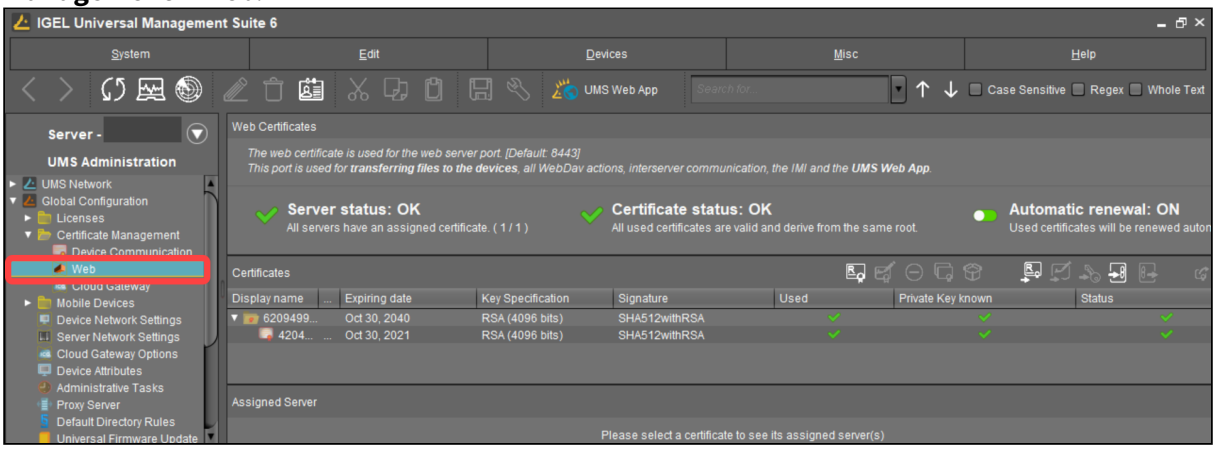
Deploying a Self-Signed Corporate Certificate Chain

Prerequisites

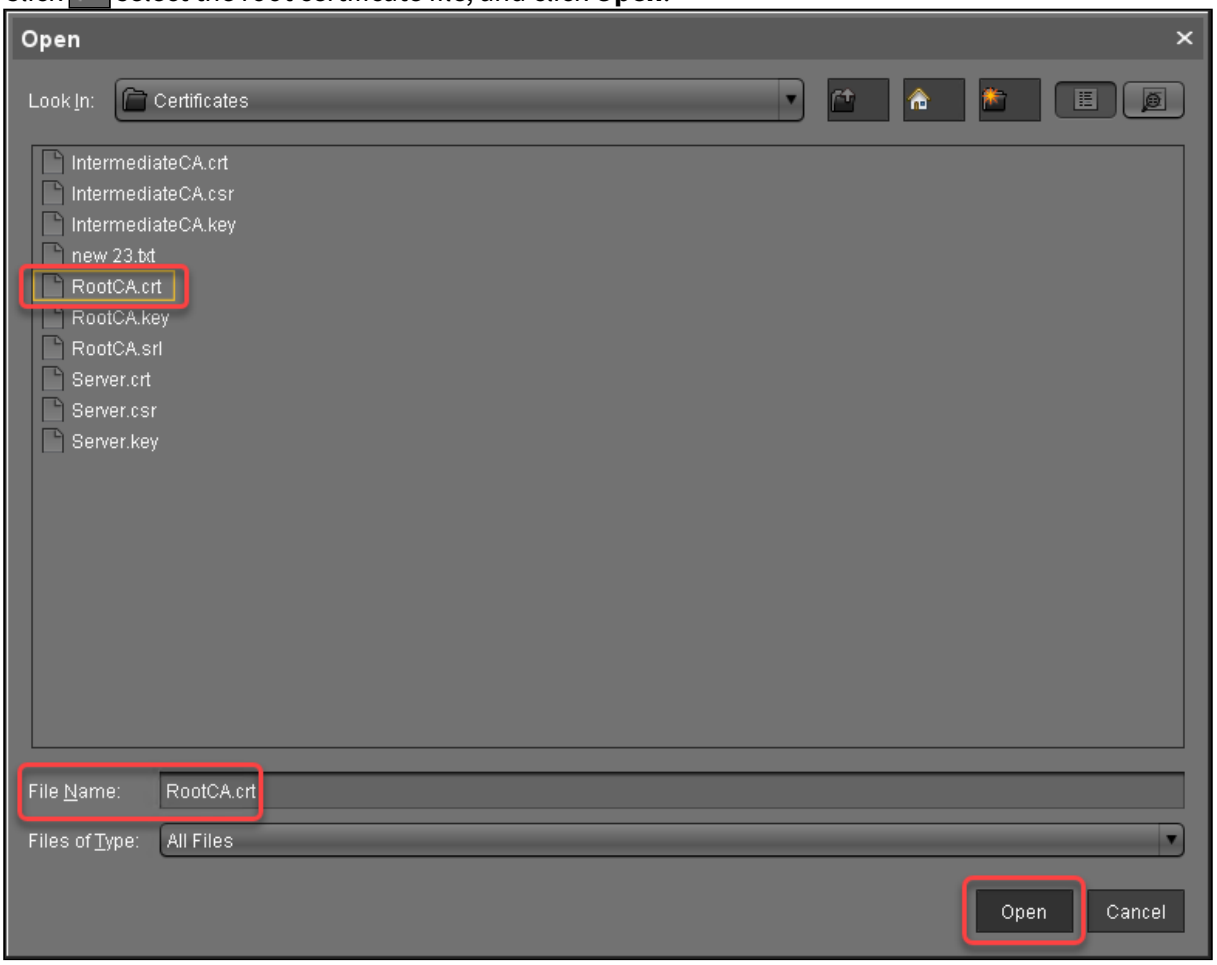
- You have a self-signed root CA certificate that serves as a trusted “root” certificate company-wide.
- Your self-signed root CA certificate has been applied to all relevant trust stores within your company.
- You have an intermediate CA certificate that is signed by your root CA certificate and a corresponding private key.

Importing the Root Certificate

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.



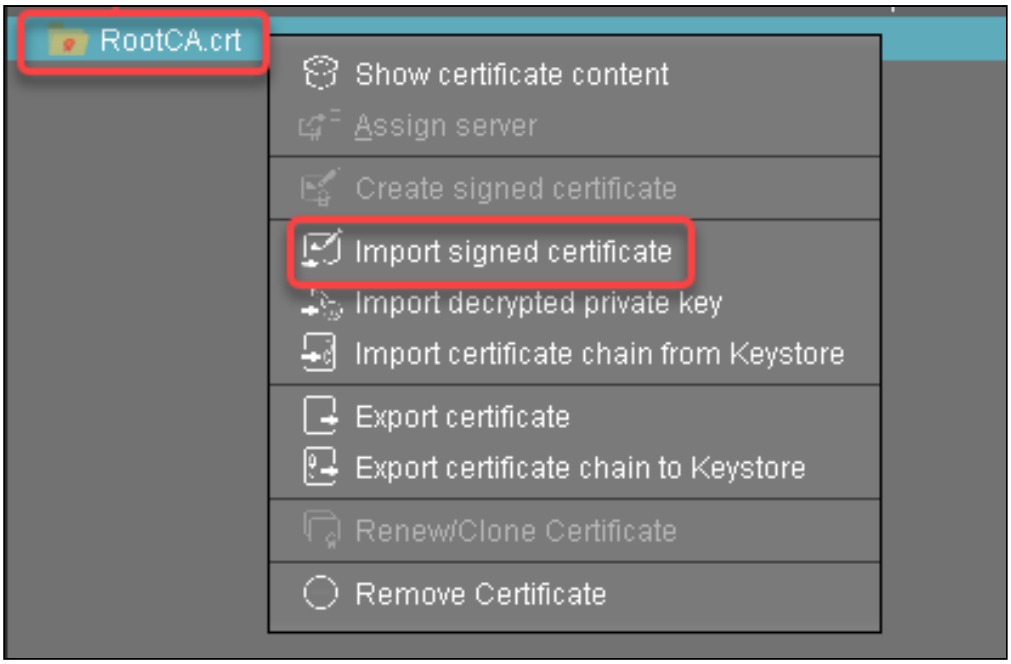
2. Click  select the root certificate file, and click **Open**.



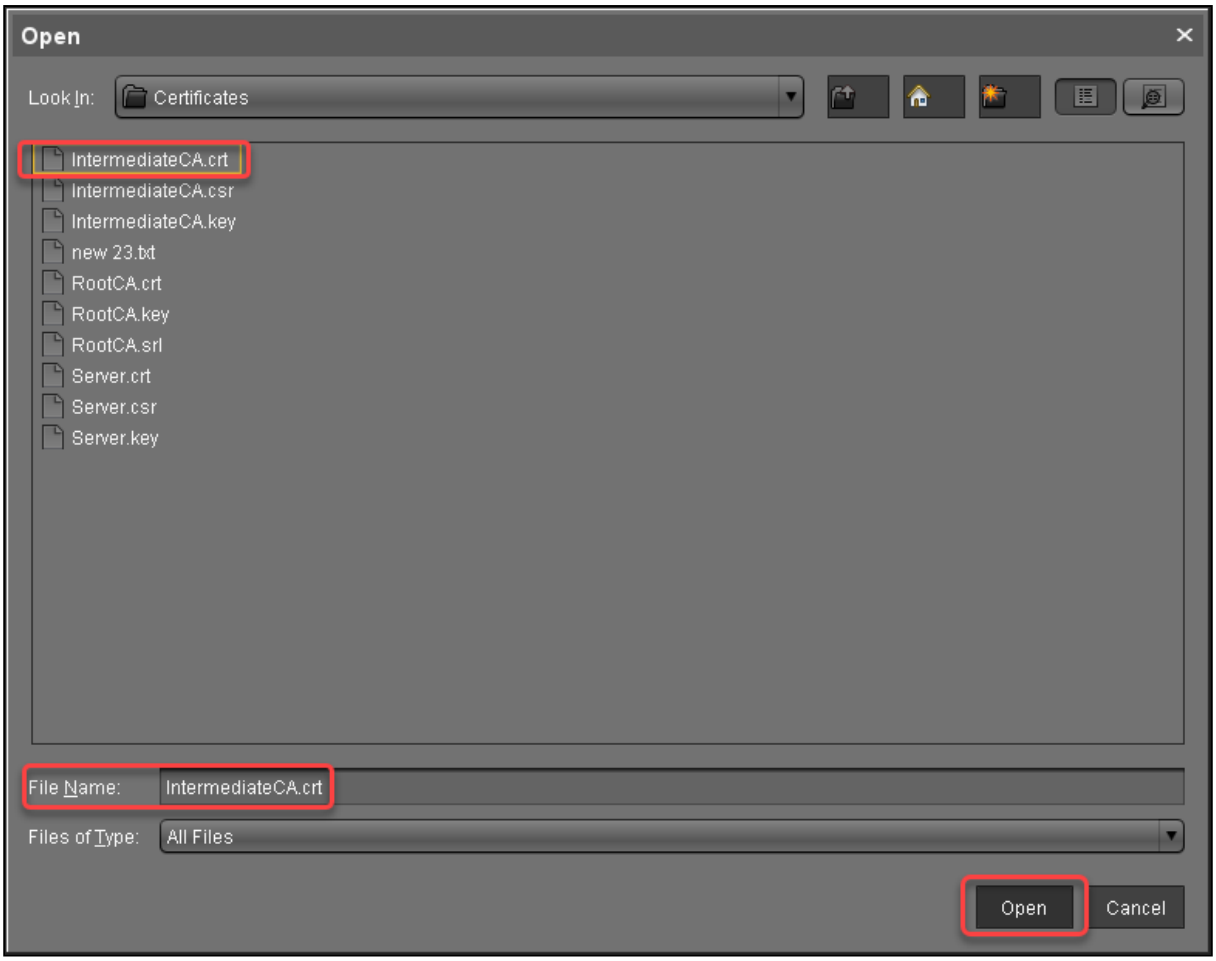
The root certificate is imported.

Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.

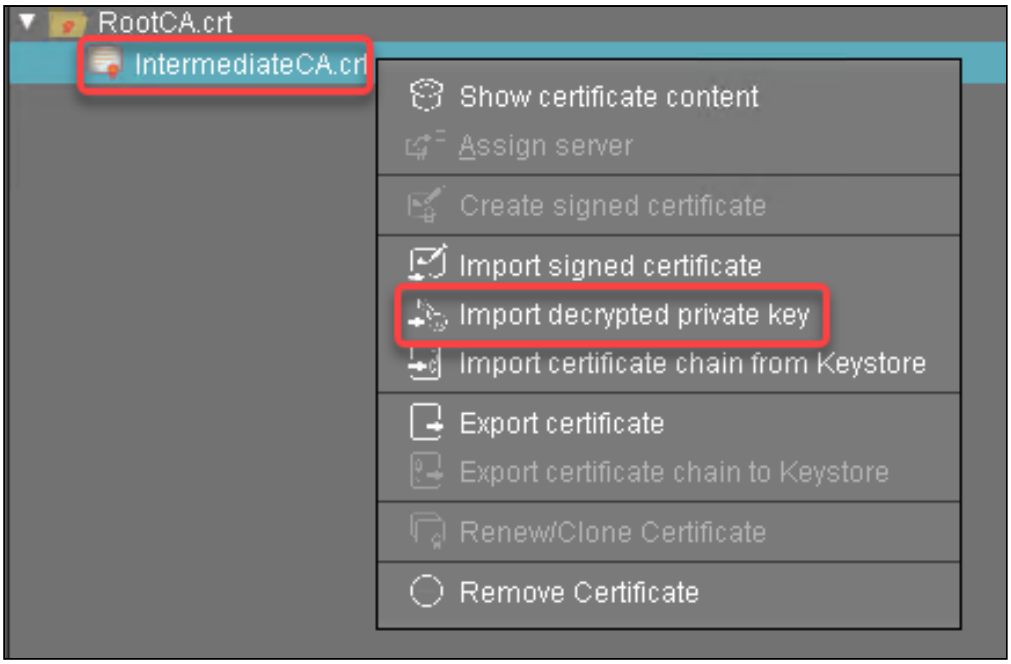


2. Select the intermediate certificate file and click **Open**.

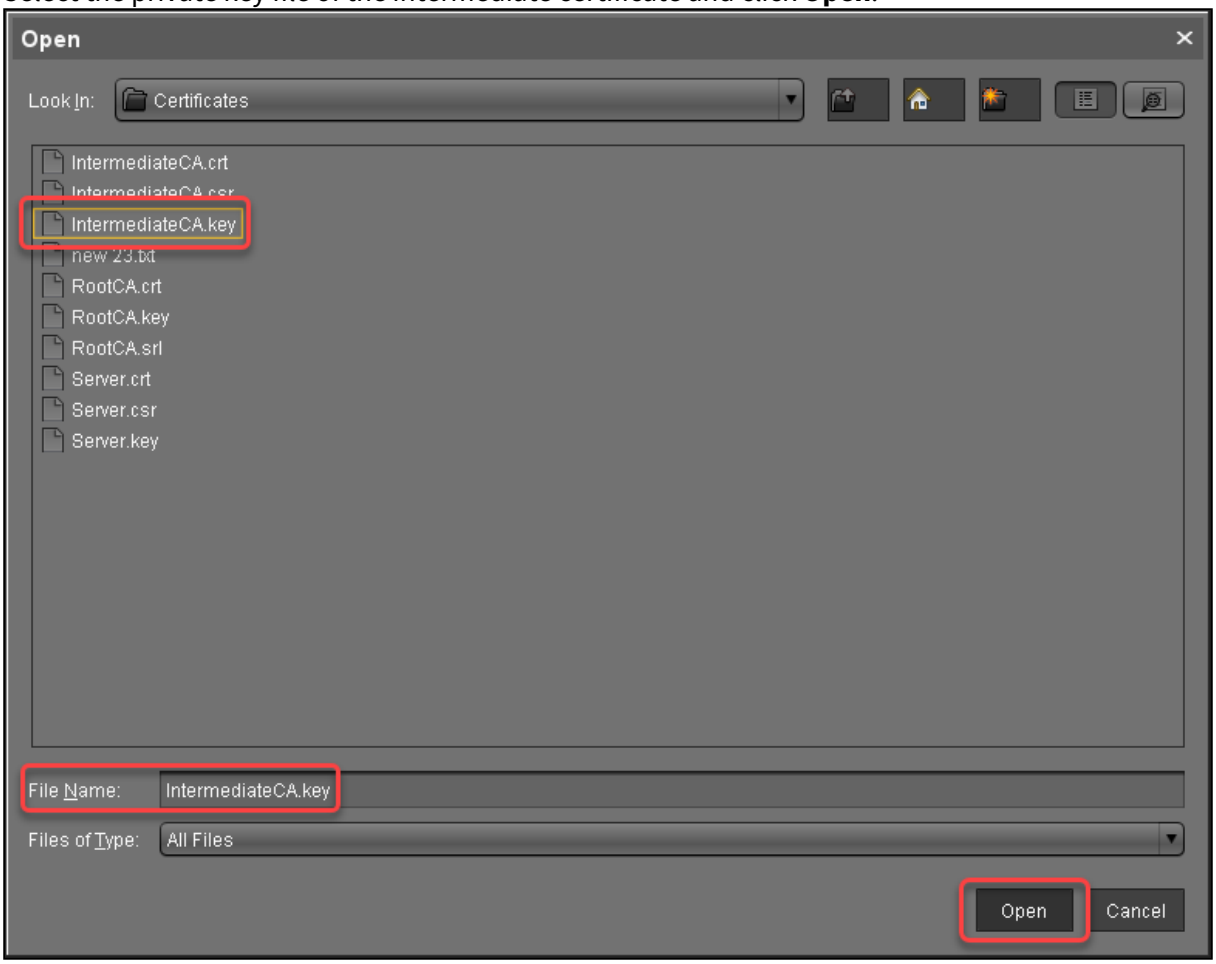


The intermediate certificate is imported.

3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.


RootCA.crt
IntermediateCA.crt
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone Certificate
Remove Certificate

4. Select the private key file of the intermediate certificate and click **Open**.



The private key of the intermediate certificate is imported.

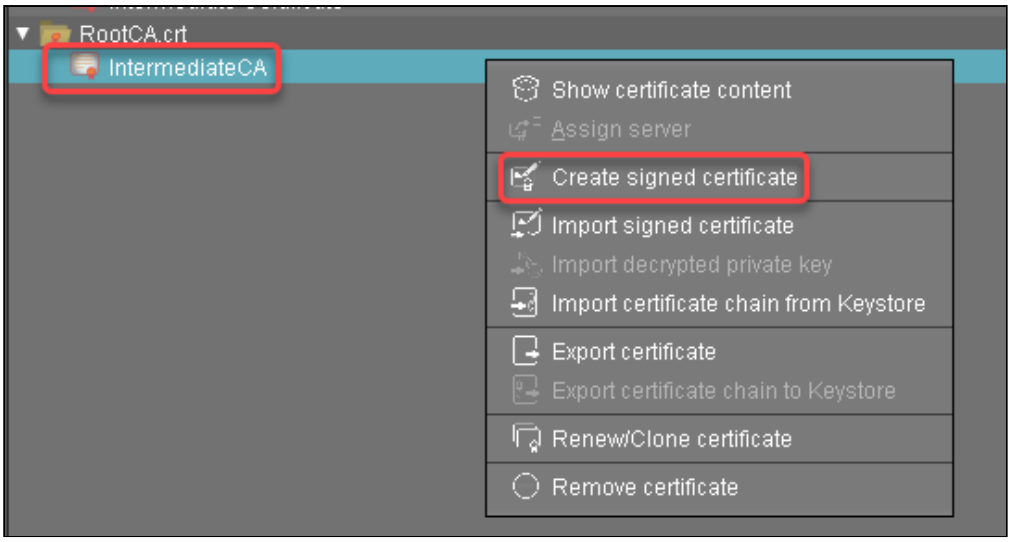
⚠ The private key is encrypted again when saved into the UMS Database.

5. Continue with Creating the End Certificates.

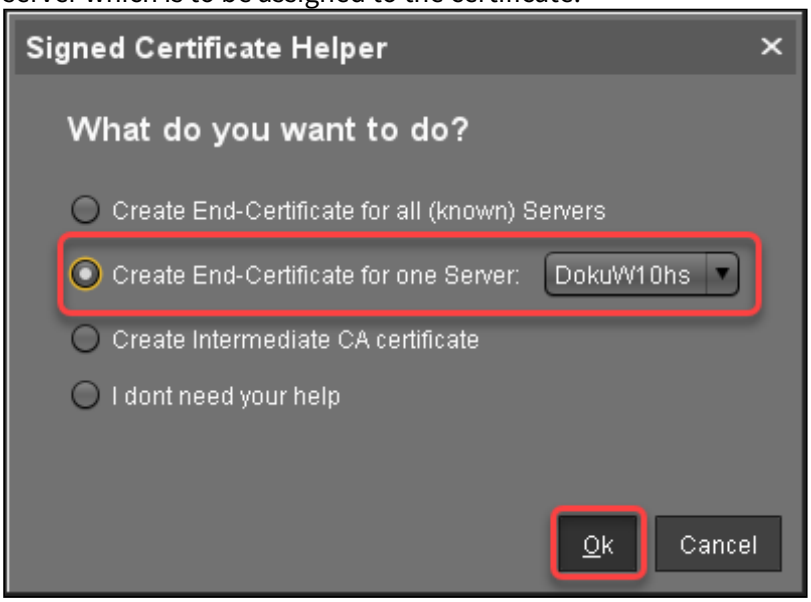
Creating the End Certificates

Repeat the following steps for each server in your UMS environment:

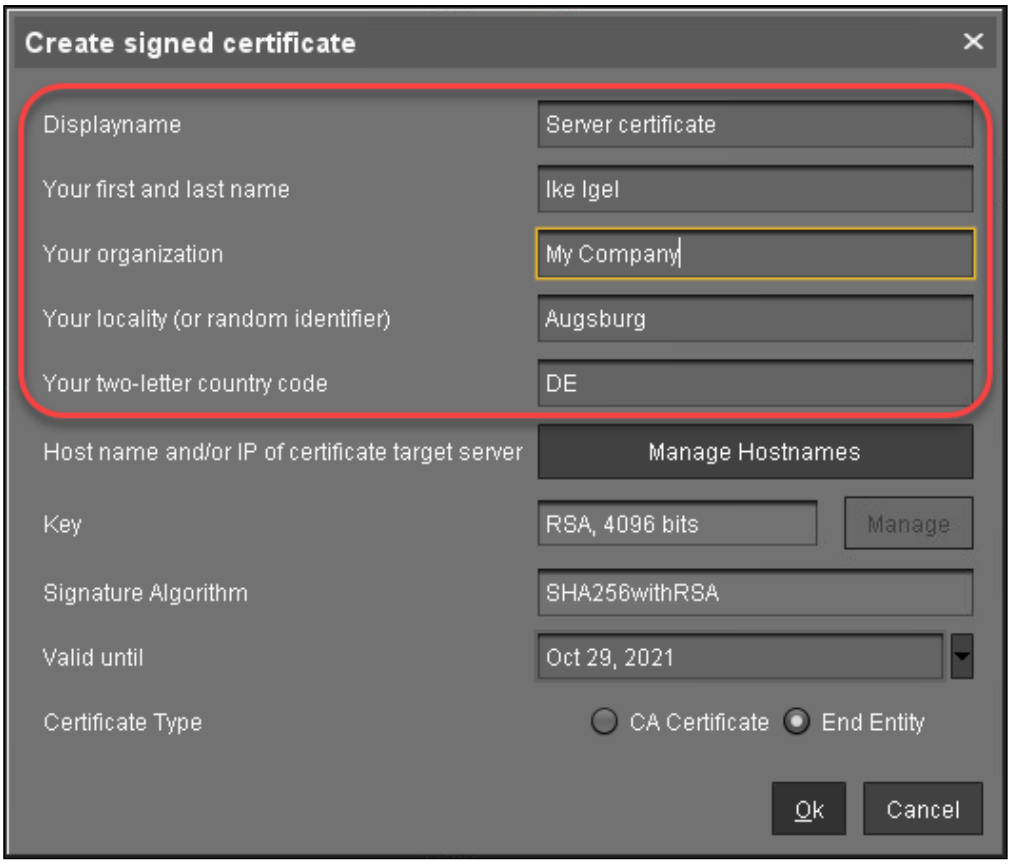
1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.



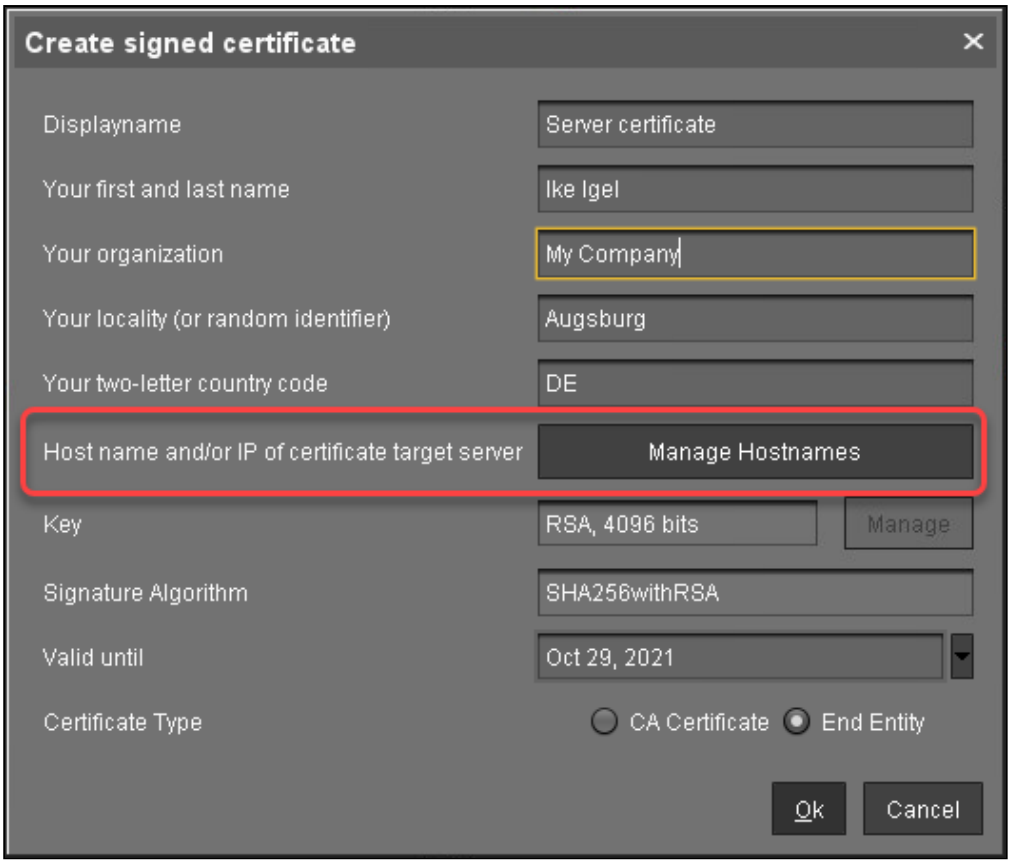
2. In the **Signed Certificate Helper**, select **Create end certificate for one server** and select the server which is to be assigned to the certificate.



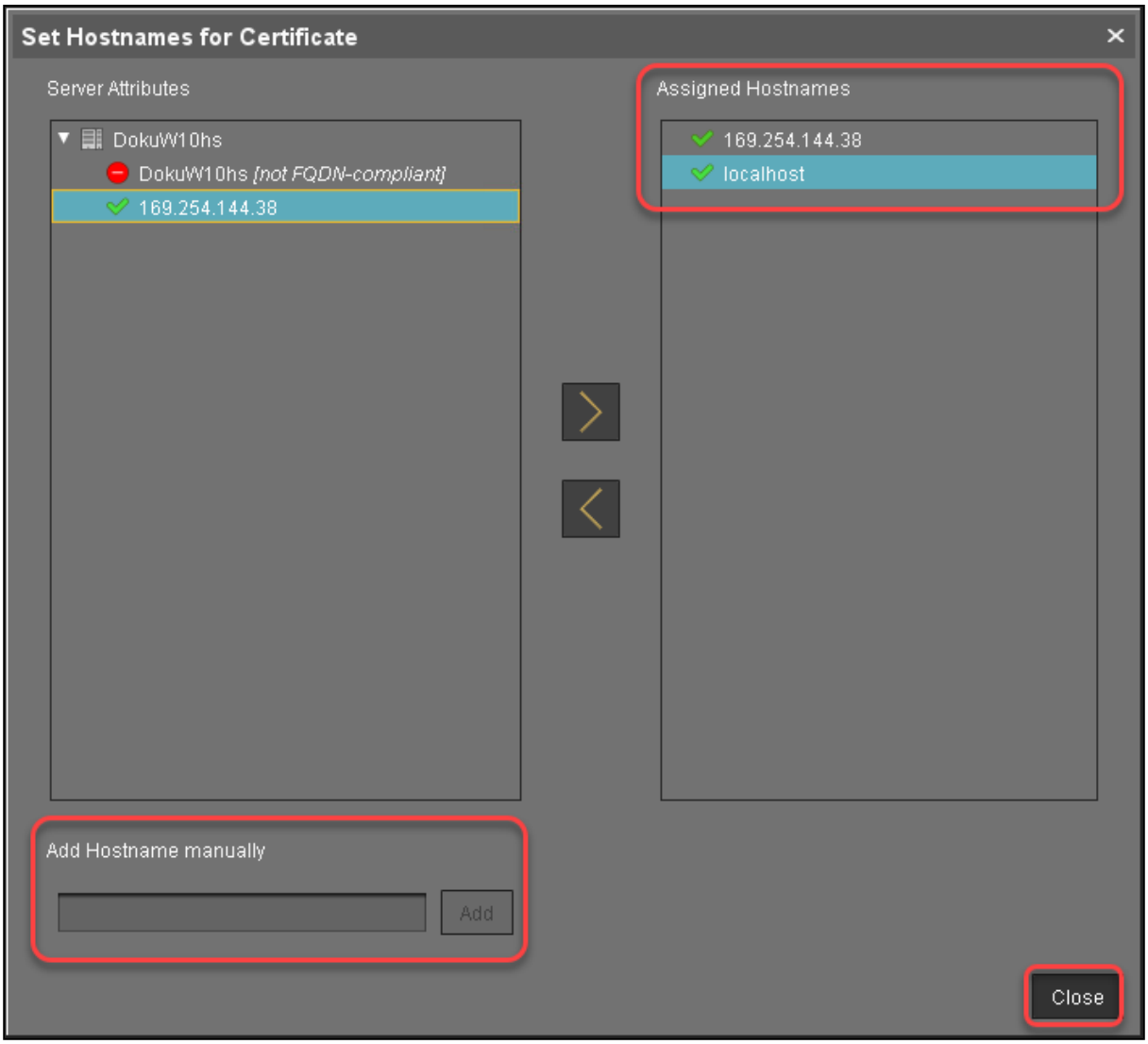
3. In the dialog **Create Signed Certificate**, fill in the data as required.



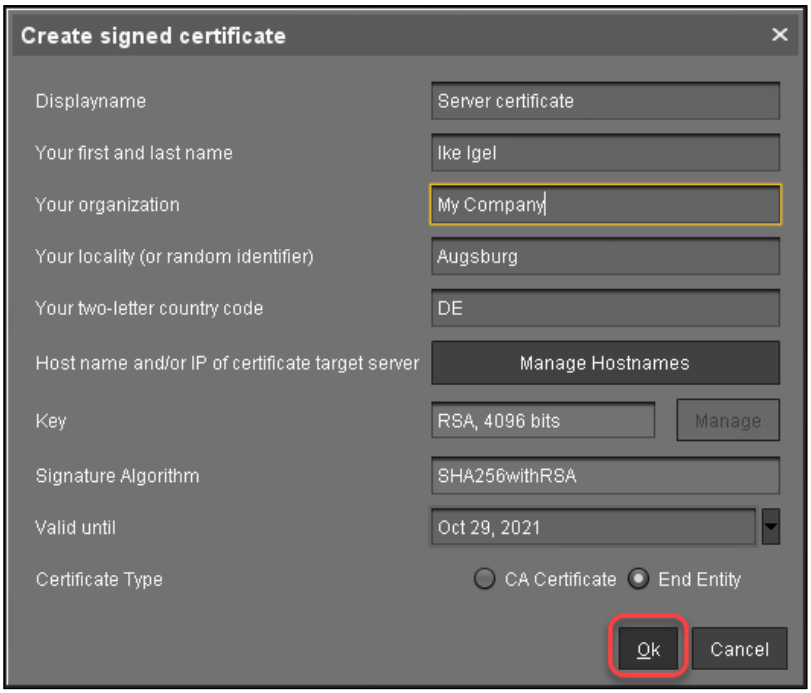
4. Click **Manage hostnames**.



5. In the dialog **Set Hostnames for Certificate**, check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.



6. Close the dialog **Create Signed Certificate** with **Ok**.



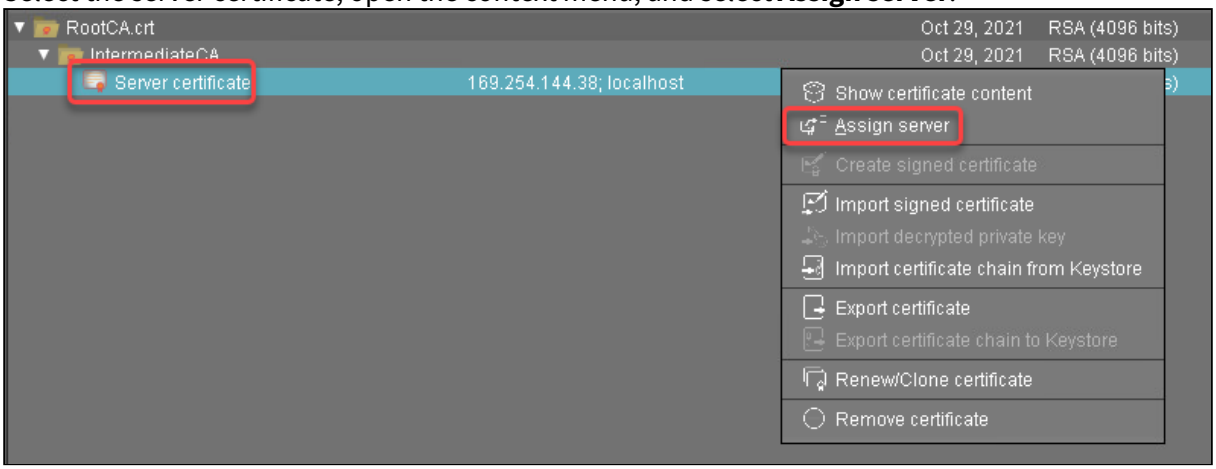
The signed server certificate is created.

7. Continue with Assigning the Certificate to All Servers.

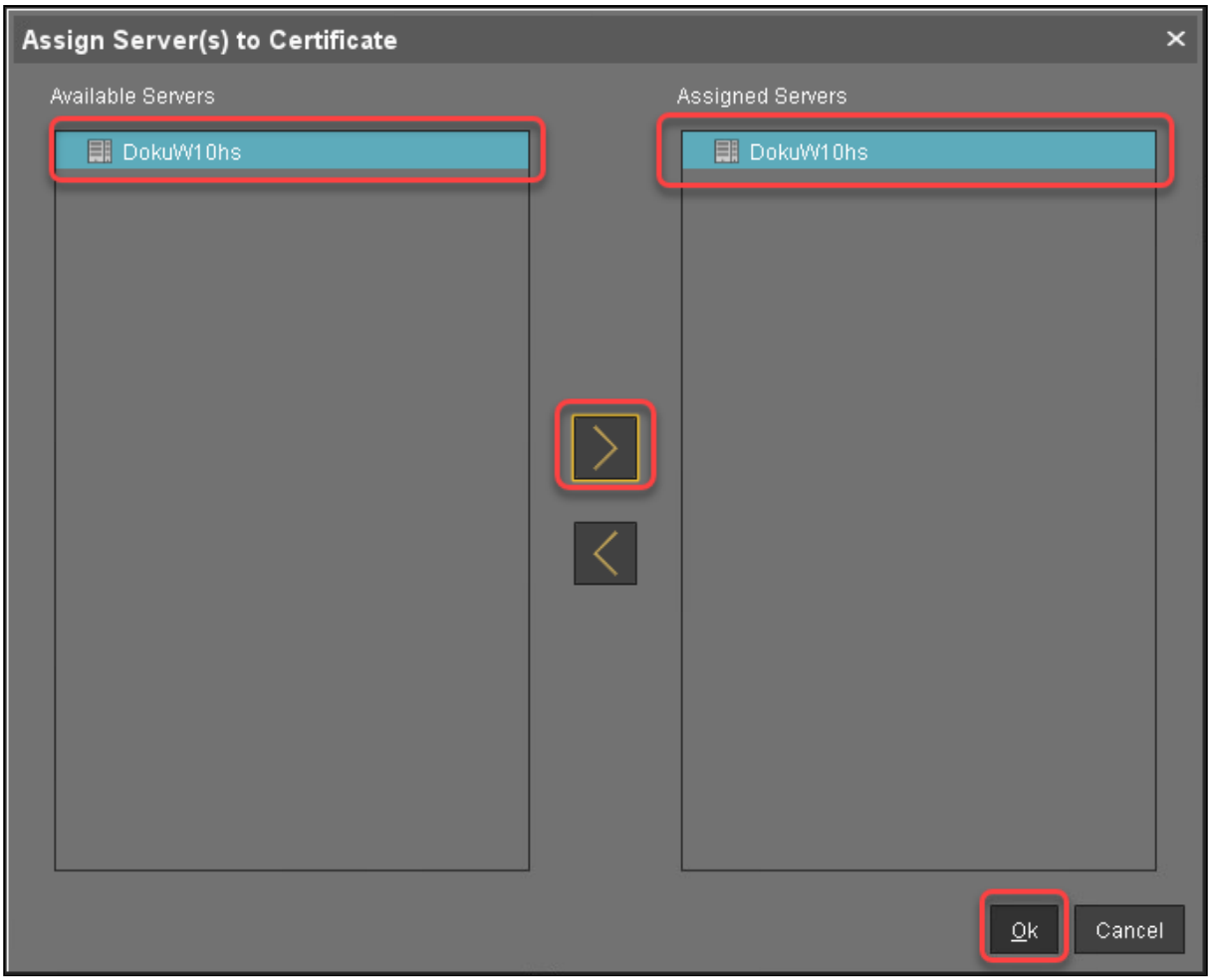
Assigning All Servers to the Certificate

Repeat the following steps for each server in your UMS environment:

1. Select the server certificate, open the context menu, and select **Assign server**.



2. Assign the server to the certificate as appropriate.



3. If you are managing IGEL OS 12 devices, see If You Exchange a Root Web Certificate for IGEL OS 12 Devices.
4. If you are using the UMS Web App: To avoid warning messages from browsers, you must make the new certificates known to the browsers. For instructions, see Troubleshooting: Browser Displays a Security Warning (Certificate Error) when Opening the UMS Web App (see page 564).

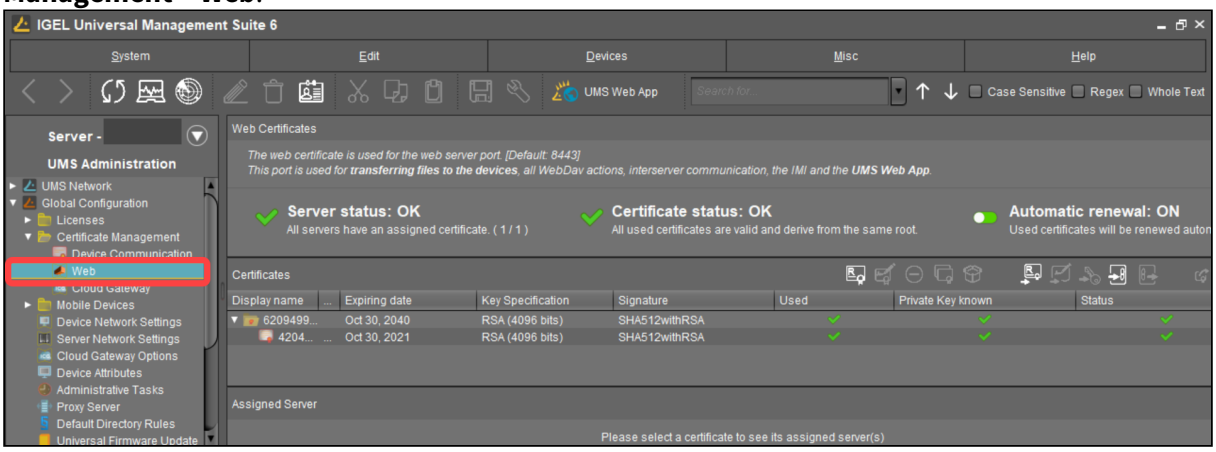
Deploying a Certificate Chain with a Public Root CA

Prerequisites

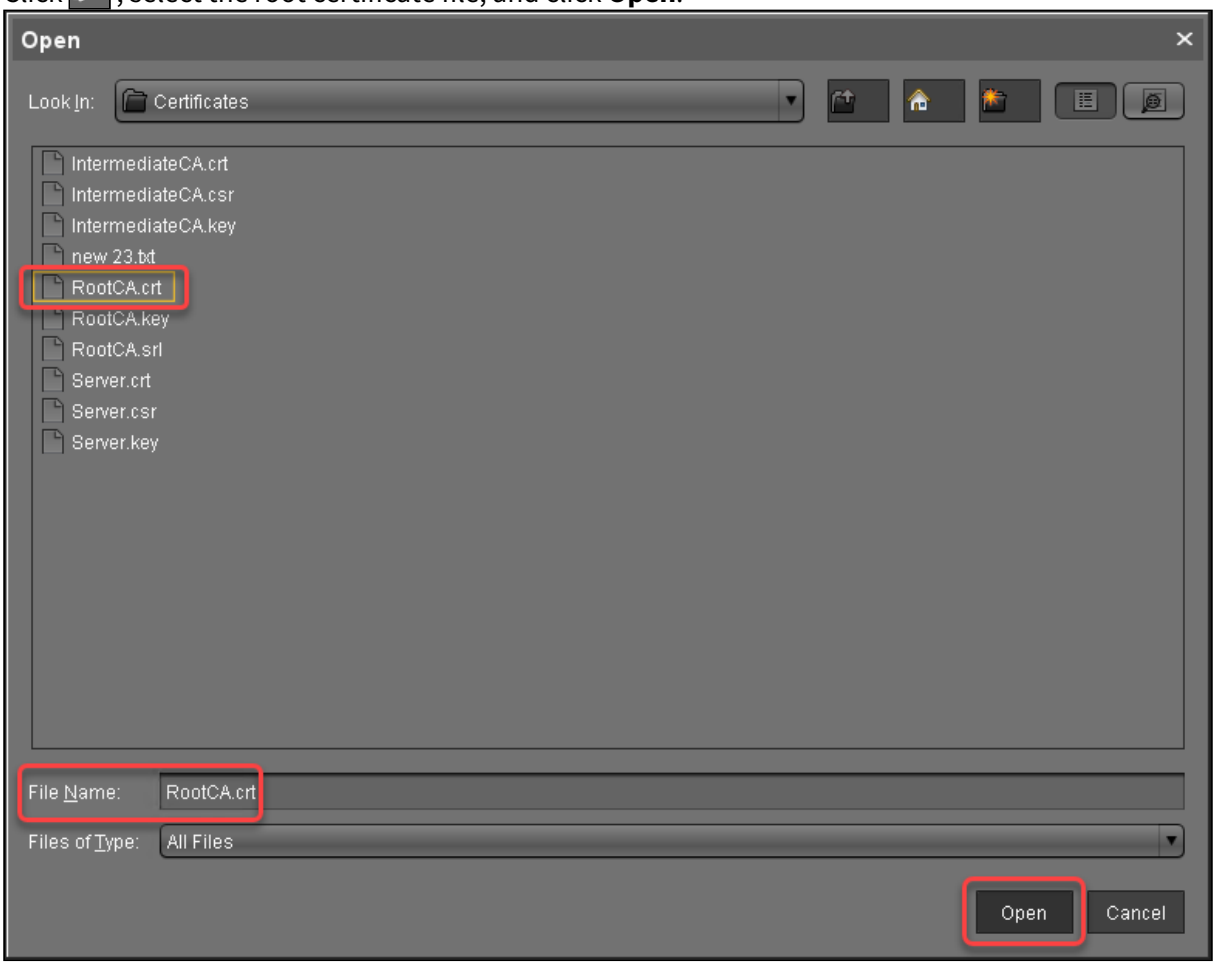
- You have a public certificate that is able to serve as a CA.
- All UMS Servers follow the same naming scheme, e.g. “something.ums.mycompany.de” if the company name is "mycompany.de".

Importing the Root Certificate

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.



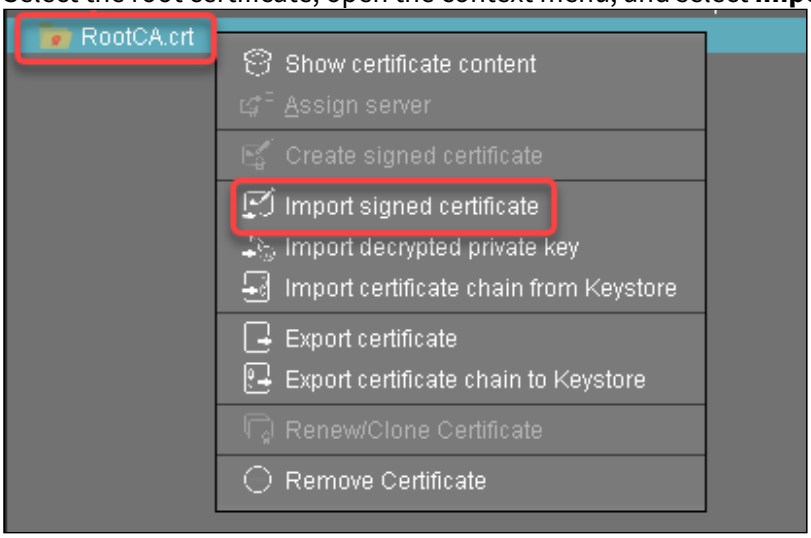
2. Click  , select the root certificate file, and click **Open**.



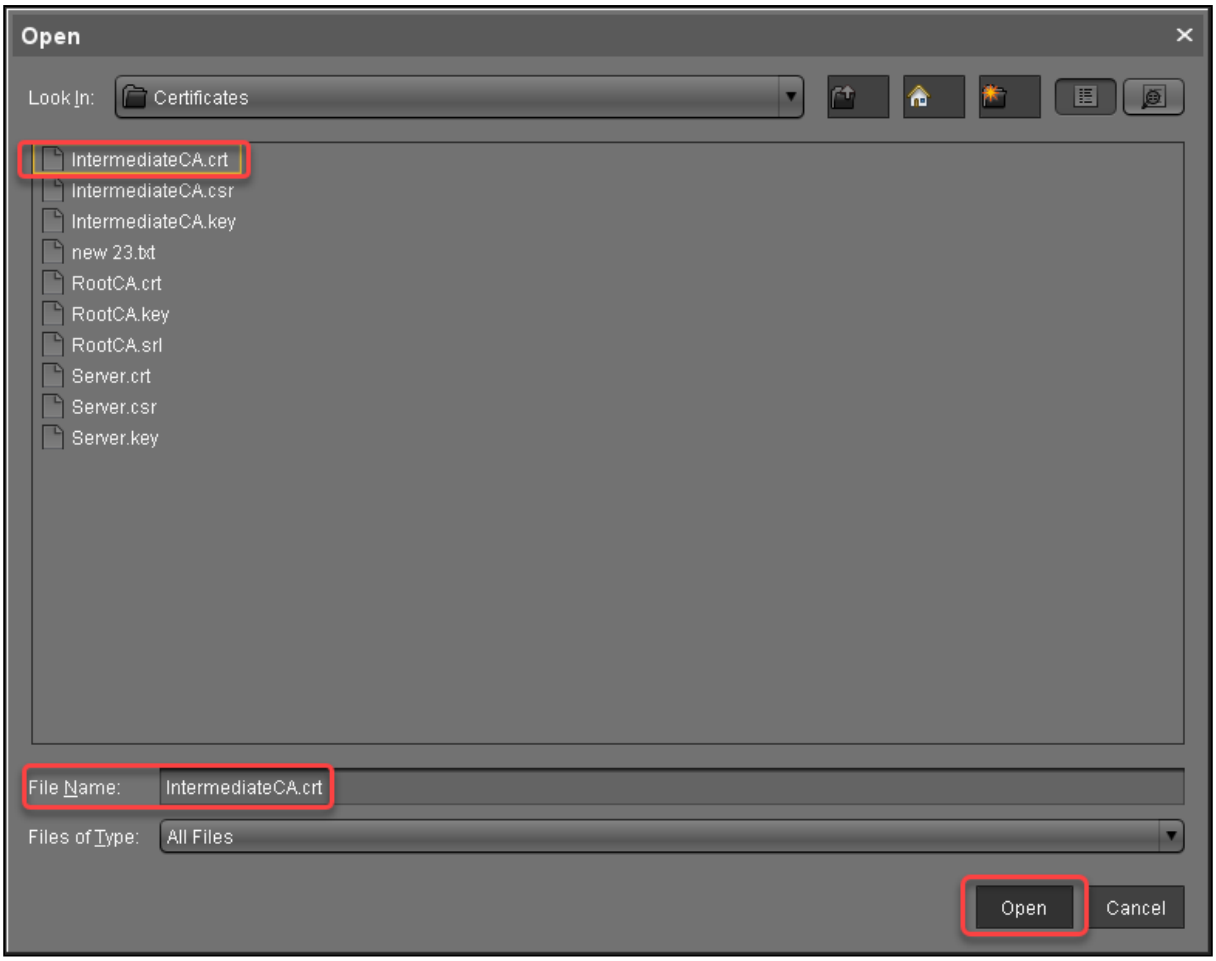
The root certificate is imported.

Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.

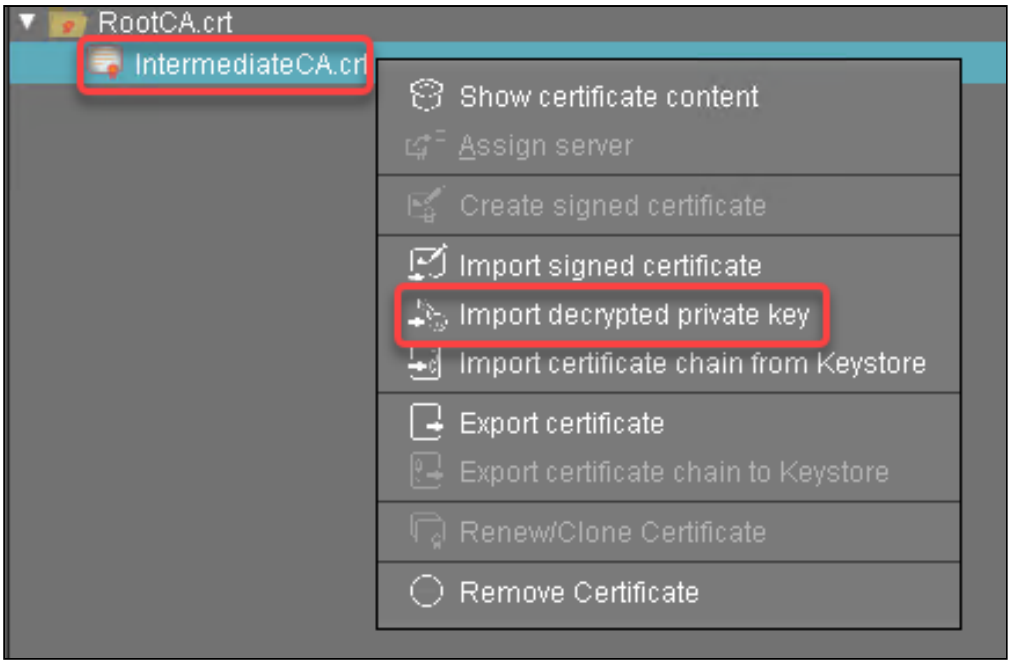


2. Select the intermediate certificate file and click **Open**.

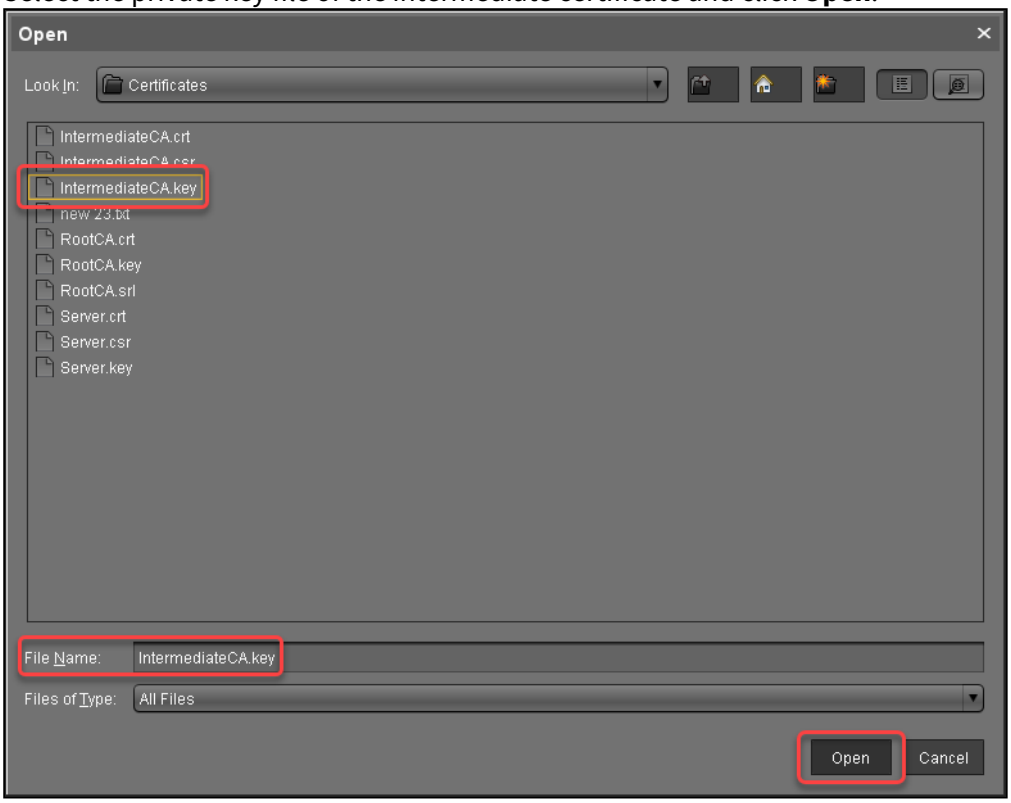


The intermediate certificate is imported.

3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.



4. Select the private key file of the intermediate certificate and click **Open**.



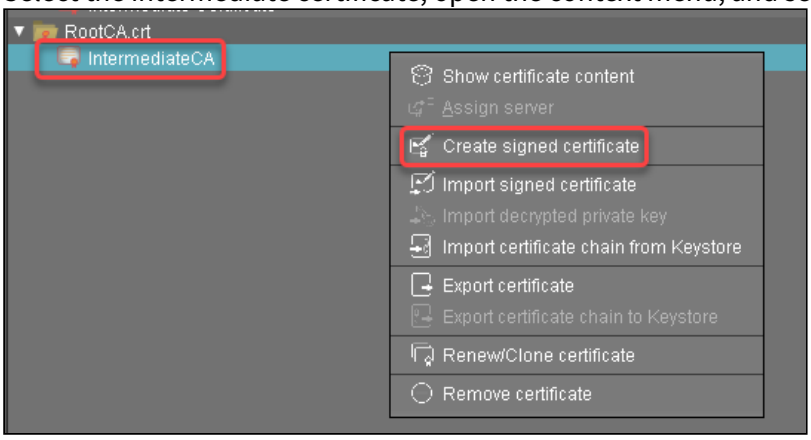
The private key of the intermediate certificate is imported.

The private key is encrypted again when saved into the UMS Database.

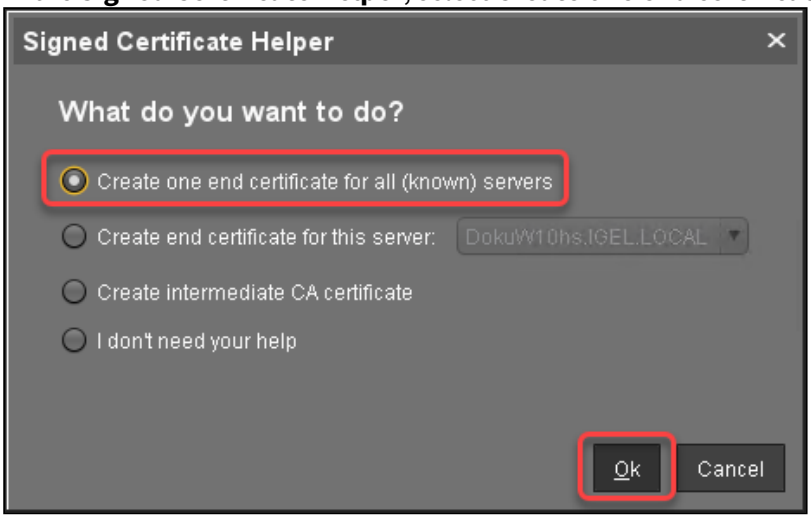
Creating End Certificates

Repeat the following steps for each server in your UMS environment:

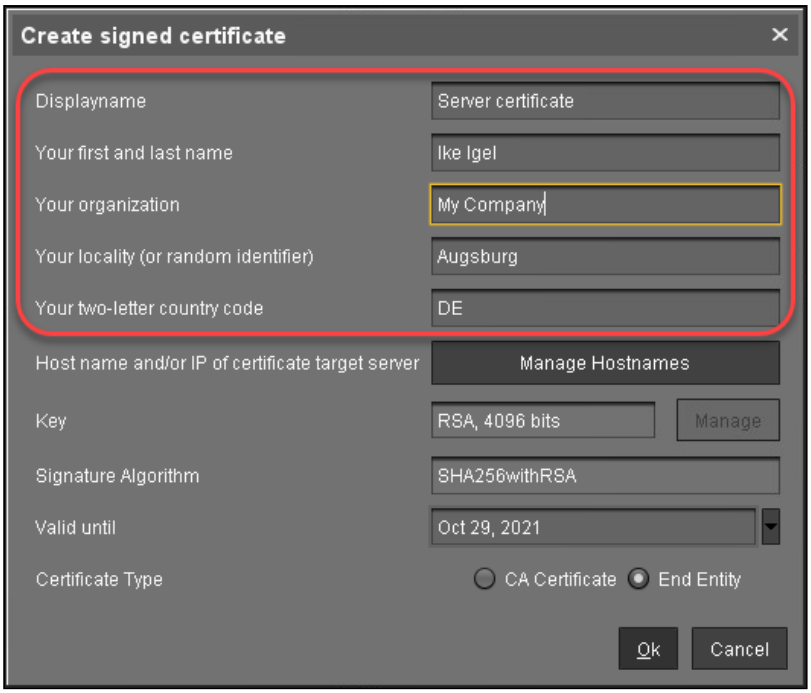
1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.



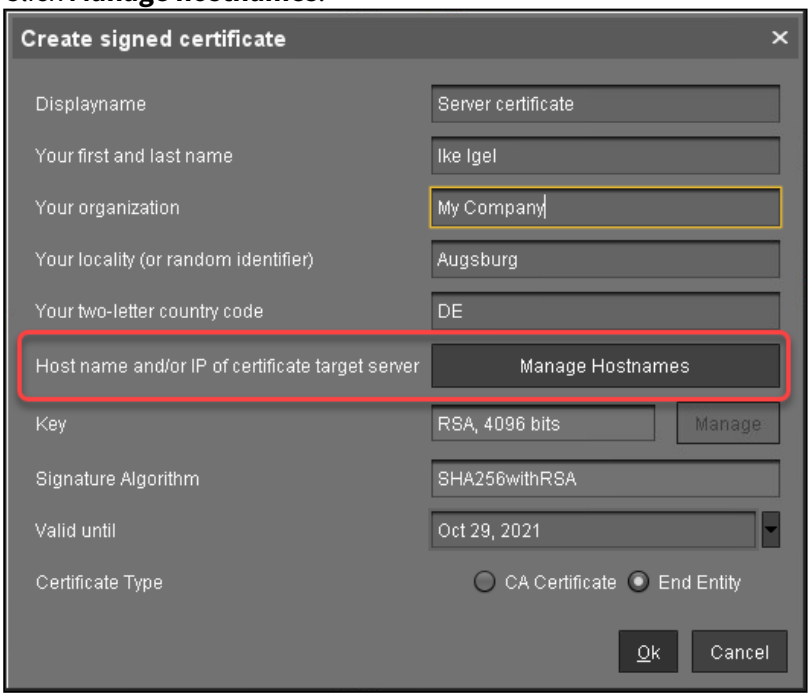
2. In the **Signed Certificate Helper**, select **Create one end certificate for all (known) servers**.



3. In the dialog **Create Signed Certificate**, fill in the data as required.

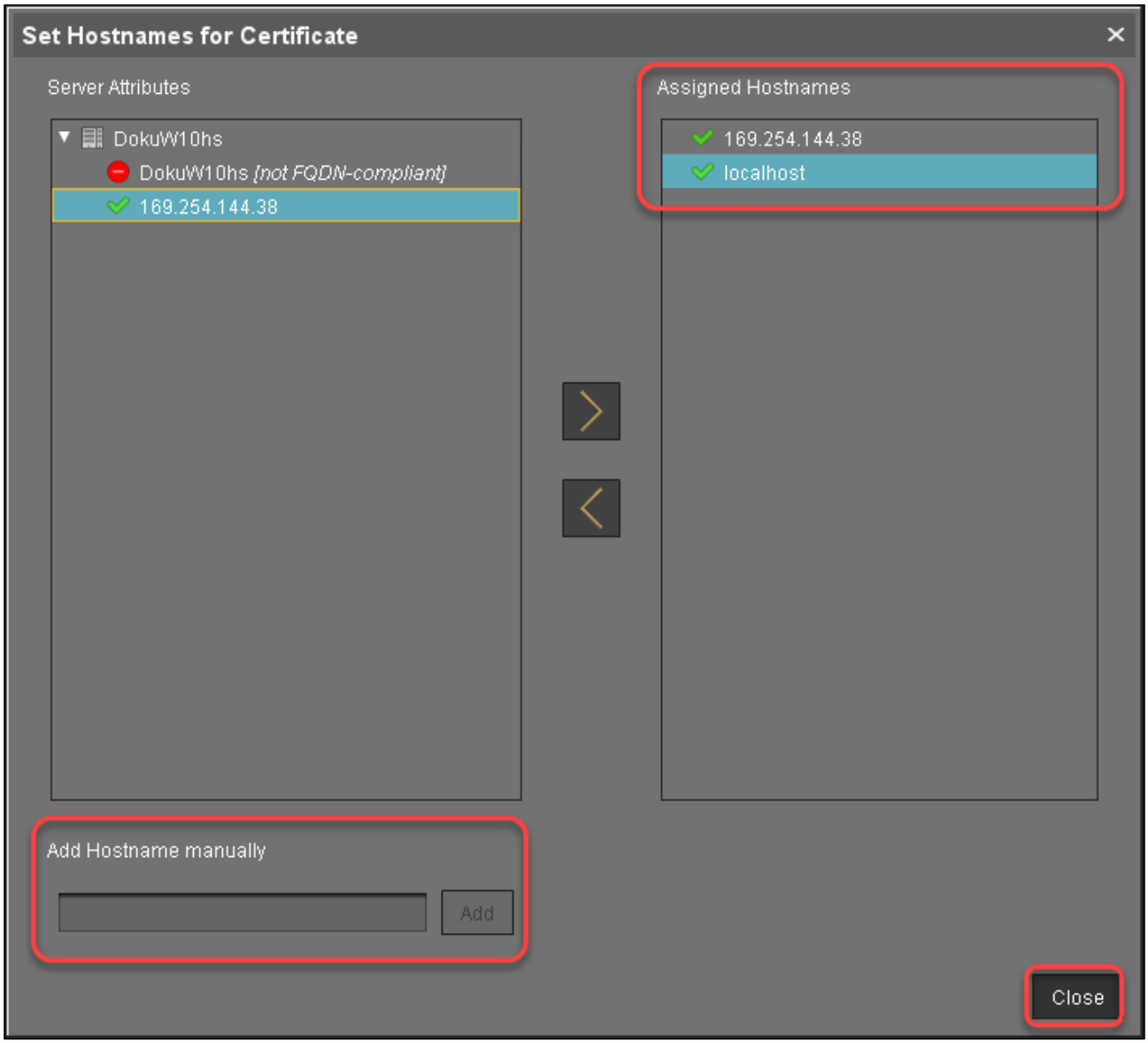


4. Click **Manage hostnames**.

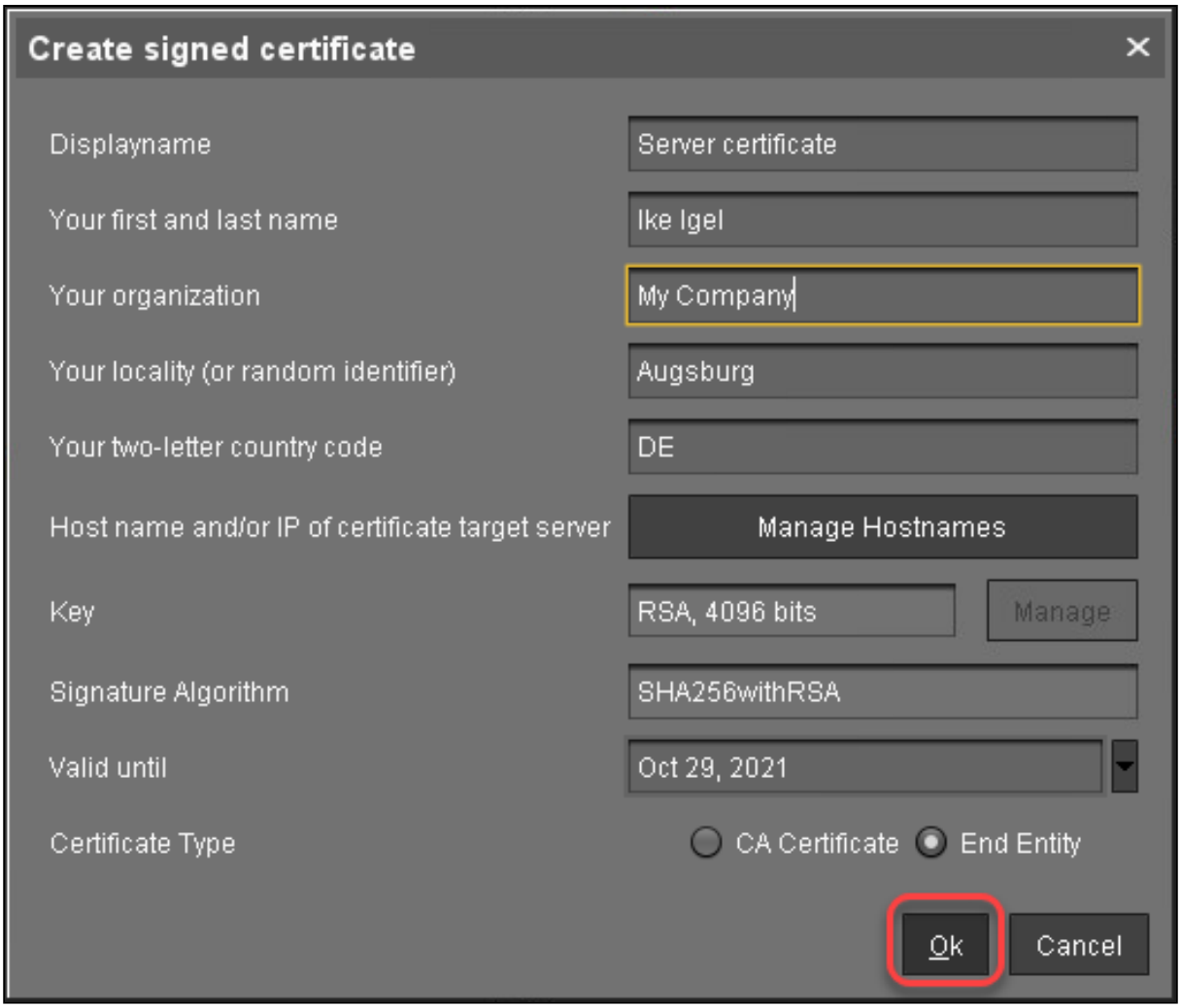


5. In the dialog **Set Hostnames for Certificate**, adjust the settings as follows:

- Check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.
- Remove all IP addresses and FQDNs you do not want to be part of the certificate.



6. Close the dialog **Create Signed Certificate** with **Ok**.

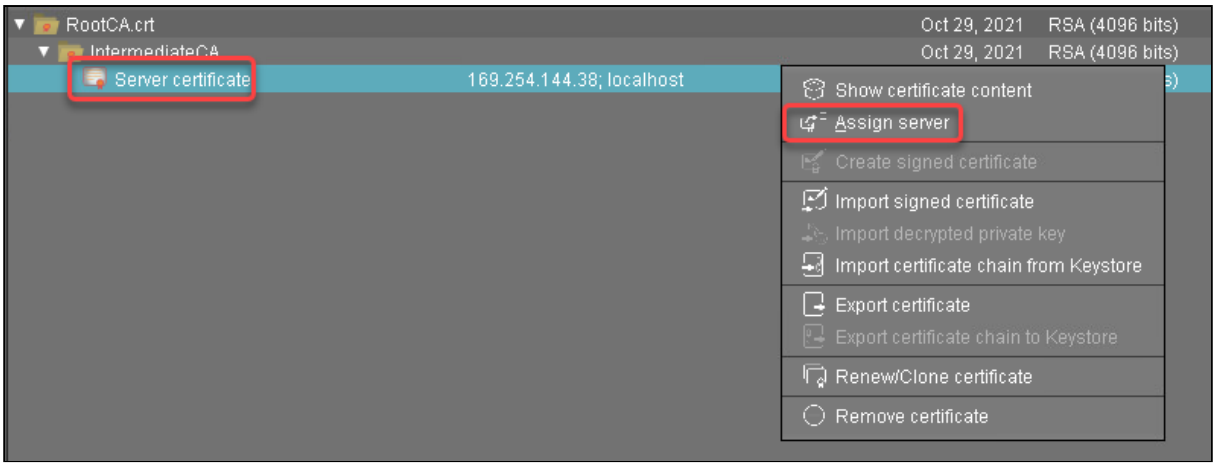


The signed server certificate is created.

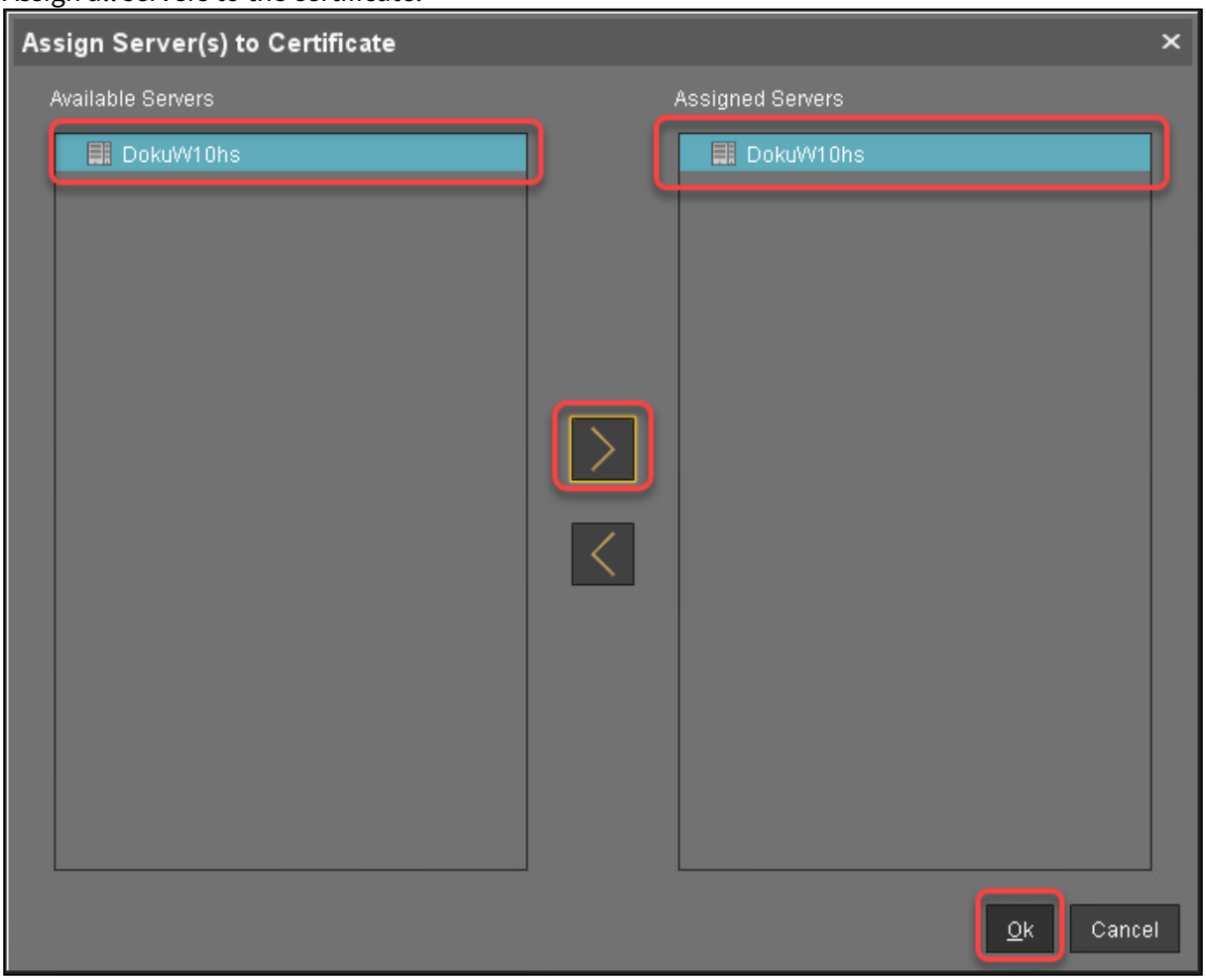
7. Continue with Assigning all Servers to the Certificate.

Assigning All Servers to the Certificate

1. Select the server certificate, open the context menu, and select **Assign server**.



2. Assign all servers to the certificate.



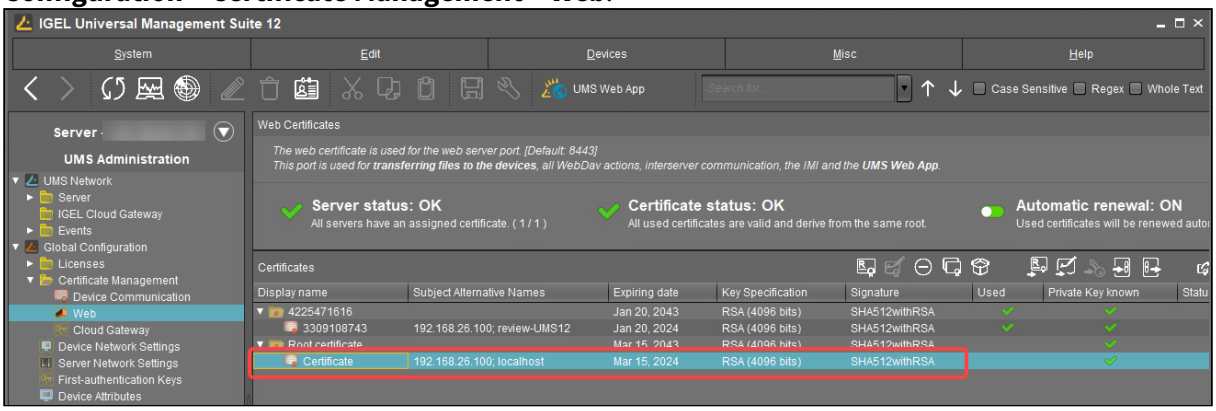
3. If you are managing IGEL OS 12 devices, see If You Exchange a Root Web Certificate for IGEL OS 12 Devices.

If You Exchange a Root Web Certificate for IGEL OS 12 Devices

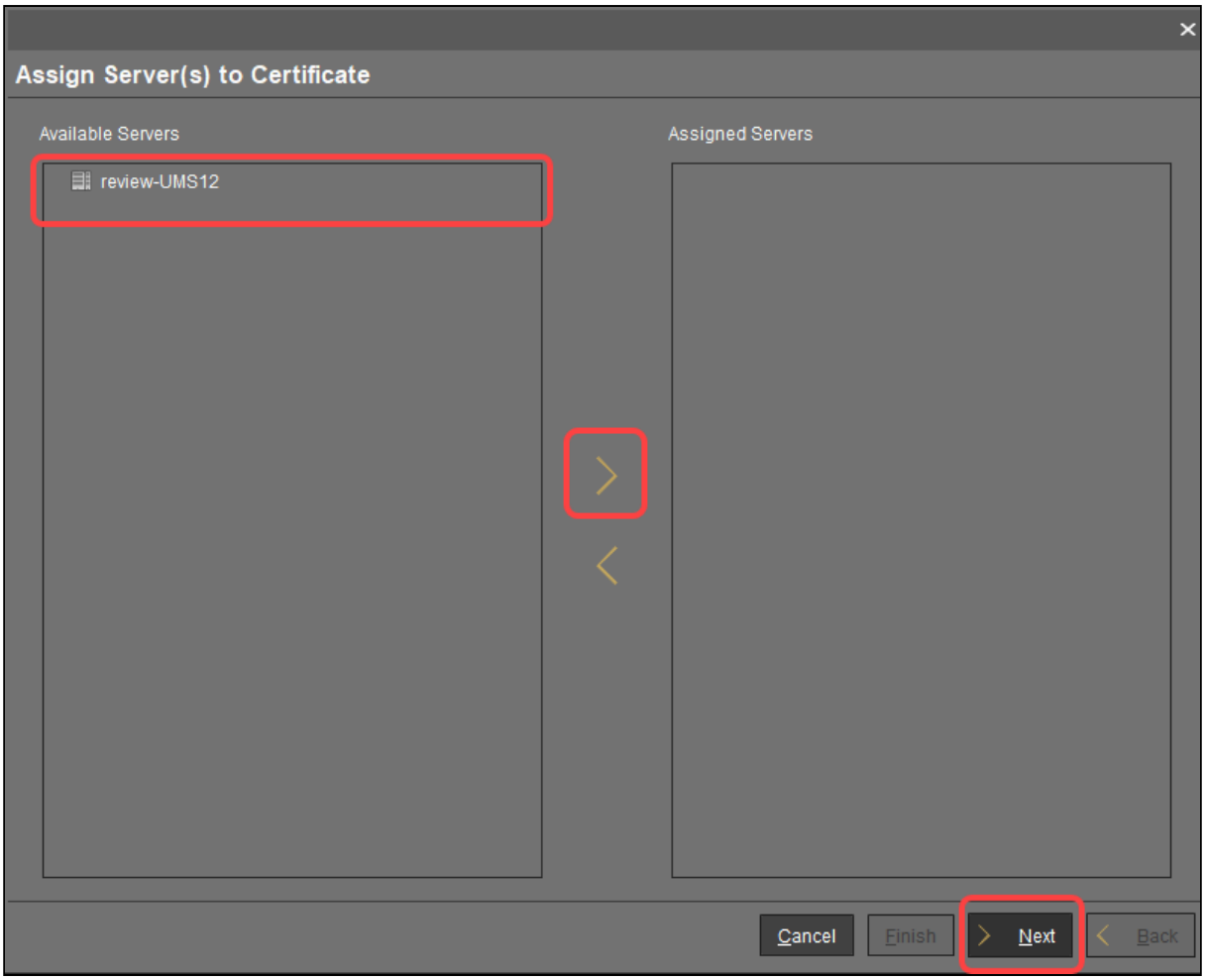
> New root web certificates are deployed to IGEL OS 12 devices on reboot.

For IGEL OS 12 devices, you can view which devices will no longer trust the UMS and will be unmanageable when you assign a new root certificate:

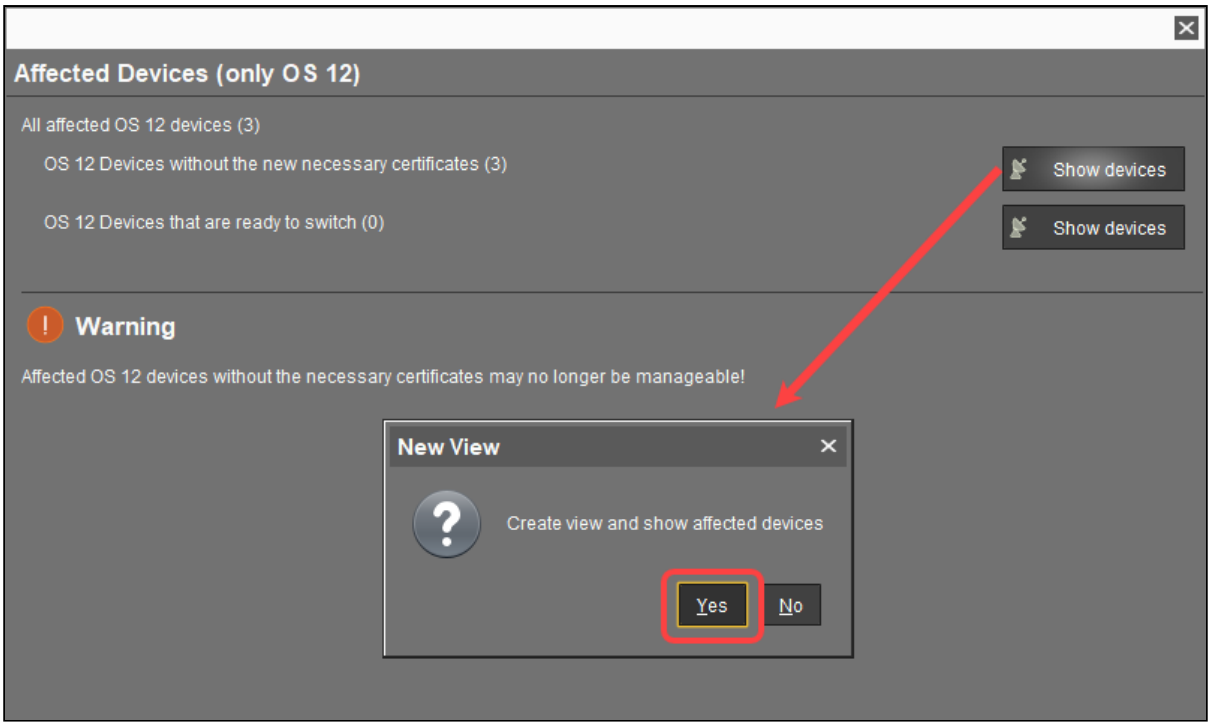
1. Select the certificate you want to be used under **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**.



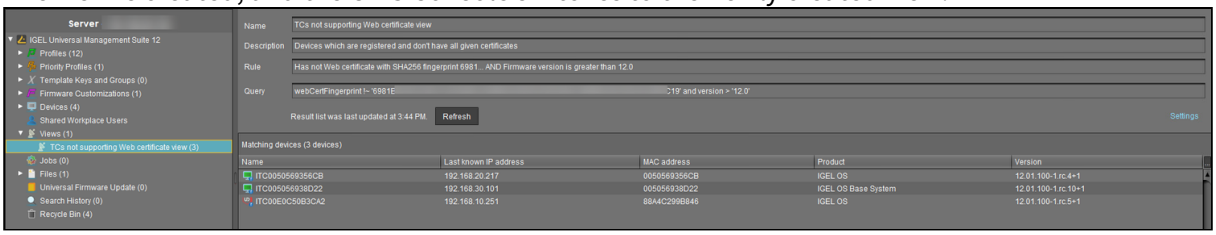
2. Click  or select **Assign server** in the context menu.
3. In the dialog **Assign Servers(s) to Certificate**, assign the required server(s) and click **Next**.



4. For IGEL OS 12 devices, you will see the **Affected Devices** dialog. Review it:
   If the **OS 12 devices without the new necessary certificates** number = 0 and there is no warning dialog, you can complete the assignment. The devices will safely switch to the new certificate.
   If the **OS 12 devices without the new necessary certificates** number > 0, click **Show devices** to create a view that collects the affected devices:

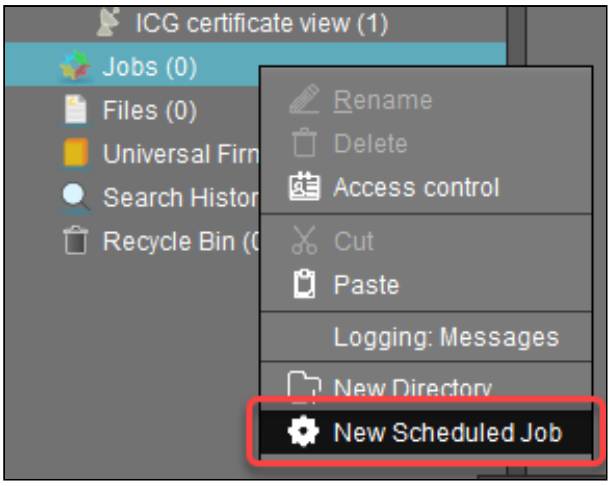


The view is created, and the UMS Console switches to the newly created view.

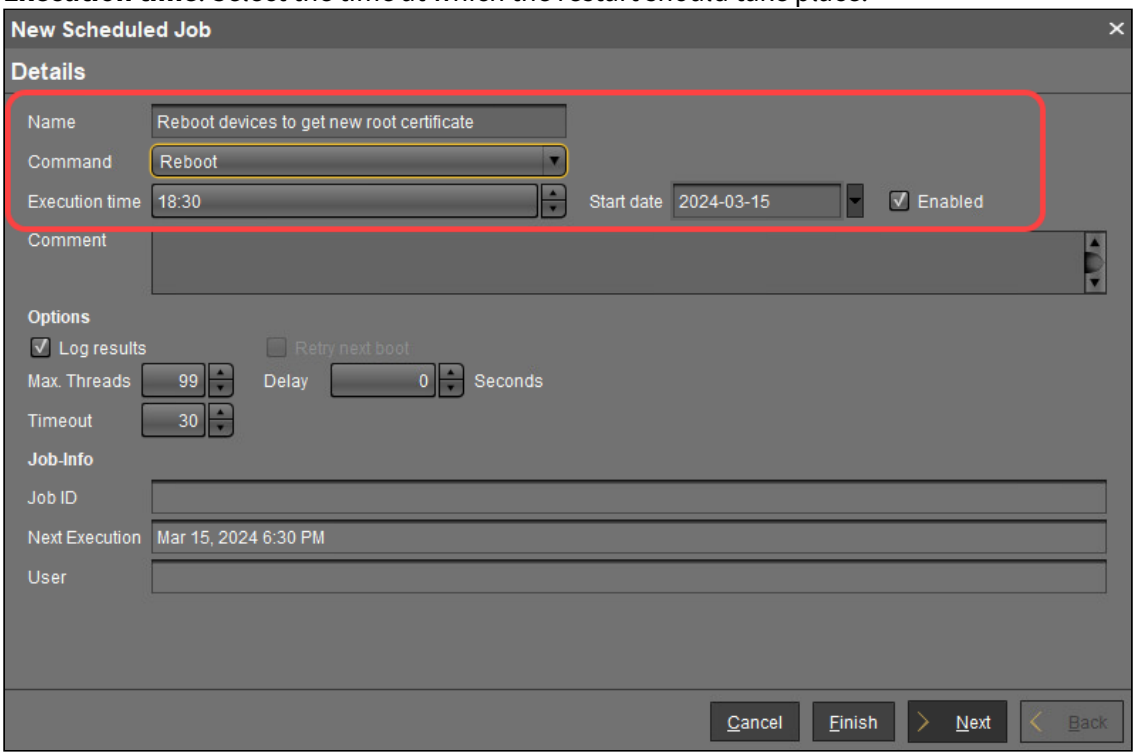


Now, it is necessary to restart the affected devices. On reboot, the devices will receive all certificates from the UMS; afterward, they are ready to switch to the new certificate.
To restart all affected devices at a defined time, it makes sense to create a scheduled job.

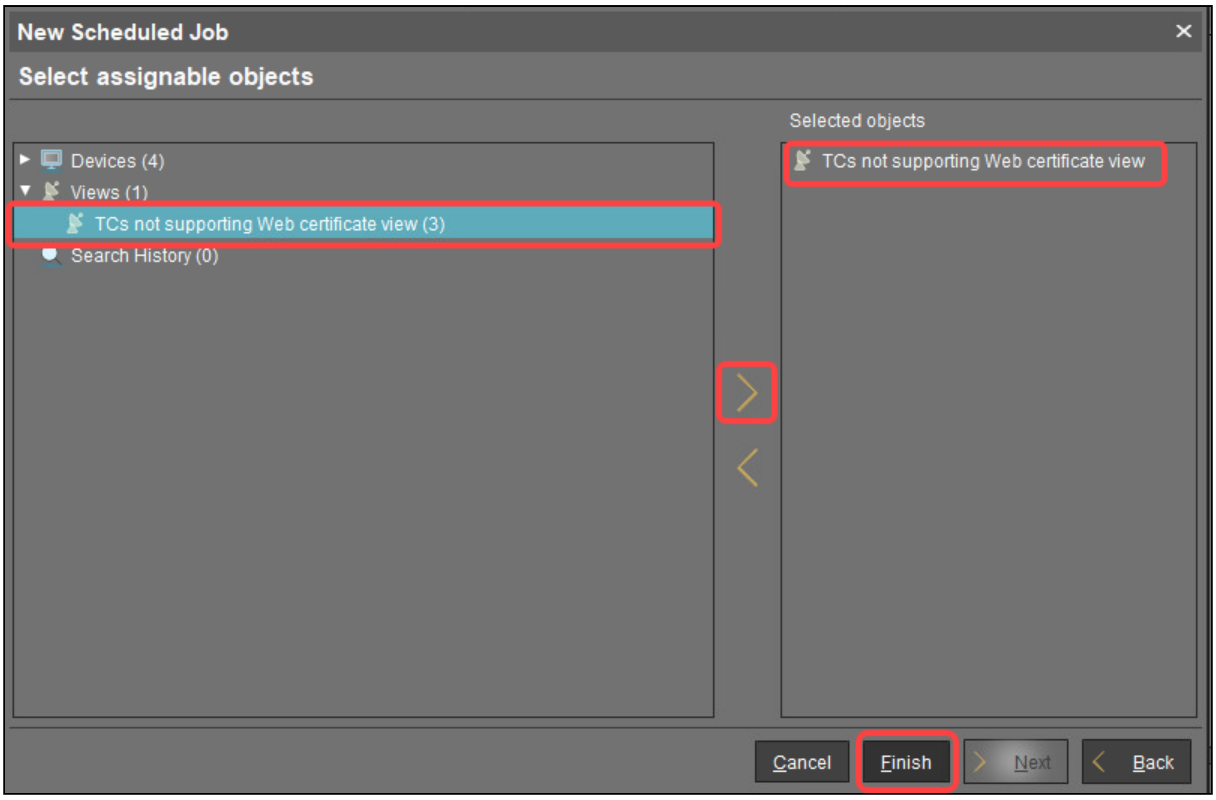
5. Go to **Jobs**, open the context menu, and select **New Scheduled Job**.



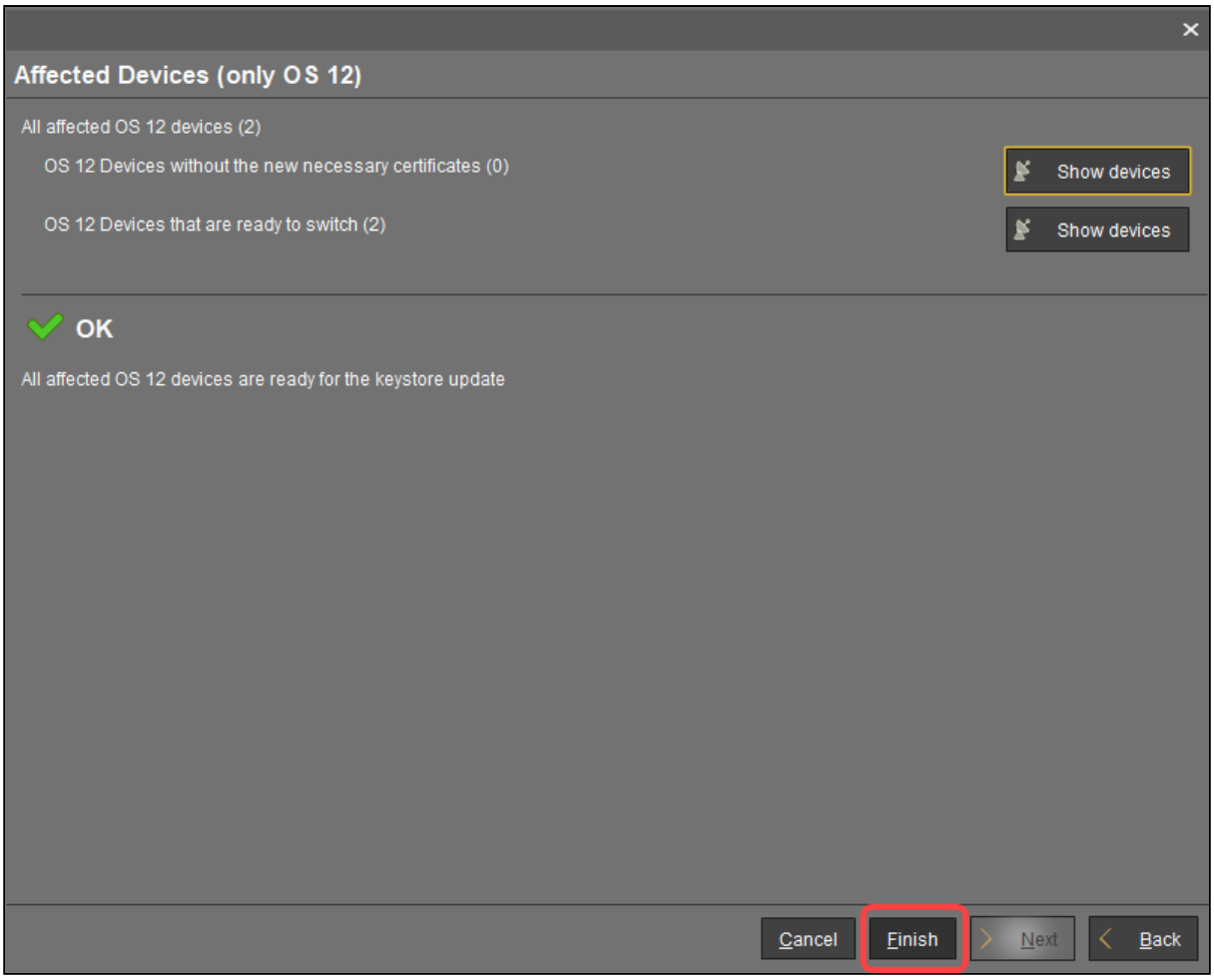
6. In the **New Scheduled Job** window, change the settings as follows and click **Next**:
   - **Name**: A name for the job
   - **Command**: Select "Reboot"
   - **Execution time**: Select the time at which the restart should take place.



7. In the next step, leave the settings as they are and click **Next**.
8. Assign the view created beforehand to the job and click **Finish**.



9. After the reboot, complete the assignment: Under **UMS Administration > Global Configuration > Certificate Management > Web**, select the required certificate and click  or **Assign server** in the context menu.
   If the output in the **Affected Devices** dialog is like this, click **Finish**. The devices will safely switch to the new certificate.

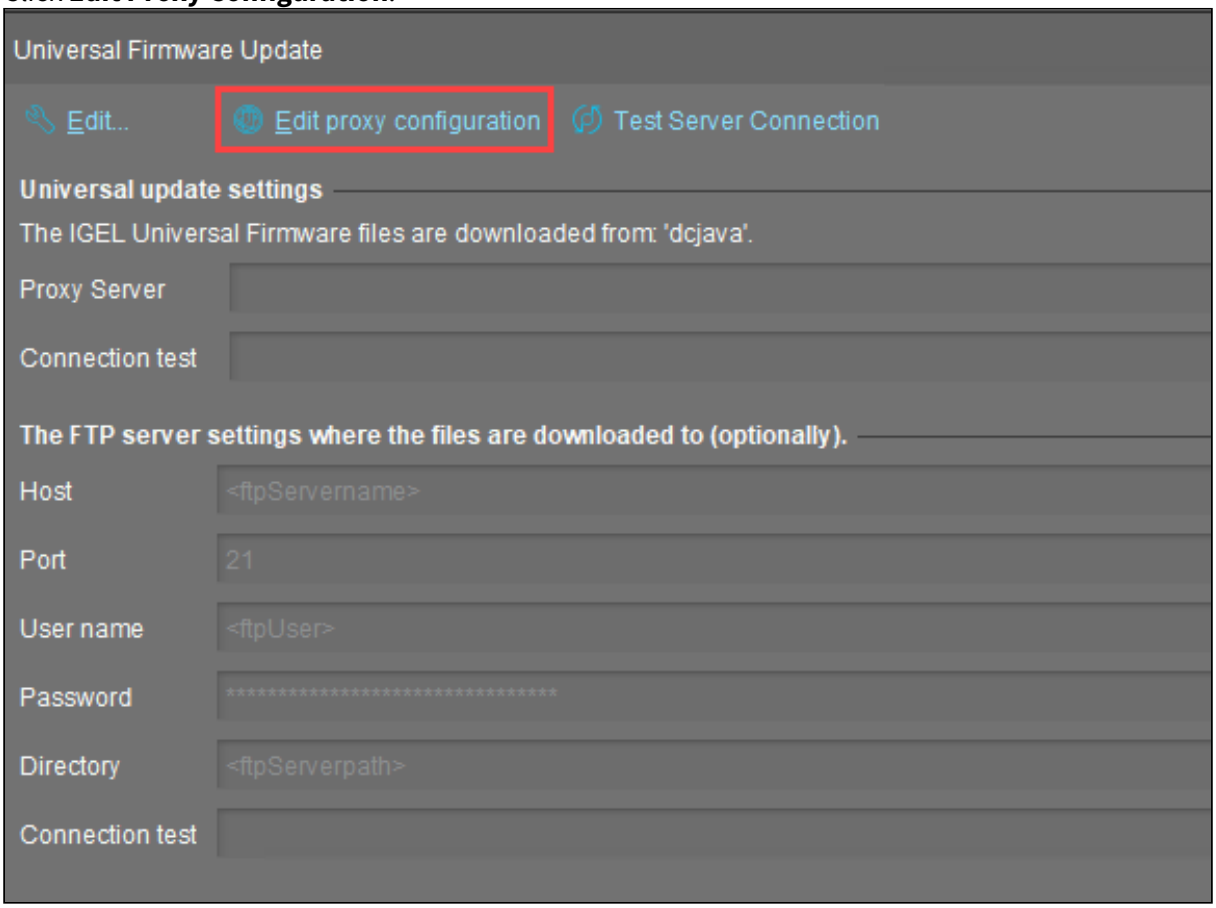

Affected Devices (only OS 12)
All affected OS 12 devices (2)
OS 12 Devices without the new necessary certificates (0)
Show devices
OS 12 Devices that are ready to switch (2)
Show devices
OK
All affected OS 12 devices are ready for the keystore update
Cancel
Finish
Next
Back

How to Use an HTTP Proxy for Firmware Updates in IGEL UMS

This article describes how to download firmware updates to the UMS if internet access is only available via an HTTP proxy in your environment.

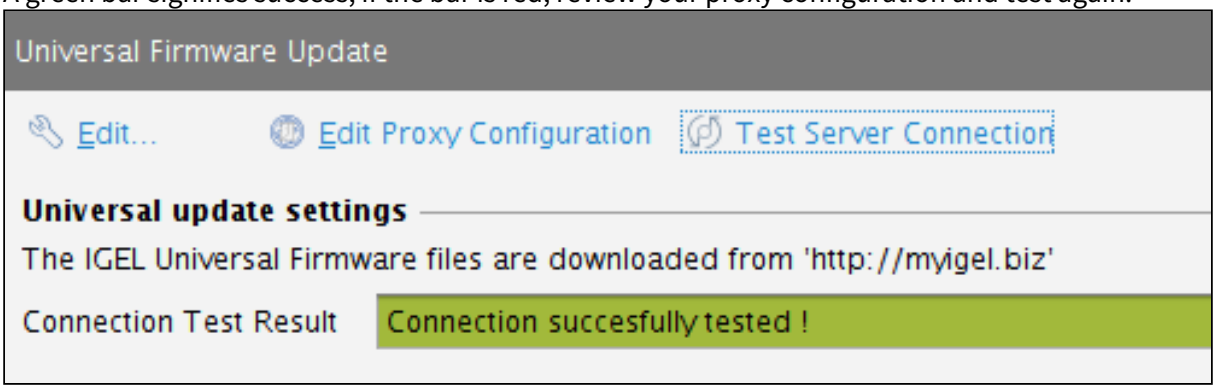
Configure an HTTP proxy for firmware downloads in UMS:

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



   The **Edit Proxy Configuration** dialog opens.
3. Check **Use proxy for HTTP connection to firmware update server**.
4. Enter the **Proxy-Host** name or IP address.
5. Enter the proxy host **Port**.
6. Enter the proxy **User**.
7. Enter the proxy **Password**.
8. Click **Save**.
   The dialog closes.

9. To test the connection via the proxy, click **Test Server Connection**.
   A green bar signifies success, if the bar is red, review your proxy configuration and test again.



Troubleshooting UMS Cannot Contact Download Server Any More

After the UMS has been updated to version 6.03.130 or higher, it can not reach the download server anymore.

Environment

- UMS 6.03.130 or higher

Problem

From UMS 6.03.130 onwards, the UMS contacts https://fwus.igel.com (port 443) instead of http://fwu.igel.com (port 80). This may be blocked by a firewall.

Solution

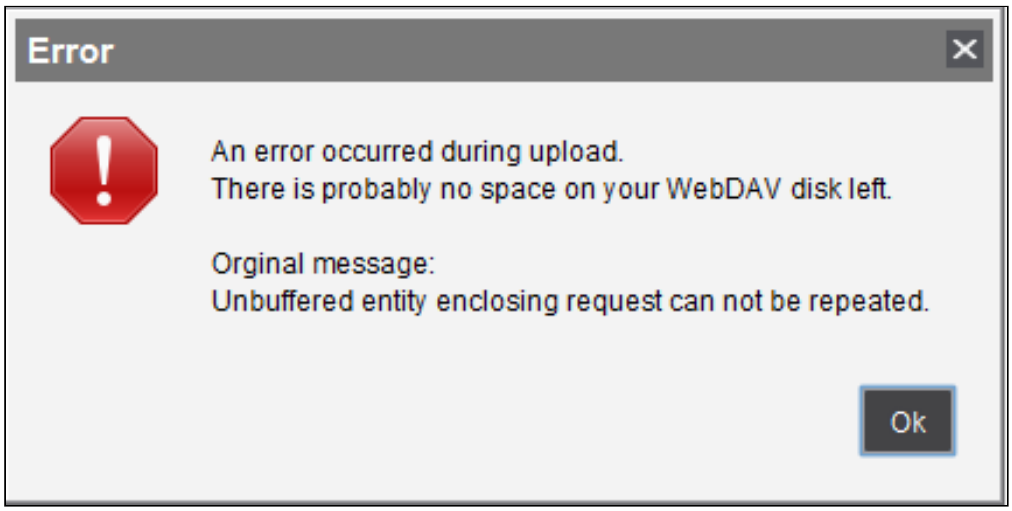
→ Allow https://fwus.igel.com (port 443) in your firewall.

Error During Firmware Upload in UMS: No Space on WebDAV

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

Issue

When importing a firmware into the UMS, the following error message appears:




```
An error occurred during upload.
There is probably no space on your WebDAV disk left.
```

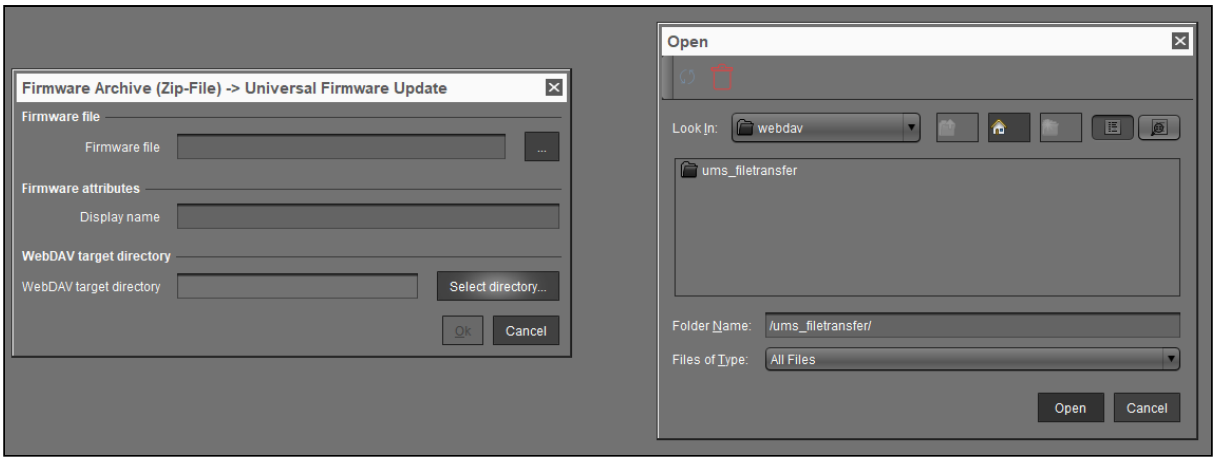
```
Original message:
Unbuffered entity enclosing request can not be repeated.
```

Cause

This error is caused when a file is being imported into a WebDAV folder which has no available space remaining.

Solution

1. Check that the host system of the UMS Server has available storage.
2. Ensure that the **ums_filetransfer** folder is selected during the firmware import process:


Firmware Archive (Zip-File) -> Universal Firmware Update
Firmware file
Firmware file
...
Firmware attributes
Display name
WebDAV target directory
WebDAV target directory
Select directory...
OK
Cancel
Open
Look In:
webdav
ums_filetransfer
Folder Name:
/ums_filetransfer/
Files of Type:
All Files
Open
Cancel

How to Configure Java Heap Size for the UMS Server

You experience performance issues with IGEL Universal Management Suite (UMS). Manifold reasons can underlie performance degradation, and there are various solutions like optimizing the UMS according to recommendations under Performance Optimizations in IGEL UMS (see page 225), expanding the server's physical RAM, switching from the embedded database to the external database, updating the UMS components, etc. The following article covers only the increase of UMS Server memory (Java heap size).

Symptom

You face performance problems and encounter memory issues in the UMS Server log files (`ums-server.log` ; see Where Can I Find the IGEL UMS Log Files? (see page 624)), e.g. `java.lang.OutOfMemoryError` .

Problem

The default Java heap size may be insufficient for the UMS Server. This usually happens if you have

- numerous jobs
- numerous administrative tasks
- a lot of concurrent device requests (e.g. hundreds of devices booting up in a narrow time frame)
- a large number of devices in the database (>10.000)
- the UMS Web App installed
- the combination of the above factors

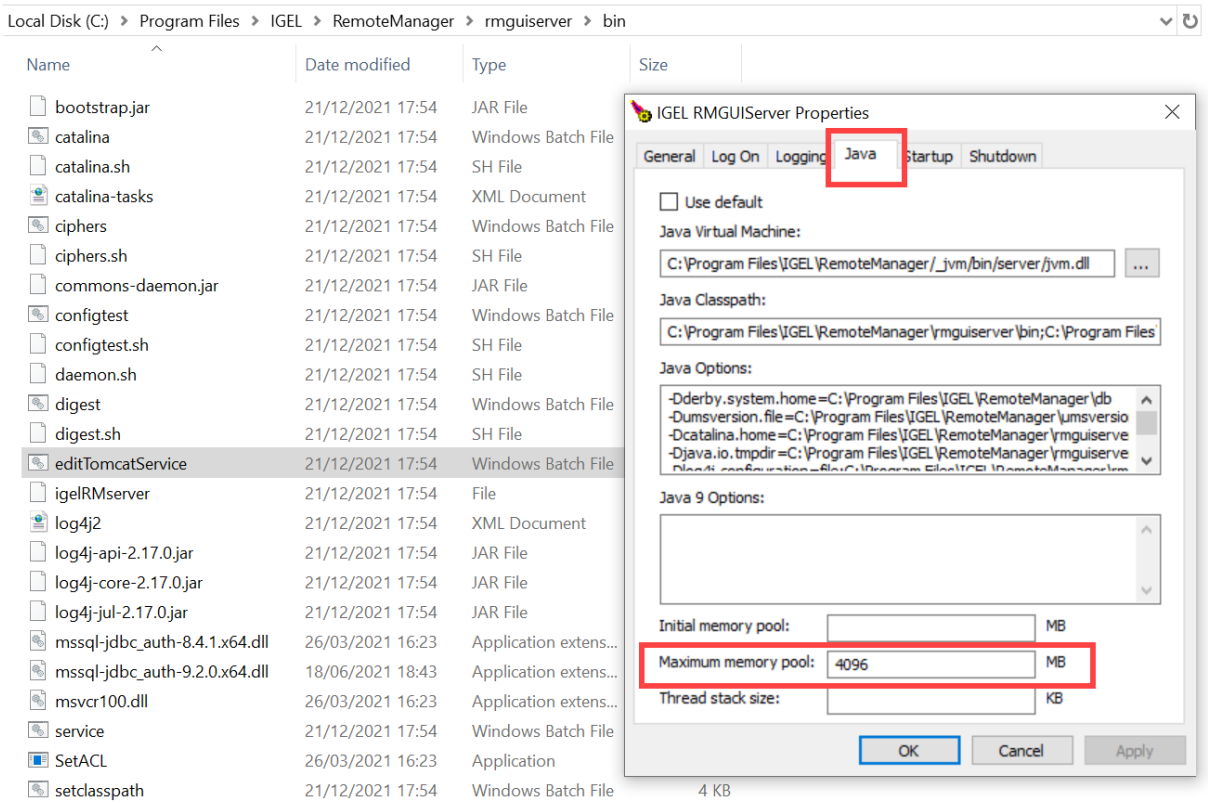
The more jobs, administrative tasks, etc. are created, the more heap is "eaten up", so there may be no memory left for additional tasks. In such situations, it can make sense to increase the Java heap size for the UMS Server.

Solution: Change Java Heap Size for the UMS Server

Windows

For the UMS Server installed on Windows, you can modify the Java heap size during the UMS update/installation. For details, see IGEL UMS Installation under Windows (see page 48). You can also modify the heap size as follows:

1. Stop the `IGEL RMGUIServer` service. For details on how you can stop it, see IGEL UMS HA Services and Processes (see page 1425).
2. Navigate to `C:\Program Files\IGEL\RemoteManager\rmguiserver\bin` .
3. Launch `editTomcatService.bat` .
4. Select the **Java** tab and adapt the **Maximum memory pool** value according to your needs. (Default: 4096 MB)



> ⚠ The Java heap size must always be defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but it must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[108]; see also the `-Xmx` option there.
>
> Note also the following:
>
> - All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Server will be unable to run.
> - Reducing the memory may affect the function of the UMS and is NOT recommended.

5. Click **Ok**.
6. Restart the `IGEL RMGUIServer` service.

Linux

For the UMS Server installed on Linux, you can modify the Java heap size as follows:

108. https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

1. Stop the UMS Server process. For details on how you can stop it, see IGEL UMS HA Services and Processes (see page 1425).
2. Edit `/opt/IGEL/RemoteManager/rmguiserver/conf/ums-server.env`
3. Find the option `CATALINA_OPTS=-Xmx4096m` and change the `-Xmx` value according to your needs. (Default: 4096 MB)

   > ⚠ The Java heap size must always be defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but it must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[109]; see also the `-Xmx` option there.
   >
   > Note also the following:
   > - All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Server will be unable to run.
   > - Reducing the memory may affect the function of the UMS and is NOT recommended.
   > - During the UMS update, the heap size value is set to the default. Therefore, you have to adapt it again.

4. Restart the UMS Server process.

109. https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

How to Configure Java Heap Size for the UMS Console

You use IGEL Universal Management Suite (UMS) and experience performance issues with the UMS Console. Manifold reasons can underlie performance degradation, and there are various solutions like optimizing the UMS according to recommendations under Performance Optimizations in IGEL UMS (see page 225), updating the UMS components, etc. The following article covers only the increase of UMS Console memory (Java heap size).

Symptom

You face performance problems and encounter memory issues in the UMS Console log files (`igel-ums-console.log` ; see Where Can I Find the IGEL UMS Log Files? (see page 624)), e.g. `java.lang.OutOfMemoryError` .

Problem

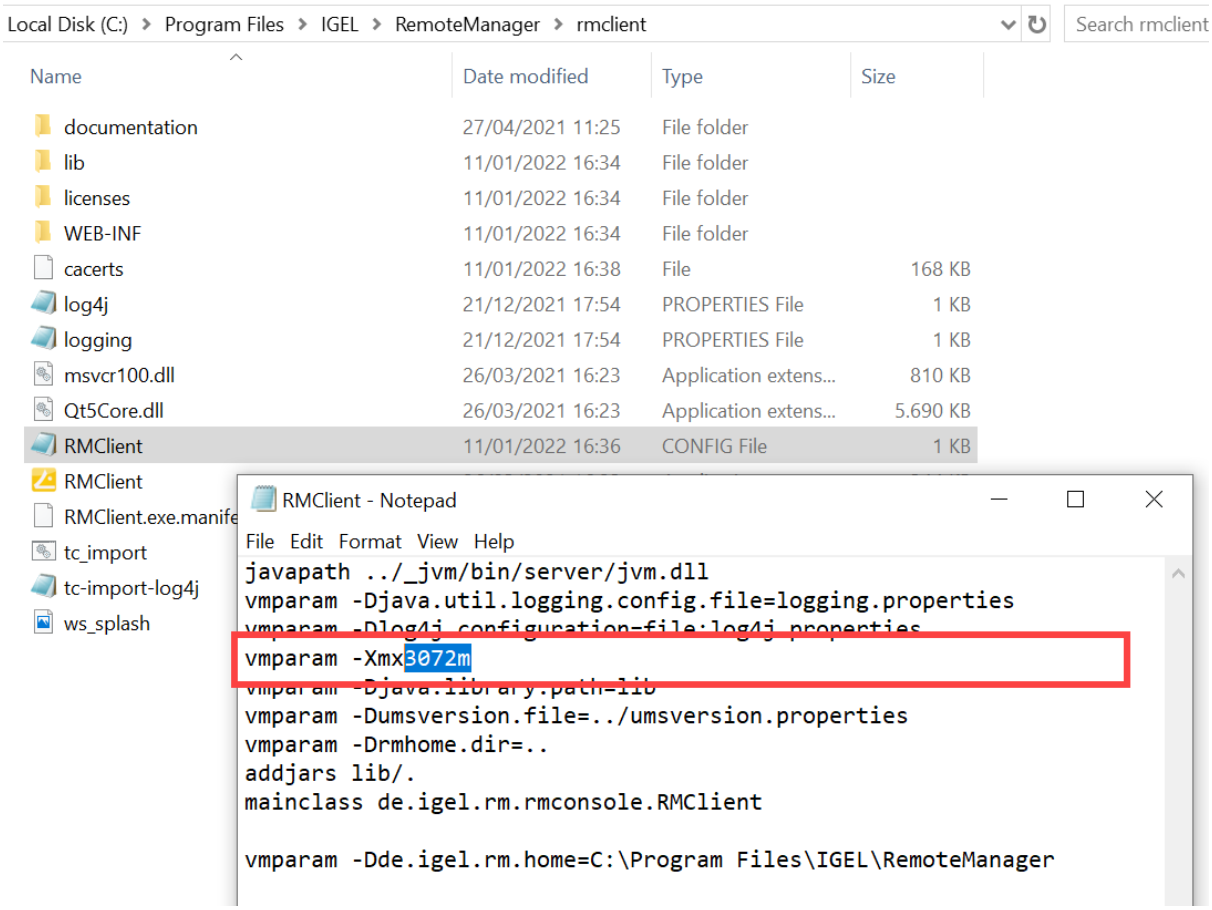
The default Java heap size may be insufficient for the UMS Console. This usually happens if you have

- a large number of devices registered (>10.000)
- a lot of devices in one folder (a flat directory structure under **Devices** in the UMS Console; >1.000 per folder)

Solution: Change Java Heap Size for the UMS Console

For the UMS Console, you can modify the Java heap size during the UMS update/installation. For details, see IGEL UMS Installation under Windows (see page 48). You can also modify the heap size as follows:

1. Close the UMS Console.
2. Open the following file:
   Default path on Windows: `C:\Program Files\IGEL\RemoteManager\rmclient\RMClient.config`
   Default path on Linux: `/opt/IGEL/RemoteManager/rmclient/RemoteManager.config`
3. Find the line `vmparam -Xmx3072m` and change the `-Xmx` value according to your needs. (Default: 3072 MB)



The Java heap size is defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[110]; see also the `-Xmx` option there.

Note also the following:

- All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Console will be unable to run.
- Reducing the memory may affect the function of the UMS and is NOT recommended.

4. Save the changes.
5. Restart the UMS Console.

110. https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution

IGEL Universal Management Suite (UMS) includes a monitoring endpoint solution, which you can integrate into your existing monitoring infrastructure (e.g. Nagios, SolarWinds, Paessler, Logic Monitor, Sensu, etc.). With the monitoring endpoint, you can check the process/service states for the IGEL UMS Server and, thus, react accordingly if any problems are detected.

IGEL Environment

- IGEL UMS 6.09.100 or higher

How to Request the Current Status of the UMS Server

Use the following requests to check the status of the UMS Server. If you use a browser for this purpose and the UMS deploys a self-signed certificate, the browser may display a security/certificate warning. Accept the risk and continue, or make the certificate known to the browser.

https://[server]:[web_server_port]/ums/check-status

OR

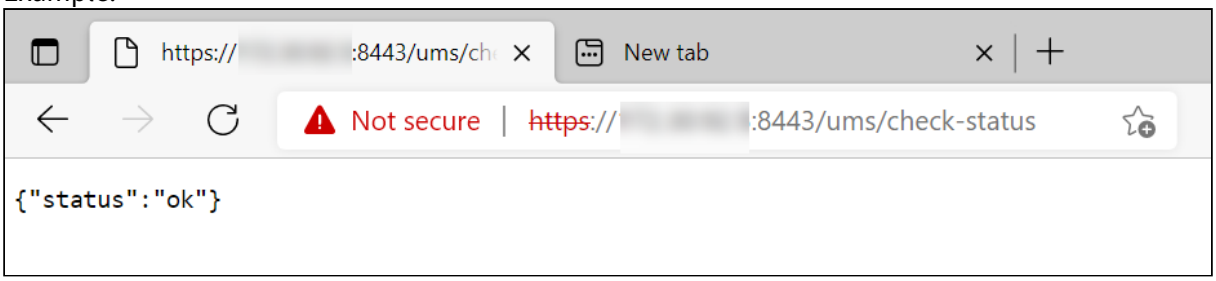
`http://[server]:[jws_server_port]/ums/check-status`

The following responses are possible:

- If the (check status) service is up and running, HTTP status code 200 is returned. The response body contains a `JSON` document with information on the UMS Server status:
  `{“status”: ”init|ok|warn|err”}`

  For the details, see Monitoring the UMS Server: Possible Statuses (see page 501) below.

  Example:

- If the check status service is not reachable, HTTP status code 404 is returned.
- Other common HTTP status codes indicating standard HTTP errors might occur.

Note that the status of the server updates every minute. For performance reasons, the status is NOT recalculated on each monitoring request, i.e., if a monitoring request is received, but a one-minute interval is not over, the previously saved server status will be shown.

Monitoring the UMS Server: Possible Statuses

The response statuses returned during the monitoring of the UMS Server indicate the following situations:

ok	The server is up and running.
warn	• The server is in HA (see page 1387) update mode; see Updating the Installation of an HA Network (see page 1407). • The server is not connected to one or more configured IGEL Cloud Gateways; see (12.04-en) How to Connect the IGEL UMS to the ICG . • Certificates used for communication with endpoint devices (see page 896), i.e., certificates of the `tc.keystore` file, are not in sync with the database. This might happen, for example, if you make changes to certificates and the automatic synchronization stops functioning due to some network issues or if the IGEL network token differs between the components, e.g., when a wrong network token was chosen during the server installation.
err	• There is no database connection – no database is configured, or the database connection has failed. For where to configure the database, see How to Set Up a Data Source in the IGEL UMS Administrator (see page 1073). • The device communication port is not ready. For where to configure the device communication port, see Settings - Change Server Settings in the IGEL UMS Administrator (see page 1038); for details on UMS ports, see IGEL UMS Communication Ports (see page 256).
init	Server initialization has not been completed yet. Note: If the initialization process is not finished within 120 seconds, the status automatically changes to **err**.

Related Topics

(12.04-en) How to Monitor the IGEL Cloud Gateway

Monitoring Device Health and Searching for Lost Devices (see page 543)

UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems (see page 1420)

How to Start with IGEL with Limited or No Internet Access (Air-Gapped Environment)

This article gives you an overview on how you can operate your IGEL environment with limited or no internet access. We list here the topics that require special handling in such an environment and links to detailed instructions. The order of topics follows the logic of starting new with IGEL.

What You Need for the IGEL Environment

Similar to a normal IGEL environment, you will use several products and services to operate IGEL without internet.

The core environment that requires no internet access is made up of:

- IGEL Universal Management Suite (UMS) 12 - for managing IGEL OS 12 and IGEL OS 11 devices.

> Use version UMS 12.04.120 or higher, as some features supporting the internetless operation are available from this version.

- IGEL OS 12 or IGEL OS 11

Essential cloud-based services that require internet access, but are not connected to the IGEL UMS or the IGEL OS:

- https://cosmos.igel.com/csm - where you register your company account, invite other users and assign them specific roles, e.g. for opening support cases.
- https://app.igel.com/ - where you can find and download all applications currently available for IGEL OS 12 to then distribute them through the UMS.
- https://activation.igel.com/login - where you manage licenses for your IGEL OS devices and IGEL UMS.

Using the IGEL Customer Portal

Registering your company account in the IGEL Customer Portal is the first step to start using IGEL products. After registration, you can also reach IGEL Support through the IGEL Customer Portal. For detailed instructions, see https://kb.igel.com/display/howtocosmos/Registering+for+the+IGEL+Customer+Portal and https://kb.igel.com/display/howtocosmos/Managing+Users+and+Roles+in+the+IGEL+Customer+Portal .

Installing and Configuring UMS 12

- For details on how to install IGEL Universal Management Suite (UMS) 12 and what should be considered during the installation, see https://kb.igel.com/display/howtocosmos/Installing+or+Upgrading+to+IGEL+UMS+12.
- For the basic configuration of the UMS, follow the section First Steps in the IGEL UMS in https://kb.igel.com/display/howtocosmos/IGEL+UMS+12%3A+Basic+Configuration .

> Since the UMS cannot connect to the IGEL License Portal (ILP), you need to manually license your UMS. For details, see https://kb.igel.com/en/igel-subscription-and-more/current/how-to-license-the-igel-ums .

Distributing Apps to OS 12 Devices - UMS as App Proxy

To distribute apps to the IGEL OS 12 devices, first you have to configure your UMS as an Update Proxy under **Apps > Settings > UMS as an Update Proxy**:

1. Under **Devices should download the apps from** select **Download from UMS.**
2. Enable the **Enable Automatic Cleanup of unused Versions** parameter.
3. Enable the **Block devices from downloading apps from the public App Portal as a fallback option** parameter.
   For details, see Configuring Global Settings for the Update of IGEL OS Apps (see page 1342) .
4. Optionally, configure distributed app repositories as described in How to Use Distributed App Repositories in IGEL UMS (see page 427) .

> To distribute apps, you will have to manually download them from the IGEL App Portal and upload them to the UMS as described in How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access (see page 1305) .
> Keep this difference in mind as you follow the instruction in https://kb.igel.com/display/howtocosmos/IGEL+UMS+12%3A+Basic+Configuration , and instead of importing IGEL OS Apps from the IGEL App Portal, use the manual process.

Installing the IGEL OS 12 Base System on the Device

IGEL OS 12

For instructions on how to install the OS 12 Base System on the device, see https://kb.igel.com/pages/viewpage.action?pageId=77865870 or https://kb.igel.com/display/basesystem124/How+to+Use+IGEL+OS+12+with+UD+Pocket , depending on your use case.

IGEL OS 11

For instructions on how to install the OS 11 on the device, see the following methods:

- https://kb.igel.com/display/igelos1110/IGEL+OS+Creator+1
- https://kb.igel.com/igelos-11.10/en/igel-os-creator-for-windows-oscw-126857733.html
- https://kb.igel.com/display/igelos1110/IGEL+UD+Pocket+Manual

Licencing IGEL Devices

Licenses for IGEL products can be managed through the IGEL License Portal (ILP). Since the UMS does not have access to the internet, it cannot connect to the ILP. Therefore, you need to use the manual license deployment process described in https://kb.igel.com/display/licensesmoreigelos11/Manual+License+Deployment+for+IGEL+OS for IGEL device licensing.

Onboarding Devices

Options to onboard OS 12 devices

- Alternative Onboarding with One-time password method as described here: https://kb.igel.com/display/howtocosmos/Onboarding+IGEL+OS+12+Devices (Second Subtitle)
- Scanning the Network , as described here: How to Scan the Network for Devices and Register Devices on the IGEL UMS (see page 1136)
- Importing device data beforehand: Importing Devices (see page 1143)

Options to onboard OS 11 devices

- Scanning the Network , as described here: How to Scan the Network for Devices and Register Devices on the IGEL UMS (see page 1136)
- Importing device data beforehand: Importing Devices (see page 1143)
- Use the UMS Registration to trigger the onboarding from the device: https://kb.igel.com/display/igelos1107/Using+UMS+Registration+Function

Managing Devices

Upgrading from IGEL OS 11 to IGEL OS 12

⚠ Use IGEL OS 11.09.260 or later as a starting point, as many upgrade-related issues have been fixed with that version. You can find further requirements in Upgrading (Migration) from IGEL OS 11 to IGEL OS 12[111].

For the upgrade you need to download the Base System app from the IGEL App Portal and import in the UMS Web App, as described in How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access (see page 1305) .

ℹ If you are planning to use the unattended upgrade method, download IGEL OS 12.2.1 or later. With lower versions of IGEL OS 12, a manual reboot is required to finish the upgrade.

You can do the rest of the upgrade as described in https://kb.igel.com/en/igel-os/11.10/upgrading-migration-from-igel-os-11-to-igel-os-12 .

Updating the Base System & App Versions

After the manual upload of apps to the UMS Web App, app management is the same as for any other environment. For information on how to manage apps through the UMS Web App, see:

- How to Configure Update Settings for Apps in the IGEL UMS Web App (see page 1337)

111. https://kb.igel.com/display/igelos1110/Upgrading+%28Migration%29+from+IGEL+OS+11+to+IGEL+OS+12

How to Deploy a Wake on LAN Proxy for Distributed Environments in IGEL

When the UMS is residing outside the network which contains your devices, it cannot wake up your devices by Wake on LAN. In this case, you can make a device act as a proxy which sends the Wake on LAN packets on behalf of the UMS, so that the UMS can wake up your devices from outside their network.

> To use the feature, you need to use UMS version 5.02.100 or higher and devices running IGEL OS version 5.09.100 or higher.
> To use the feature with IGEL OS 12 devices, you need to use UMS version 12.06.100 or higher and IGEL OS version 12.5.1 or higher.

For details, see:

- How to Use a WoL Proxy for Waking up Devices in the IGEL Environment (see page 507)
- Distributing Wake on LAN Packets (see page 509)
- How to Remove a Wake on LAN Proxy in IGEL UMS (see page 510)

How to Use a WoL Proxy for Waking up Devices in the IGEL Environment

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

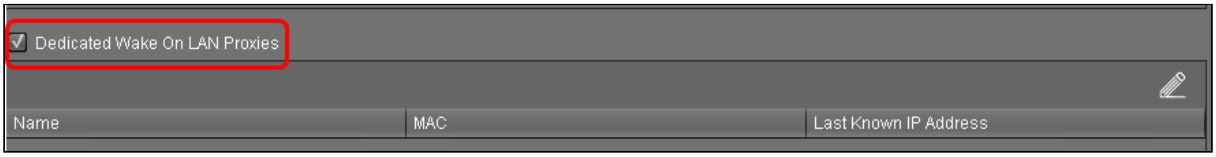
> To use the feature, you need to use UMS version 5.02.100 or higher and devices running IGEL OS version 5.09.100 or higher.
> To use the feature with IGEL OS 12 devices, you need to use UMS version 12.06.100 or higher and IGEL OS version 12.5.1 or higher.

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

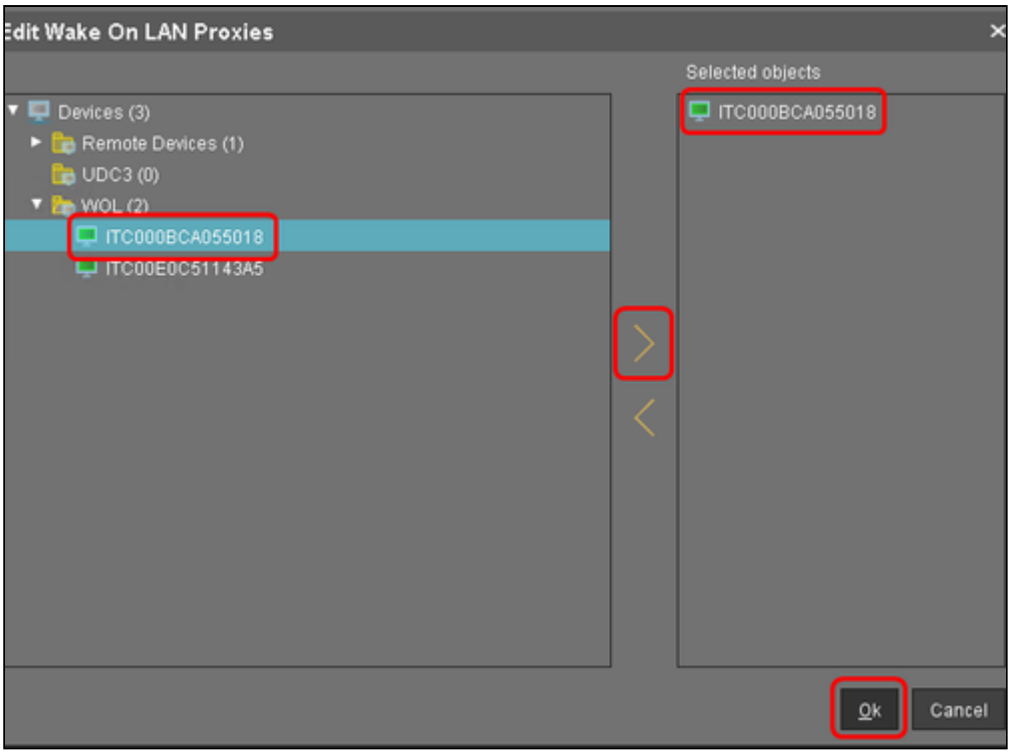
For detailed information, see the Wake on LAN (see page 981) chapter in the UMS Reference Manual.

To define a dedicated Wake-on-LAN proxy:

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



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



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

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

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

Distributing Wake on LAN Packets

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

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

UMS supports sending Wake on LAN magic packets to

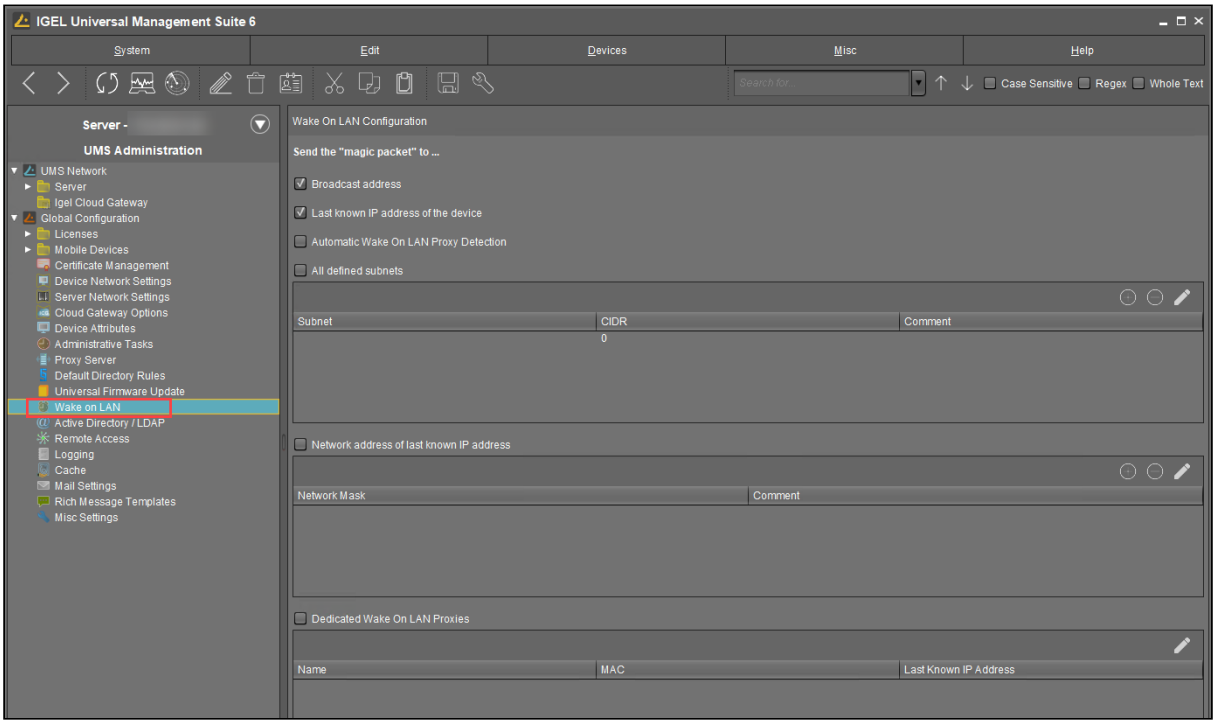
- the broadcast address
- the last known IP address of the device
- all defined subnets
- the network address of the last known device IP address (define one or more network masks to be applied)
- a dedicated Wake on LAN proxy to wake up thin clients in another network; see How to Use a WoL Proxy for Waking up Devices in the IGEL Environment (see page 507)

How to Remove a Wake on LAN Proxy in IGEL UMS

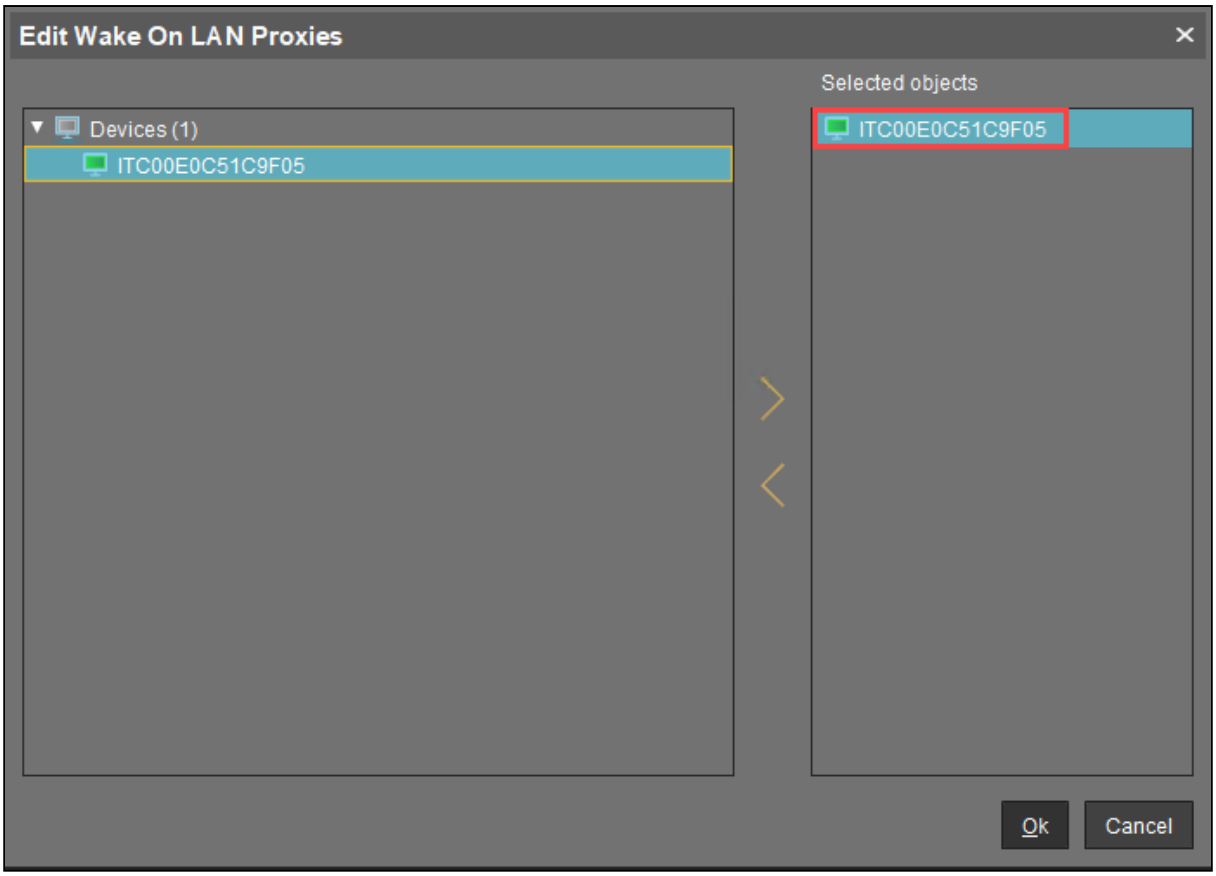
You can remove the Wake on LAN proxy function from a device through the IGEL Universal Management Suite (UMS).

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

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



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



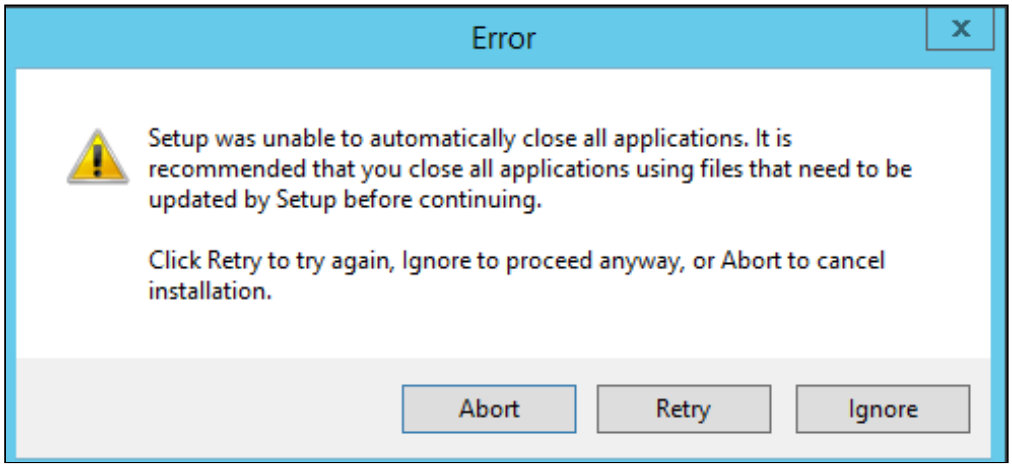
6. Click  .
7. Click **Ok**.
   The selected device is no longer configured as a Wake on LAN proxy. As soon as the device has received its settings from the UMS, it can be set to standby and shut down as normal. In the device's registry, the parameter **system > remotemanager > wol_proxy > enabled**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

High Availability UMS

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

Symptom

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

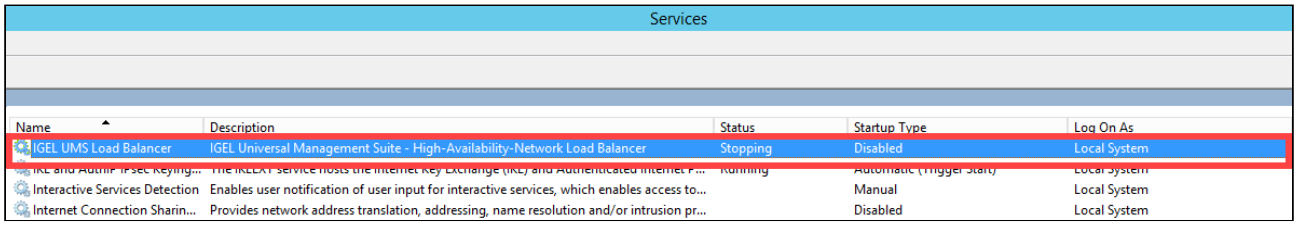


Environment

- UMS HA installation

Problem

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



Solution

→ Stop the load balancer manually and proceed with the update. For information regarding stopping the HA services, see IGEL UMS HA Services and Processes (see page 1425).

Which Files Are Automatically Synchronized between the IGEL UMS Servers?

You have a multi-instance IGEL Universal Management Suite (UMS) installation (see page 13) and want to know which files are automatically synchronized between the servers.

Prerequisites

- A High Availability (HA) environment with UMS version 6.06.100 or higher
- A Distributed UMS installation with UMS version 6.10.100 or higher

General Overview

The following files are synchronized between the UMS Servers automatically:

- Files registered in the UMS Console

  > Files that are not created as file objects in UMS, but only stored in the file system in `ums_filetransfer`, are NOT synchronized. For details on how/where you can create a file object, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices (see page 1123) and How to Create Corporate Identity Customization in the IGEL UMS Console (see page 765).

- The files of Universal Firmware Updates (see page 856) if the synchronization is enabled under **UMS Administration > Global Configuration > Universal Firmware Update** and a WebDAV directory is set as the target path for the download. For details, see the section "Synchronization of Universal Firmware Updates (see page 514)" below.

The objects are synchronized immediately – unless a UMS Server is temporarily unreachable. In that case, the synchronization takes place every 5 minutes or at server startup.

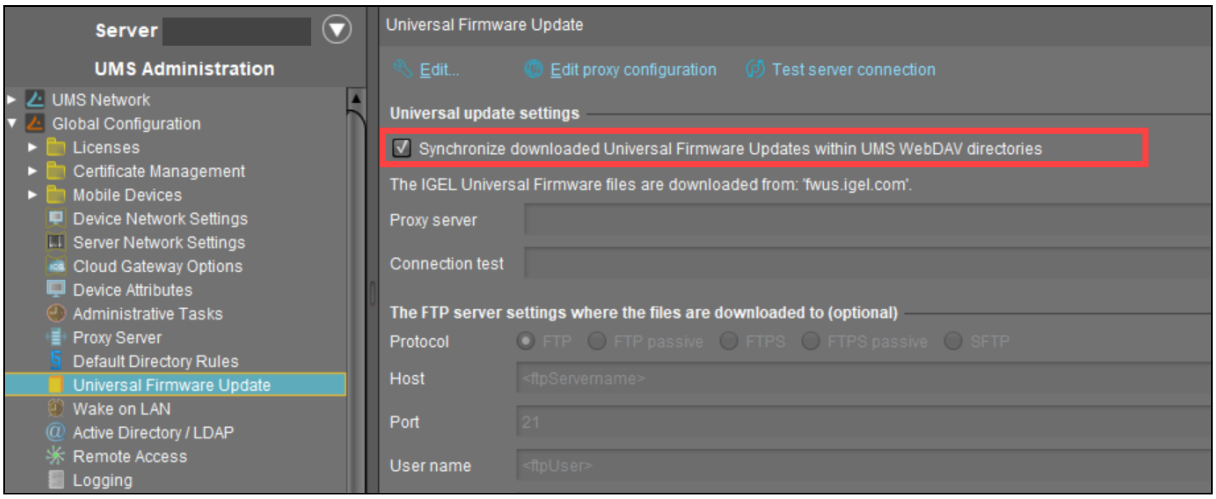
The synchronization applies to the file system and does not refresh the view in any UMS Console other than the one in which the object has been created. Thus, you may need to press [F5] or the refresh button to view the object in the UMS Console on the other server.

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

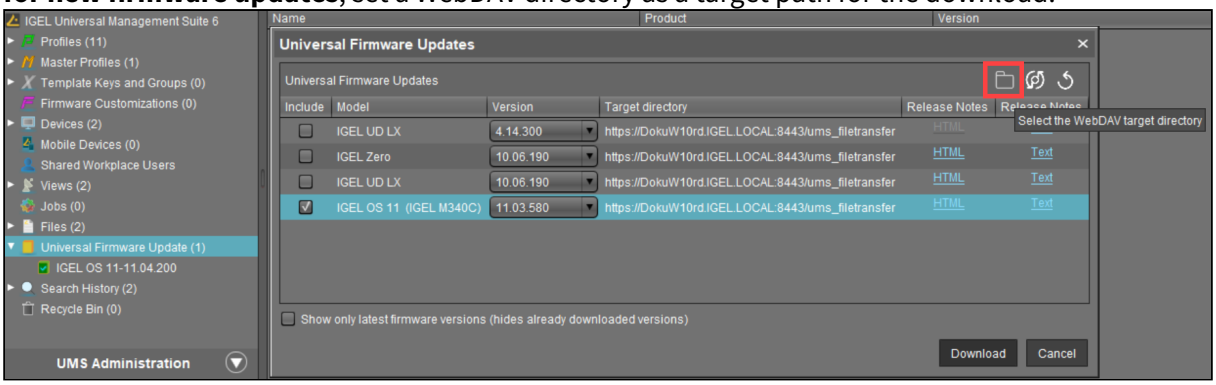
Synchronization of Universal Firmware Updates

To enable the automatic synchronization of the firmware updates between the UMS Servers, proceed as follows:

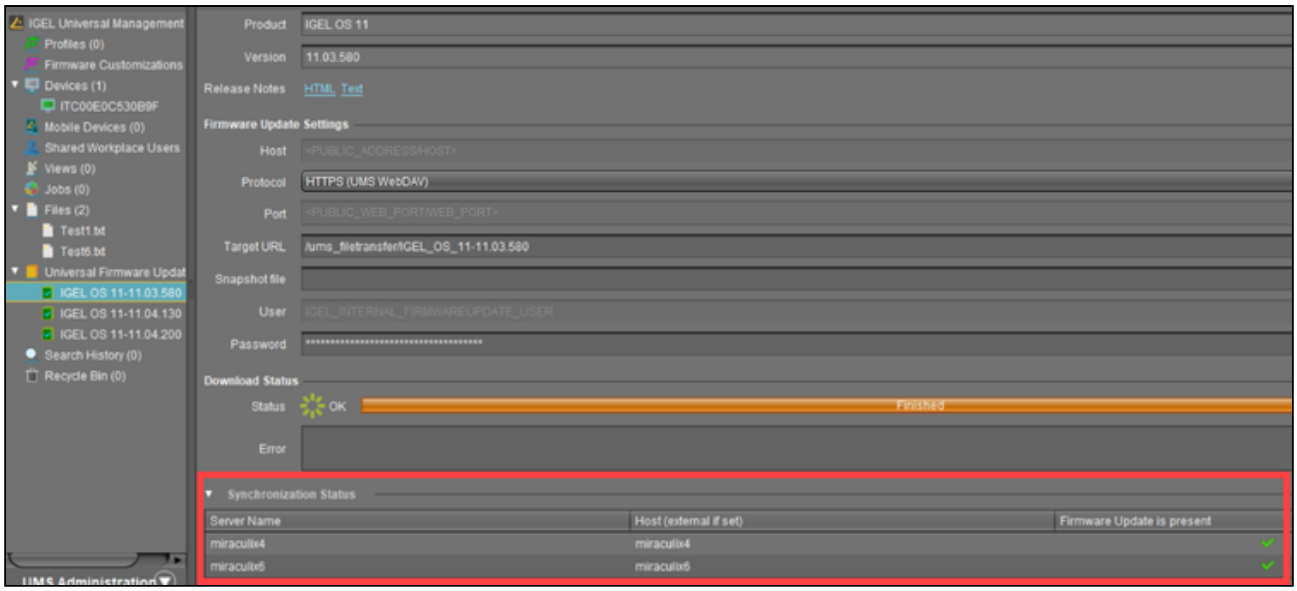
1. In the UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**.
2. Activate **Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories**.



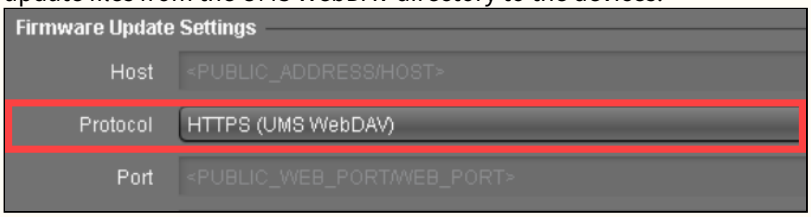
3. When adding a firmware update under **Universal Firmware Update > [context menu] > Check for new firmware updates**, set a WebDAV directory as a target path for the download.



When the download is complete, you can see under **Synchronization Status** the servers for which the firmware update has already been synchronized.



Universal Firmware Updates are synchronized between the UMS Servers only if **HTTPS (UMS WebDAV)** or **HTTP (UMS WebDAV)** is selected under **Protocol**. These protocols are used for transferring the firmware update files from the UMS WebDAV directory to the devices.



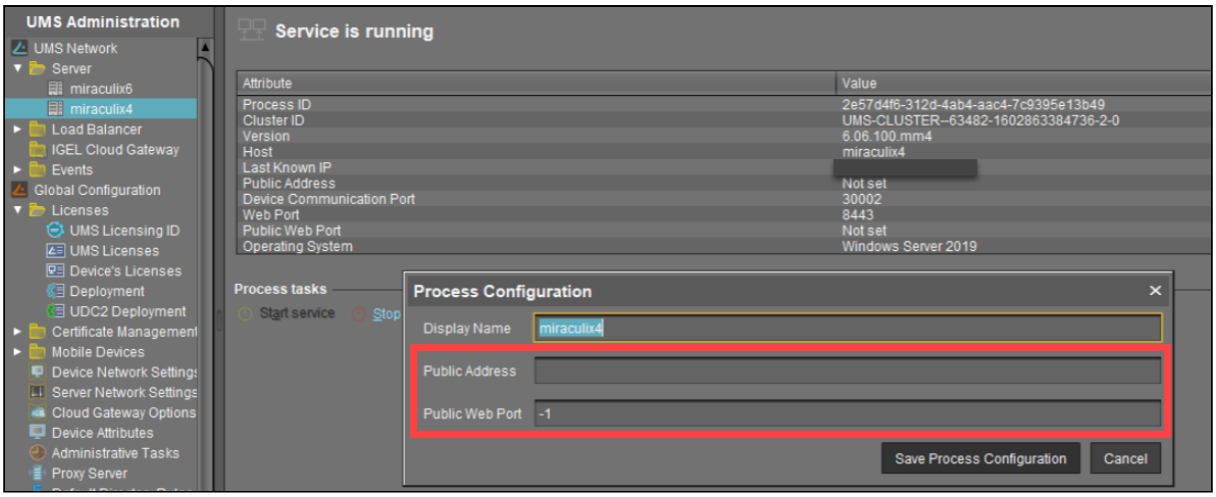
With any other protocol, firmware updates are not synchronized between the servers.

Connection Data Used during the Update

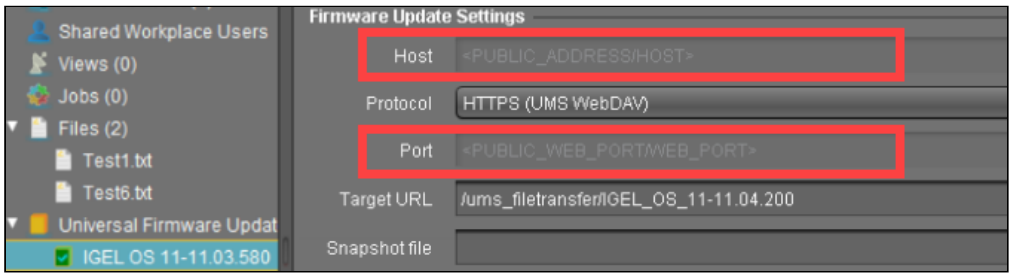
When a firmware update is assigned to a device, the connection information of the current server is sent to the device if the firmware update is present in the UMS WebDAV directory of the server. If the firmware update is absent for some reason, the connection information of a server with the firmware update available is sent.

The connection information contains

- a **Public Address** if it is configured for the server under **UMS Administration > UMS Network > Server > [server's context menu] > Edit**. Otherwise, the stored hostname is used.
- a **Public Web Port** if it is configured for the server under **UMS Administration > UMS Network > Server > [server's context menu] > Edit**. Otherwise, the stored web port is used.



Since the connection information is dynamically adjusted, **Host** and **Port** data are not editable for the downloaded firmware update (with the HTTP(S) (UMS WebDAV) protocol set):



Load Distribution with a Number of Load Balancers

If a UMS Server and Load Balancer are installed on a shared computer, the UMS Server communicates with the IGEL OS 11 devices via port 30002, otherwise via port 30001 as is customary with a single server installation. The Load Balancer always communicates with the IGEL OS 11 devices via port 30001.

Load distribution to the load balancers can be performed as follows. When booting, the OS 11 devices attempt to establish contact with the UMS Server in this order:

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

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

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

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

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

Troubleshooting: License Error Because HA Servers Are out of Sync

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

Symptom

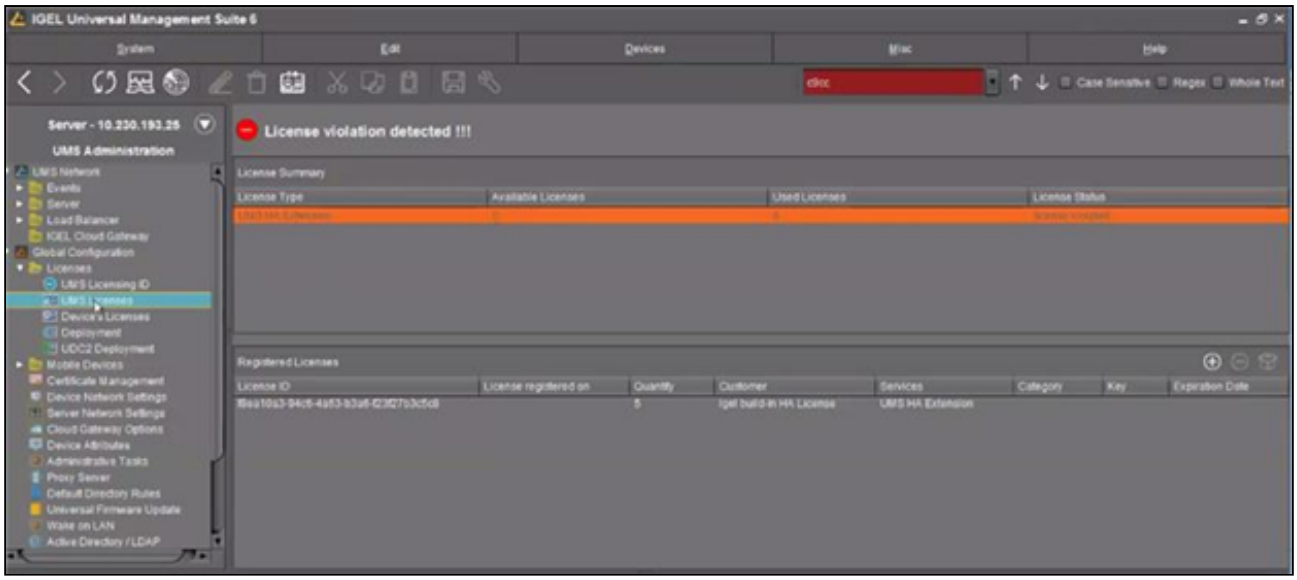
HA servers are out of sync preventing devices from registering in the UMS and throwing a license error.

Environment

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

Problem

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



Solution

Issue is related to the UMS ID. If a restart of the out-of-sync server does not help, a workaround / solution is to back up the UMS ID from the UMS Administrator and restore it to the out-of-sync server. See Manual Synchronization of the UMS ID (see page 521).

How to Manually Synchronize the UMS ID

When the main UMS ID is not synchronized between the IGEL UMS Servers, **UMS ID status** under **UMS Administration > Global Configuration > UMS ID** reads "Not in sync, please restart server", see UMS ID (see page 964). However, even when you restart the UMS Server, the UMS ID sometimes remains unsynchronized. In this case, the manual synchronization is required.

Environment

- UMS 12.01.100 or higher
- High Availability (HA) or Distributed UMS environment

Instructions

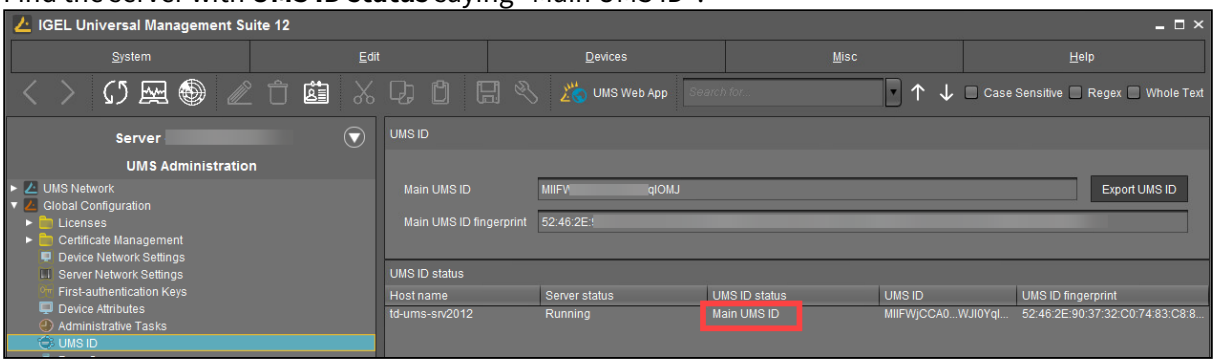
The manual synchronization of the UMS ID includes the following steps:

1. Locating the server holding the main UMS ID (see page 521)
2. Creating a backup of the UMS ID (see page 521) on that server
3. Restoring the created backup on all servers with the UMS ID unsynchronized (see page 522) and restarting all servers

Locating the Server Holding the Main UMS ID

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

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



Creating a Backup of the UMS ID

1. Open the UMS Administrator on the server with the main UMS ID you located in the previous step.
2. Go to **UMS ID Backup** and create a backup as described under UMS ID Backup in the IGEL Administrator (see page 1043).
3. Transfer the created backup to every server where the UMS ID is not in sync.

Restoring the Backup on All Servers with the UMS ID Unsynchronized

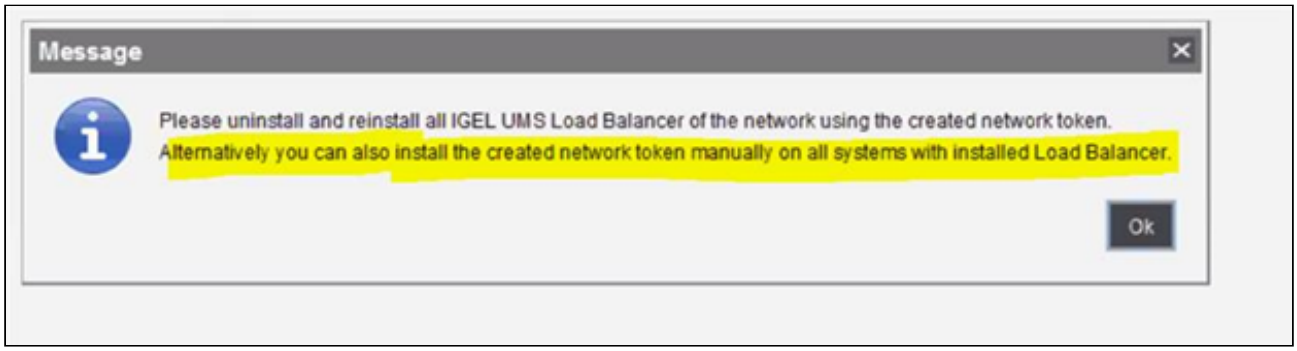
1. Open the UMS Administrator on every server where the UMS ID is not in sync.
2. Go to **UMS ID Backup** and restore the backup as described under UMS ID Backup in the IGEL Administrator (see page 1043).
3. Repeat the procedure for all servers with the UMS ID unsynchronized.
4. When the backup restoring procedure is complete, restart all servers if you have not yet done so. In the UMS Console, the **UMS ID status** under **UMS Administration > Global Configuration > UMS ID** should show that the UMS ID is now synchronized on all servers.

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

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

Symptom

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



Environment

- UMS HA; UMS version: any

Solution

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

How to Migrate a UMS High Availability Installation to a Standalone UMS

This article describes a step-by-step procedure to manually migrate from a High Availability IGEL Universal Management Suite (UMS) to a Standard UMS installation. You can find the procedure for Windows and for Linux.

You can use this procedure, for example, if you are currently using IGEL Load Balancers with one UMS Server as a HA installation but do not need that anymore because OS12 devices do not use the Load Balancers for the communication. It can either be used:

- on an existing installation of UMS 6 or UMS 12 if you want to keep your installed version.
- during an upgrade to UMS 12.

Before the migration, learn about the differences between High Availability UMS and Standard UMS under IGEL UMS Installation (see page 13).

The migration procedure consists of the following tasks:

1. Removal of some objects from the current installation which indicate High Availability to the installer, like UMS Watchdog, Load Balancer, and config file for ActiveMQ.
2. Normal installation or upgrade workflow with downtime. For details, see Updating HA Installation: With Downtime of the Servers (igel.com)[112].
3. Validation of the installation.

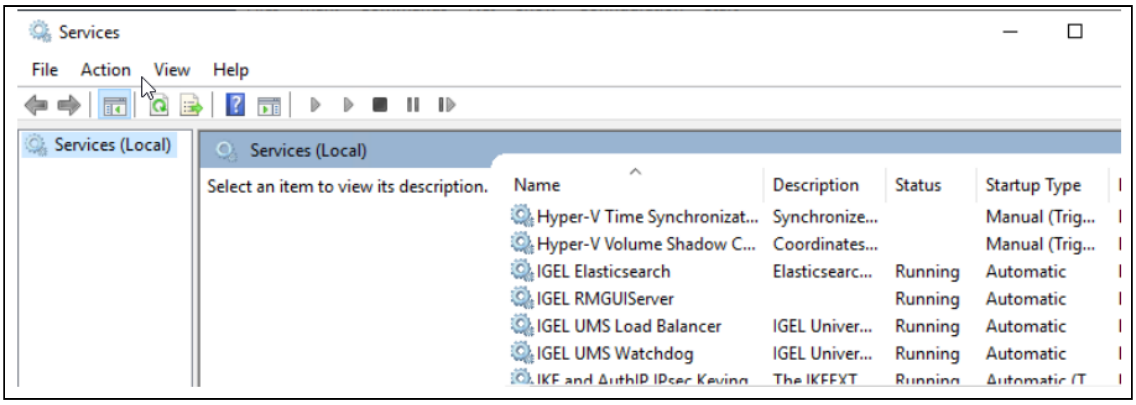
Switch the Installation on Windows

Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All the steps must be executed with Administrator privileges:

1. Stop the UMS Server service on all servers.
2. Choose the server you want migrate for the next steps.
    a. Go to the installation folder of the UMS.
    b. Stop the Windows Services for the Load Balancer and the Watchdog.

112. https://wiki.test.toolchain.igel.kreuzwerker.net/endpointmgmt-12.03/en/updating-ha-installation-with-downtime-of-the-servers-108342809.html



c. Execute the following commands in the Windows command shell:
   - `umswatchdog\etc\bin\jsl.exe -remove`
   - `umsbroker\etc\bin\jsl.exe -remove`

   Both Windows Services should now be removed from the Windows Services.
d. Delete the folders `umswatchdog` and `umsbroker` from the installation home directory.
e. Delete the file `rmguiserver\conf\IAMQ_info_storage.xml`.
f. Reinstall the current UMS version or upgrade the UMS.
g. You should get the possibility to choose Standard UMS in the selection dialog of the installation. Choose Standard UMS and finish the installation.
h. Verify in the UMS Administrator that the Device Communication Port is set to 30001.
i. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is not selected. If it is selected, deselect it and restart the UMS.

3. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.
4. Update load balancing configurations if they are using UMS Load Balancer addresses.
5. Uninstall UMS on the other servers if you are happy with the Standard UMS.

Switch the Installation on Linux

⚠ Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All steps must be executed with Administrator privileges. We omit *sudo* in the following description:

1. Stop the UMS Server service on all servers.
2. Choose the server you want to migrate for the next steps.
   a. Go to the installation folder of the UMS.
   b. Stop the Windows Services for the Load Balancer and the Watchdog:
      - `systemctl stop igel-ums-broker.service`
      - `systemctl disable igel-ums-broker.service`

- `rm /etc/systemd/system/igel-ums-broker.service`
- `systemctl stop igel-ums-watchdog.service`
- `systemctl disable igel-ums- watchdog.service`
- `rm /etc/systemd/system/igel-ums- watchdog.service`

c. Delete the folders `umswatchdog` and `umsbroker` from the installation home directory.
d. Delete the file `rmguiserver/conf/IAMQ_info_storage.xml`.
e. Reinstall the current UMS version or upgrade UMS.
f. You should get the possibility to choose Standard UMS in the selection dialog of the installation. Choose Standard UMS and finish the installation.
g. Verify in the UMS Administrator that the Device Communication Port is set to 30001.
h. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is not selected. If it is selected, deselect it and restart the UMS.

3. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.
4. Update load balancing configurations if they are using UMS Load Balancer addresses.
5. Uninstall UMS on the other servers if you are happy with the Standard UMS.

Final Steps - Validation

To validate the Standard UMS installation you can do the following:

- Test the communication to some devices.
- Check if IGEL Cloud Gateway (ICG) is still connected to the UMS Server.
- Perform other checks that you do after an upgrade of UMS.

How to Migrate a UMS High Availability Installation to a Distributed UMS

This article describes a step-by-step procedure to manually switch from a High Availability IGEL Universal Management Suite (UMS) to a Distributed UMS installation. You can find the procedure for Windows and for Linux.

Before the migration, learn about the differences between High Availability UMS and Distributed UMS under IGEL UMS Installation (see page 13).

The migration procedure consists of the following tasks:

1. Removal of some objects from the current installation which indicate High Availability to the installer, like UMS Watchdog, Load Balancer, and config file for ActiveMQ.
2. Normal installation or upgrade workflow with downtime. For details, see Updating HA Installation: With Downtime of the Servers (igel.com)[113].
3. Validation of the installation.

Switch the Installation on Windows

Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All the steps must be executed with Administrator privileges:

1. Stop the UMS Server service on all servers.
2. Choose one server and perform the following:
    a. Go to the installation folder of the UMS.
    b. Stop the Windows Services for the Load Balancer and the Watchdog.
    c. Execute the following commands in the Windows command shell:
        - `umswatchdog\etc\bin\jsl.exe -remove`
        - `umsbroker\etc\bin\jsl.exe -remove`

        Both Windows Services should now be removed from the Windows Services.
    d. Delete the folders *umswatchdog* and *umsbroker* from the installation home directory.
    e. Delete the file *rmguiserver\conf\IAMQ_info_storage.xml.*
    f. Reinstall the current UMS version or upgrade the UMS.
    g. You should get the possibility to choose Distributed UMS in the selection dialog of the installation. Choose Distributed UMS and finish the installation.
    h. Verify in the UMS Administrator that the Device Communication Port is set to 30001.
    i. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is selected.
3. Execute step 2 for the remaining servers. This can be done in parallel.

113. https://wiki.test.toolchain.igel.kreuzwerker.net/endpointmgmt-12.03/en/updating-ha-installation-with-downtime-of-the-servers-108342809.html

4. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.
5. Update load balancing configurations if they are using UMS Load Balancer addresses.

Switch the Installation on Linux

⚠ Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All steps must be executed with Administrator privileges. We omit *sudo* in the following description:

1. Stop the UMS Server service on all servers.
2. Choose one server and perform the following:
    a. Go to the installation folder of the UMS.
    b. Stop the Windows Services for the Load Balancer and the Watchdog:
        - `systemctl stop igel-ums-broker.service`
        - `systemctl disable igel-ums-broker.service`
        - `rm /etc/systemd/system/igel-ums-broker.service`
        - `systemctl stop igel-ums-watchdog.service`
        - `systemctl disable igel-ums- watchdog.service`
        - `rm /etc/systemd/system/igel-ums- watchdog.service`
    c. Delete the folders *umswatchdog* and *umsbroker* from the installation home directory.
    d. Delete the file *rmguiserver/conf/IAMQ_info_storage.xml.*
    e. Reinstall the current UMS version or upgrade UMS.
    f. You should get the possibility to choose Distributed UMS in the selection dialog of the installation. Choose Distributed UMS and finish the installation.
    g. Verify in the UMS Administrator that the Device Communication Port is set to 30001.
    h. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is selected.
3. Execute step 2 for the remaining servers. This can be done in parallel.
4. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.
5. Update load balancing configurations if they are using UMS Load Balancer addresses.

Final Steps - Validation

To validate the Distributed UMS installation you can do the following:

- Test the communication to some devices.
- Check if IGEL Cloud Gateway (ICG) is still connected to all UMS Servers.
- Create a ‘Save Support Information’ archive. The archive should contain log files from all UMS Servers.

- Perform other checks that you do after an upgrade of UMS.

Troubleshooting: UMS 12 HA Not Working After Upgrade

Problem

The UMS HA is not starting correctly after an upgrade from UMS 6 to UMS 12.

Environment

- UMS 12 HA Installation
- Windows Server

Solution

Enable the TCP/IPv6 option in the network adapter settings of the Windows server. For more details on installation requirements, see HA: Installation Requirements (see page 1392) .

Device

Troubleshooting: Device Scan or Online Check Fails

Symptom

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

Problem

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

Solution

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

See also IGEL UMS Communication Ports (see page 256).

Troubleshooting Registration of a Device via Scanning for Devices Fails

The following article explains the possible reasons and solutions for device registration failure in the IGEL Universal Management Suite (UMS) when using the scan and register method. For details on the method, see How to Scan the Network for Devices and Register Devices on the IGEL UMS (see page 1136) .

Symptom

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

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

Problem

This may be caused by

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

Solution

Solving the Certificate Problem

> **For IGEL OS 12 and IGEL OS 11 devices**:
> If you cannot register your endpoint device in the UMS, it is recommended to check initially 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 more information on the recycle bin, see How to Use the Recycle Bin in the IGEL UMS Web App[114] or Recycle Bin - Deleting Objects in the IGEL UMS[115].

With OS 11 devices:

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

OR

114. https://kb.igel.com/en/universal-management-suite/current/how-to-use-the-recycle-bin-in-the-igel-ums-web-app
115. https://kb.igel.com/en/universal-management-suite/current/recycle-bin-deleting-objects-in-the-igel-ums

→ If you know from which UMS Server exactly the device has received the certificate and have access to this UMS Server, you can remove the certificate as described under How to Remove a UMS Certificate from an OS 11 Device (see page 639).

With OS 11 or OS 12 devices:

→ Reset the device to factory defaults and try to register the device again. For how to reset the IGEL OS device to factory defaults, see (11.10-en) Reset to Factory Defaults.

Solving the Firewall Problem

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

> If you have changed the standard port 30001 in the UMS Administrator, open the firewall accordingly for this port. For more details on ports, see IGEL UMS Communication Ports (see page 256) .

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

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

Solving the Database Problem

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

For details on the UMS Administrator, see The IGEL UMS Administrator (see page 1037).

Checking the Network

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

```
ping -s <SIZE> -c 10 -M do
```

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

> For "pinging" the UMS Server on a device with IGEL OS, you can use the built-in network tools (see Network Settings in the IGEL UMS Web App[116] and, for OS 11, (11.10-en) Network Tools).

Checking Time and Date

→ Check if the time and date are set correctly on the device and on the UMS Server.

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

- if the registration directly from the endpoint device functions, see (11.10-en) Using UMS Registration Function. If not, it is usually a sign of some network problems.
- if there is another UMS on the network, and the DHCP and/or DNS server configuration points to the "wrong" UMS.

116. https://kb.igel.com/en/universal-management-suite/current/network-settings-in-the-igel-ums-web-app

Troubleshooting: Device Registration Fails with Error Message: Unexpected end of input stream

Symptom

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

Problem

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

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

Solution

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

Troubleshooting: Device Registration Behind SonicWall Firewall Fails

Symptom

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

Possible Causes

The following causes have been reported with firewalls by SonicWall;

- Large packets: Troubleshooting: Device Registration Fails with Error Message: Unexpected end of input stream (see page 536)
- SonicWall DPI-SSL replaces the UMS certificate: If SonicWall DPI-SSL is enabled, it functions as intermediate CA and sends its own certificate to the devices instead of the original UMS certificate. As a consequence, the devices refuse to register because they would only accept the original UMS certificate.

Solution

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

How to Rename IGEL OS Devices

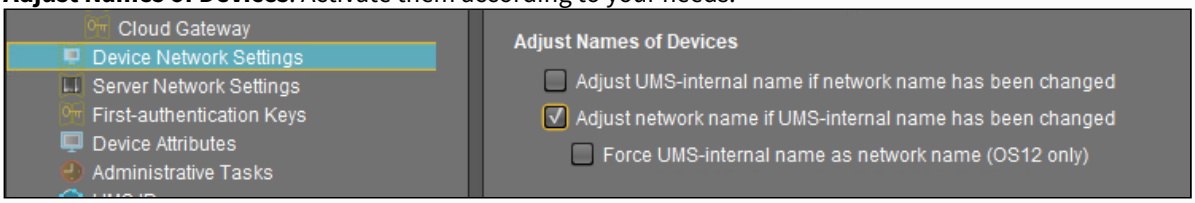
This article shows the options to rename IGEL OS devices through the IGEL Universal Management Suite (UMS) or locally on the device. The options are listed for devices that are not yet registered in the UMS and for devices that are already registered.

Default Naming Convention

By default, if no naming convention is activated and the original hostname of the IGEL OS device has not been changed, the name a device gets upon registration in the UMS is composed of the prefix “ITC” ("TC-", in the case of import with the serial number) and the MAC address of the device.

Example: ITC00E0C520XXXX; TC-00E0C520XXXX

Before renaming/registering the devices, it is recommended, first of all, to pay attention to the following settings in **UMS Console > UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**. Activate them according to your needs:



Renaming upon Registration

Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Before registering the devices, activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see Device Network Settings (see page 903).
2. If the network name, i.e. terminal name, of the device, should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.
3. For OS 12 devices, enable **Force UMS-internal name as network name (OS12 only)** to block the changing of the network name on the devices.
4. Save the changes.

If the network name remained unchanged after the device registration is complete, click **Other commands > Settings UMS >Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can import the devices with the names that fulfill your requirements. For the general instruction, see Importing Devices (see page 1143).

1. When preparing the import file, specify the required device names. See Import with Short Format (see page 1144) or Import with Long Format (see page 1146).
2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed**.

Option 3: Via IGEL Setup > Accessories > UMS Registration (only for IGEL OS 11 or Earlier)

If the **Naming Convention** is not activated and you need to register only a small number of devices, you can specify the required name when registering the device as follows:

→ On the device, open **IGEL Setup > Accessories > UMS Registration** and specify the device name you need under **New host name**. For more information, see (11.10-en) Using UMS Registration Function .

Option 4: Via IGEL Setup > Network

If the **Naming Convention** is not activated:

→ Before registering the device in the UMS, adjust its name locally

- IGEL OS 12: under **IGEL Setup > Network > Common Settings > Computer name**
- IGEL OS 11 and earlier: under **IGEL Setup > Network > LAN Interfaces > Terminal name**

When the device is registered, this name will also be used in the UMS.

Renaming Already Registered Devices

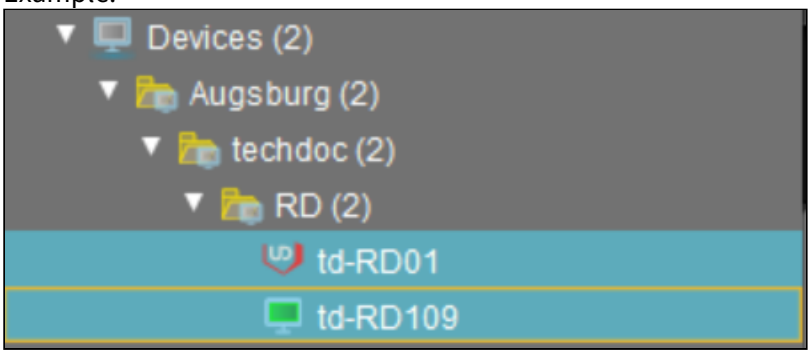
General Notes

- After renaming via UMS, it may be necessary to reboot the endpoint up to three times before the changed network name is displayed correctly.
- Scripts under **System > Firmware Customization > Custom Commands** as well as some DNS or DHCP infrastructure settings may interfere and obstruct the renaming of devices.
- If SCEP certification is in use with **Type of CommonName/SubjectAltName** parameter set to **DNS name (auto)**, SCEP will continue to function using the old hostname by default when you rename the device. This can later lead to client certificate failure at certificate renewal. You can change the behavior through the **network.scepclient.cert%.hostname_change_handling** registry key. For details and troubleshooting, see (12.4-en) Troubleshooting: SCEP Certificate Renewal Failure due to Hostname Change .

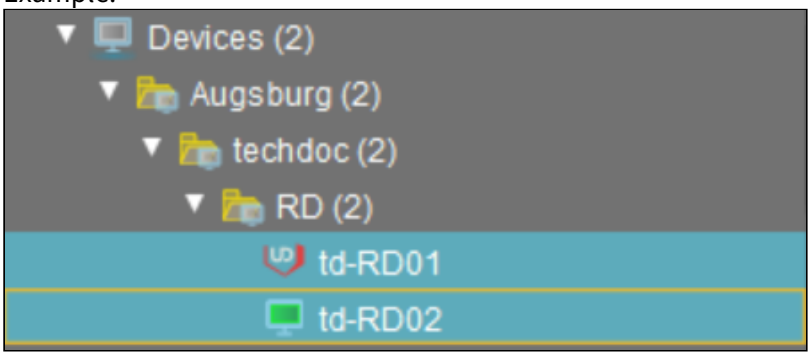
Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see Device Network Settings (see page 903).
2. If the network name, i.e. terminal name, of the device should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.
3. Save the changes.
4. To rename the devices, select one of the following options:

- **Rename all devices**: All devices registered in the UMS will be renamed in accordance with the naming convention.
  Example:



- **Rename and renumber all devices**: All devices will be renamed in accordance with the naming convention. If the parameter Identifier under **UMS Administration > Global Configuration > Device Network Settings** has been set to **Sequential Number** (UMS 12.02.120 or higher) or you are using UMS 12.02.100 or lower, this will result in continuous, end-to-end numbering. All names will be reallocated. If numbers have become free because devices were taken out of service, these numbers will be used for other devices. For details on the naming options, see Device Network Settings (see page 903).
  Example:



If the network name remains unchanged, click **Other commands > Settings UMS->Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can reimport the devices with the names that fulfill your requirements. For the general instruction, see Importing Devices (see page 1143).

1. When preparing the import file, specify the required device names. See Import with Short Format (see page 1144) or Import with Long Format (see page 1146).

2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed**.

Option 3: Via UMS Console > [device's context menu] > Rename or via Setup > Network

→ If you have to rename individual devices, see Changing the Hostname of an IGEL Device via UMS (see page 542).

Option 4: Via IGEL Management Interface (IMI)

→ If you are using IGEL Management Interface, you can rename your devices as described under PUT /v3/thinclients/{tcId}.

Changing the Hostname of an Endpoint Device via IGEL UMS

There are two different ways to change the hostname of an endpoint device via the IGEL Universal Management Suite (UMS).

Option 1:

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

For IGEL OS 12:

1. In the **UMS Web App > Devices**, select the device.
2. Click **Edit Configuration**.
3. Go to **Network > Common Settings > Computer name** and specify the required hostname.
4. Save the settings.
5. Select that you want the settings to be applied **Now**.
6. Refresh the browser window in order to see the changed hostname.
7. Reboot the device.

For IGEL OS 11 and earlier:

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

Option 2:

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

1. In the **UMS Console > Devices**, right-click the device.
2. Choose **Rename**.
3. Change the name.
4. Click **OK**.
5. Right-click the device.
6. Choose **Other commands > Settings UMS -> Device**.
7. Reboot the device.

Monitoring Device Health and Searching for Lost Devices in the IGEL UMS

You have two possibilities of monitoring the devices' health through the IGEL Universal Management Suite (UMS):

- Online check: The UMS initiates a regular poll to all devices.
- Last contact between the UMS and the devices: The UMS is aware of the time and date when it had its last interaction with devices; with IGEL OS 11.05.100 or higher, devices can send periodical heartbeat signals to the UMS.

Both methods can be combined; it is recommended to review the advantages and disadvantages. Generally speaking, a combination makes sense if network load is not an issue.

Environment

- Reportable heartbeat: Endpoint devices with IGEL OS 11.05.100 or higher or with IGEL OS 12.01.100 or higher
- Checking the last contact between the device and the UMS: UMS 12.01.100 or higher
- UMS and endpoint devices are connected directly or via ICG

Online Check (UMS Polls the Devices)

The UMS Server polls the devices in a configurable time interval. When a device responds to the poll, its icon is green  ; when a device does not respond, its icon turns red  . (When the online check is disabled, the icon is grey ). For more information on icons, see:

- for the UMS Console: Devices - Managing Devices in the IGEL UMS (see page 776)
- for the UMS Web App: Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App (see page 1176)

The online check can be enabled or disabled under **Misc > Settings > Online Check**; also, the time interval can be configured there.

Advantages:

- Works with any firmware version (and any UMS version).
- Provides an instant insight into device health by means of colored icons.
- Status updates can be very frequent (max. every 0.1 seconds).

Disadvantages:

- Causes relatively high network load, as all devices are polled at the same time (the overall network load is dependent on the time interval).
- Offline devices cannot be traced systematically, must be looked up manually in the structure tree.

Last Contact between Device and UMS (Devices Send Data to the UMS)

You can search explicitly for devices that did not have any interaction with the UMS for a given time. By creating an appropriate view, you can determine which device last had contact with the UMS at which time. This may be useful for detecting devices that are not operational anymore.

In addition to the previously existing contacts, devices with IGEL OS 11.05.100 or higher can send periodical heartbeat signals to the UMS to indicate that they are still operational.

Advantages:

- Systematic searches for lost devices are possible.
- The search results can be saved and sent by e-mail.
- Low network load, or no additional load at all:
  - When the heartbeat feature is used: The heartbeat signals are sent with random delay times. (Of course, the overall network load is dependent on the time interval).
  - When the heartbeat feature is not used: No additional network load is generated.

Disadvantage:

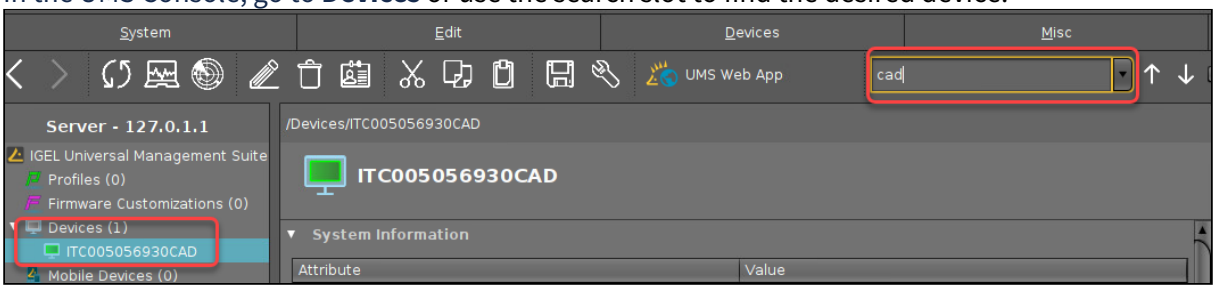
- Status updates cannot be as frequent as with the online check.

Tracing Devices by Their Last Contact with the UMS

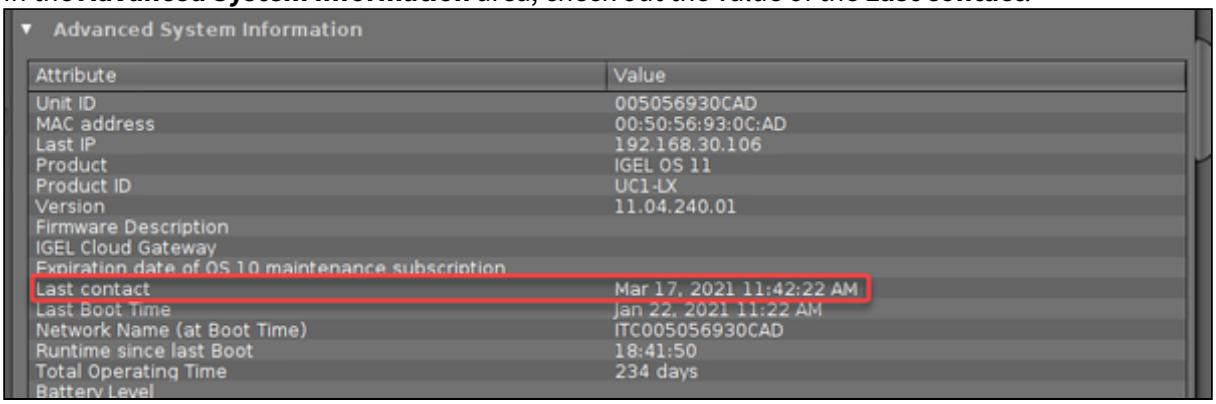
Tracing a Specific Device

UMS Console:

1. In the UMS Console, go to **Devices** or use the search slot to find the desired device.

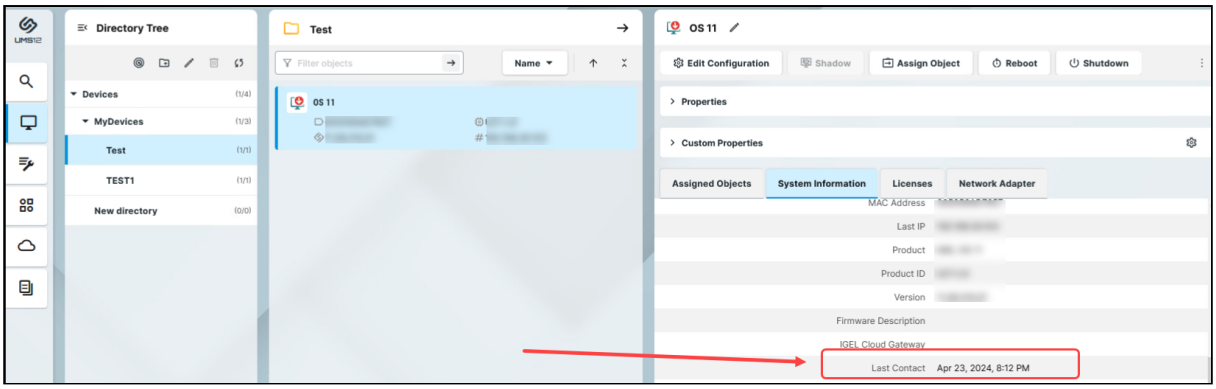


2. In the **Advanced System Information** area, check out the value of the **Last contact**.



UMS Web App:

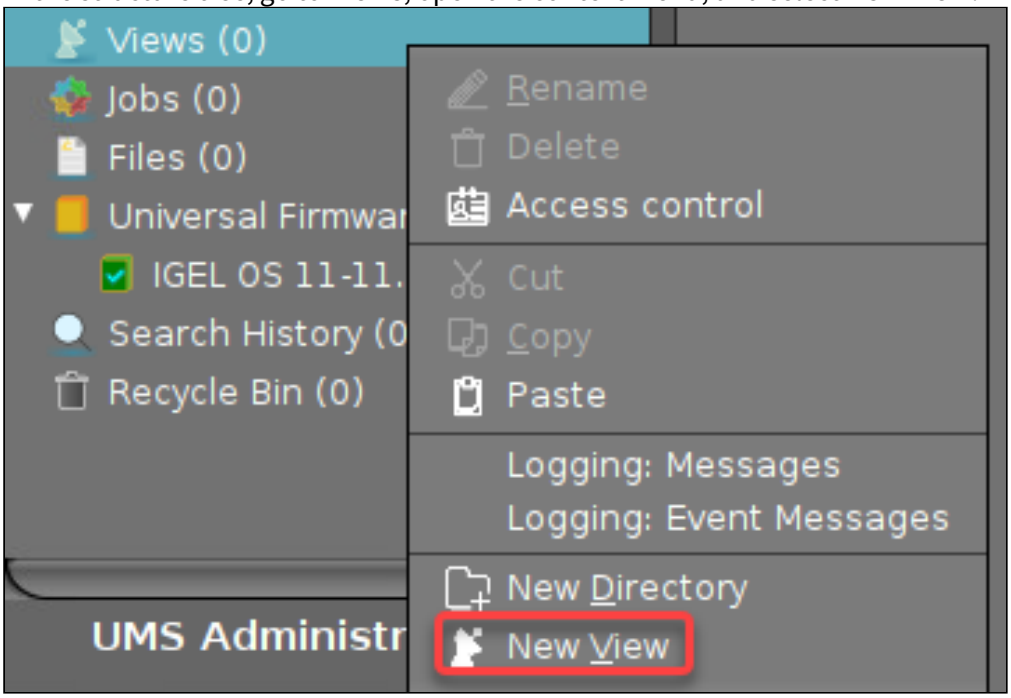
1. In the UMS Web App, go to **Devices** and select the required device.
2. Under **System Information**, check out the value of the **Last contact**.



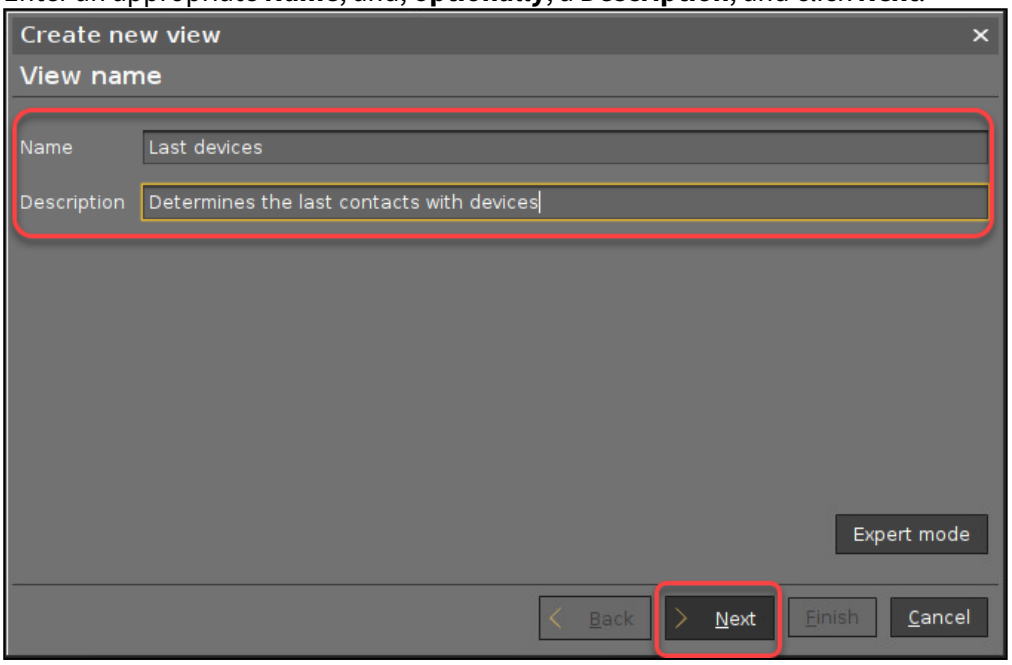
For IGEL OS 11 devices, the **Last contact** timestamp is updated on each command sent from a device to the UMS. Or, if you configure a reportable heartbeat interval, a heartbeat command will be sent in a certain time period if no other command has been sent, and the timestamp will be updated correspondingly.
For IGEL OS 12 devices, the **Last contact** timestamp is updated not on each command, but only in the configured heartbeat interval (for online devices only).
For how to configure a reportable heartbeat interval, see Configuring Devices to Send a Reportable Heartbeat (see page 550) below.

Finding Devices That Have Not Shown Up since a Given Time

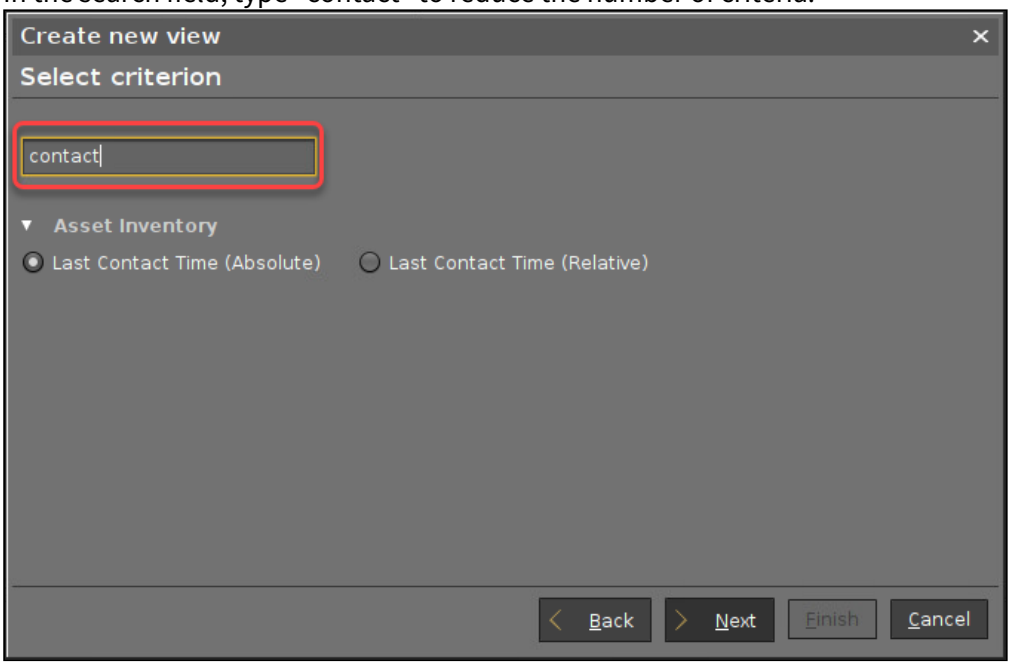
1. In the structure tree, go to **Views**, open the context menu, and select **New View**.



2. Enter an appropriate **Name**, and, **optionally**, a **Description**, and click **Next**.

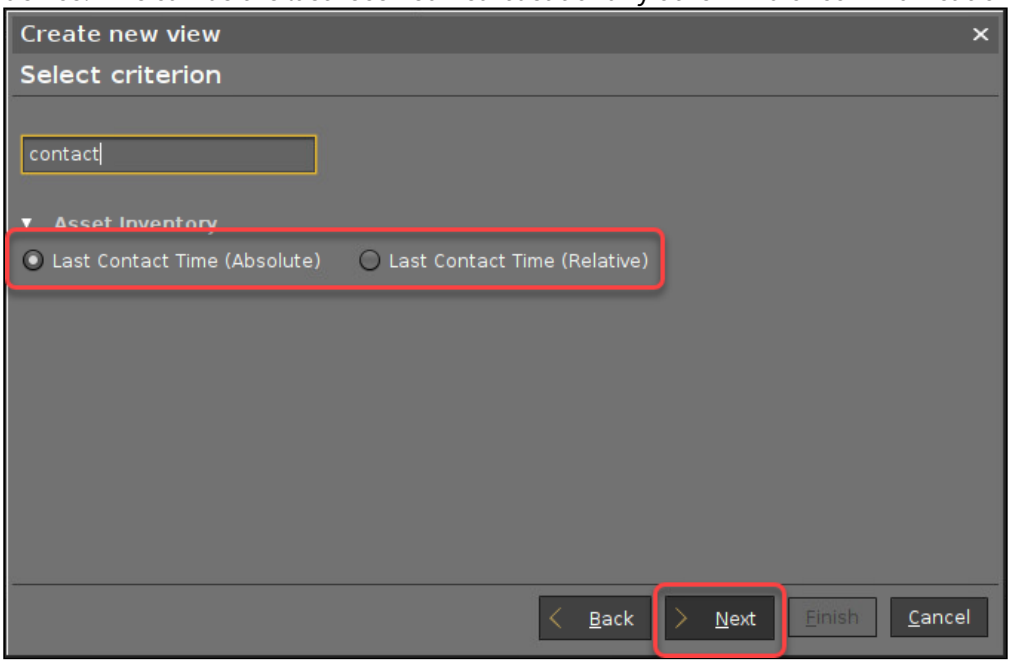


3. In the search field, type "contact" to reduce the number of criteria.

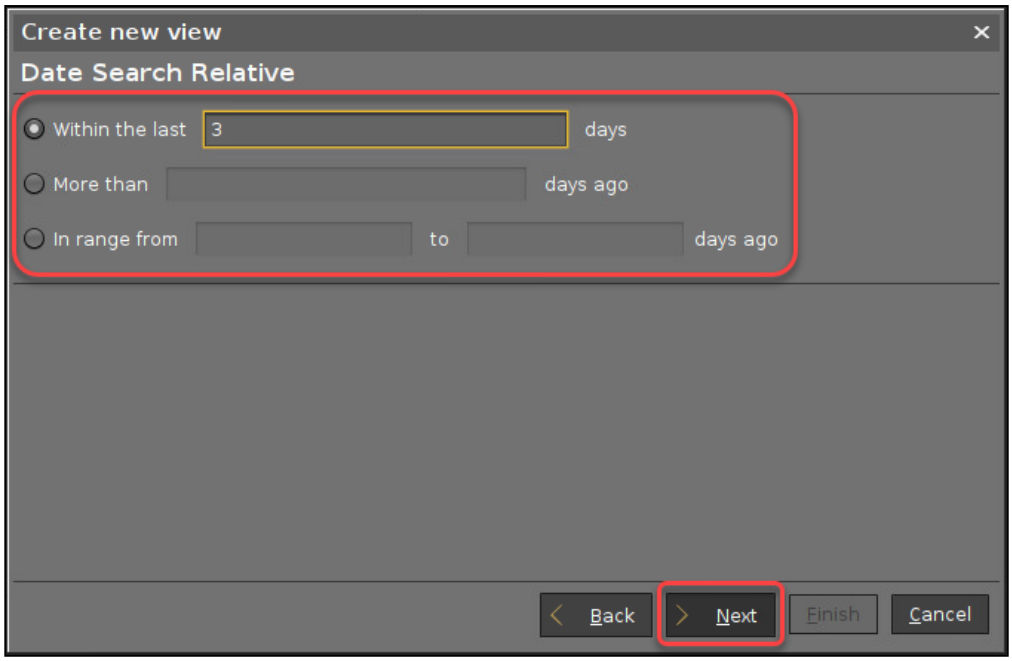


4. Choose one of the following criteria and click **Next**:
   - **Last contact time (relative)**: The time interval between the last contact between the UMS and the device and now. This can be the last received heartbeat or any other kind of communication.

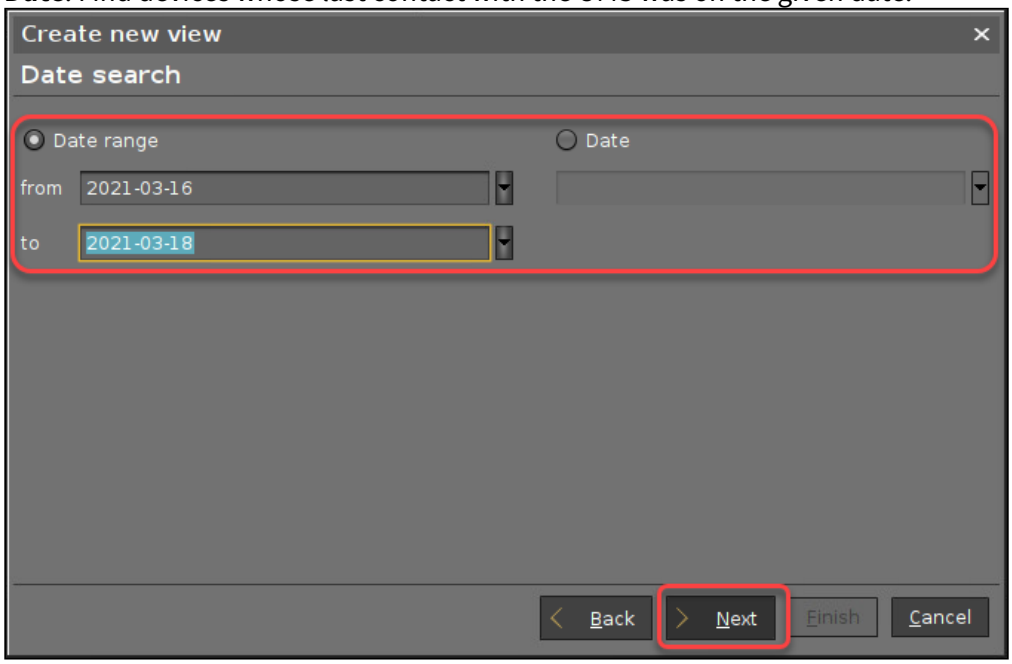
- **Last contact time (absolute)**: The date of the last contact between the UMS and the device. This can be the last received heartbeat or any other kind of communication.



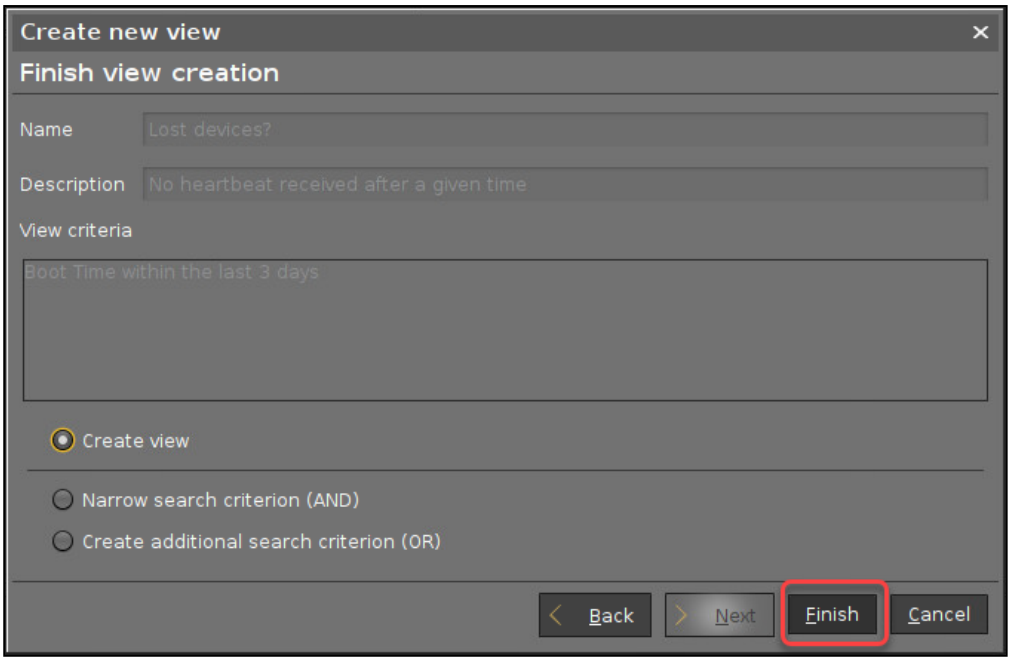
5. Provide the data, depending on whether you chose **Last contact time (relative)** or **Last contact time (absolute)**, and then click **Next**.
    - If you have selected **Last contact time (relative)**:
        - **Within the last [number of] days**: Find devices whose last contact with the UMS was between yesterday and the given number of days ago.
        - **More than [number of] days ago**: Find devices whose last contact with the UMS is more than the given number of days ago.
        - **In range from [number] to [number of] days ago**: Find devices whose last contact with the UMS was within the given time interval.



- If you have selected **Last contact time (absolute)**:
  - **Date range**: Find devices whose last contact with the UMS was within the given date range.
  - **Date**: Find devices whose last contact with the UMS was on the given date.

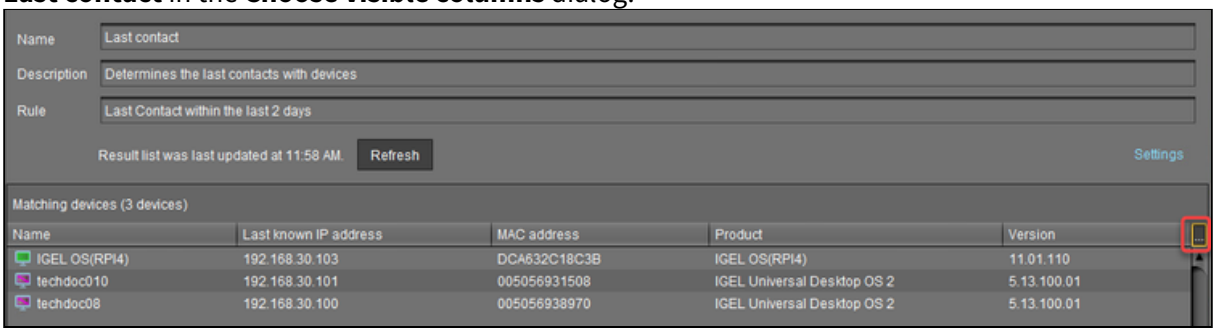


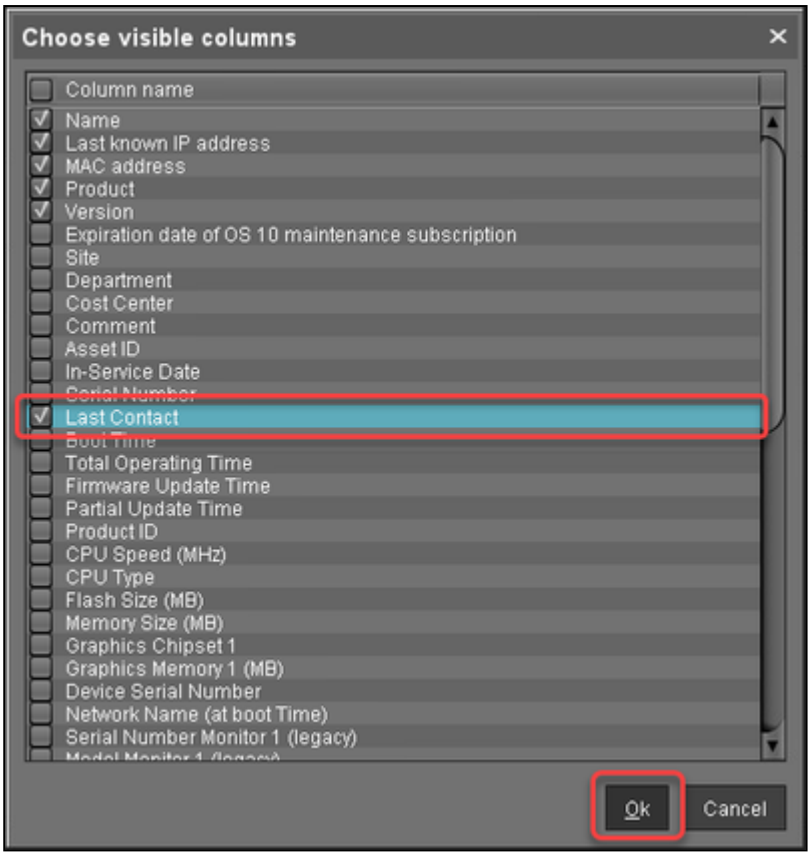
6. Review your settings and click **Finish**.



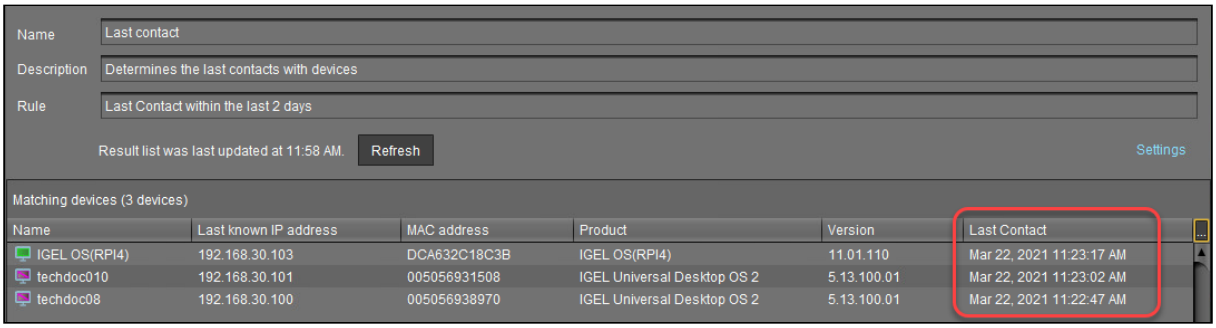
7. If the devices are not shown immediately, click **Load devices**.

8. To make the **Last contact** column visible, click the icon that is shown underneath and then select **Last contact** in the **Choose visible columns** dialog.





The results are shown.

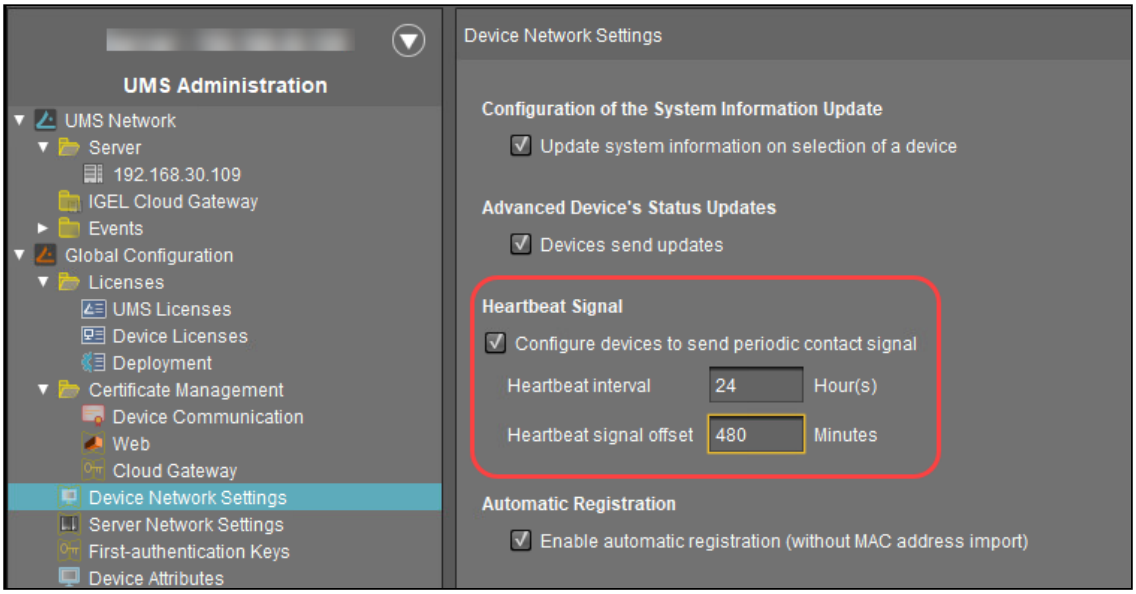


You can save the results in various formats (see How to Save the View Results List in the IGEL UMS (see page 841)) or send them via e-mail (see How to Send a View as Mail in the IGEL UMS (see page 844)).

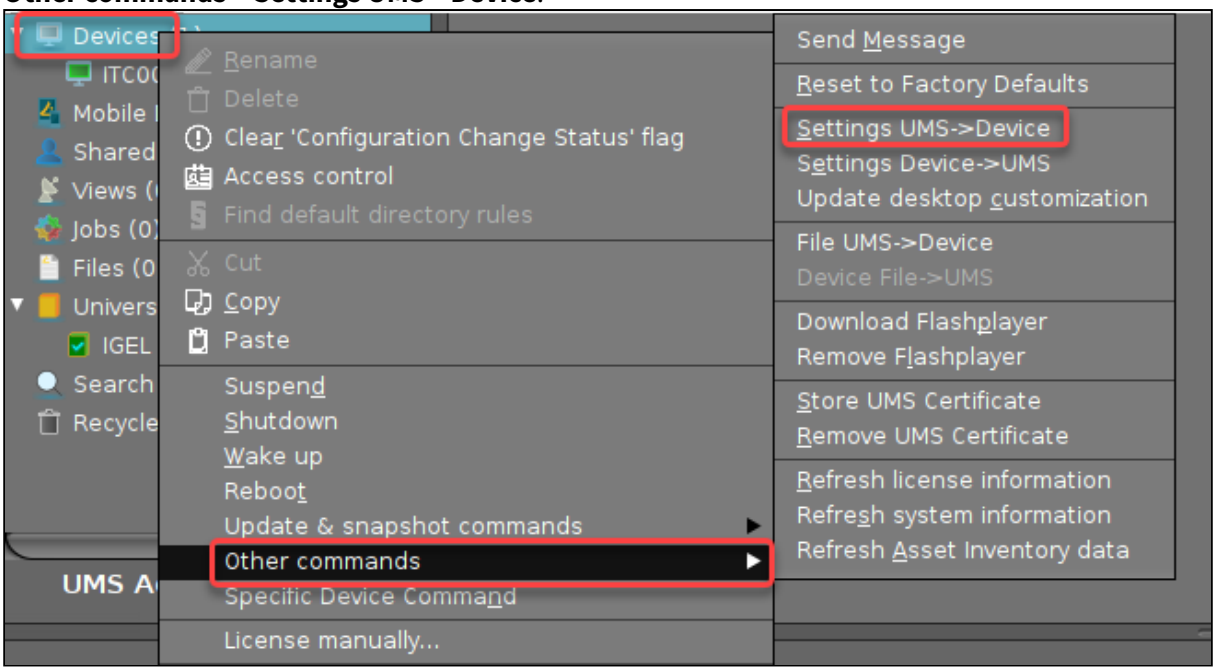
Configuring Devices to Send a Reportable Heartbeat

1. In the UMS Console, go to **UMS Administration > Device Network Settings** and edit the settings as follows:
   - Activate **Configure devices to send periodic contact signal**
   - Set **Heartbeat interval** to the desired value.
   - Set the **Heartbeat signal offset** to the desired value.

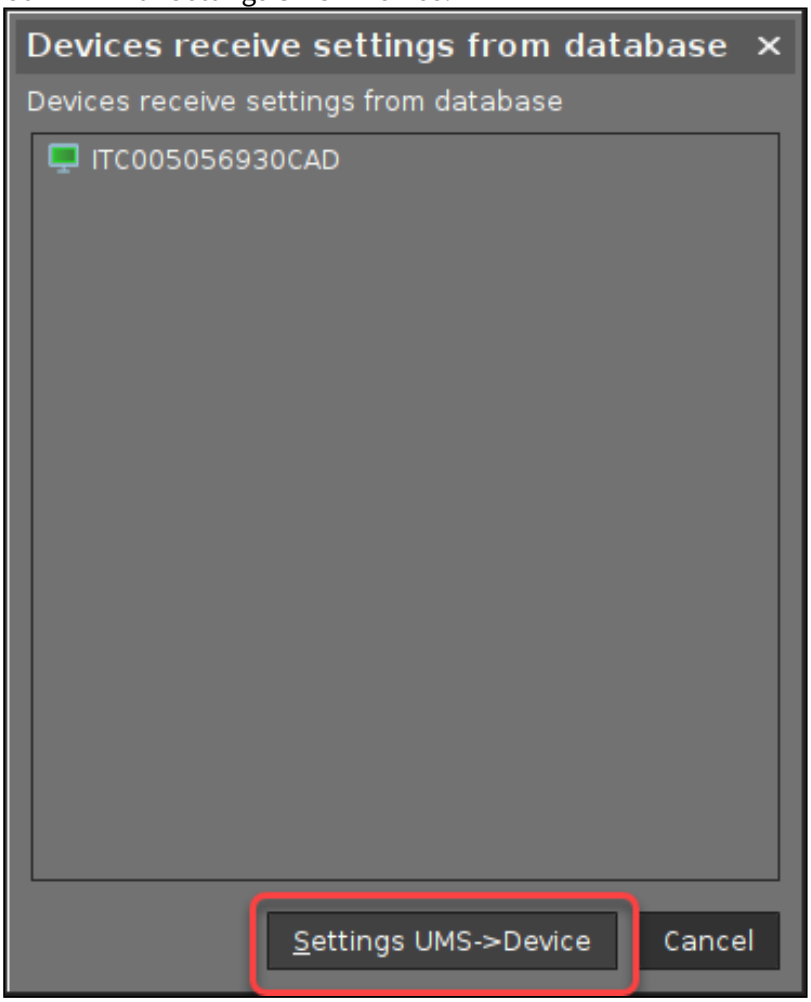
The heartbeat signal will have a random delay between 0 and the value specified here. This is to avoid overloads which might occur when large amounts of devices send their heartbeat signals simultaneously.



2. Click  to save your settings.
   The settings will become effective the next time the devices receive their settings from the UMS.
3. To make the new settings effective immediately, go to **Devices**, open the context menu, and select **Other commands > Settings UMS->Device**.



4. Confirm with Settings **UMS->Device**.



How to Manage IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You

Self-defined device attributes can be used to configure devices with the IGEL Universal Management Suite (UMS) according to device-specific data like location, department, or attached hardware.

To use this functionality, you create a custom script on the device that retrieves the desired data and sets the value of the relevant device attribute accordingly.

Note that you must use the UMS internal name of an attribute, not the display name. The UMS internal identifier is displayed in the UMS Console under **UMS Administration > Global Configuration > Device Attributes**; see also Managing Device Attributes for IGEL OS Devices (see page 879).
Also, note that permission to change attribute values must be granted by the UMS. This is the case if the **Overwrite Rule** is set to **Devices** or **All** in the UMS Console under **UMS Administration > Global Configuration > Device Attributes**; see also Managing Device Attributes for IGEL OS Devices (see page 879).

The character limit for device attributes is 100 characters. Longer entries will not be synchronized with the UMS.

Environment

For OS 11 Devices

- IGEL UMS 6.10 or higher
- Devices with IGEL OS 11.07.100 or higher

For OS 12 Devices

- IGEL UMS 12.03.100 or higher
- Devices with IGEL OS 12.3.0 or higher

Command Reference

List All Device Attributes

```
/sbin/rmagent-devattrs-enum
```

Lists all device attributes including the current value for this device. The enumeration is ordered according to the attribute's order id.

Example:

```
root@ITC005056930CAD:~# rmagent-devattrs-enum
country:range:US
division:range:First division
location:range:San Francisco
root@ITC005056930CAD:~#
```

Device Attribute of the Type "List": List All Possible Values

```
/sbin/rmagent-devattrs-enum-range <ATTRIBUTE_NAME>
```

Enumerates entries of the given range. The enumeration is ordered according to the range item's order id.

Example:

```
root@ITC005056930CAD:~# rmagent-devattrs-enum-range location
Augsburg
Karlsruhe
San Francisco
root@ITC005056930CAD:~#
```

Print Attribute Type

```
/sbin/rmagent-devattrs-get-type <ATTRIBUTE_NAME>
```

Prints the type of the given attribute. Possible types are:

- string
- number
- date (format: yyyy-mm-dd)
- range

Example:

```
root@ITC005056930CAD:~# rmagent-devattrs-get-type location
range
root@ITC005056930CAD:~#
```

Print Attribute Value

```
/sbin/rmagent-devattrs-get <ATTRIBUTE_NAME>
```

Prints the current value of the given attribute.

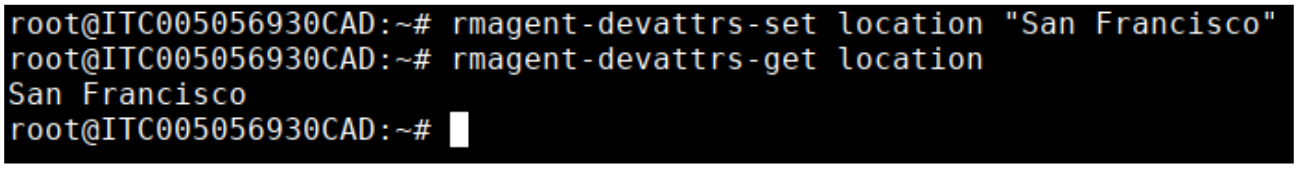
Example:

Set Attribute Value

```
/sbin/rmagent-devattrs-set <ATTRIBUTE_NAME> <ATTRIBUTE_VALUE>
```

Sets the given attribute to the specified value. If the overwrite rule for this attribute does not permit the device to change the value, an error is returned. Note that this command does not check the value type.

Example:

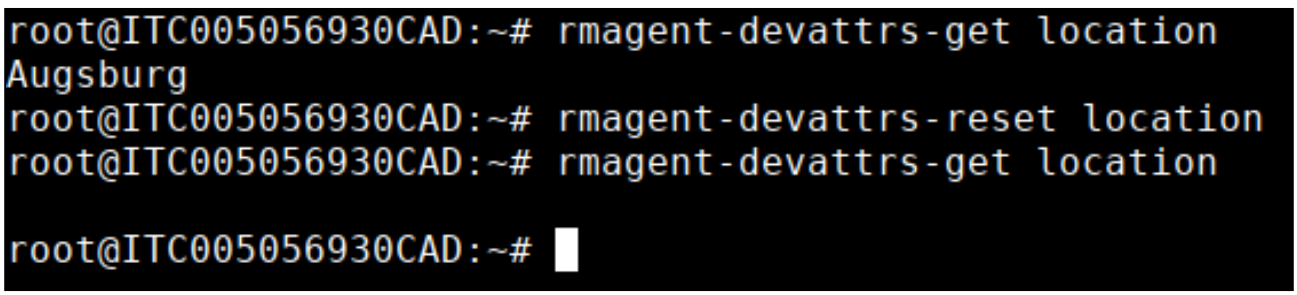


Reset Attribute Value

```
/sbin/rmagent-devattrs-reset <ATTRIBUTE_NAME>
```

Resets the given attribute to an empty value.

Example:



Send Attributes to UMS If a Value Has Been Changed by Device

```
/sbin/rmagent-devattrs-sync
```

If any of the attribute values have been changed by the device, the complete set of attributes is sent to the UMS.

Send Attributes to UMS

```
/sbin/rmagent-write-device-attributes
```

The complete set of attributes is sent to the UMS.

Troubleshooting: IGEL OS 12 Devices Failing to Connect to UMS Due to Expired Client Certificates

IGEL OS 12 devices need to have valid client certificates to connect to the IGEL Universal Management Suite (UMS). Client certificates expire 1 year after device registration in the UMS. For devices running IGEL OS 12.4.1 or newer, the client certificates are renewed automatically, but for devices running IGEL OS 12.4.0 or older, the client certificates are not renewed in some cases, making the devices unmanageable through the UMS. The mitigation of the issue is done by allowing expired client certificates to be temporarily accepted through a custom `TrustManager`. This way, the devices can be updated without manual intervention.

For details on how to enable the custom `TrustManager` for the IGEL Cloud Gateway, see Troubleshooting: IGEL OS 12 Devices Failing to Connect to the ICG Due to Expired Client Certificates[117].

Requirements

- UMS version 12.08.130 or higher
- Administrator / root access to terminal to run commands of the command line interface (CLI). For details, see IGEL UMS Administrator Command-Line Interface (see page 1079)

Error Message of Expired Client Certificate

When a device has an expired client certificate, the connection to the UMS fails because the TLS handshake is aborted during the establishment of a TLS connection to the UMS.

You can see the following error message in the UMS tray app: `ERROR: Connection failure: read failed`

You can also see the same error message in the device log files when the device is trying to connect to the UMS.

```
00E0C51885D6 igel-rmagent-connector[7921]: Try to connect ...
ITC00[redacted] igel-rmagent[1976]: Dispatch local request: Connect [redacted]
ITC00[redacted] igel-rmagent[1976]: Connecting to device connector [redacted]
ITC00[redacted] igel-rmagent[7942]: WS connector process terminated: status=0
ITC00[redacted] igel-rmagent[1976]: ERROR: Connection failure: read failed
ITC00[redacted] igel-rmagent[1976]: Response to local command Connect: id=4cc192df45a742beb8c14379a8bbba65 status=1 message='ERROR: Connection failure: read failed'
ITC00[redacted] igel-rmagent[1976]: Disconnected
```

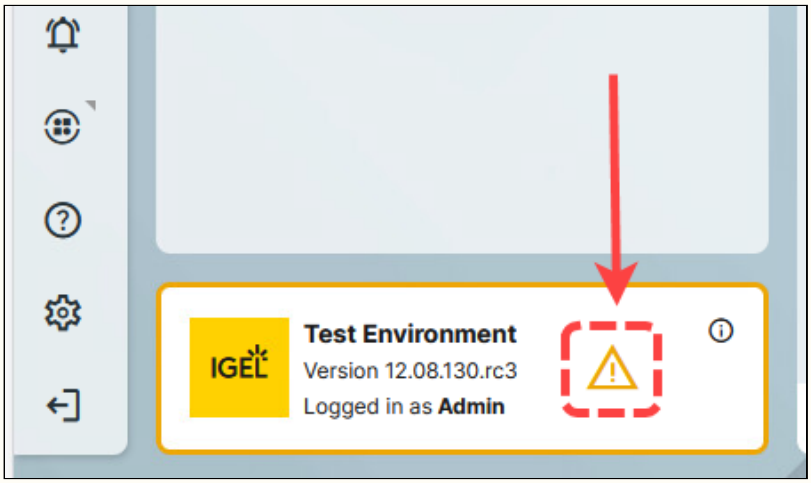
Using the Custom TrustManager

Starting from UMS 12.08.130, a custom `TrustManager` is integrated in the UMS that can be enabled to accept expired client certificates. The `TrustManager` can be managed using the following CLI commands:

- Enable: `umsadmin-cli accept-expired-client-certs enable`
- Disable: `umsadmin-cli accept-expired-client-certs disable`
- Check current state: `umsadmin-cli accept-expired-client-certs state`

117. https://kb.igel.com/en/igel-cloud-gateway/current/troubleshooting-igel-os-12-devices-failing-to-conn

When the custom `TrustManager` is enabled, a warning is shown in the UMS Web App system info box to highlight the potential security and compliance risk. You can get further information if you click the warning icon.
The warning is only shown to administrators with write access to the **UMS Console > UMS Administration > UMS Network** node.



Step-by-Step Instructions to Renew Expired Client Certificates

To handle devices with expired client certificates:

1. Open the command prompt as Administrator in Windows or a terminal as root in Linux.

2. Enter `umsadmin-cli accept-expired-client-certs enable`
   This enables the custom `TrustManager` in the UMS to accept expired client certificates and restarts the UMS server.
   You should see the corresponding response.

```
C:\Windows\system32>umsadmin-cli accept-expired-client-certs enable
Accept expired Client Certificate enabled! UMS Server restarted!
```

3. To check that the option is enabled, use the `umsadmin-cli accept-expired-client-certs state` command and see that the option is enabled.

```
C:\Windows\system32>umsadmin-cli accept-expired-client-certs state
Accept expired Client Certificate value: enabled
```

4. Restart the IGEL OS 12 devices with the expired certificates.
   The devices should be connect to the UMS after restart.

5. Go to the UMS Console or UMS Web App and check if the IGEL OS 12 devices are connected to the UMS now.

6. Go to the UMS Web App and update the IGEL OS 12 Base System version on the devices to the latest available version.
   The devices will get their client certificates renewed by the update.

7. Go back to the UMS CLI and enter `umsadmin-cli accept-expired-client-certs disable`
   This disables the custom `TrustManager` and devices with expired client certificates cannot connect to the UMS anymore.

8. To check that the option is disabled, use the `umsadmin-cli accept-expired-client-certs state` command.

9. Go to the UMS Console or UMS Web App and check if the updated IGEL OS 12 devices are connected to the UMS.

UMS Web App Sends Commands to the Wrong Devices

Environment

- UMS Web App version 12.03.110 up to and including version 12.05.100

Problem

A command from the UMS Web App is mistakenly sent to the wrong device folder. This can happen if you select a folder, then send a command to this folder, and then repeat these steps with a different folder.

This is valid for all types of commands, e.g. reboot, update, ...

Solution

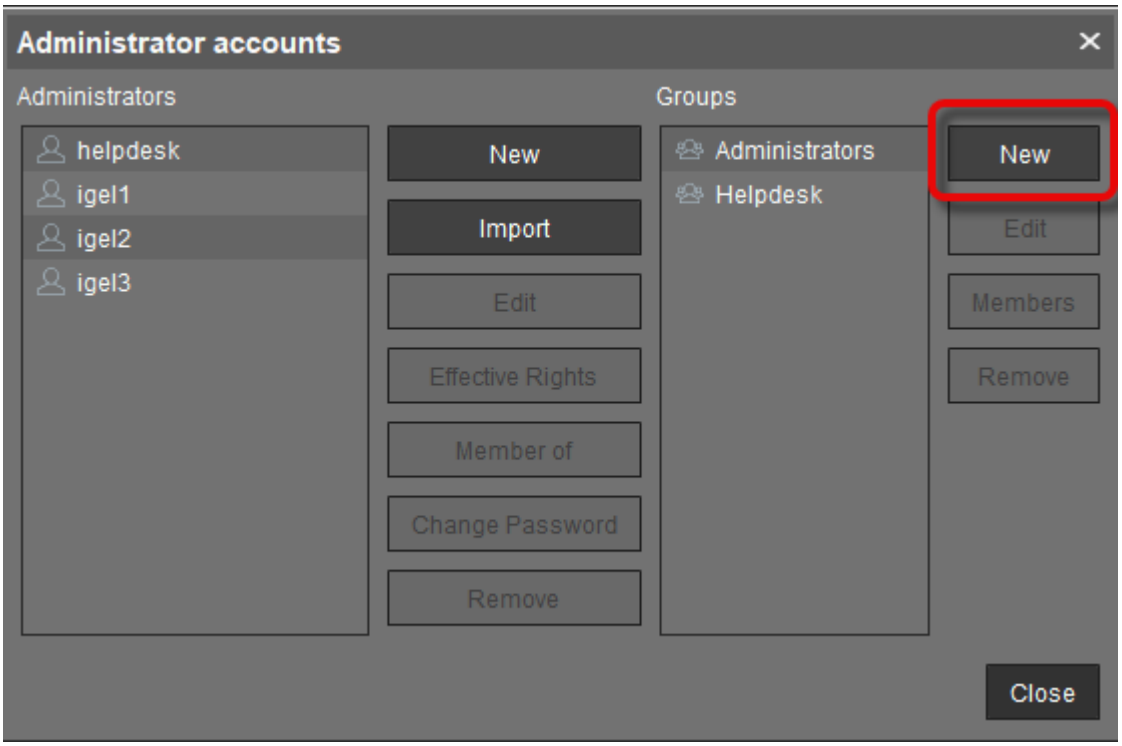
→ Update your UMS to version 12.05.110 (released: 2024-07-23)

Mitigation (If an Update Is Not Possible Yet)

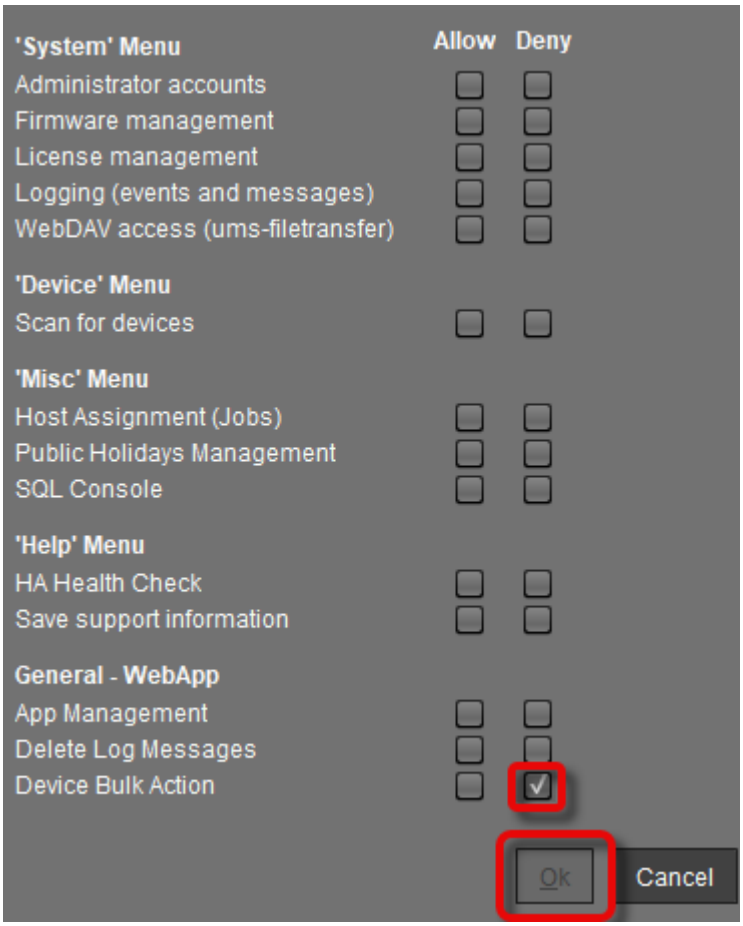
To mitigate this issue, you must restrict the user permissions so that the users can no longer execute bulk actions on devices.

⚠ The following mitigation only applies to regular users. The superuser can still perform bulk actions.

1. In the UMS Console, go to **System > Administrator accounts** and click **New** to create a new user group.



2. For this user group, set the **Device Bulk Action** permission to **Deny**. Do not set any other permissions for this group.



3. Add every user to this group.

Start of the UMS Console / Web App

Troubleshooting: Browser Displays a Security Warning (Certificate Error) when Opening the UMS Web App

Symptom

When opening the UMS Web App, the browser displays a security warning and/or reports a certificate error.

Environment

- UMS Web App (UMS 6.06 or higher)

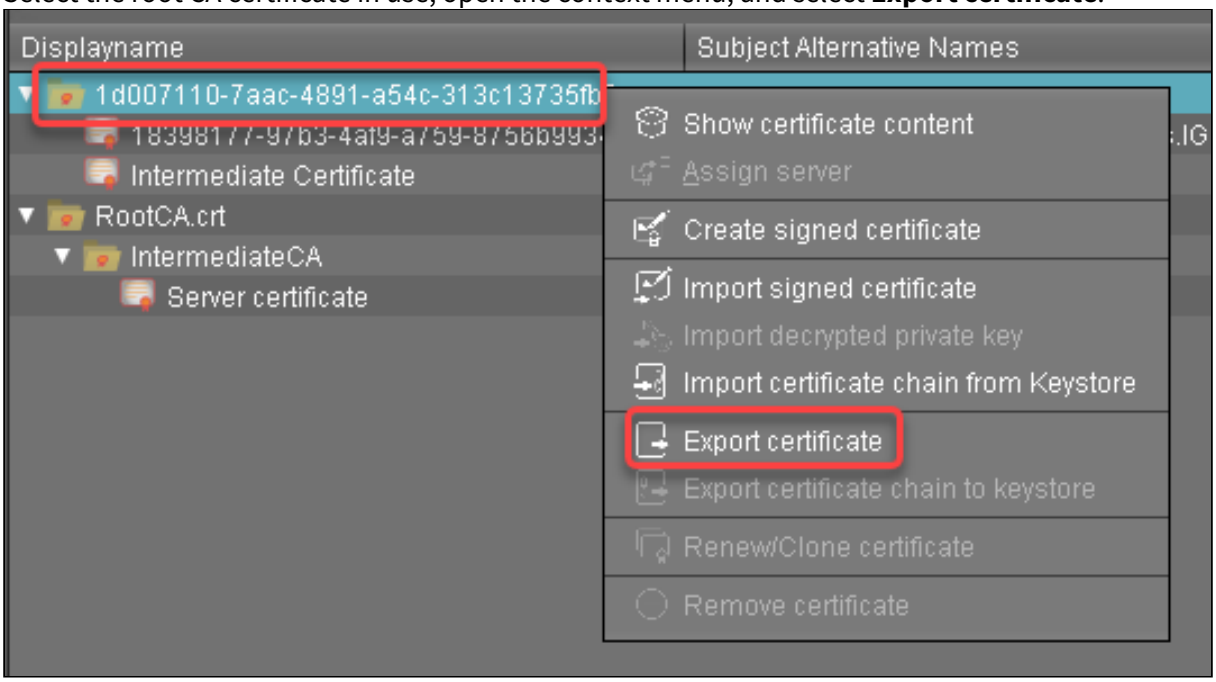
Problem

You are using an end certificate from a root CA that is not known to the browser. This is the case for self-signed certs, e.g. the default implementation.

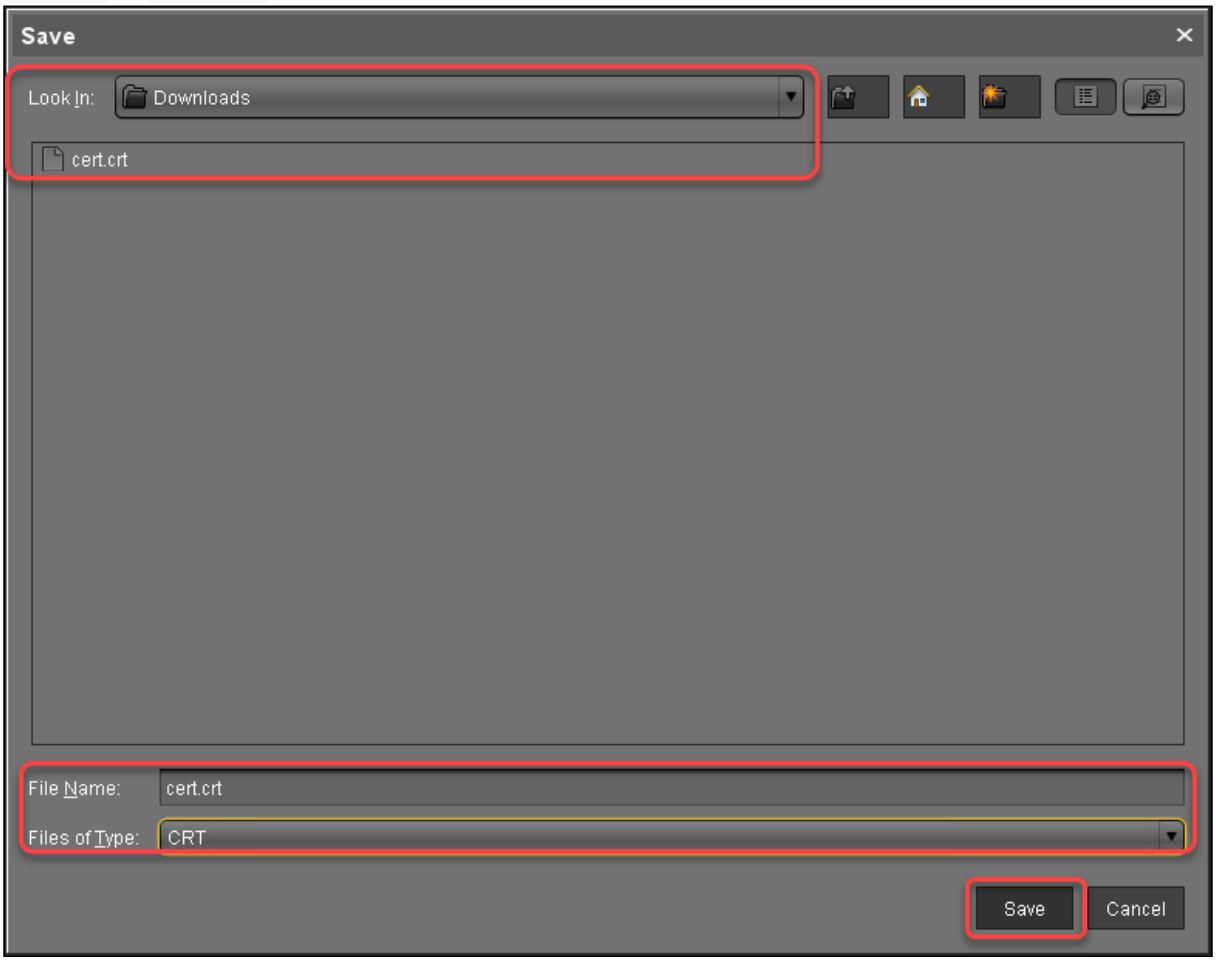
Solution

Exporting the Certificate from the UMS

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Make sure all end certificates in use are derived from the same root CA certificate.
3. Select the root CA certificate in use, open the context menu, and select **Export certificate**.



4. Select an appropriate location, select the correct file extension for your browser (most common: `*.crt` or `*.cert`), and click **Save**.



5. Add the certificate to the trusted certificates of your browser. For instructions, see Importing the Certificate into the Browser (see page 565).

Importing the Certificate into the Browser

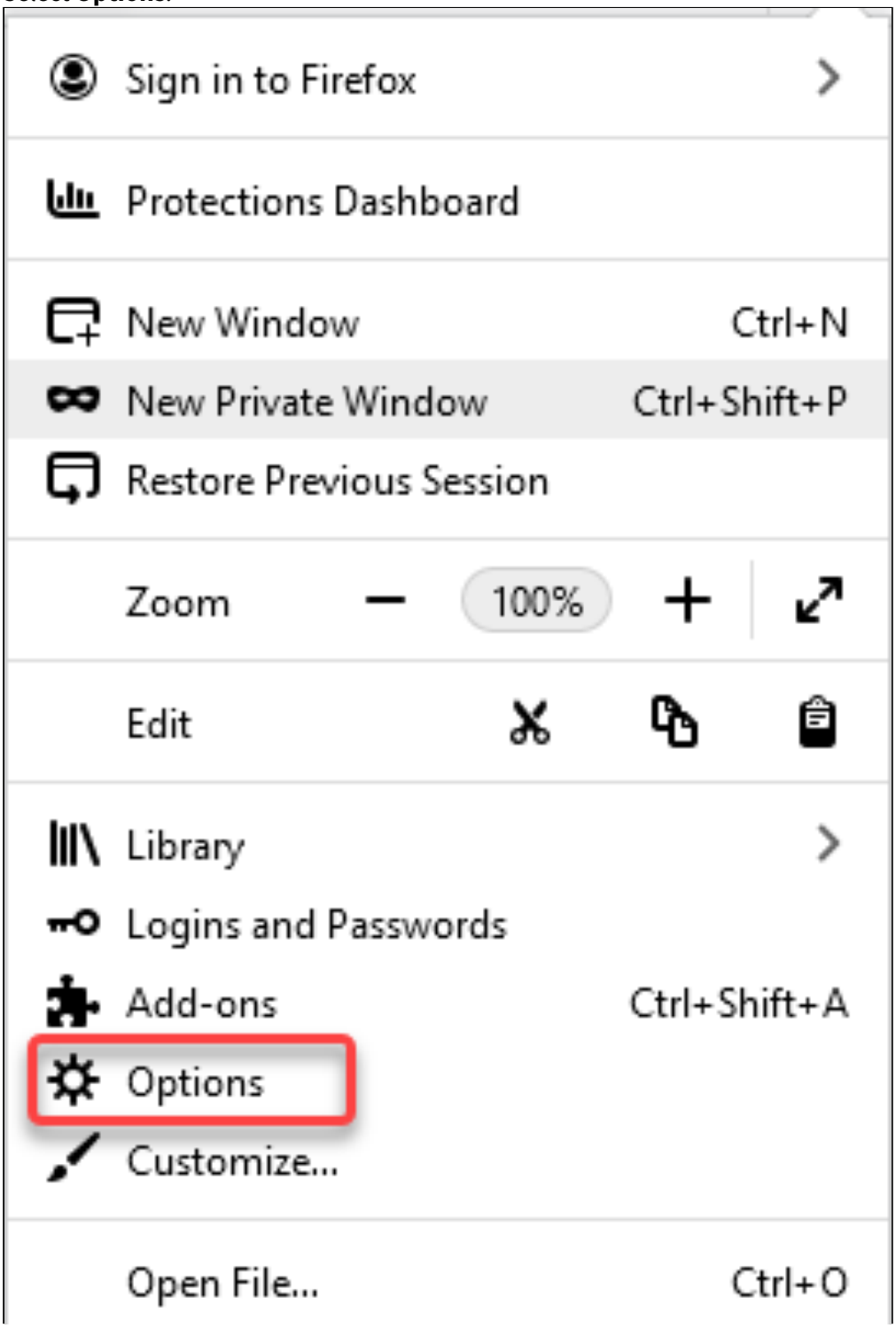
> ⚠ The procedures described here may differ if you have a different browser version.

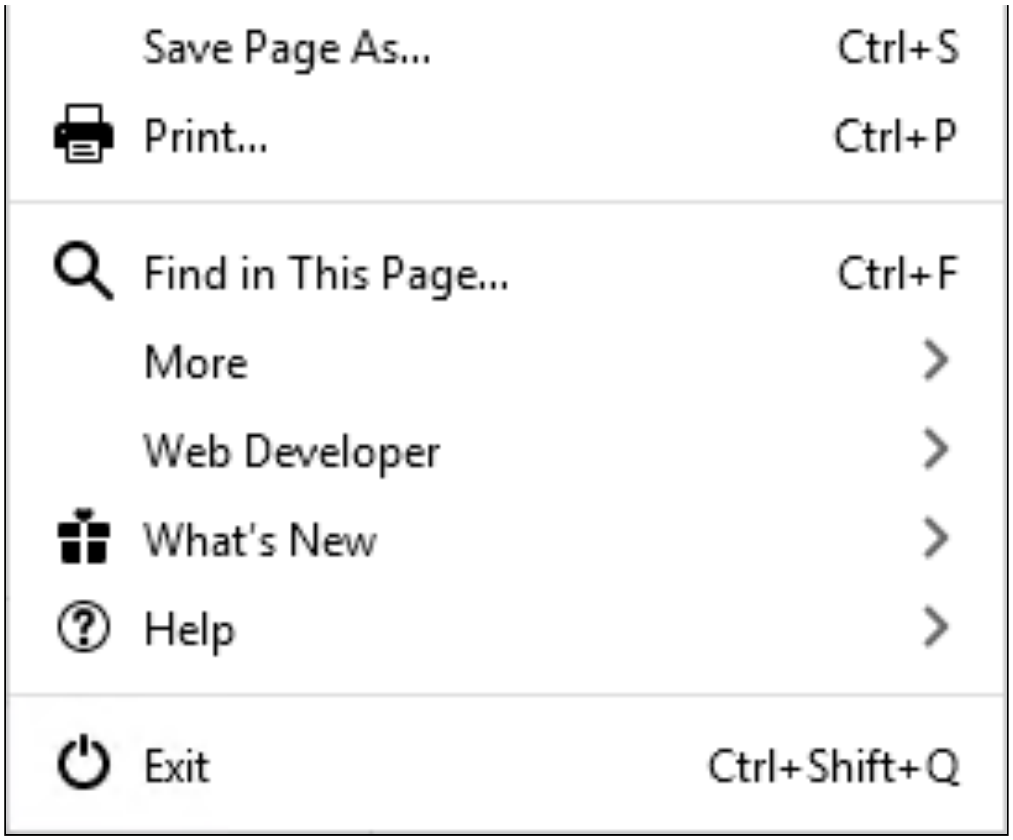
The following browsers are described here:

- Firefox (see page 566)
- Chrome (see page 571)
- Microsoft Edge (see page 582)

Firefox

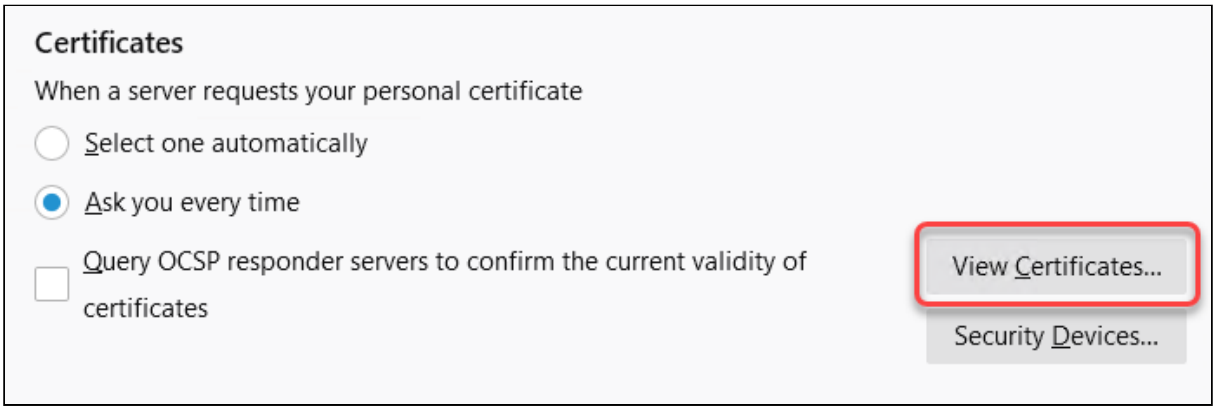
1. Click ☰ to open the menu.
2. Select **Options**.



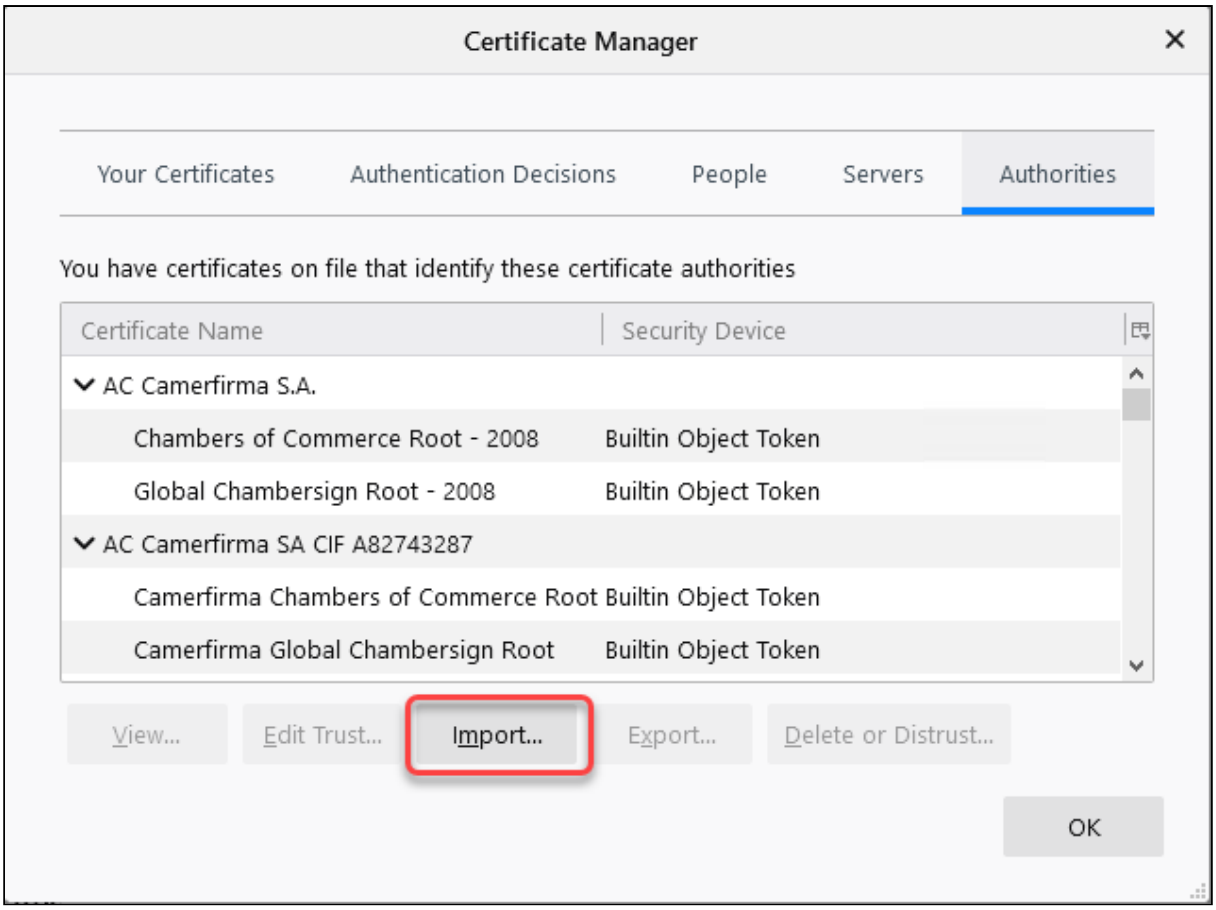


3. Select **Privacy & Security**.

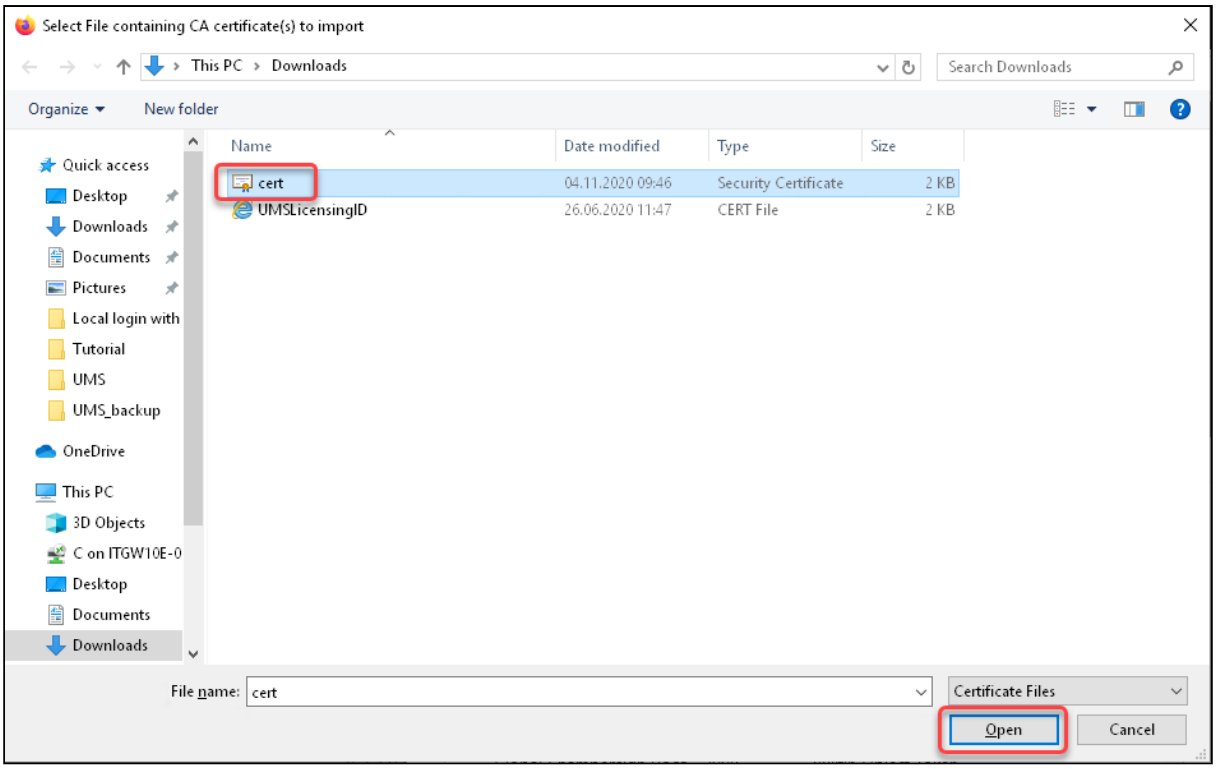
4. Scroll down to Certificates and click **View Certificates**.



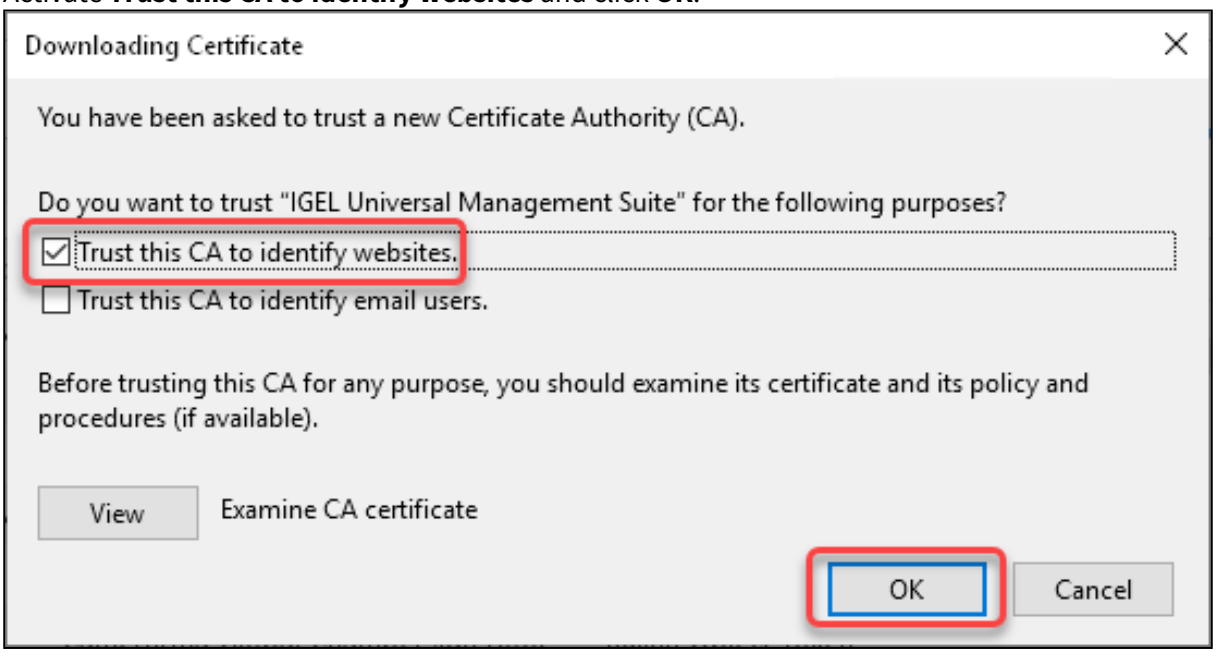
5. Click **Import**.



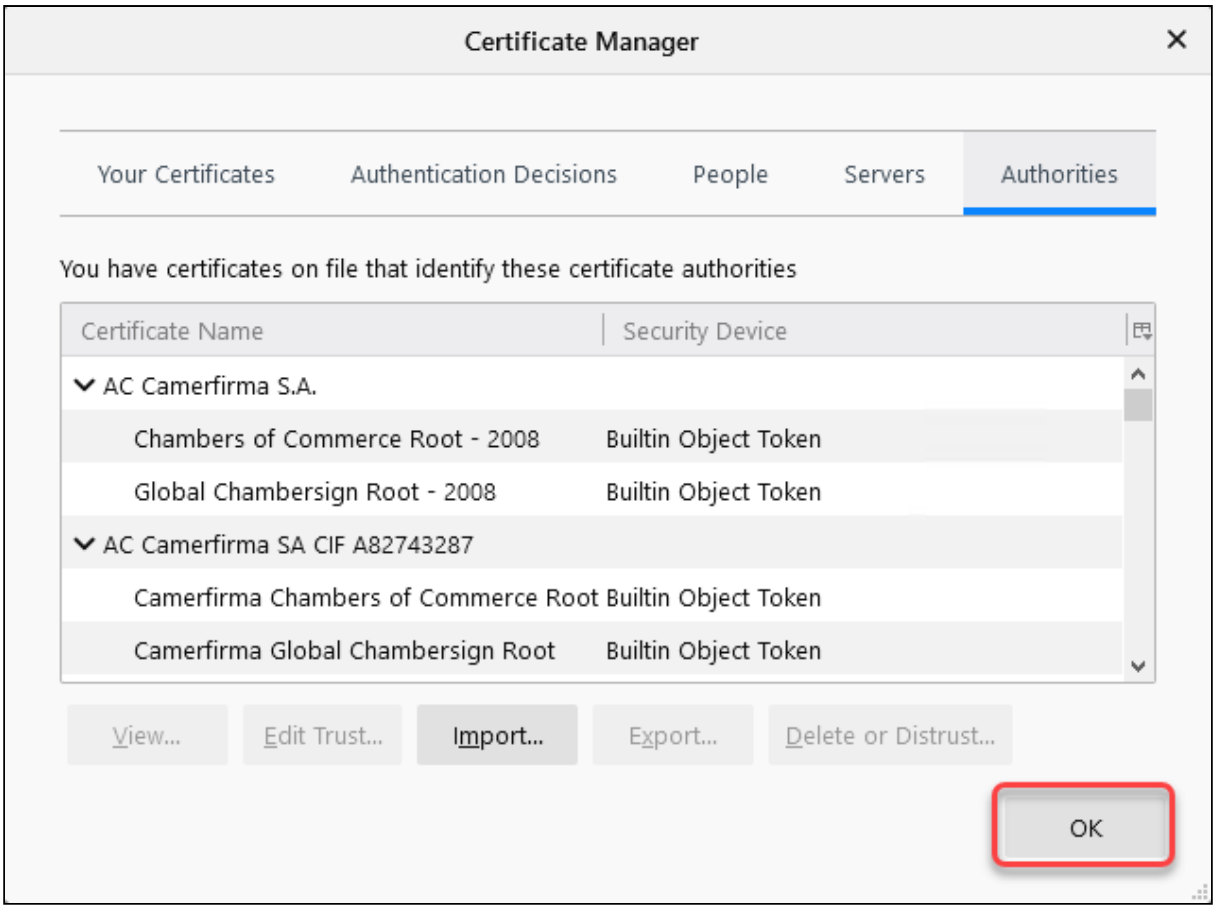
6. Select your certificate file and click **Open**.



7. Activate **Trust this CA to identify websites** and click **OK**.



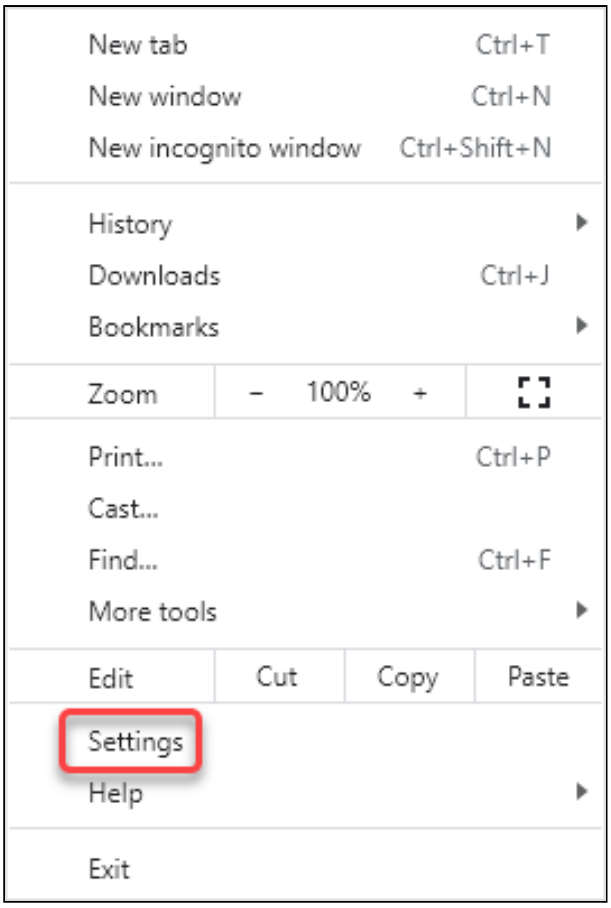
8. Close the Certificate Manager window with **OK**.



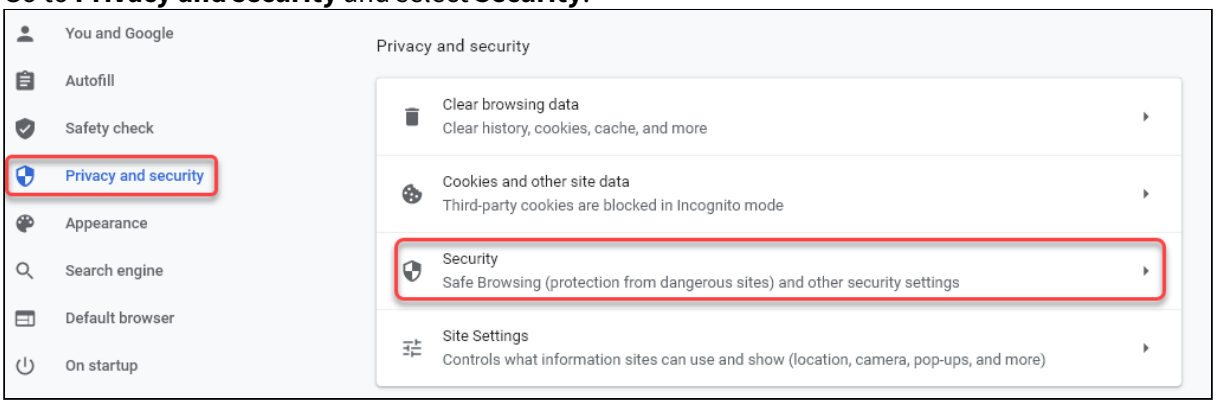
9. Restart the browser.
   The browser can access the UMS Web App without problems.

Chrome

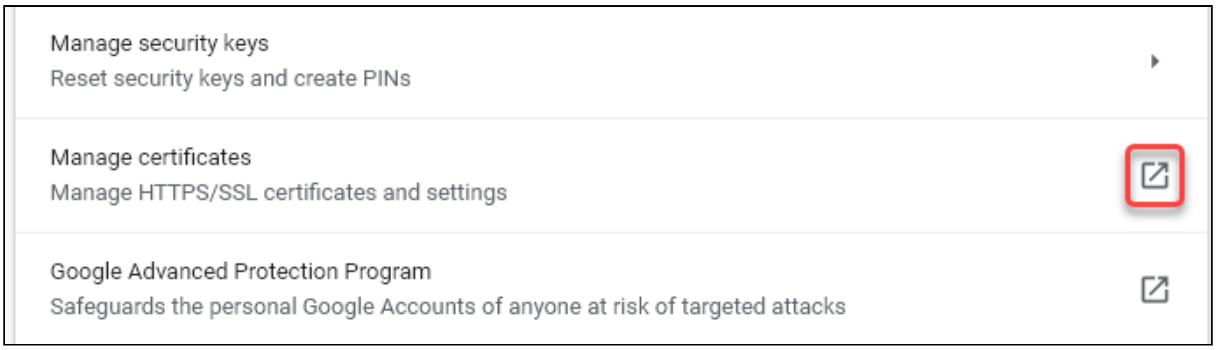
1. Click ⋮ to open the menu.
2. Select **Settings**.



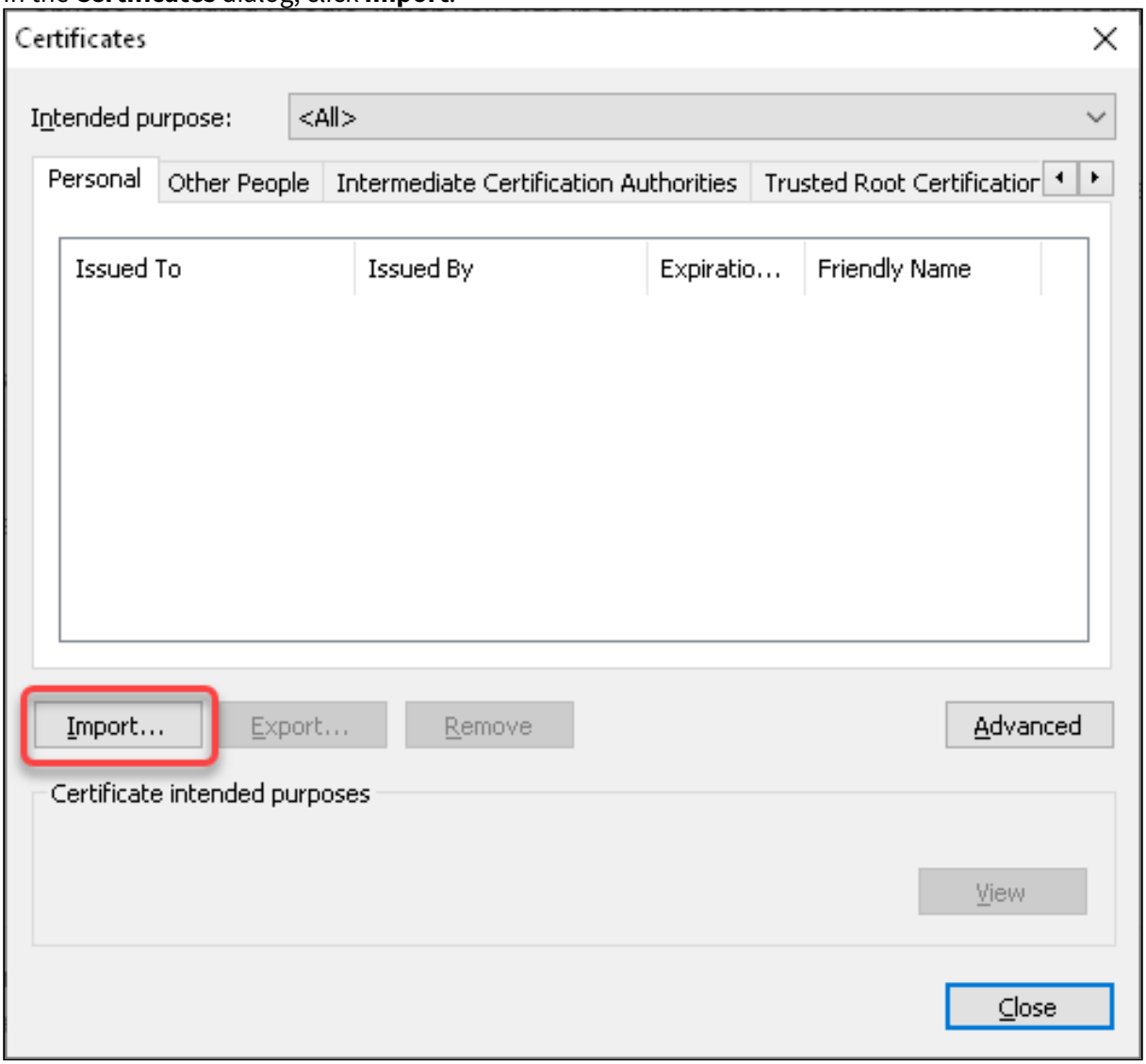
3. Go to **Privacy and security** and select **Security**.



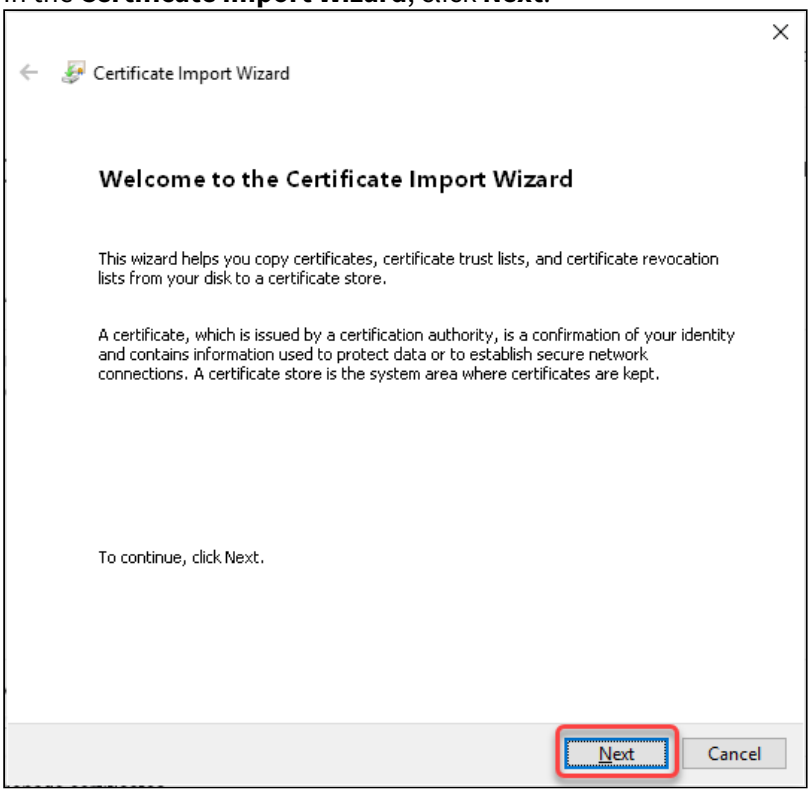
4. Scroll down and click the symbol next to **Manage certificates**.



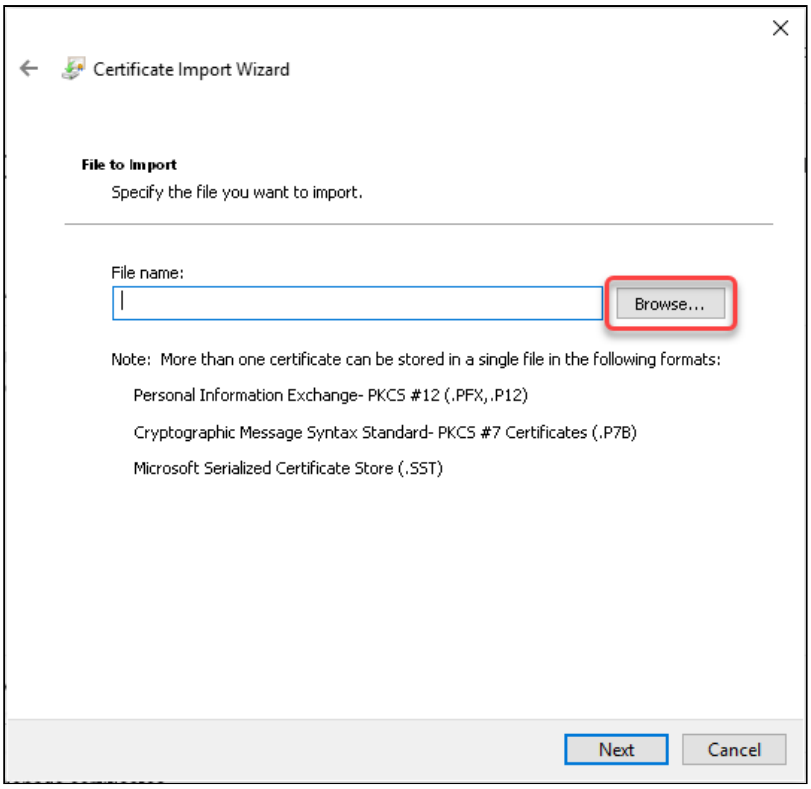
5. In the **Certificates** dialog, click **Import**.



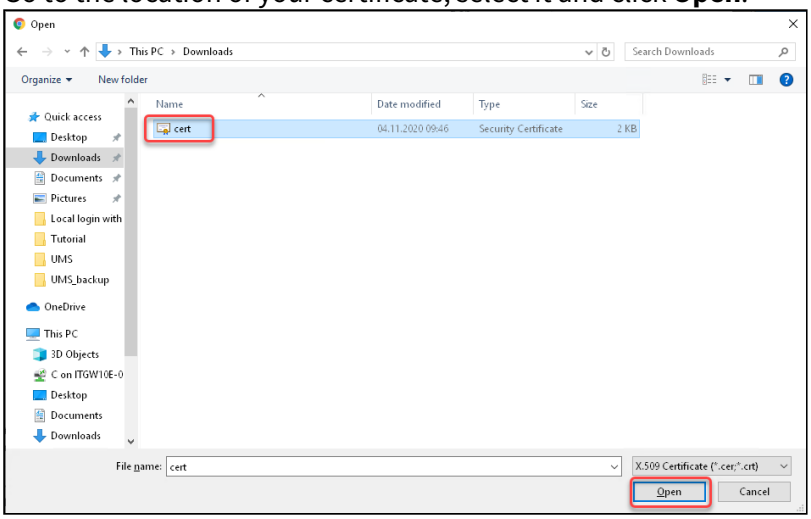
6. In the **Certificate Import Wizard**, click **Next**.



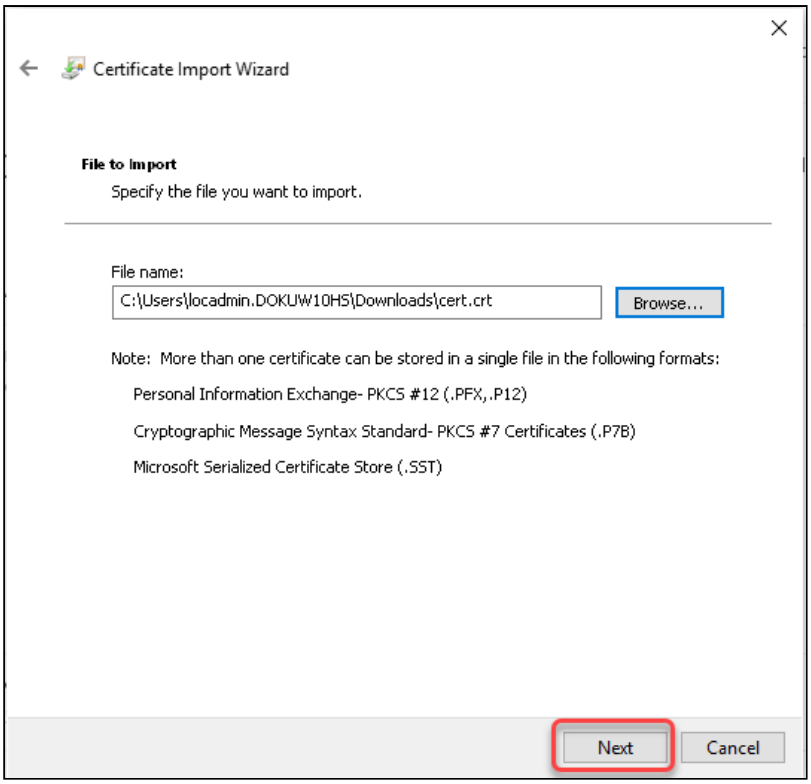
7. Click **Browse** to open the file chooser.



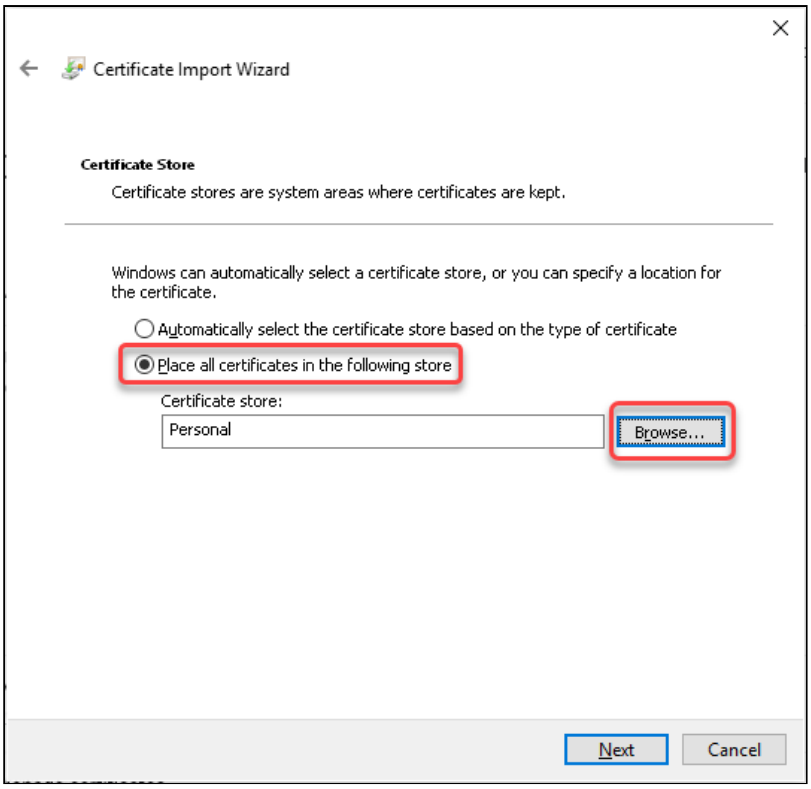
8. Go to the location of your certificate, select it and click **Open**.



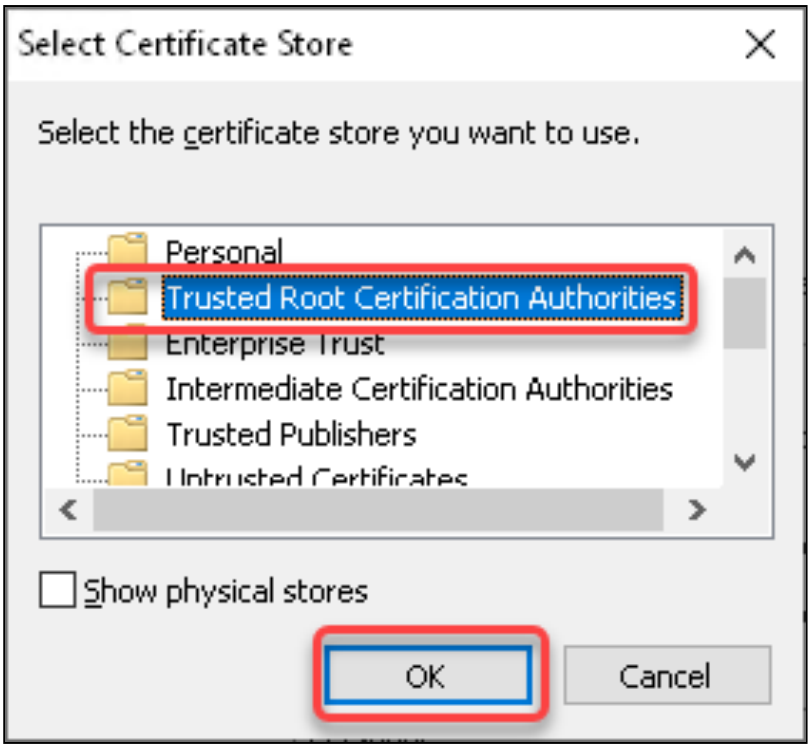
9. Back in the Certificate Import Wizard, click **Next**.



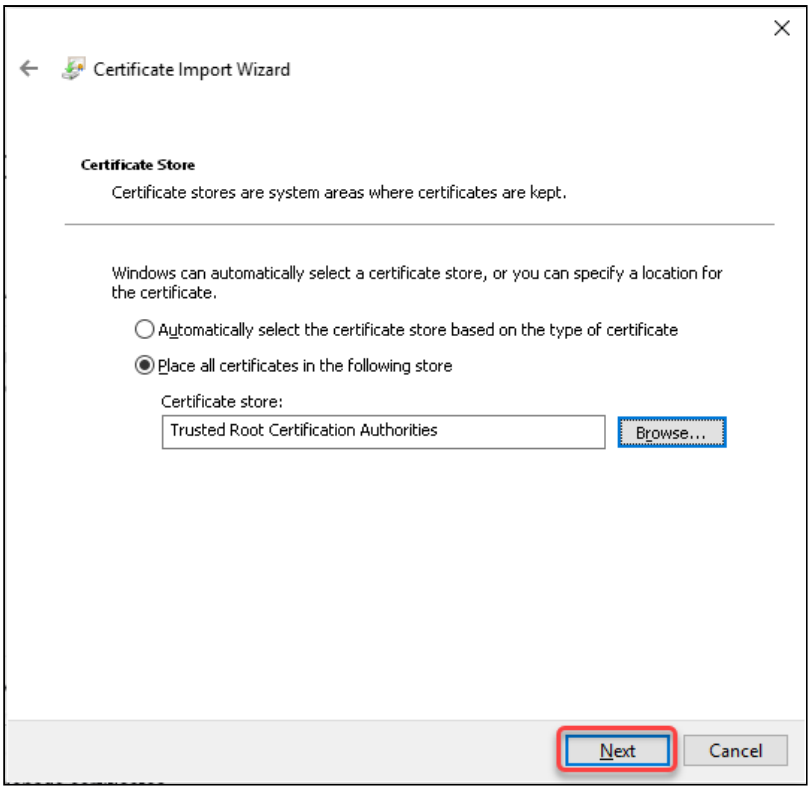
10. Select **Place all certificates in the following store** and click **Browse** to determine the certificate store.



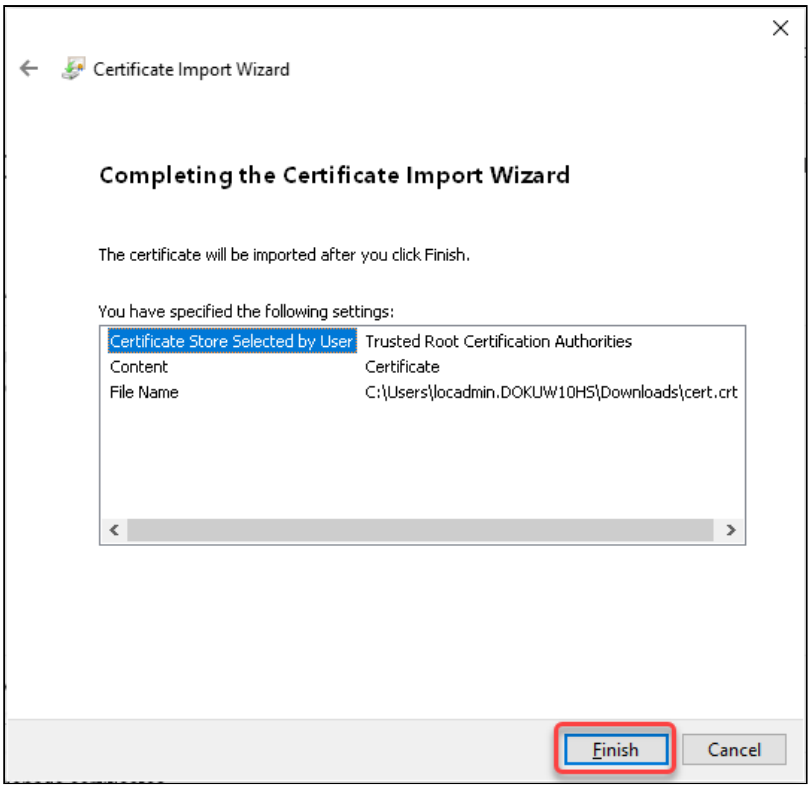
11. In the **Select Certificate Store** dialog, select **Trusted Root Certificate Authorities** and click **OK**.



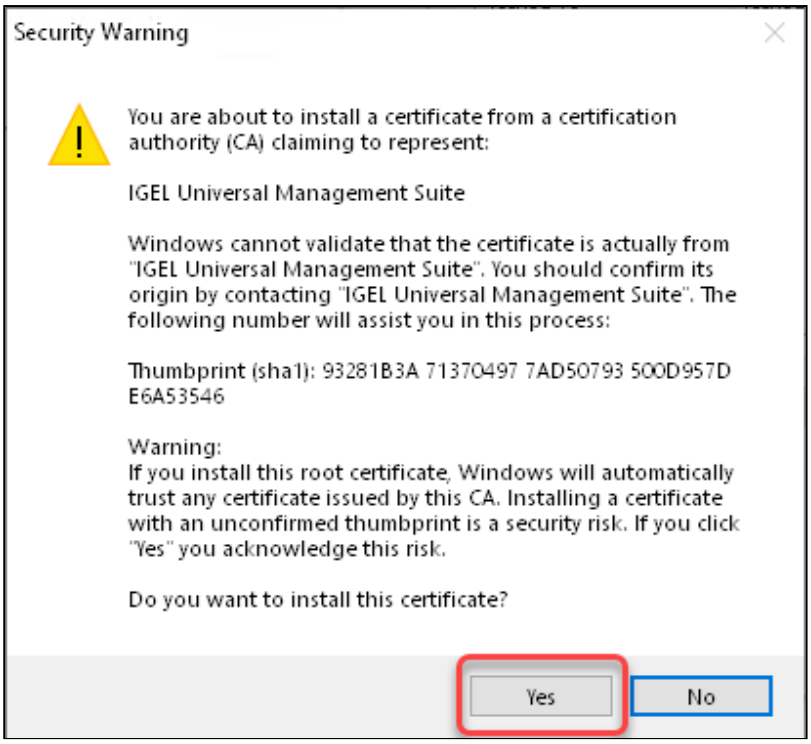
12. Back in the **Certificate Import Wizard**, click **Next**.



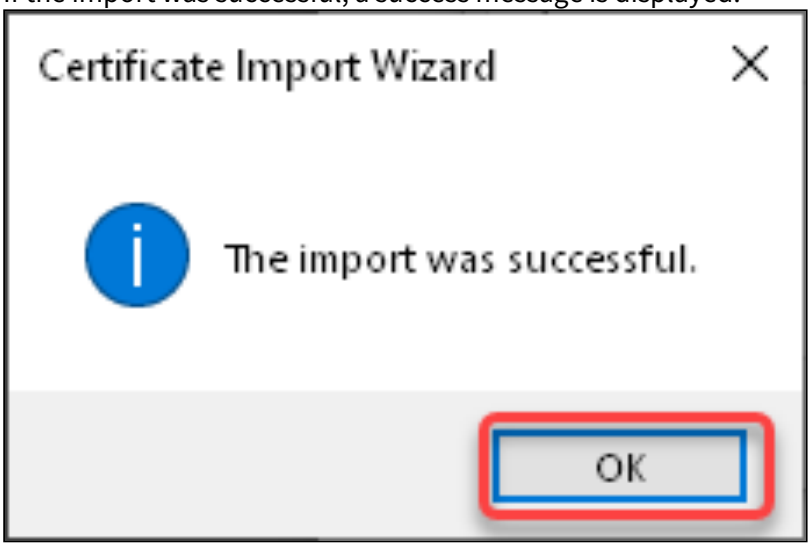
13. Review your settings and click **Finish**.



14. Confirm the **Security Warning** with **Yes**.



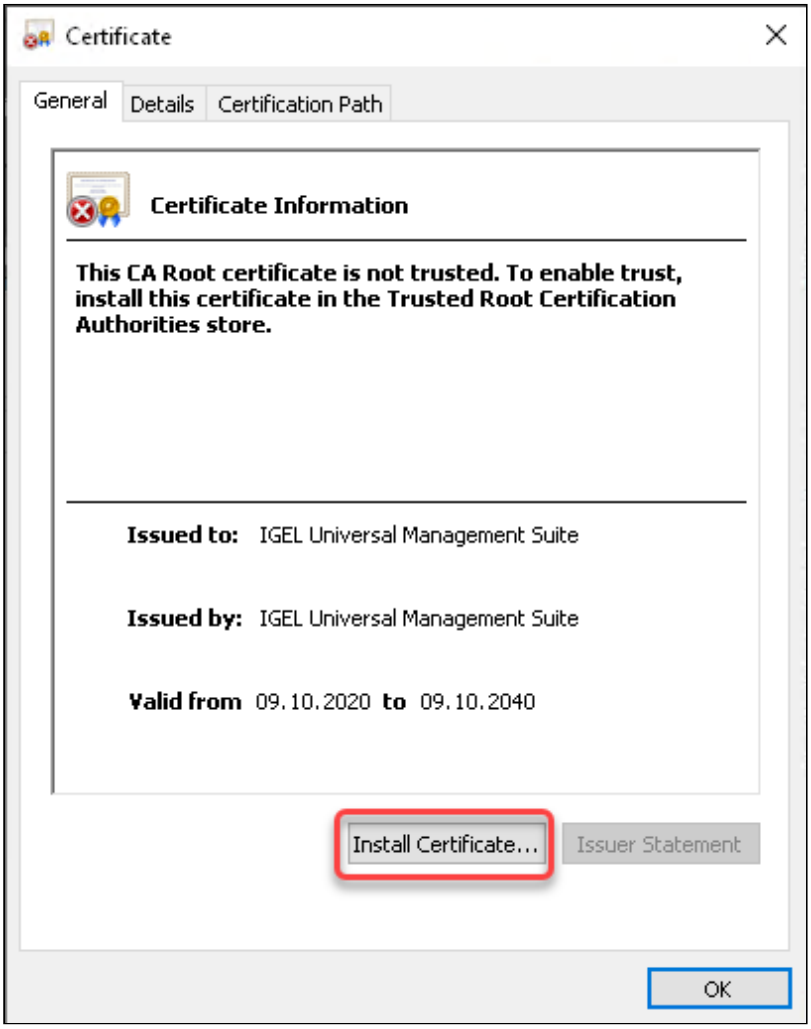
15. If the import was successful, a success message is displayed.



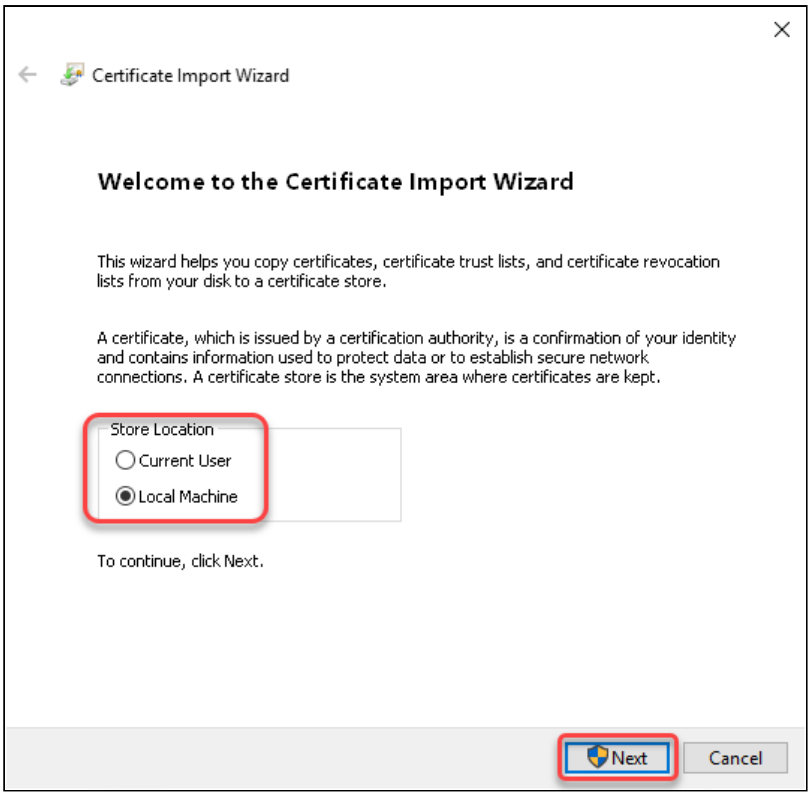
    The certificate is installed on your system.
16. Restart the browser.
    The browser can access the UMS Web App without problems.

Microsoft Edge

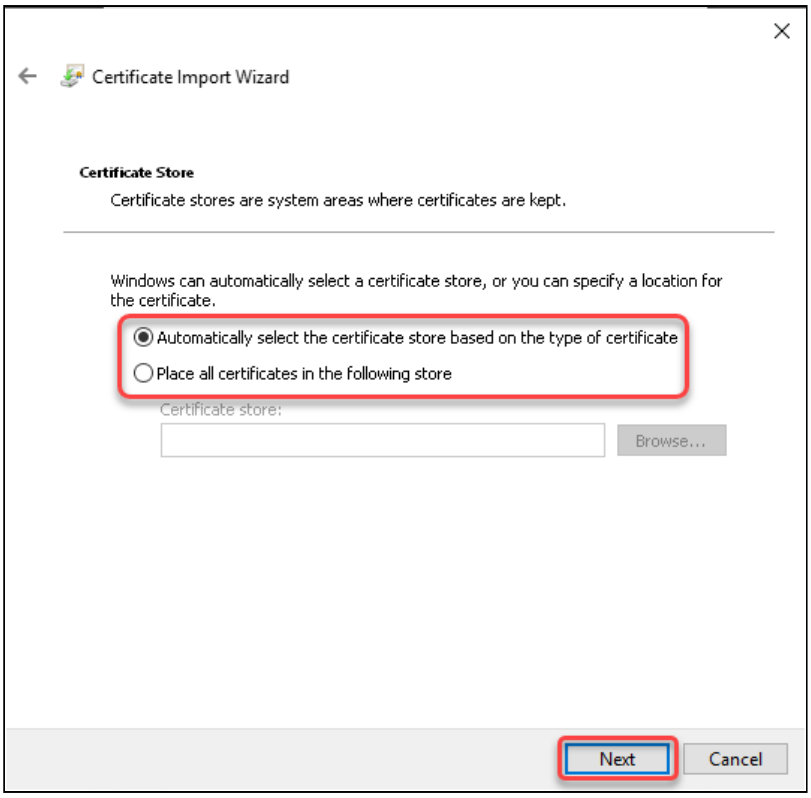
1. Make sure you have administrator permissions.
2. Go to the location where you have stored the certificate and double-click the certificate file.
   The **Certificate** dialog of your Windows system opens.
3. Click **Install Certificate...**.



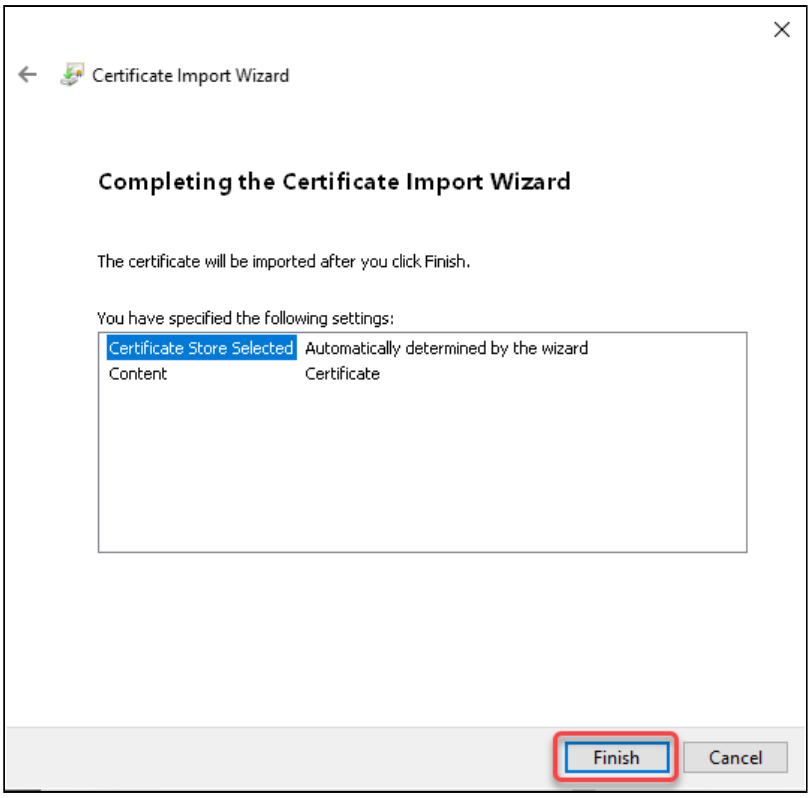
4. Define whether the certificate should be installed for the current user only or for all users (**Local Machine**) and click **Next**.



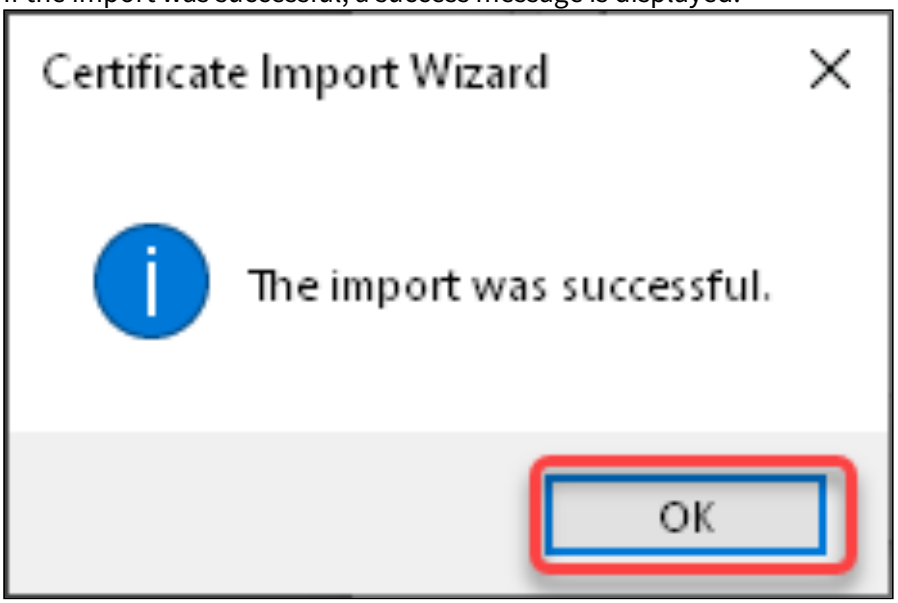
5. Confirm the **User Account Control** dialog.
6. Define whether the certificate store should be determined automatically or manually and click **Next**.



7. Review your settings and click **Finish**.



If the import was successful, a success message is displayed.



The certificate is installed on your system.

8. Restart the browser.
   The browser can access the UMS Web App without problems.

Troubleshooting: Starting the UMS Console Crashes NX Session

Symptom

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

Solution

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

Troubleshooting: UMS Console Does Not Start on Linux System without X11

Symptom

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

Problem

The UMS console application needs X11 to run.

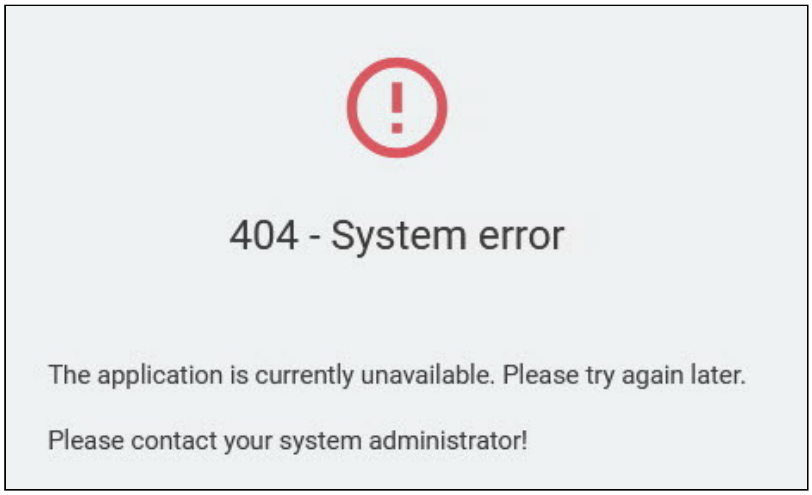
Solution

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

Troubleshooting: 404 - System Error Message at UMS Web App Startup

Symptom

After the installation of the Universal Management Suite, the UMS Web App starts with a 404 system error.



Environment

- UMS 6.08.100 or higher with the embedded database
- Microsoft Windows Server 2019

Problem

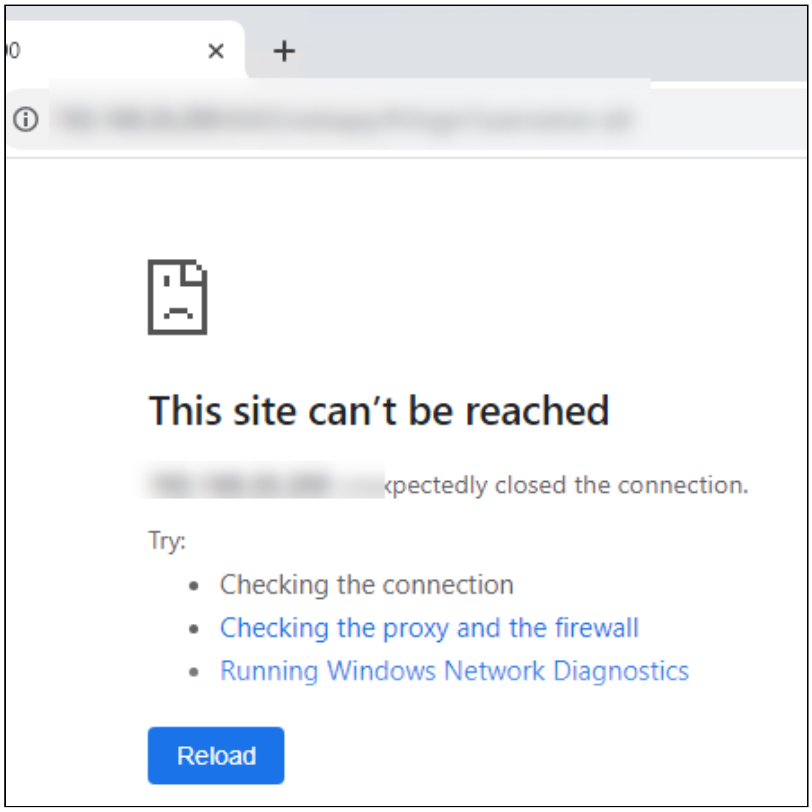
This might happen at startup when the UMS Web App is starting faster than the UMS Server service.

Solution

Restart the Windows service `IGEL RMGUIServer`. Details on how to do this can be found under IGEL UMS HA Services and Processes (see page 1425).

Troubleshooting: Chromium Rejects the Connection to UMS Web App

When opening the IGEL UMS Web App in Chromium browser, Chromium rejects the connection.

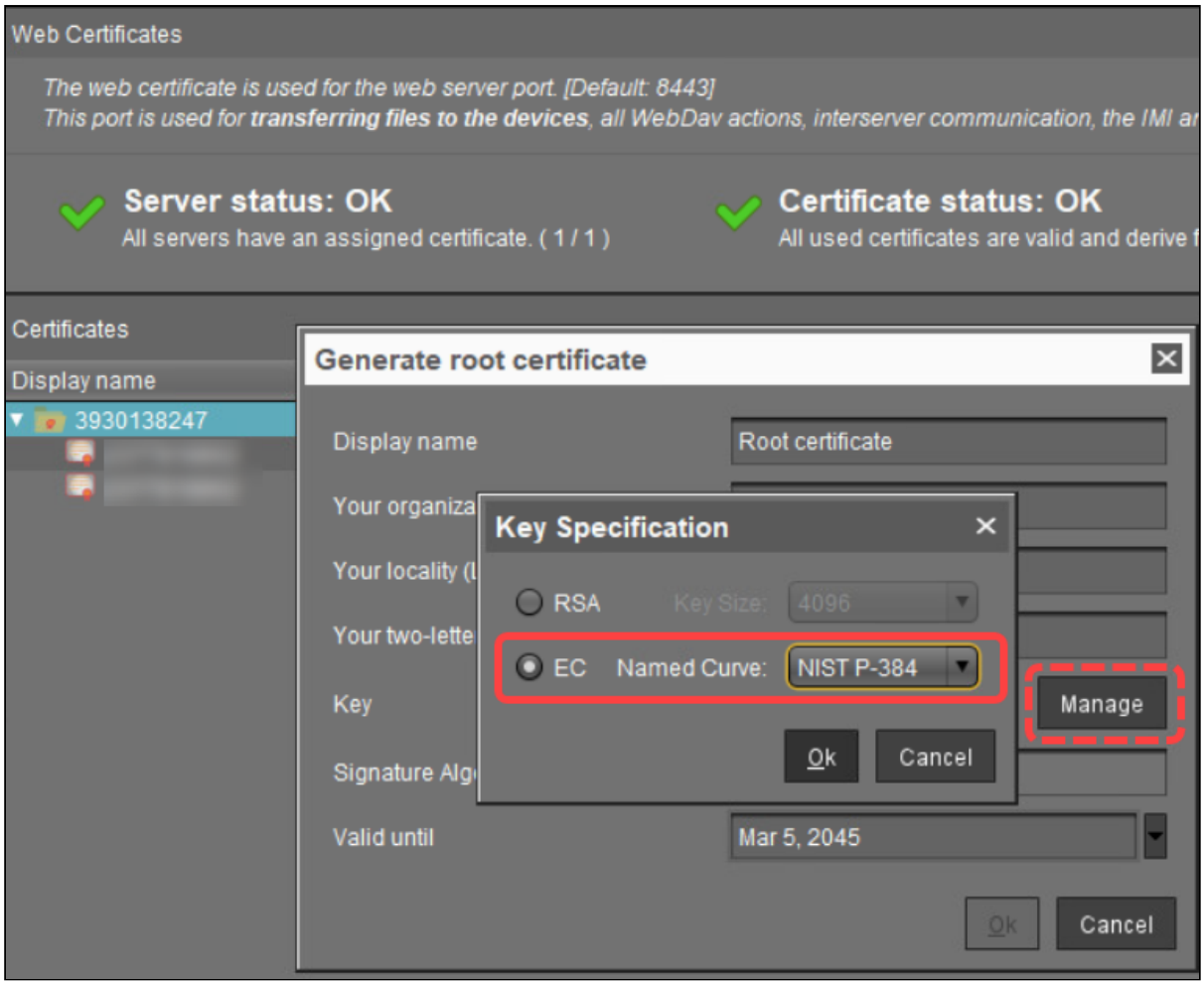


Problem

You are using an ECS based certificate, with NIST P-521 named curve setting in the root certificate of your web certificate. This curve setting is not supported by Chrome.

Solution

Use named curves NIST P-384 (default) or NIST P-256 when generating the root certificate for the web certificate.


Web Certificates
The web certificate is used for the web server port. [Default: 8443]
This port is used for transferring files to the devices, all WebDav actions, interserver communication, the IMI ar
Server status: OK
All servers have an assigned certificate. (1 / 1)
Certificate status: OK
All used certificates are valid and derive f
Certificates
Display name
3930138247
Generate root certificate
Display name
Root certificate
Your organiza
Your locality (l
Your two-lette
Key
Signature Alg
Valid until
Mar 5, 2045
Manage
Ok
Cancel
Key Specification
RSA
Key Size:
4096
EC
Named Curve:
NIST P-384
Ok
Cancel

Troubleshooting Active Directory Login Not Working After Update to UMS 12.08.100

After upgrading to version 12.08.100 of the IGEL UMS (Universal Management Suite), you might find that logging in with an Active Directory (AD) or LDAP account no longer works.

Problem

UMS now requires something called a “Browse User” to be set up for AD/LDAP logins to work. This change improves security by making sure only authorized users can be looked up and verified in the directory.

Solution

You’ll need to tell UMS which AD account it should use to “browse” or look up user information. This account:

- Must be a valid AD user
- Needs read access to:
  - User account details
  - Group memberships
  - Other necessary AD data

To set up a browse user:

1. Open **UMS**, then go to **AD Configuration.**

2. Enter the **Username** and **Password** for the AD user that will act as the “browse user”.

3. Confirm that this AD account has permission to view the needed user and group information.

For more help, see the IGEL Knowledge Base article: Configuring an AD Connection[118]

118. https://kb.igel.com/en/universal-management-suite/current/configuring-an-ad-connection

Troubleshooting Login Issue with “Bad Request” Error After Update to UMS 12.08.100

After updating the IGEL Universal Management Suite (UMS) to the latest version 12.08.100, some users might see this error when trying to log in:

```
HTTP Status 400 – Bad Request
```

```
invalid_request – OAuth 2.0 Parameter: redirect_uri
```

Problem

This error appears when the web address (URL) you’re using to access UMS is not one of the approved addresses saved in the system settings. For security reasons, the system now only allows login links that match a list of “trusted addresses.”

Solution

Make sure you are using a login address that is allowed by UMS. Here are the valid types:

- Local Address – for example: `https://localhost:<ums-server-port>`
- Internal Server Address – for example: `https://<server-address>:<server-port>`
- Cluster Address – for example: `https://<cluster-address>`

> If you’re using a different address, the system will block the login attempt.

To fix the issue:

1. Check and update your UMS settings to include the correct address(es). You may need to look in:
   - Server Network Settings[119]
   - Post-Install Configuration[120]
   - If you use a URL to login to your UMS, which is not detected automatically, you can add additional redirect URIs: Check the section “Redirect URIs for UMS Web App Login” in UMS Login Requirements[121]
2. After making changes, restart the UMS services to apply them.

119. https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums#id-(12.07.110-en)ServerNetworkSettingsintheIGELUMS-ClusterAddress
120. https://kb.igel.com/en/universal-management-suite/current/post-installation-configuration-of-the-igel-ums-se
121. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Important Note

These settings don’t just affect login. Devices managed by UMS also need to reach these trusted addresses. Be sure all devices are using the correct one.

Troubleshooting Endless Loop of Web App Login when UMS Installed with Non-default Port

After installing or upgrading to the newest version of IGEL UMS (Universal Management Suite), version 12.08.100 with a non-default port (e.g. 443), you might find that logging in to the IGEL UMS Web App leads to an endless browser loop.

Problem

The configuration file of the `wums-app` is misconfigured, which activates the fallback to the default port.

Solution

1. Open the file `{installation.path}/rmguiserver/webapps/wums-app/WEB-INF/classes/config/application-embedded.yml`
2. Move the config for `auth-service` port from `igel.wums` to `igel.client`
3. The file should now have a section like this:

```
client:
    permission-service:
      port: ${igel.embedded.tomcat.port}
    license-service:
      port: ${igel.embedded.tomcat.port}
    auth-service:
      port: ${igel.embedded.tomcat.port}
```

4. Restart the UMS Service.

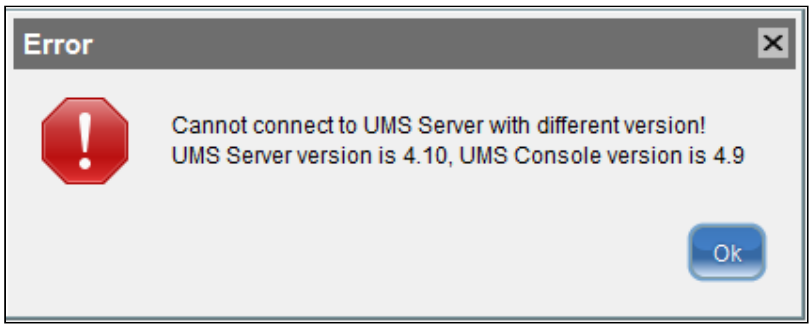
Logon Failures in the IGEL UMS

Troubleshooting UMS Console Logon Fails

Symptom

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

More recent UMS versions show the following error message:



Problem

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

Solution

Check the version status:

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

Troubleshooting UMS Console Login with AD User Account Fails

Symptom

UMS console login fails for Active Directory user.

Problem

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

Solution

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

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

Troubleshooting Login to the UMS Fails after Update

Symptom

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

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

Problem

The IGEL RMGUI Server Service has not fully started yet.

Solution

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

Active Directory / LDAP

How to Integrate Active Directory in IGEL UMS

Instead of creating and organizing UMS administrators manually you are looking for an easy way of importing them from your existing Active Directory, using the same AD group assignments and credentials as already defined in the AD. In this chapter you will find the best way of importing users from the Active Directory as UMS administrator accounts.

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

Configuring an AD Connection

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

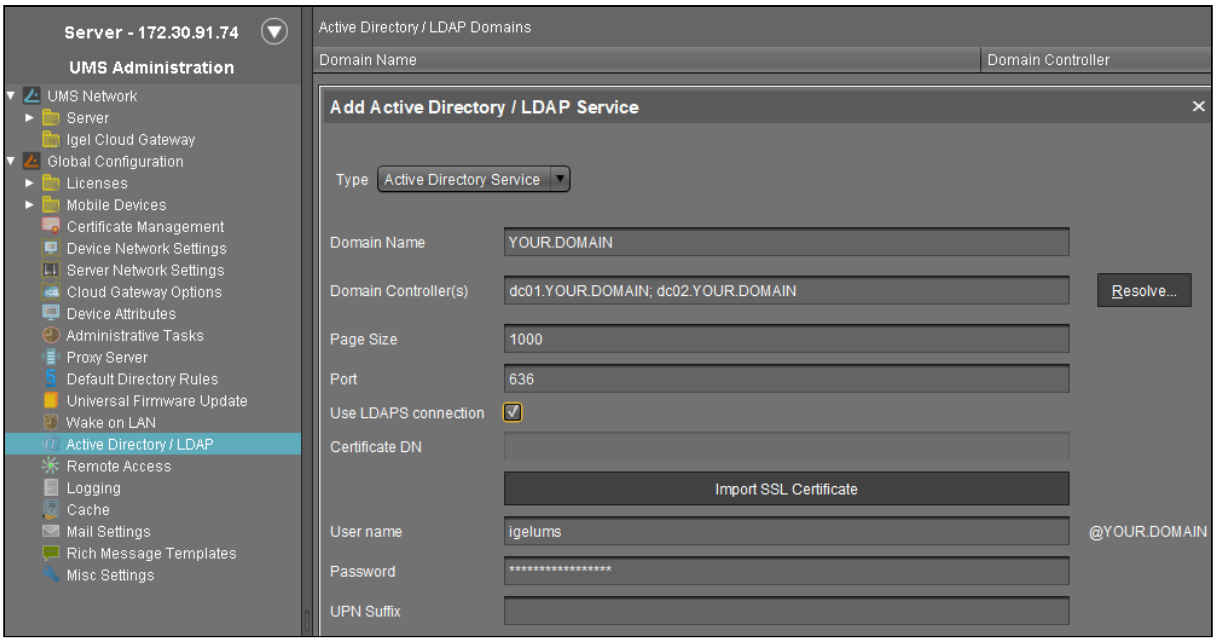
In this article, the terms "Active Directory" and "LDAP" are, to an extent, used interchangeably:
- Administrative users / UMS administrators can be imported both from an AD and from LDAP.
- Shared Workplace users can only authenticate against an Active Directory. An LDAP service cannot be used for this purpose.

1. If you have user and group dependencies between different configured domains/subdomains, then 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. Click **Add (+)** under UMS console > **UMS Administration > Global Configuration > Active Directory / LDAP**.
The **Add Active Directory / LDAP Service** dialog opens.



3. Select **Active Directory Service** as **Type.**

4. Enter the **Domain Name**.

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

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

If the option **Use LDAPS connection** (see below) is enabled, make sure that a fully qualified name of the **Domain Controller** has been entered, e.g. `dc01.your.domain` f the option **Use LDAPS connection** (see below) is enabled, make sure that a fully qualified name of the **Domain Controller** has been entered. See Troubleshooting Problems When Configuring an Active Directory with LDAP over SSL (see page 613) .

6. Enter **Page Size**.
   The **Page Size** property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but not the number of overall results. The standard value is "1000". Change this value in line with your server configuration.

7. Activate **Use LDAPS connection** to secure the connection with the provided certificate.
   The **Port** changes automatically to default "636".

8. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

⚠ Since the name of the **Domain Controller** is checked against the certificate, they must correspond. If more than one domain controller is used, the root certificate of the domain must be configured. See Troubleshooting Problems When Configuring an Active Directory with LDAP over SSL (see page 613) .

ℹ The supported certificate extensions are `.cer`, `.pem` and `.der`; the format is Base64.

9. Under **User name** and **Password**, enter your user credentials. This user must have read access in Active Directory.

ℹ Please pay attention to upper and lower case when entering the username.

10. Enter **UPN Suffixes** (aliases) if you have defined any (semicolon separated list). Example: `domain.local;test.local`

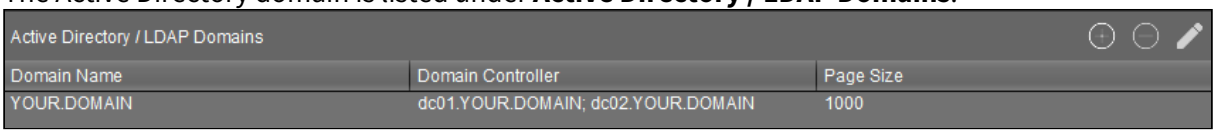
⚠ The UPN Suffix is required for UMS version 12.08.100 and higher.

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

11. Click on **Test Connection** to check that you have entered a valid configuration.

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).

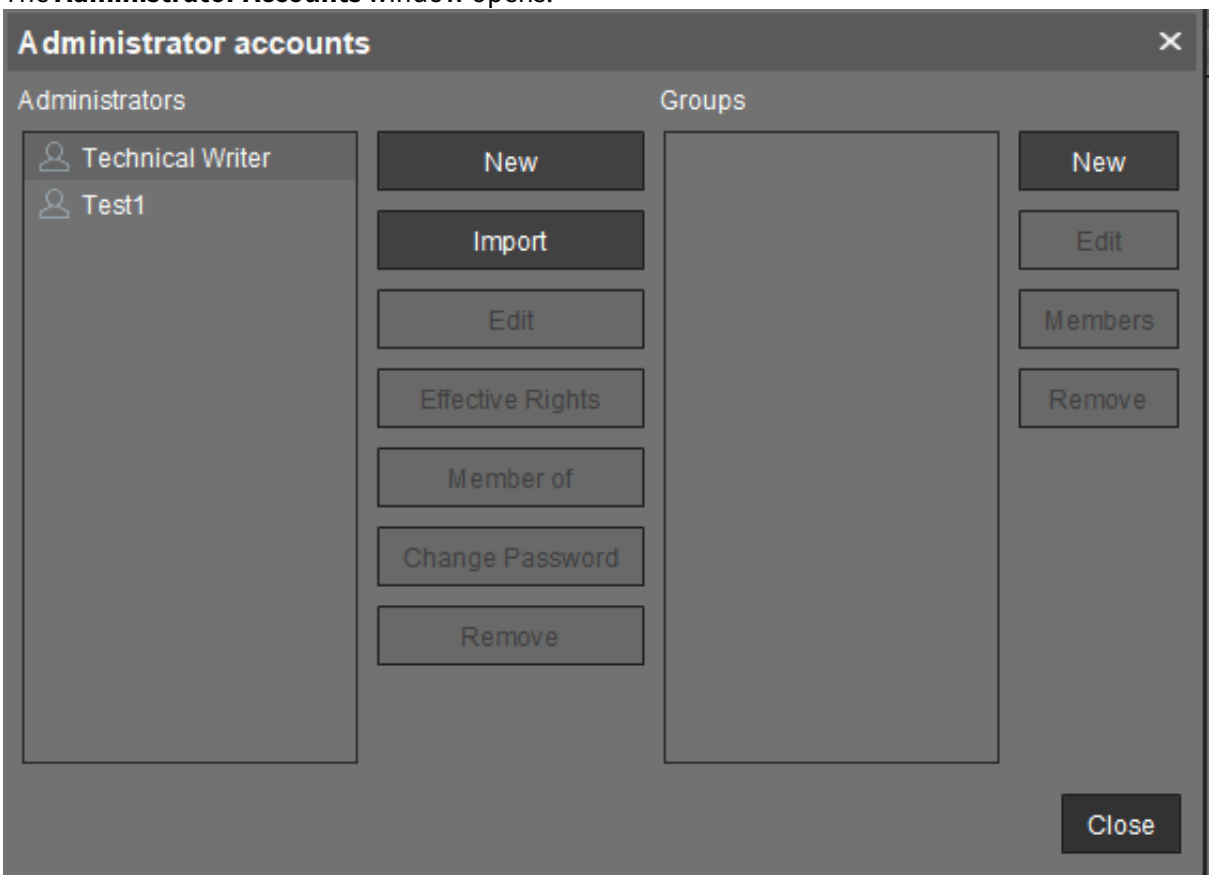
12. Click **Ok** to confirm your settings.
The Active Directory domain is listed under **Active Directory / LDAP Domains**.



Importing Users from AD to UMS

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

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



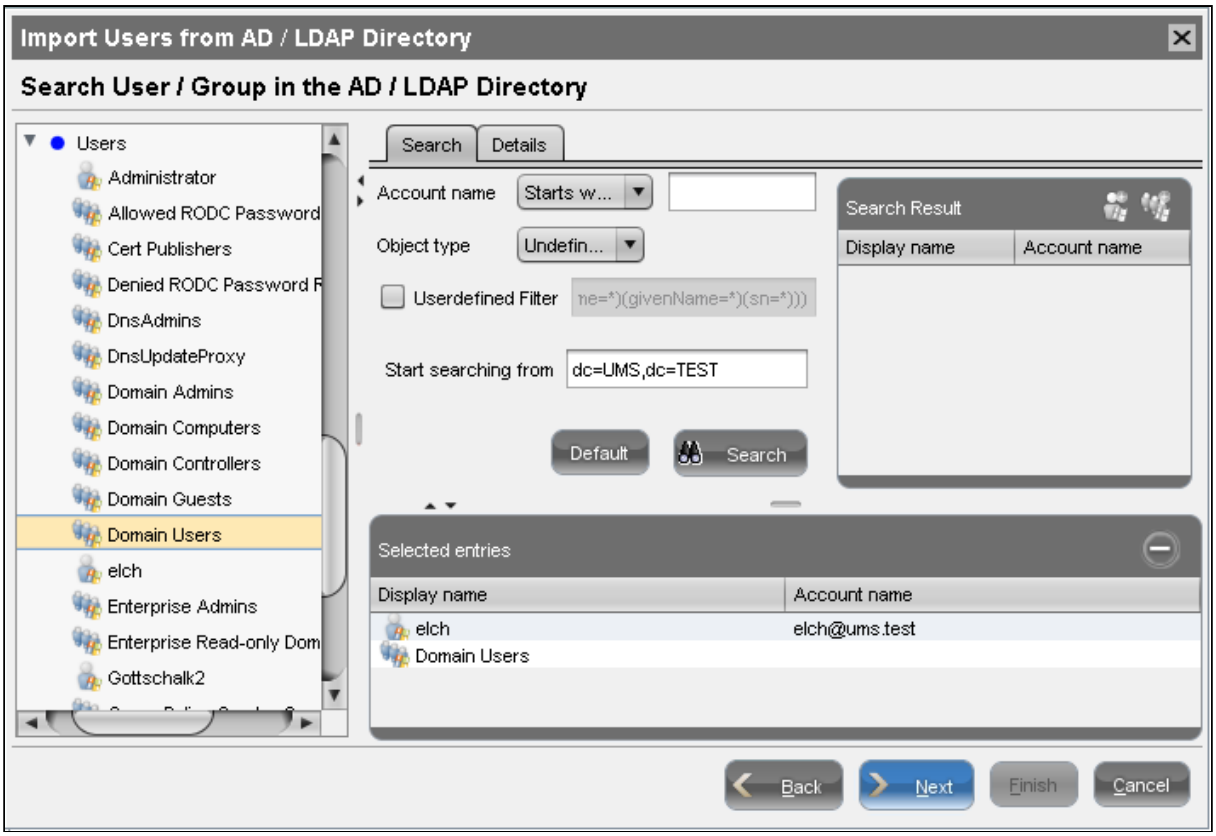
2. Click **Import** to log in to the AD/LDAP service.

3. Select the domain and enter your credentials, if not already defined.

4. Click **Next** to open the Active Directory browser.

5. Select individual users or groups from the structure tree of your AD.

6. Use drag and drop to add your selection to the **Selected Entries** list.



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

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

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

If the result list is either empty or some accounts are missing from the list, see Troubleshooting Import of Administrator Accounts from Active Directory Fails (see page 614).

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

Assigning Permissions

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

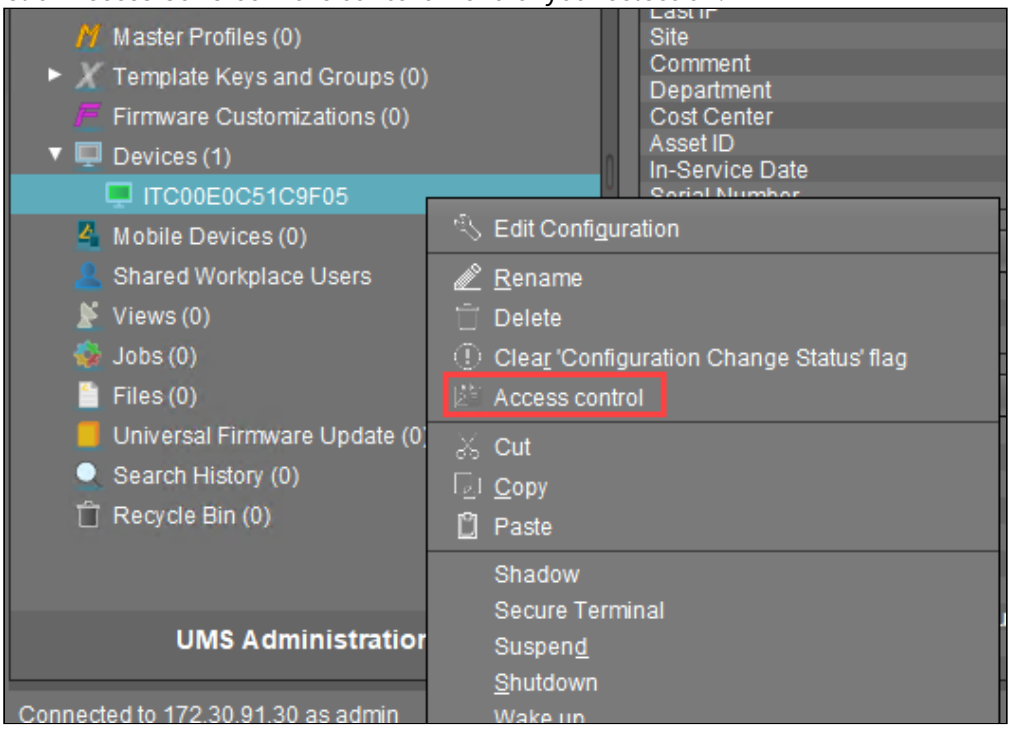
As UMS administrators, the users still need individual access rights.

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

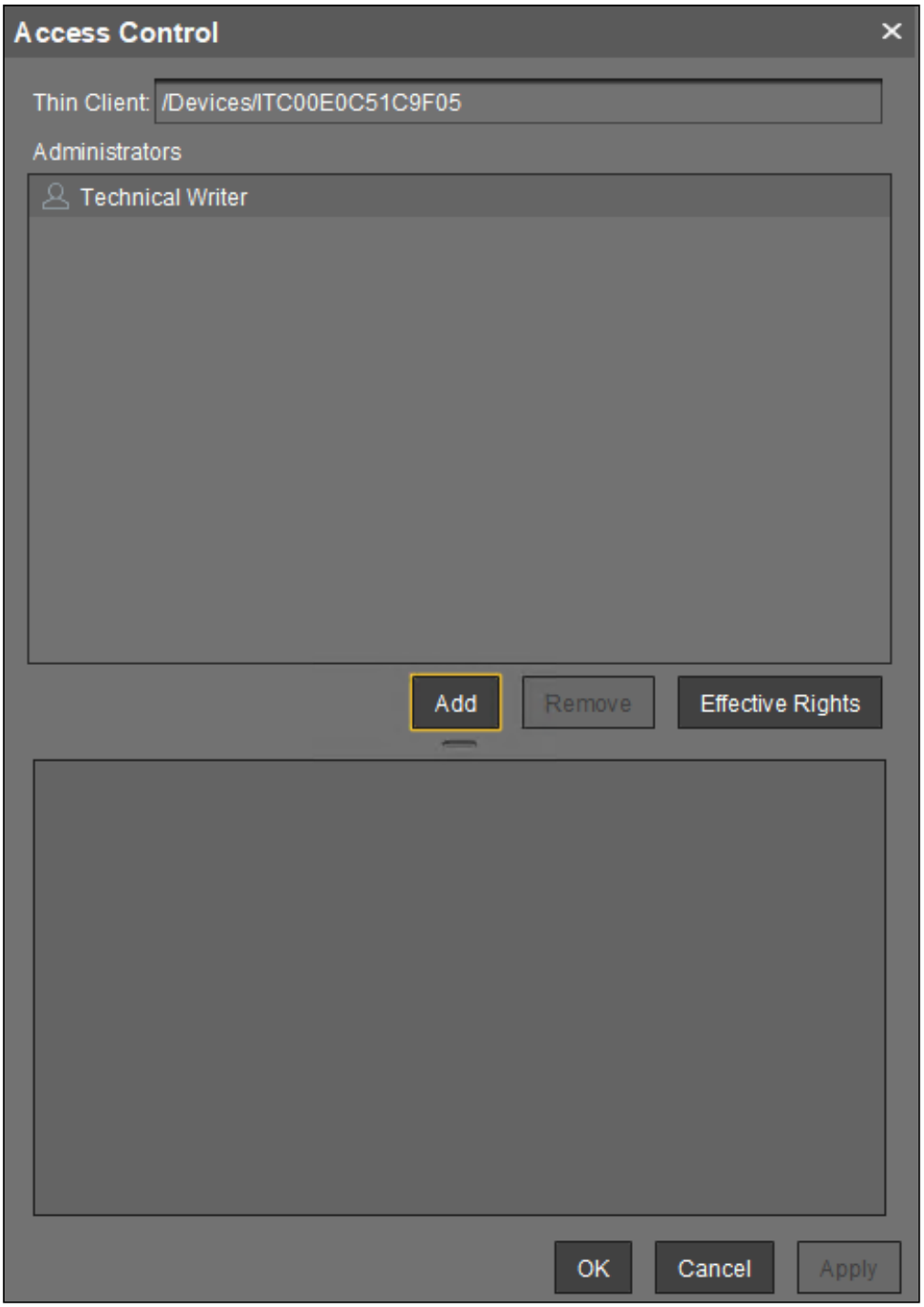
> For example, in order to be able to change the configuration of a thin client, a user requires authorization to browse the thin client's directory path and configure the thin client itself.

To assign these rights, proceed as follows:

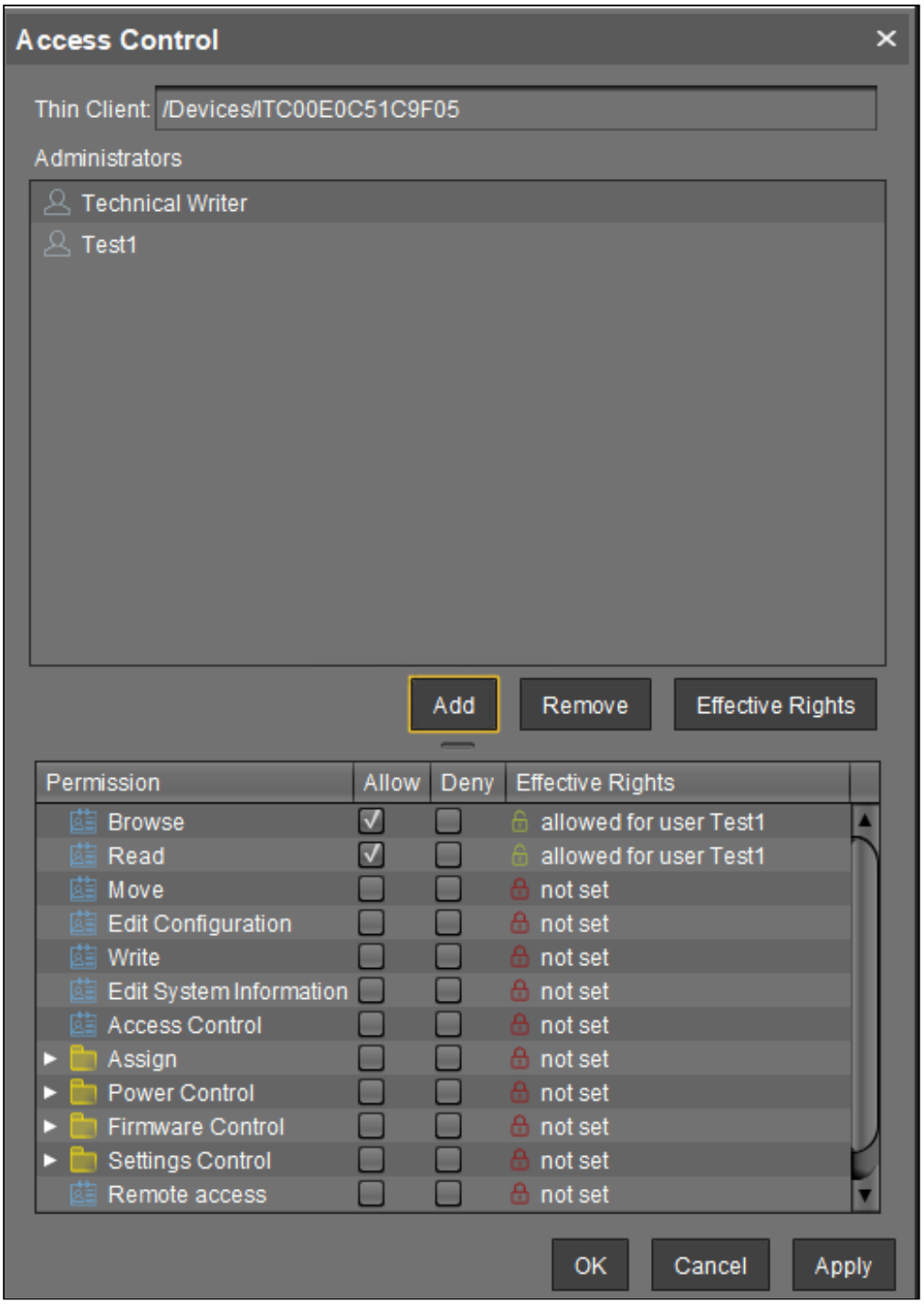
1. In the structure tree of the UMS console choose the **Devices** node or a subgroup of devices or a single client.
2. Click **Access Control** in the context menu of your selection.



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



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



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

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

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

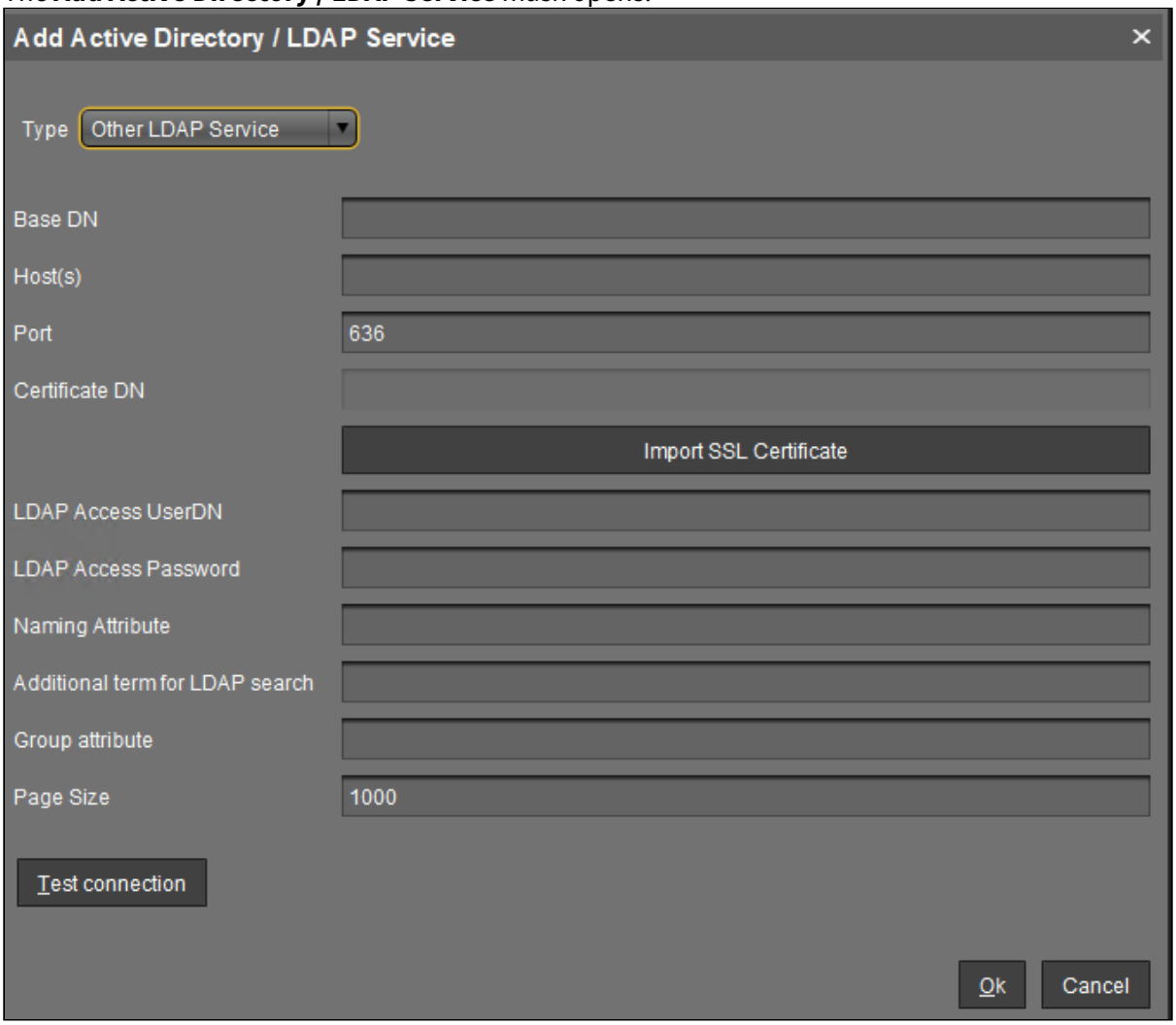
For further details about authorization rules see our How-To IGEL UMS: User Authorization Rules (see page 414).

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

Configuring an LDAP Connection

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

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



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

For security reason UMS supports secure LDAP connections only.

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

Troubleshooting Problems When Configuring an Active Directory with LDAP over SSL

Symptom

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

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

Problem

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

Solution

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

Troubleshooting Import of Administrator Accounts from Active Directory Fails

Symptom

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

Problem

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

Solution

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

How to Configure IGEL UMS As Identity Broker

You can use the IGEL Universal Management Suite (UMS) as identity broker for IGEL OS 12 devices. With this configuration, users of IGEL OS 12 devices can login to the company Active Directory (AD) through the UMS even if they are outside of the company network. You need to connect the AD to the UMS and configure devices as described below to use the UMS as identity broker.

Prerequisites

To use the UMS as an identity broker for OS 12 devices, you need the following:

- You need to have an IGEL OS Edition in place that includes the license. For details, see https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions .
- IGEL OS version 12.6.1 or higher
- IGEL UMS version 12.07.100 or higher

Overview

When the UMS is configured as identity broker, users are authenticated with their AD credentials through the UMS:

1. The user of the IGEL OS 12 device types in the AD credentials in the login screen.
2. The credentials are forwarded through to the IGEL UMS.
3. The UMS executes a login in AD.
4. If the login is successful, the user gets access to the device.

> The authentication also works if IGEL OS 12 devices are connected to the UMS through the IGEL Cloud Gateway (ICG).

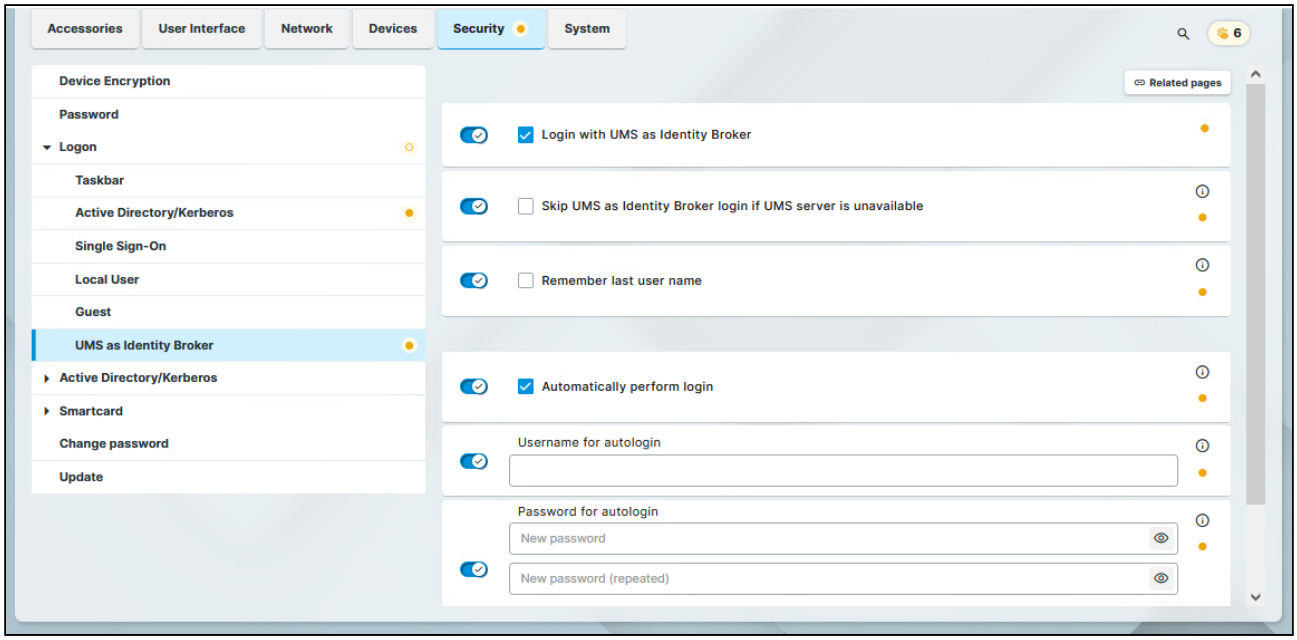
Connect Active Directory to the UMS

To connect an AD to the UMS, proceed as follows:

1. Go to **UMS Administration > Active Directory/LDAP** in the UMS Console.
2. Configure the Active Directory connection. For details, see Configuring an AD Connection (see page 601) .
   Your Active Directory is now connected to your IGEL UMS and is listed under Active Directory domains.

> Other LDAP servers (*Novell eDirectory*, *OpenLDAP* etc.) cannot be used for user authentication purposes.

Configure the IGEL Device



You can configure the settings from the IGEL Universal Management Suite (UMS) via a profile or directly in device settings.

For details on how to create a profile, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252) .

1. In the profile/device configuration go to **Security > Logon > UMS as Identity Broker**.
2. Enable the **Login with UMS as Identity Broker** option.
3. Configure other options according to your needs. For more information, see UMS as Identity Broker with IGEL OS 12[122] .
4. Assign the profile to the devices. For details, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252)

Once the profile is assigned to the IGEL OS device, the user has to enter the AD credentials in the login screen and lock screen after a reboot.

122. https://kb.igel.com/en/igel-os-base-system/12.6.1/ums-as-identity-broker-with-igel-os-12

Profiles in IGEL UMS

How to Find Out a Profile's Priority in the IGEL UMS

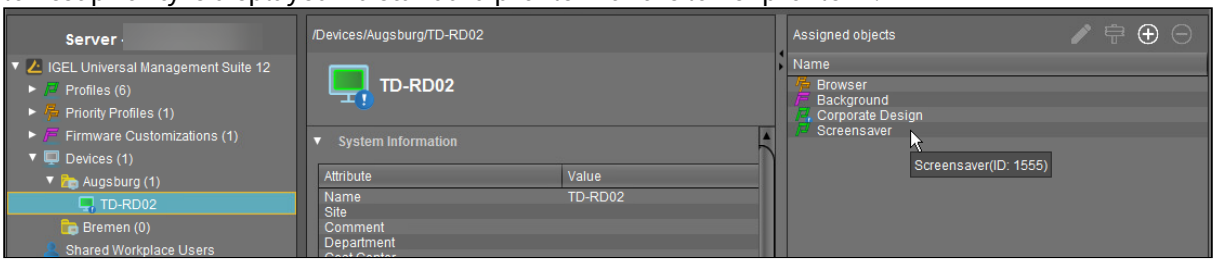
Using profiles is a very powerful method to manage and configure one, ten, or thousands of endpoint devices with the IGEL Universal Management Suite (UMS). However, when you are deploying a great number of profiles, things can get confusing. Some profiles may have overlapping scopes and thus try to set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

For a comprehensive reference of profiles, see Profiles in the IGEL UMS (see page 695); the prioritization is covered in Prioritization of Profiles in the IGEL UMS (see page 728).

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

1. In the **UMS Console > Devices**, select the device for which you want to see the order of profile priorities.
2. Take a look at the **Assigned objects** area. All profiles that are assigned to the device are listed by priority, in descending order. The profile with the highest priority is listed first, and so on.

   In the following screenshot, the profile with the highest priority is a so-called priority profile. It is followed by a firmware customization, which has in turn higher priority than a standard profile, see Firmware Customizations in the IGEL UMS (see page 764). And at the bottom, the object with the lowest priority is displayed – a standard profile with the lower profile ID.



Precedence of IGEL UMS Profiles and Universal Firmware Updates

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

General Order of Priority

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

- Universal Firmware Update
- Profile
- Local settings

For details, see the following sections.

Universal Firmware Update vs. Profile

If both a Universal Firmware Update and a profile that contains update settings are assigned to your device, the Universal Firmware Update has priority over the profile. This is also valid if the profile is a so-called priority profile; for further information, see Prioritization of Profiles in the IGEL UMS (see page 728) .

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

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

Profile vs. Local Settings

The settings of a profile always overwrite the local settings.

Universal Firmware Update vs. Universal Firmware Update

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

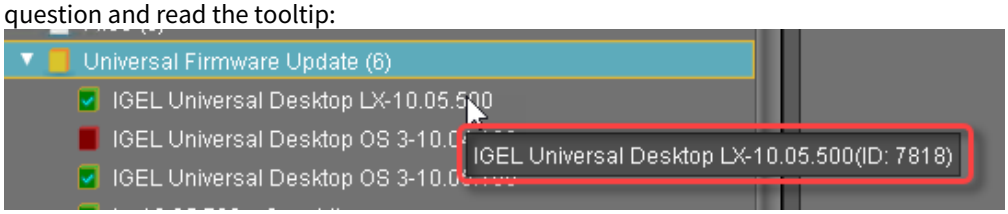
Assignment to Different Levels in a Hierarchical Order of Folders

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

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

Assignment on the Same Level

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



In this example, the ID is 7818.

Compatibility

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

How to Assign Profiles to Devices Filtered by Views or Search in IGEL UMS

If you need to assign a profile in the IGEL Universal Management Suite (UMS) to a group of devices which meet a certain criterion, you can proceed in the following way.

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

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

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

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

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

Troubleshooting: Profile Settings Not Applied

Problem

When an IGEL Universal Management Suite (UMS) profile is applied to a OS 11 or OS 12 device, some settings from the profile are not applied correctly to the device.

Solution

Adding an automatic reboot to the UMS profile ensures the correct application of the settings from the profile to the device.

To trigger the automatic reboot when the profile is applied to the device:

1. In the UMS profile go to **System > Firmware Customization > Custom Commands > Desktop**.
2. Add the following as a **Final desktop command**:
   ```
   if [ ! -f /wfs/.one_more_reboot_done ] ; then touch /wfs/.one_more_reboot_done ; systemctl reboot ; fi
   ```
3. Save the profile.

Misc

Where Can I Find the IGEL UMS Log Files?

The following article details where you can find and configure IGEL Universal Management Suite (UMS) log files.

For enabling the logging of UMS user actions and actions initiated by a device, see Logging in the IGEL UMS (see page 987) .

If you manage IGEL OS 12 devices, see Debugging / How to Collect and Send Device Log Files to IGEL Support[123].

If you require UMS log files for IGEL Support, see Save Support Information / Send Log Files to Support (see page 1031) .

UMS 12.01 or Higher

To change the logging settings for UMS 12.01 or higher, see the file `README.md` under `[IGEL installation directory]/RemoteManager/rmguiserver/logs` .

If you change the logging configuration, the restart of the UMS Server is not required.

UMS Server

`rmguiserver/logs` (Read `rmguiserver/logs/README.md` for configuring the logs)	
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`ums-api.log`	Logging of the API service
`ums-server.log` (= `catalina.log` before UMS 12) `ums-server-err.log`	Central log file for all logging events
`device-connector.log` `device-connector-err.log`	Logging of the device connector
`ums-device-service.log` `ums-device-service-err.log`	Logging of OS 12 device functionality

123. https://kb.igel.com/en/how-to-start-with-igel/current/debugging-how-to-collect-and-send-device-log-files

`ums-appproxy.log` `ums-appproxy-err.log`	Logging of the UMS as an Update Proxy (see page 1342)

`rmguiserver/logs/ums-server` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging (High Availability and Distributed UMS)
`ums-server-communication.log`	Logging of communication with UMS Console or devices Edit at `<!-- Logging of UMS communication -->`
`ums-server-threaddump.log`	Periodic logging of the threads
`ums-server-icg-communication.log`	Logging of communication with ICG Edit at `<!-- Logging of UMS communication -->`
`ums-server-health.log`	Logging of the UMS HA Health Check (see page 1420)
`ums-server-monitoring.log`	Performance logging (see page 987) Edit at `<!-- Logging of monitoring data -->`; change INFO to DEBUG to get detailed information on each method call

Example of where to edit the logging configuration for the UMS Server

This is an example of `rmguiserver/conf/logback.xml` where you can configure the logs for the UMS Server, i.e. switch the logging on/off, change the scan period or the number of days for the logging history, etc.:

```
<?xml version="1.0" encoding="UTF-8"?>
-<configuration scanPeriod="60 seconds" scan="true" debug="false">

<!-- The length of logging history in days -->
<property value="30" name="logs.history"/>
```

```
<!-- The maximum size of one log file -->
<property value="100MB" name="logs.maxsize"/>

<!-- The maximum size of the history -->
<property value="1GB" name="logs.historysizecap"/>

<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property value="INFO" name="monitoring.level"/>

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property value="OFF" name="server2console.level"/>
<property value="OFF" name="server2tc.level"/>
<property value="OFF" name="server2usg.level"/>
<property value="OFF" name="usg2server.level"/>
<property value="OFF" name="server2server.level"/>

<!-- Logging level of domain service -->
<!-- OFF, INFO, DEBUG, ERROR -->
<property value="WARN" name="domainservicelog.level"/>
<!-- The appenders -->
```

```
rmguiserver/logs/unifiedprotocol
```

`communication.log`	Logging of communication between the device and UMS (both ingoing and outgoing commands) Edit `rmguiserver/webapps/device-connector/WEB-INF/classes/config/logback.xml` for configuring the logs. Edit at `<!-- Logging of device communication -->`; change `OFF` to `INFO` for logging command headers or to `ALL` for logging command headers and payload
`domain-service.log`	Central log file for all events in the command handling Edit `rmguiserver/conf/logback.xml` for configuring the logs. Edit at `<!-- Logging level of domain service -->`
`device-auth.log`	Logging of device onboarding and device authentication issues

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - for configuring the logs)	
`ums-broker.log`	Central log file for all logging events
`ums-broker-msg.log`	Logging of the messages exchanged
`ums-broker-health.log`	Logging of the UMS HA Health Check (see page 1420)

`ums-broker-monitoring.log`	Performance logging (see page 987) Edit at `<!-- Logging of monitoring data -->`; change `INFO` to `DEBUG` to get detailed information on each method call

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - for configuring the logs)	
`ums-watchdog.log`	Central log file for all logging events
`ums-watchdog-msg.log`	Logging of the messages exchanged
`ums-watchdog-health.log`	Logging of the UMS HA Health Check (see page 1420)

UMS Console

`$HOME/.igel`	
`RMClient.exe.log`	Startup logging

`$HOME/.igel/logs` (`rmclient/logback.xml` - for configuring the logs)	
`ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging

`rmguiserver/logs` (`rmadmin/logback.xml` - for configuring the logs)	
`ums-admin.log`	Central log file for all logging events

UMS 6.10.110 or Higher

In UMS version 6.10.110, the outdated logging framework Log4j 1.x was replaced with Logback[124]; see also (en) ISN 2022-19: Log4j 1.x Remainder in UMS.

To change the logging settings for UMS 6.10.110 or higher, use `logback.xml`.

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`catalina.log`	Central log file for all logging events
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging
`ums-server-communication.log`	Logging of communication with UMS Console or devices Edit at `<!-- Logging of UMS communication -->`
`localhost.log`	Technical logging of the Apache Tomcat server
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`ums-server-threaddump.log`	Periodic logging of the threads
`ums-server-icg-communication.log`	Logging of communication with ICG Edit at `<!-- Logging of UMS communication -->`
`ums-server-health.log`	Logging of the UMS HA Health Check (see page 1420)

124. https://logback.qos.ch/

`ums-server-monitoring.log`	Performance logging (see page 987) Edit at `<!-- Logging of monitoring data -->` ; change INFO to DEBUG to get detailed information on each method call (the server restart is then required)

Example of where to edit the logging configuration for the UMS Server

This is an example of `rmguiserver/conf/logback.xml` where you can configure the logs for the UMS Server, i.e. switch the logging on/off, change the scan period or the number of days for the logging history, etc.:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false" scan="true" scanPeriod="60 seconds">

<!-- General settings -->


<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property name="monitoring.level" value="INFO" />

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property name="server2console.level" value="OFF" />
<property name="server2tc.level" value="OFF" />
<property name="server2usg.level" value="OFF" />
<property name="usg2server.level" value="OFF" />


<!-- The base folder for log files -->
<property name="base.dir" value="${catalina.home}/logs" />

<!-- The default logging pattern -->
<property name="pattern.format" value="%-5(%d{[yyyy-MM-dd HH:mm:ss.SSS]})
%-5level [%thread] %logger{10}.%M - %msg%n" />

<!-- The length of logging history in days -->
<property name="logs.history" value="30" />


<!-- The appenders -->
```

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`ums-api.log`	Logging of the API service

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - for configuring the logs)	
`ums-broker.log`	Central log file for all logging events
`ums-broker-msg.log`	Logging of the messages exchanged
`ums-broker-health.log`	Logging of the UMS HA Health Check (see page 1420)
`ums-broker-monitoring.log`	Performance logging (see page 987) Edit at `<!-- Logging of monitoring data -->`; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - for configuring the logs)	
`ums-watchdog.log`	Central log file for all logging events
`ums-watchdog-msg.log`	Logging of the messages exchanged
`ums-watchdog-health.log`	Logging of the UMS HA Health Check (see page 1420)

UMS Console

`$HOME/.igel`

`RMClient.exe.log`	Startup logging

`$HOME/.igel/logs` (`rmclient/logback.xml` - for configuring the logs)	
`ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging

`rmguiserver/logs` (`rmadmin/logback.xml` - for configuring the logs)	
`ums-admin.log`	Central log file for all logging events

Before UMS 6.10.110

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/log4j.properties` - for configuring the logs)	
`catalina.log`	Central log file for all logging events
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging
`communication.log`	Logging of communication with UMS Console or devices Edit at `# communication logging - define the log levels`; refer to Log4j documentation[125]

125. https://logging.apache.org/log4j/2.x/manual/index.html

`license_deployment.log`	Logging of licenses Edit at `# license deployment logging` ; refer to Log4j documentation[126]
`localhost.log`	Technical logging of the Apache Tomcat server
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`umsthreaddump.log`	Periodic logging of the threads Edit with `# threaddump logging` ; refer to Log4j documentation[127]
`usgcommunication.log`	Logging of communication with ICG Edit at `# communication logging - define the log levels` ; refer to Log4j documentation[128]
`health.log`	Logging of the UMS HA Health Check (see page 1420)
`monitoring.log`	Performance logging (see page 987) Edit at `# execution monitoring` ; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)

`rmguiserver/logs` (`rmguiserver/conf/log4japi.properties` - for configuring the logs)	
`api.log`	Logging of the API service

126. https://logging.apache.org/log4j/2.x/manual/index.html
127. https://logging.apache.org/log4j/2.x/manual/index.html
128. https://logging.apache.org/log4j/2.x/manual/index.html

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/log4j.properties` - for configuring the logs)	
`igel-ums-broker.log`	Central log file for all logging events
`broker-msg.log`	Logging of the messages exchanged
`broker-health.log`	Logging of the UMS HA Health Check (see page 1420)
`broker-monitoring.log`	Performance logging (see page 987) Edit at `# monitoring logging` ; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/log4j.properties` - for configuring the logs)	
`igel-ums-watchdog.log`	Central log file for all logging events
`watchdog-msg.log`	Logging of the messages exchanged
`watchdog-health.log`	Logging of the UMS HA Health Check (see page 1420)

UMS Console

`$HOME/.igel`	
`RMClient.exe.log`	Startup logging

`$HOME/.igel/logs` (`rmclient/log4j.properties` - for configuring the logs)	
`igel-ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging

`rmguiserver/logs` (`rmadmin/log4j.properties` - for configuring the logs)	
`igel-ums-admin.log`	Central log file for all logging events

Clearing stdout.log and stderr.log in IGEL UMS

Here, you can find options to limit the size of the files `stdout.log` and `stderr.log` created in connection with your IGEL Universal Management Suite (UMS) Server.

Problem

Besides the log files created by the IGEL UMS Server application, two log files are created by the Windows/Linux service which starts the UMS Server process. These log files (`stdout.log` and `stderr.log`) are not controlled by the logging configuration in `logback.xml` and so do not obey the sizing limits. Upon UMS Server restart these log files are cleared but if the UMS Server runs a long time the size can grow.

Solution 1 - Restart

Restart the UMS Server once in a while. The restart clears the log files, and thus keeps the size under control.

Solution 2 - Scheduled Task

Create a scheduled operating system task to clear the log files:

- On Windows, you can use the Powershell command `Clear-Content stdout.log`
- On Linux, the corresponding command is `truncate -s 0 stdout.log`
- Scripts to run as an administrator are available in the folder `rmadmin` (`truncateStdLogs.ps1` , `truncateStdLogs.sh`).

Clearing up the UMS

Problem

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

Goal

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

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

Solution

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

The following are the main steps for reorganizing the UMS:

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

Downloading the new Firmware

1. Check our download server[129] to see whether there are new updates that are relevant for your applications.
2. Download the relevant update files. Install an update directory for the files on the UMS server or on your FTP server.

Moving Clients to the New Firmware

Find out how many different firmware versions you really need.

Upgrading all clients to the same firmware:

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

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

3. Start the update process.

Moving Profiles to New Firmware

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

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

For more information see UMS Manual: Profiles in IGEL UMS (see page 617)

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

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

- Use again Views to select the clients, which are no longer required.
  For more Information see UMS Manual: How to Create a New View in the IGEL UMS (see page 820).
- Select the obsolete profiles. You can do this manually or by using the search option: **Misc > Search > Profiles > Product&Firmware**.
- Delete old firmware which is not assigned any longer to a client or profile: **Misc > Remove Unused Fimwares**.

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

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

How to Remove a UMS Certificate from an OS 11 Device

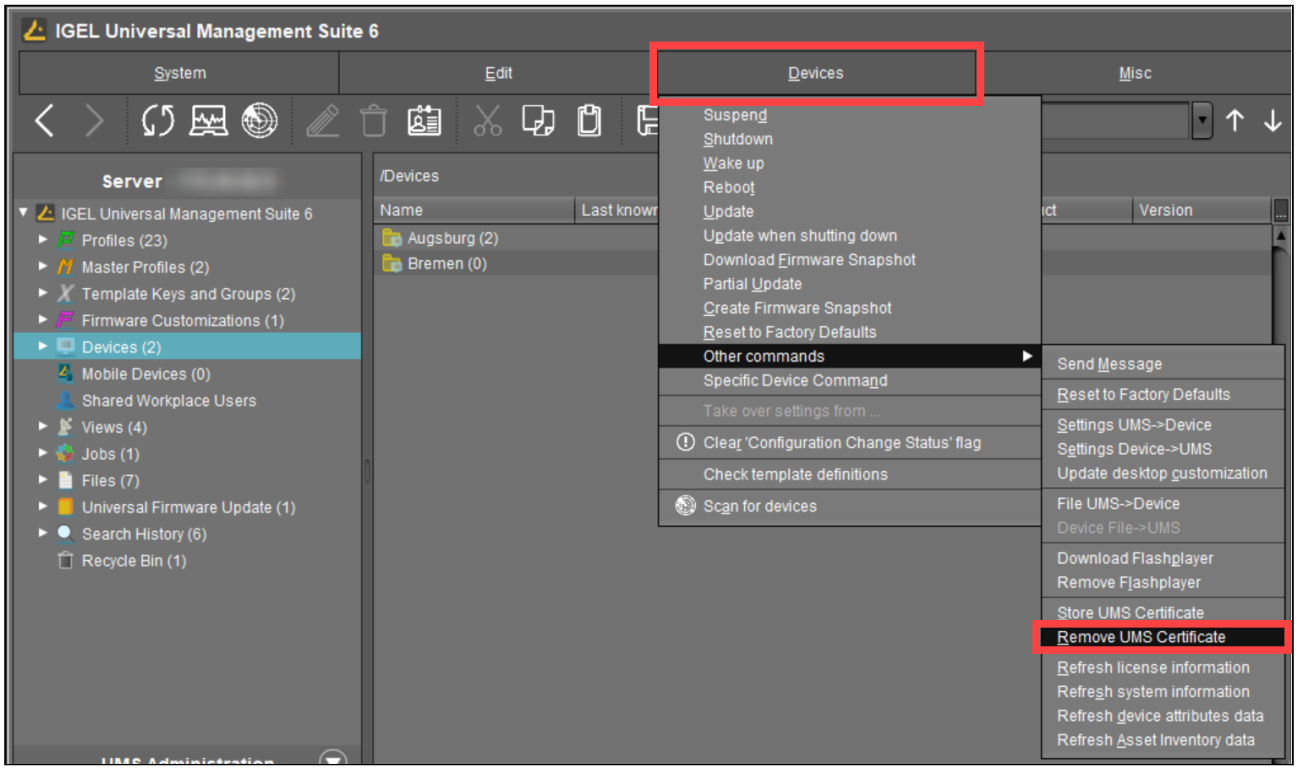
The IGEL Universal Management Suite (UMS) allows you to remove the UMS Server certificate from OS 11 devices.

The removal of the certificate from devices may be necessary

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

To remove the certificate, proceed as follows:

→ Under **Devices > Other commands**, select **Remove UMS Certificate**.
Each IGEL UMS Server can now access the device configuration until one of the servers registers the device.



Related Topics

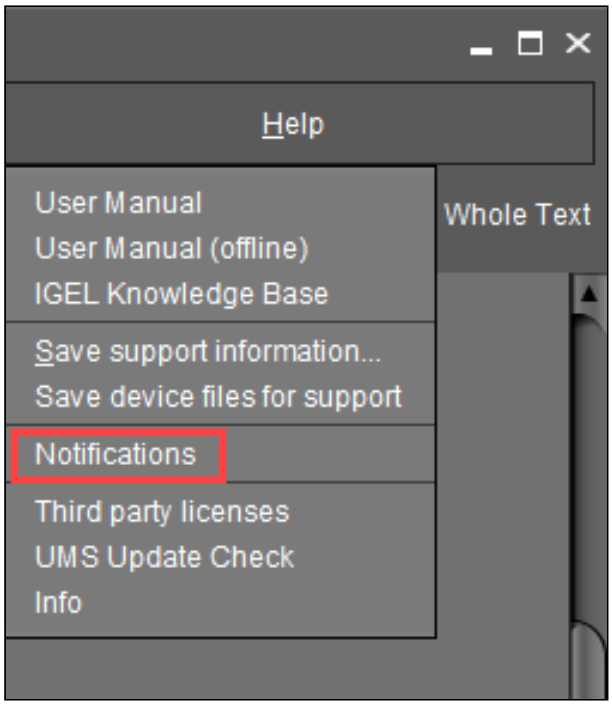
If you face problems during the device registration because of certificate issues: Troubleshooting: Registration of a Device via Scanning for Devices Fails (see page 533)

How to Configure Notifications in the IGEL UMS

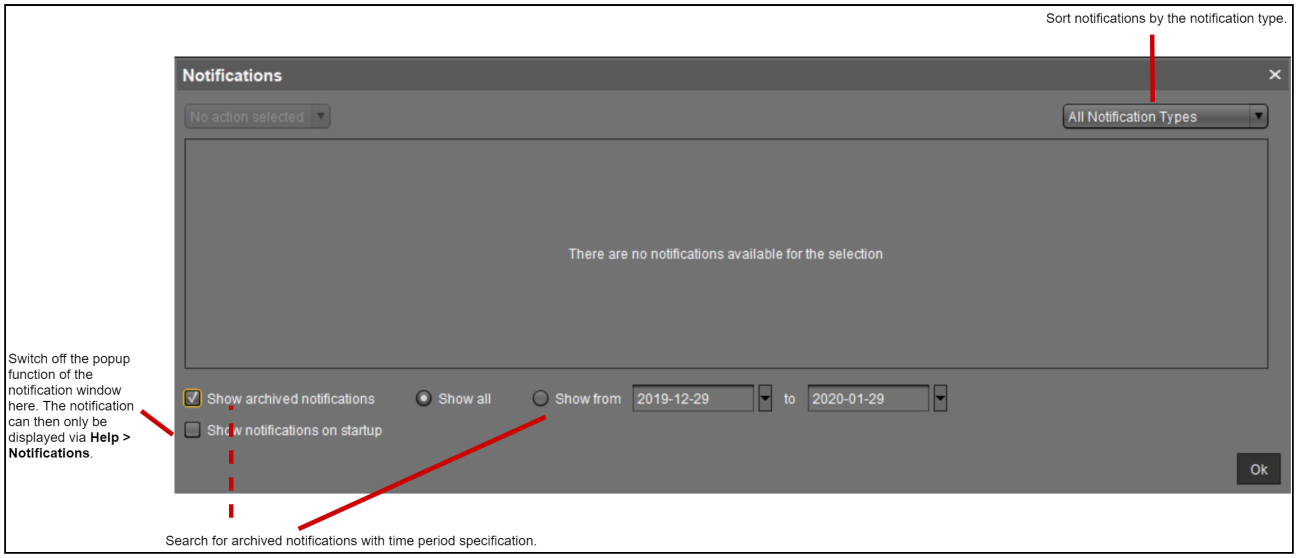
In the IGEL Universal Management Suite (UMS), you can get notifications about newly available firmware updates, device licenses, etc. By default, notifications are enabled and pop up when you start the UMS Console. In this article, you will learn how to adapt this feature to your needs.

About Notifications

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



The Notification Window



Enabling the Notification Function

1. In the UMS Console, go to **UMS Administration > Global Configuration >** Misc Settings in IGEL UMS (see page 996).
2. Activate **Enable notifications**.

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

Exporting Notifications and Sending Them by Email

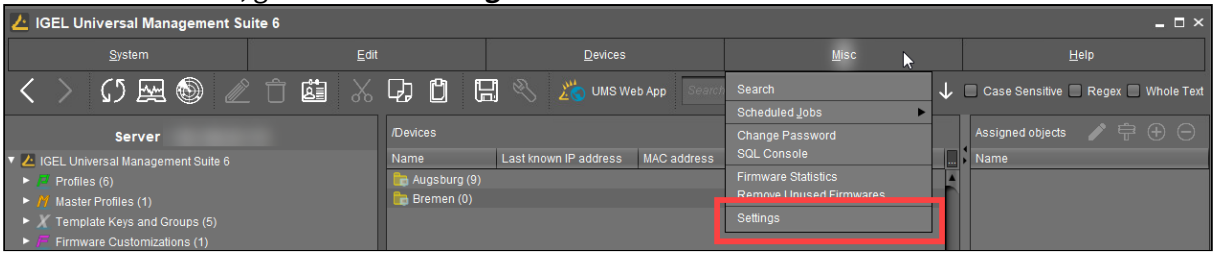
Notifications can be exported and sent via email: **UMS Administration > Global Configuration > Administrative Tasks > add > Action:** "**Send notification information via email**".

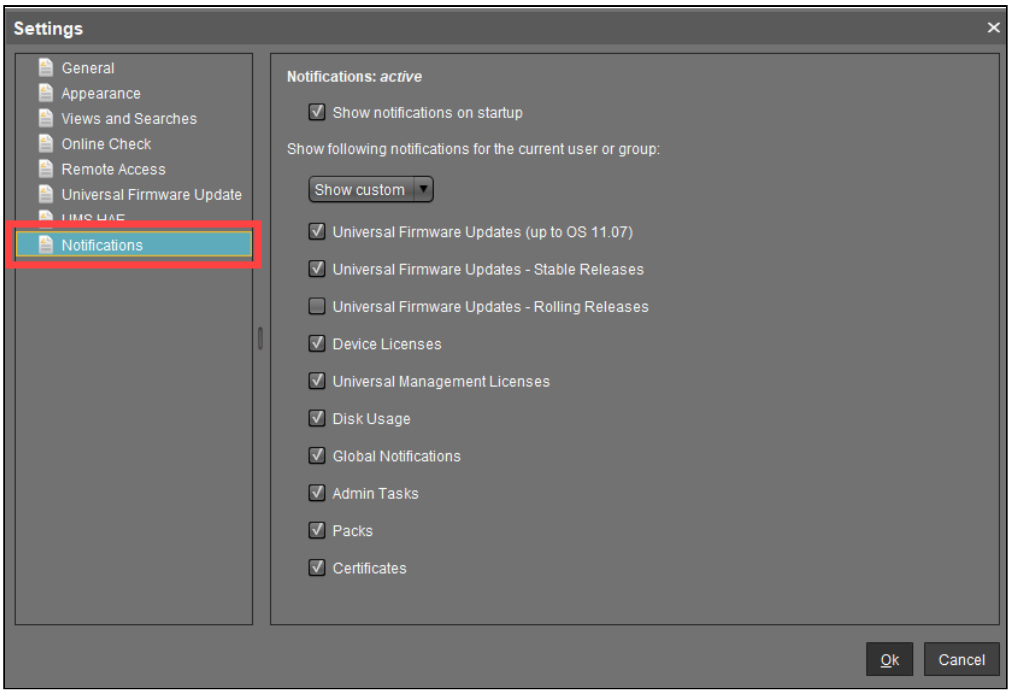
For more information, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS (see page 920).

Configuring the Notification Pop-Up and Notification Types

To configure and customize the notification pop-up:

1. In the UMS Console, go to **Misc > Settings > Notifications**.





2. Enable **Show notifications on startup** to display the notification window as a pop-up every time the UMS Console is started.
3. Under **Show following notification for the current user or group**, select **Show custom**.
4. Specify which content should be displayed in the notification.
   Possible options (as of UMS 6.10.110):
   - **Universal Firmware Updates (up to 11.07)**: Informs about the latest firmware updates for devices with IGEL OS versions before 11.07.

     To view notifications generated by UMS version below 6.10.110, leave the feature **Universal Firmware Updates (up to 11.07)** activated.

   - **Universal Firmware Updates - Stable Releases**: Informs about the latest Stable Releases. The feature is officially supported for devices with IGEL OS version 11.07 or higher.
   - **Universal Firmware Updates - Rolling Releases**: Informs about the latest Rolling Releases. The feature is officially supported for devices with IGEL OS version 11.07 or higher. For more information, see Software Releases Overview.

     Activate this feature to get the latest client versions and bug fixes.

   - **Device Licenses**: Informs about the expiration of device licenses.
   - **Universal Management Licenses**: Informs about the expiration of UMS licenses and if the available license amount is exceeded.
   - **Disk Usage**: Informs about a critical value of free disc space. For more details, see "Disk Usage" below.

- **Global Notifications**: Informs about important news like maintenance times and bug fixes. For more details, see "Global Notifications" below.
- **Admin Tasks**: Automatically informs in a set of cases if no administrative task has been defined. For more details, see "Admin Tasks" below.
- **Packs**: Informs if license packs will expire.
- **Certificates**: Informs if certificates will expire.

5. Confirm the settings with **Ok**.

Disk Usage

This notification informs the user when there is not enough free drive space anymore. The individual critical drive space value can be set under **UMS Administration > Global Configuration > Misc Settings > Notifications**.

> Each server executes an administrative task every 6 hours to check the available space on the drive and deliver the disk usage information to the notification system. In order to display the notification, the server must have been running continuously for up to 6 hours.
> Disk usage admin tasks executions older than 24 hours are considered out-of-date: An additional warning message is shown.

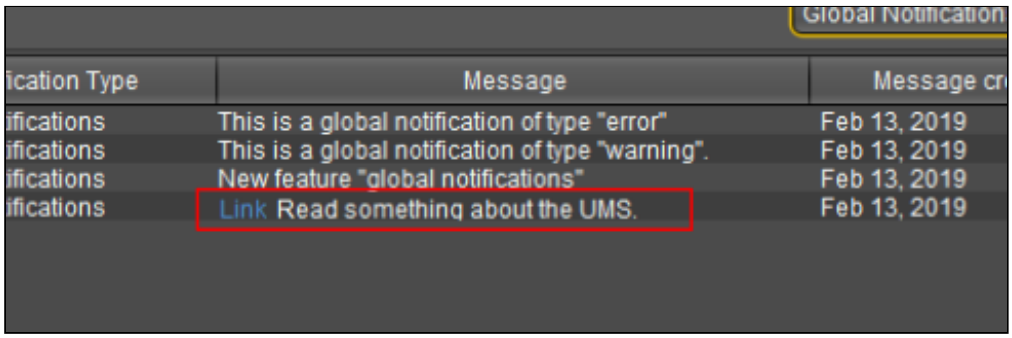
Types of disk usage notifications:

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

Global Notifications

This notification type informs the user about important news like maintenance times and bug fixes.

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



→ Click the link to open the web page in the standard browser.

→ Move the mouse over the link to display the URL.

Admin Tasks

Notifications of this type are displayed in the following cases:

- When an embedded database is active, but NO administrative task for **creating a database backup** has been set.
- When logging (see page 987) is enabled, but NO administrative task for **deleting logging data** has been set.
- When at least one job (see page 847) is available, but NO administrative task for **deleting job execution data** has been set.

For detailed information on administrative tasks, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS (see page 920).

Troubleshooting: Incorrect Timezone Information (Daylight Saving Time, DST)

Symptom

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

Problem

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

Solution

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

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

Retrieving Current Time Zone Information Files

On Windows

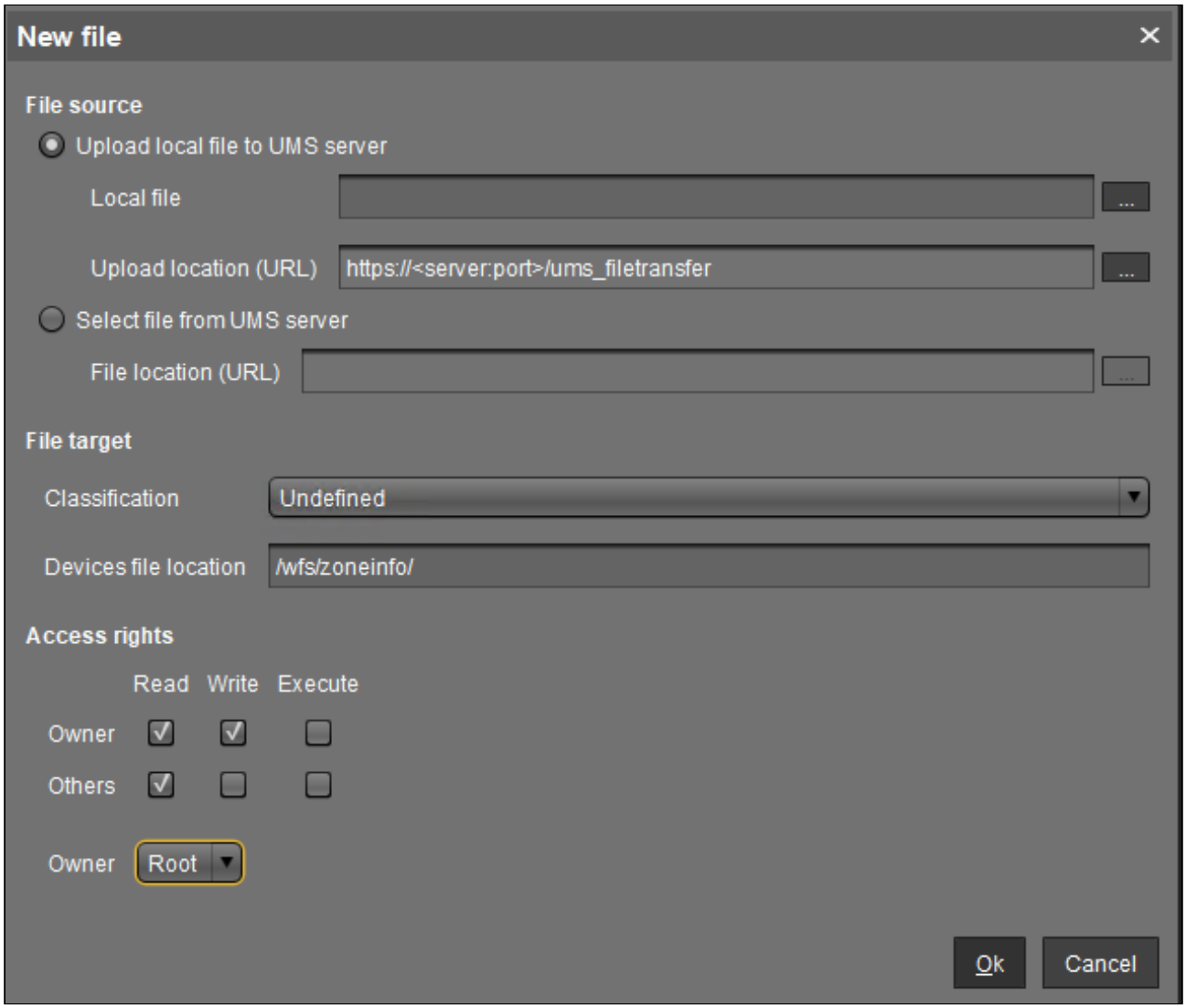
- Use your web browser to download the following package files:
  - http://packages.ubuntu.com/xenial-updates/all/tzdata/download for *IGEL Linux* version 10.x
  - http://packages.ubuntu.com/trusty-updates/all/tzdata/download (for *IGEL Linux* version 5.x)
  - http://packages.ubuntu.com/precise-updates/all/tzdata/download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

On Linux

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

Distributing the Files from IGEL Universal Management Suite

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



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

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

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

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

How to Configure the IGEL UMS to Send Emails via Gmail

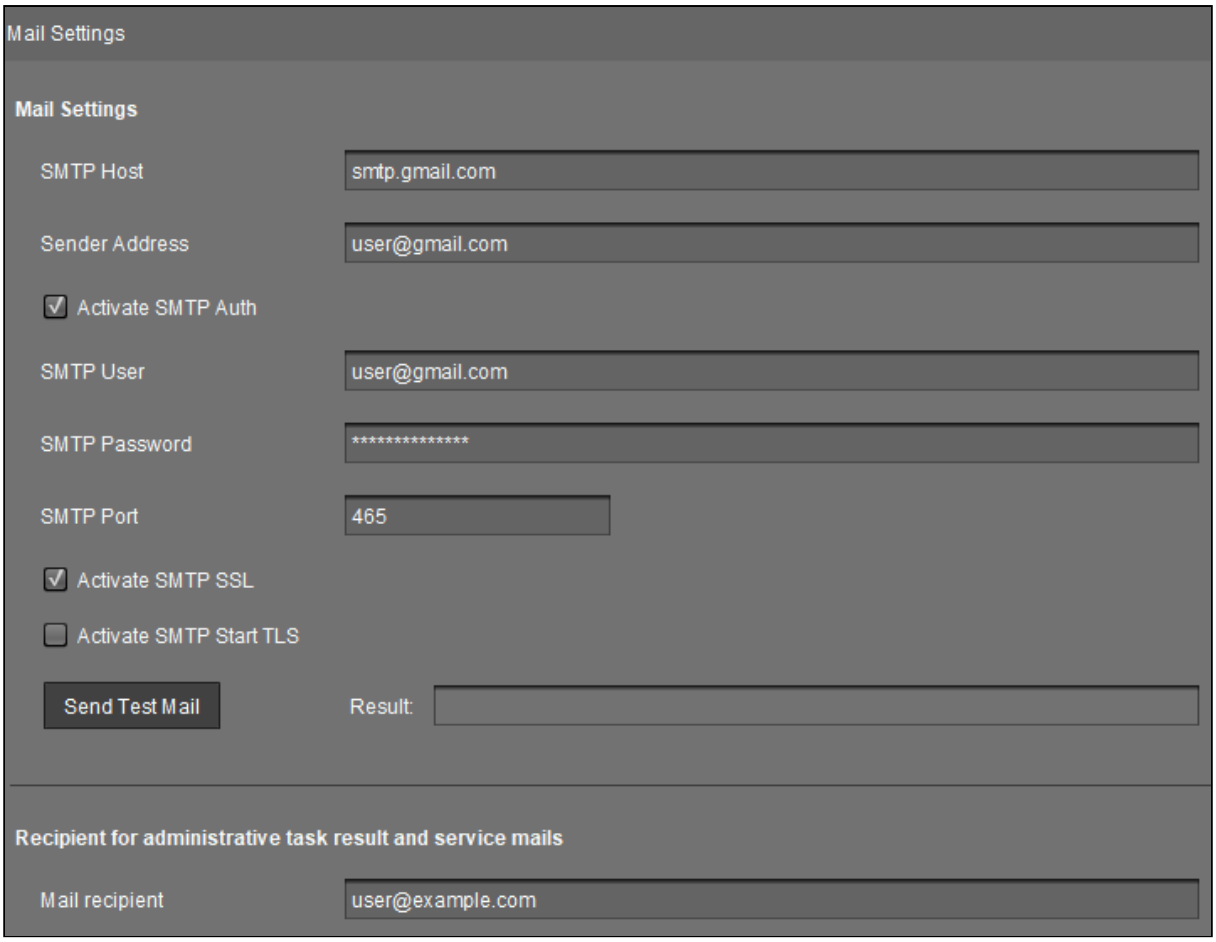
You want to send views from the IGEL Universal Management Suite (UMS) by email using a Gmail account.

Solution

In order to allow the UMS to send emails via Gmail, you have to make the following setting in your Google account:

- Log in to Google.
- Go to **My Account > Sign-in & security > Connected apps & sites**.
- Set **Allow less secure apps** to `ON`.

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



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

Additional Information

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

How to Search with Regular Expressions in IGEL UMS

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

You can use regular expressions in:

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

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

```
.*
```

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

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

```
IGEL.*
```

Something beginning with IGEL and ending with 12:

```
IGEL.*12
```

If you want to find something ending with IGEL:

```
*.IGEL
```

Find out more about Java regular expressions in Oracle's documentation[130].

130. https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

How to Copy Sessions in IGEL Setup or IGEL UMS

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

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

To copy a session, proceed as follows:

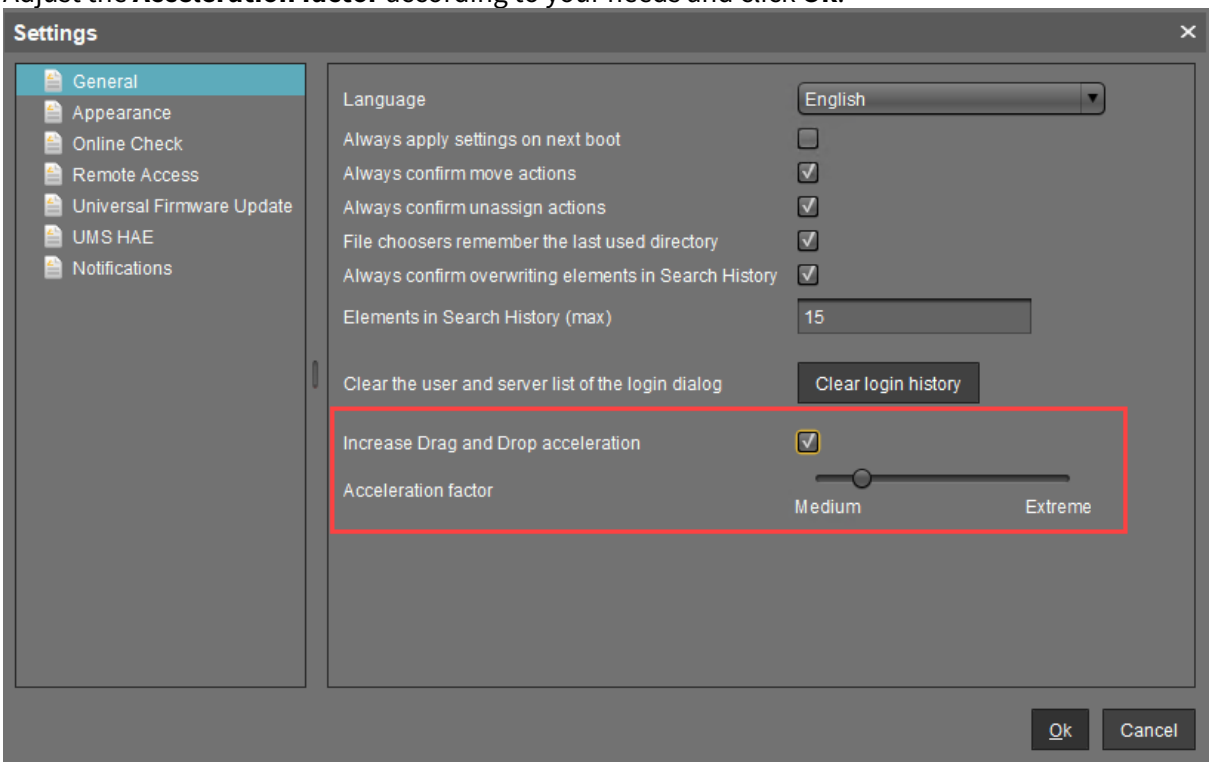
1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. Click  .
   A copy of the session will be created within the same folder.

How to Speed up Drag & Drop for Large Structure Trees

If you have a really large number of objects in your IGEL Universal Management Suite (UMS), it can be tedious to drag and drop an object to a new position if the new position is quite far away from the current position. With UMS version 5.03.100 or newer, you can increase your scrolling speed. As soon as the object you are moving touches the bottom edge of the structure tree window, the acceleration starts.

To enable drag and drop acceleration:

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



Drag & drop acceleration is ready.

Best Practices: Antivirus Configuration on IGEL UMS Server

Introduction

This article provides guidance on how to configure antivirus (AV) software for the IGEL Universal Management Suite (UMS) Server. While antivirus protection is critical for system security, incorrect AV configuration may interfere with UMS operations such as database access, firmware distribution, or device communication. This guide outlines recommended best practices for deploying AV solutions on the UMS host without disrupting core functionality.

Legal Note

- This article is based on internal IGEL experience and field feedback. It is not a one-size-fits-all solution.
- You are solely responsible for evaluating, testing (including in pre-production), approving, implementing, and maintaining any changes to your antivirus (AV) solution, allow-lists, exclusions, or other security controls. IGEL does not assume, and expressly disclaims, any responsibility or liability for increased exposure, vulnerabilities, security incidents, non-compliance, degraded protections, data loss, or other adverse outcomes arising from changes you make to your AV or related security posture, whether or not such changes were informed by this guidance.

Environment

- **UMS** 12.08 or higher; latest version recommended (for improved AV compatibility)
- **Supported Operating Systems:**
  - IGEL UMS is supported on currently maintained versions of Microsoft Windows Server and major Linux distributions. For an up-to-date list, refer to the UMS Release Notes[131].
- **Database Options:**
  - Embedded: Apache Derby (included with UMS)
  - External: For supported versions of PostgreSQL, Oracle, or Microsoft SQL Server, refer to the Universal Management Suite > UMS Release Notes > Notes for Release IGEL UMS > Supported Environment IGEL UMS.

Network Requirements

To ensure successful communication between IGEL UMS, endpoint devices, and the IGEL Cloud Gateway (ICG), proper network access must be configured.

- For required ports and firewall rules, refer to the following official IGEL documentation:
  - IGEL UMS Communication Ports[132]
  - IGEL UMS Network Configuration Overview[133]

131. https://kb.igel.com/en/universal-management-suite/current/ums-release-notes
132. https://kb.igel.com/en/universal-management-suite/current/igel-ums-communication-ports
133. https://kb.igel.com/en/universal-management-suite/current/igel-universal-management-suite-network-configurat

Procedure

1. Install an Antivirus Solution on the UMS Host
    - In case you are using an enterprise-grade antivirus solution, ensure it is fully supported on your selected server operating system and correctly configured to avoid interfering with UMS directories or processes.
    - Ensure that the antivirus engine and its signature database are configured to update automatically, either directly from the vendor or via an internal update server. This guarantees continuous protection without requiring manual updates.

2. Exclude UMS Application and File Transfer Directories

- To avoid disruptions, exclude the UMS installation and firmware transfer paths from real-time scanning:
    - **Windows**:
      `C:\Program Files\IGEL\RemoteManager\`
      Or if you need a more granular configuration:
      `C:\Program Files\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\`
    - **Linux**:
      `/opt/IGEL/RemoteManager/`
      Or if you need a more granular configuration:
      `/opt/IGEL/RemoteManager/rmguiserver/webapps/ums_filetransfer/`

⚠ Real-time scanning of these directories may result in failed firmware updates or delayed device communication.

3. Exclude App Binary Cache

- Additionally, we recommend excluding the App Binary Cache directory used by the UMS App Proxy service, which stores firmware and package binaries.
    - **Windows**:
      `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\persistent\ums-appproxy\files`
    - **Linux**:
      `/opt/IGEL/RemoteManager/rmguiserver/persistent/ums-appproxy/files`

If the Distributed App Repository option is enabled, we also recommend excluding the corresponding WebDAV directory, as it may contain executable binaries required for proper app delivery.

4. Exclude Database Directories and Processes

- If the embedded UMS database is in use, exclude its storage directories:
  - **Windows**:
    `C:\Program Files\IGEL\RemoteManager\db\`
  - **Linux**:
    `/opt/IGEL/RemoteManager/db/`
- For external databases (e.g., PostgreSQL, Oracle, Microsoft SQL Server), follow the vendor-specific antivirus best practices for process and data directory exclusions. These configurations are highly product-dependent and beyond the scope of this document.

This prevents antivirus software from interfering with database transactions, which could otherwise lead to corruption or service interruptions.

5. Configure Scheduled Scans Carefully

- Run full-system scans during defined maintenance windows or off-peak hours to minimize impact on UMS server performance.

Real-time protection should remain enabled to maintain security. However, keep in mind that real-time scanning can introduce performance overhead, especially during large firmware transfers or database operations.

- To mitigate this:
  - Follow your antivirus vendor's optimization guidelines for excluding low-risk but high-traffic directories (e.g., `ums_filetransfer`, database paths).
  - Consider performing a risk analysis if your AV product lacks granular tuning options.
  - If performance remains affected, increase server resources (CPU, memory, disk I/O) to handle the AV load.

As we cannot reflect each customer's environment in this document, it remains the customer's responsibility to assess and balance performance, protection, and operational reliability in accordance with their specific requirements.

6. Test Antivirus Behavior Before Rollout

- After configuring exclusions, restart the UMS services (Windows: `IGEL RMGUIServer` / Linux: `igelRMserver`) to ensure that they start without delay or error.
- Validate that critical operations such as firmware distribution, endpoint registration, and database access work as expected with the antivirus enabled.
  This step helps detect misconfigurations before they impact production systems.

7. Monitor and Review Logs Regularly
    - Review antivirus logs to ensure that no UMS-related files or processes are falsely flagged as malicious. Likewise, monitor UMS logs to confirm that there are no disruptions in service.
    - Configure antivirus alerts to notify administrators if actions such as quarantining or blocking occur, allowing quick response before business operations are affected.

Notes

- Ensure consistent AV configurations across all UMS nodes in High Availability (HA) and / or Distributed UMS environments to avoid behavioral drift.
- When performing UMS upgrades, you may disable real-time AV scanning on the installation path to avoid blocked operations.

Warnings

- Do not scan or quarantine UMS database or firmware transfer directories. Doing so may result in service failure, corrupted firmware files, or loss of device connectivity. Always configure the recommended exclusions to prevent these risks.
- Avoid installing multiple antivirus products on the same UMS host. This can lead to performance degradation, scanning conflicts, or critical system liability. Use a single, well-supported enterprise solution and configure it according to the best practices.

Troubleshooting: Licensing with Smartcard Fails

Symptom

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

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

Problem

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

Solution

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

Why Do Devices Appear Automatically In a New Database of the IGEL UMS?

When you create a new datasource in your Universal Management Suite (UMS) environment, you see that devices appear automatically in the database.

When Does It Happen?

You can see the previously registered devices appear automatically in the new database, when you perform the following:

1. You install a UMS and connect it to a database.
2. You register devices in the UMS.
3. You switch to another datasource which was never been used before.

Why Does It Happen?

When you switch to a new datasource but do not reinstall the UMS, the files with the device certificates still remain in the `rmguiserver` folder. When the UMS starts the first time with a new database, it is designed to import those certificates to the empty database, thus registering the devices automatically.

UMS Reference Manual

What is New - Knowledge Base Updates for IGEL UMS 12.09.110

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[134] and in the Knowledge Base under UMS Release Notes (see page 1440).

Before the installation / update of the IGEL UMS, please read the documentation (en) How to Start with IGEL .
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.

Added an Administrative Task “Delete logging data (OS12 and Web App)”

In the UMS Console, it is now possible to create an administrative task for deleting logs for IGEL OS 12 device management and the UMS Web App. See Delete Logging Data as an Administrative Task in the IGEL UMS (see page 928).

Information on Devices Connected via Reverse Proxy

You can see if a device is connected via reverse proxy in the UMS Console under **Advanced System Information.** For details, see View Device Information in the IGEL UMS (see page 778) .

You can search for devices connected via reverse proxy in the UMS Web App. See Useful IGEL UMS Features for Managing Reverse Proxy Connected Devices (see page 348) .

UMS as a CA Proxy: Optional CA Label

You can use an optional EST CA label now; for details, see UMS as a Certificate Authority (CA) Proxy

Configuration of an AWS Application Loadbalancer (ALB) for Deploying the IGEL Universal Management Suite (UMS)

You can use an AWS Application Loadbalancer (ALB) for your UMS installation. For details, see Configuration of an AWS Application Loadbalancer (ALB) for Deploying the IGEL Universal Management Suite (UMS) (see page 237).

134. https://www.igel.com/software-downloads/cosmos/

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) (see page 255).

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:

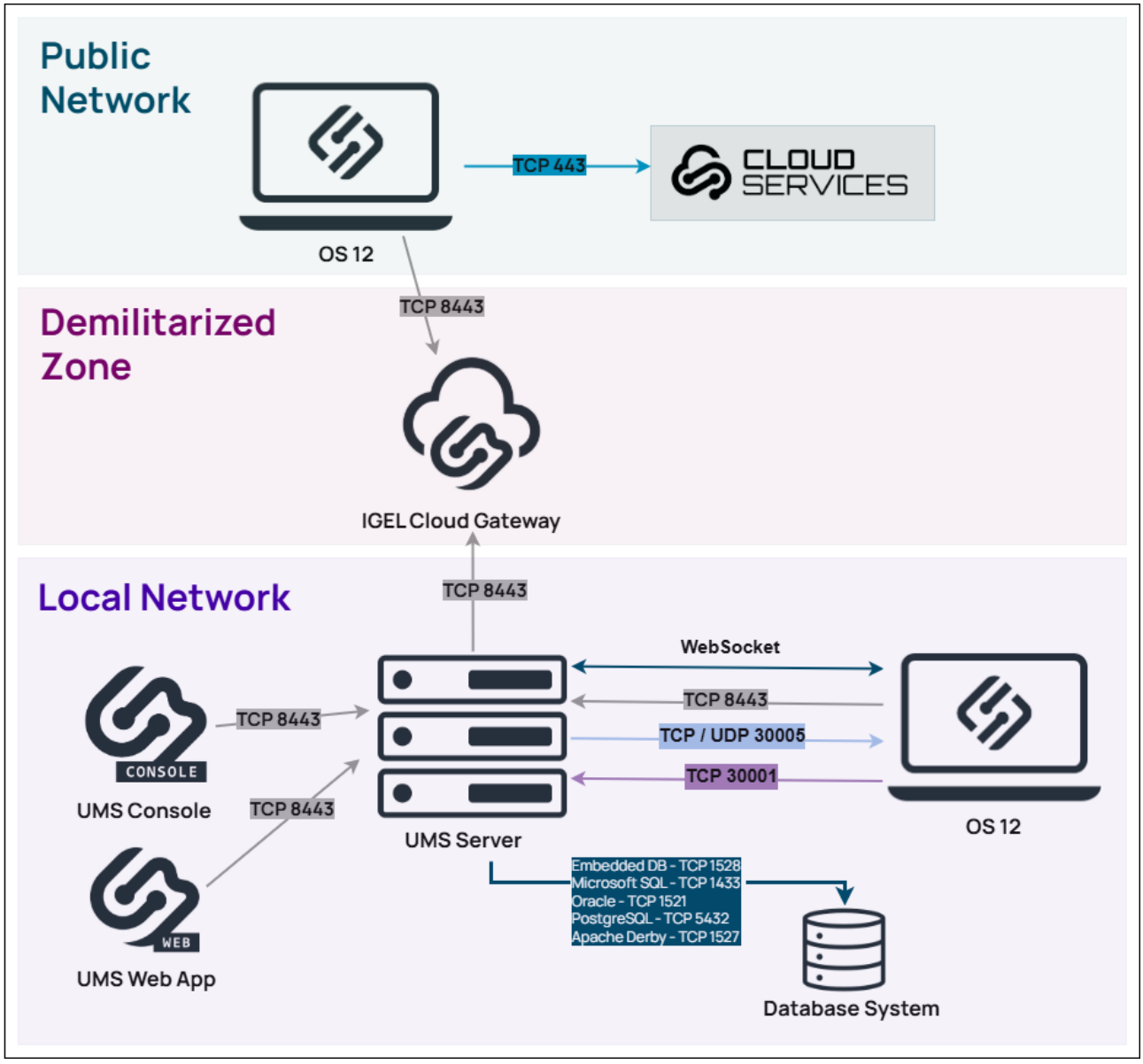
- UMS Server
- UMS Administrator
- UMS Console / UMS Web App

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 page 1440). See also Installation Requirements for the IGEL UMS (see page 10).

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 (see page 256).

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 1037).

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 669).

For how to log in to the UMS Console, see Connecting the UMS Console to the IGEL UMS Server (see page 134).

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 (see page 1154). 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). For the feature matrix, see Feature Matrix: UMS Web App vs. UMS Console[135].

135. https://kb.igel.com/en/universal-management-suite/current/feature-matrix-ums-web-app-vs-ums-console

Feature Matrix: UMS Web App vs. UMS Console

This article describes the features available in the IGEL Universal Management Suite (UMS) Console and in the IGEL UMS Web App.

- The UMS Web App can currently be used only in addition to the Java-based UMS Console.
- The range of functions available in the UMS Web App will constantly be expanded.
- All features that are already available in the UMS Web App are fully supported.

Configuration Dialog, Profiles, Assignments, and Apps

		UMS Console	UMS Web App
Edit configuration	**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 **Import devices as profiles (="Import profiles" in the UMS Web App)**	**OS 12 devices**	✗	✓
	OS 11 devices	✓	✗
Export/Import profiles	**OS 12 devices**	✗	✓
	OS 11 devices	✓	✗
Export/Upload IGEL OS Apps		✗	✓
Create and Edit Corporate Identity Customizations (CICs)		✓ (except Multi-use CIC)	✓

Assign CICs	**OS 12 devices**	✓	✓
	OS 11 devices		
Export/Import CICs		✓ (except Multi-use CIC)	✓

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 672) .

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 (see page 1176) .

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	✓	✓ (some permissions are still changed via the UMS Console only (see page 1362))
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	✓	✓

Registering the IGEL UMS

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

For detailed instructions on the registration, see *Registering the New UMS ID* in Transferring or Registering the UMS ID[136] or Registering the UMS[137] .

Only an authorized user can register the UMS, see Managing Users and Roles in the IGEL Customer Portal[138] .

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.
```

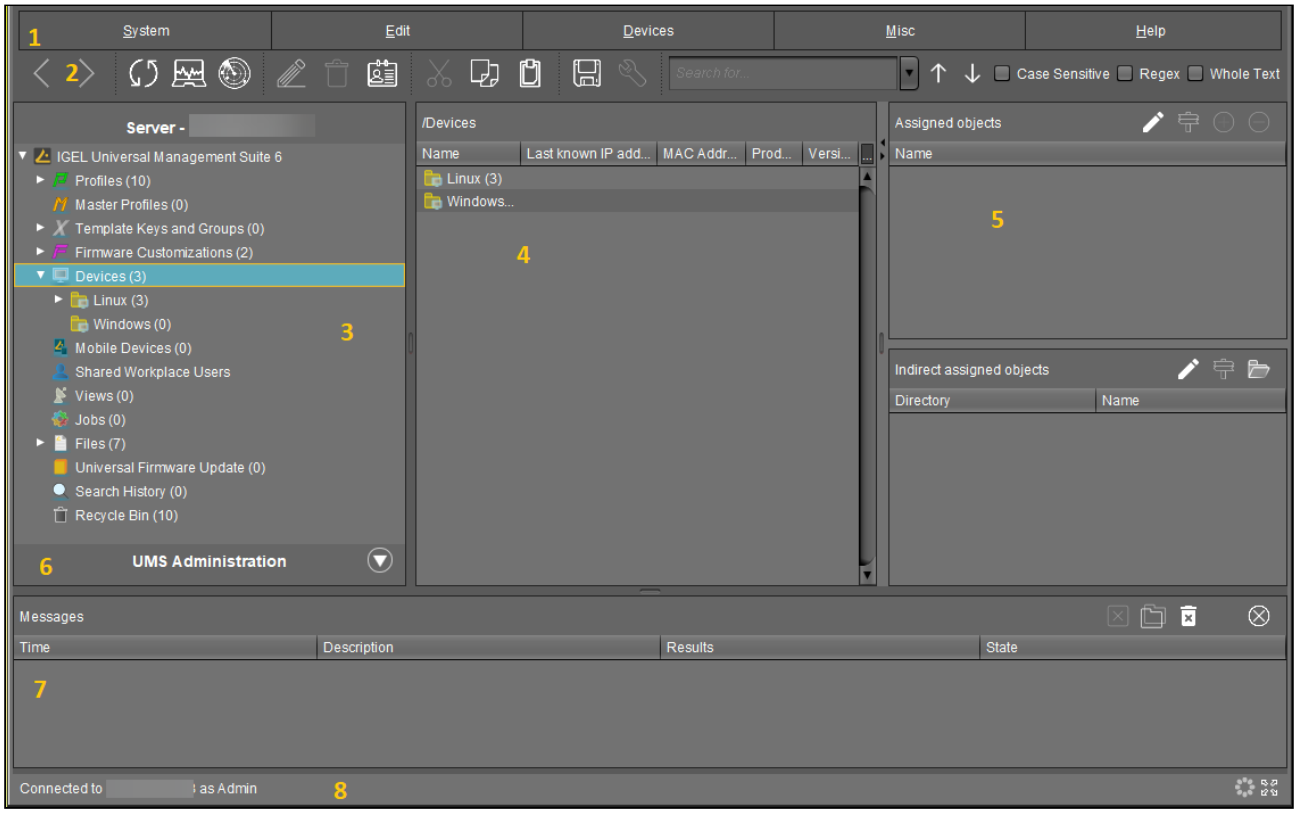
136. https://kb.igel.com/en/universal-management-suite/current/transferring-or-registering-the-ums-id
137. https://kb.igel.com/en/how-to-start-with-igel/current/registering-the-ums
138. https://kb.igel.com/en/how-to-start-with-igel/current/managing-users-and-roles-in-the-igel-customer-port

UMS Console User Interface

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

User Interface Areas of the IGEL UMS Console

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 672).
2	Symbol bar	Frequently used commands relating to objects in the structure tree. See Symbol Bar 1 (see page 684).
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 683).
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 686).

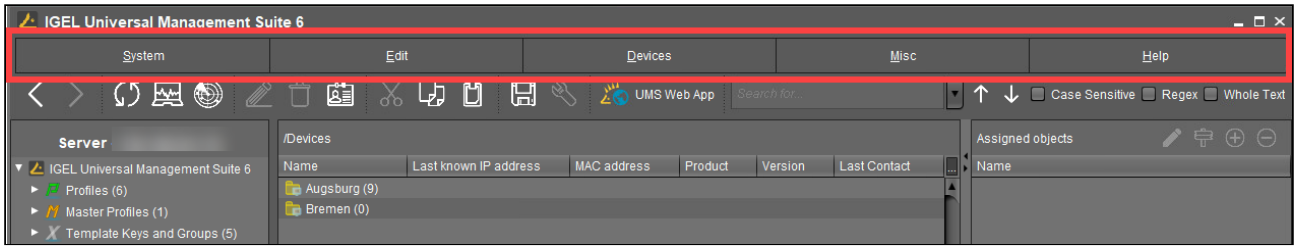
5	Assigned objects	Objects assigned to the devices or folders. See Assigned Objects (see page 690).
6	UMS Administration	Administrative tasks, e. g. configuring domains, Universal Firmware Updates, and the scheduled backup of the UMS database (only Embedded DB) See UMS Administration (see page 868).
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 688).
8	Status row	Status messages from the console, e. g. the server currently connected and the user name. See Status Bar (see page 689).

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

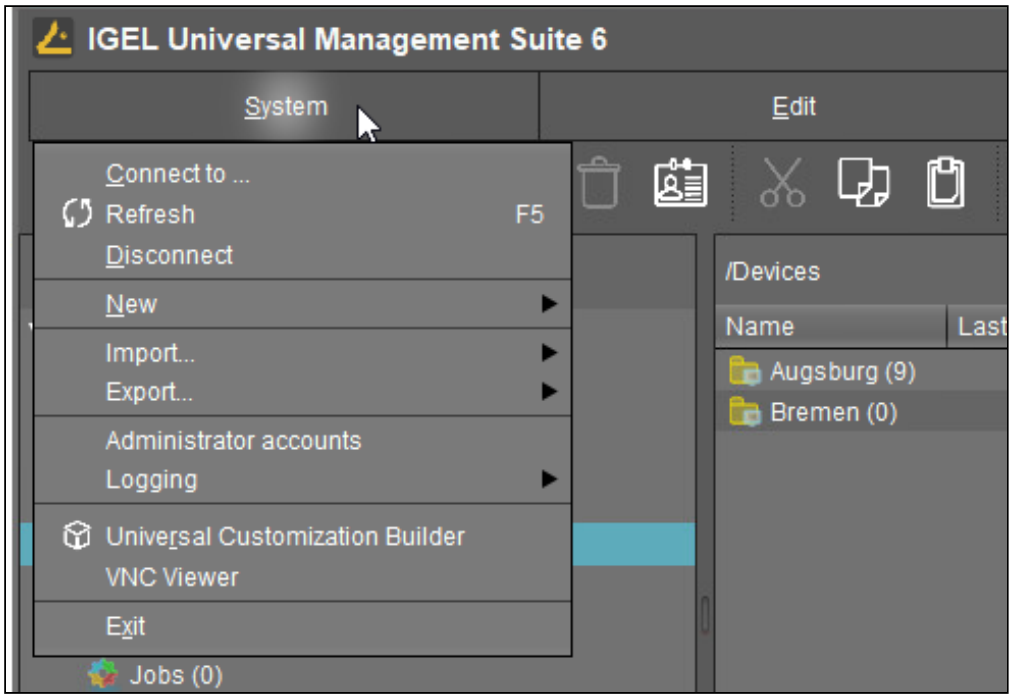
In the following article, you will learn about settings which you can configure in the menu bar of the IGEL Universal Management Suite (UMS) Console.

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 134).

- **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 798), Exporting and Importing Profiles (see page 719), and Importing Devices (see page 1143).

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.

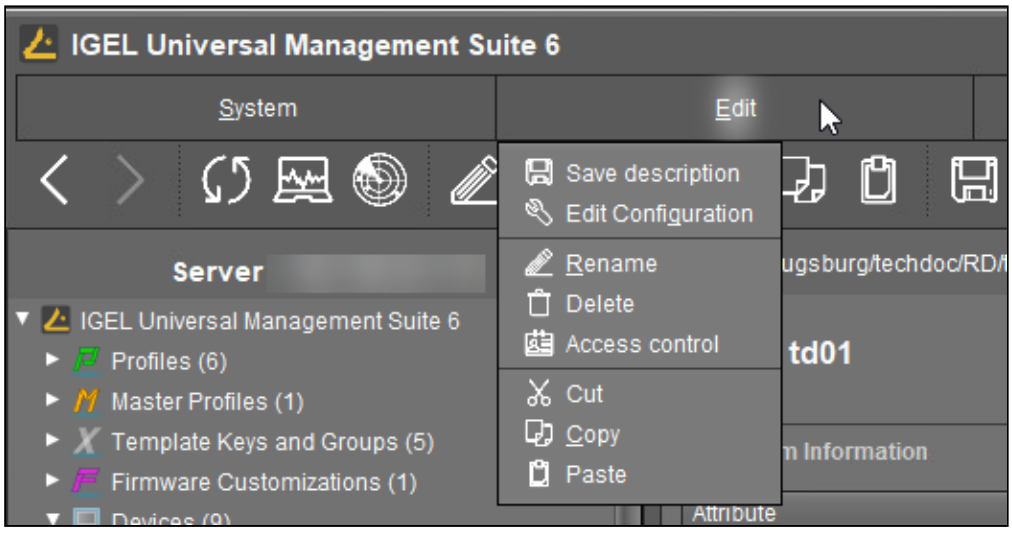
Logging: Allows you to display and export recordings of messages, events, and VNC log entries. For more information on logging, see Logging (see page 987) and User Logs (see page 1024).

VNC viewer: Allows you to shadow a device. For more details on shadowing, see Shadowing - Observe IGEL OS Desktop via VNC (see page 810).

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.

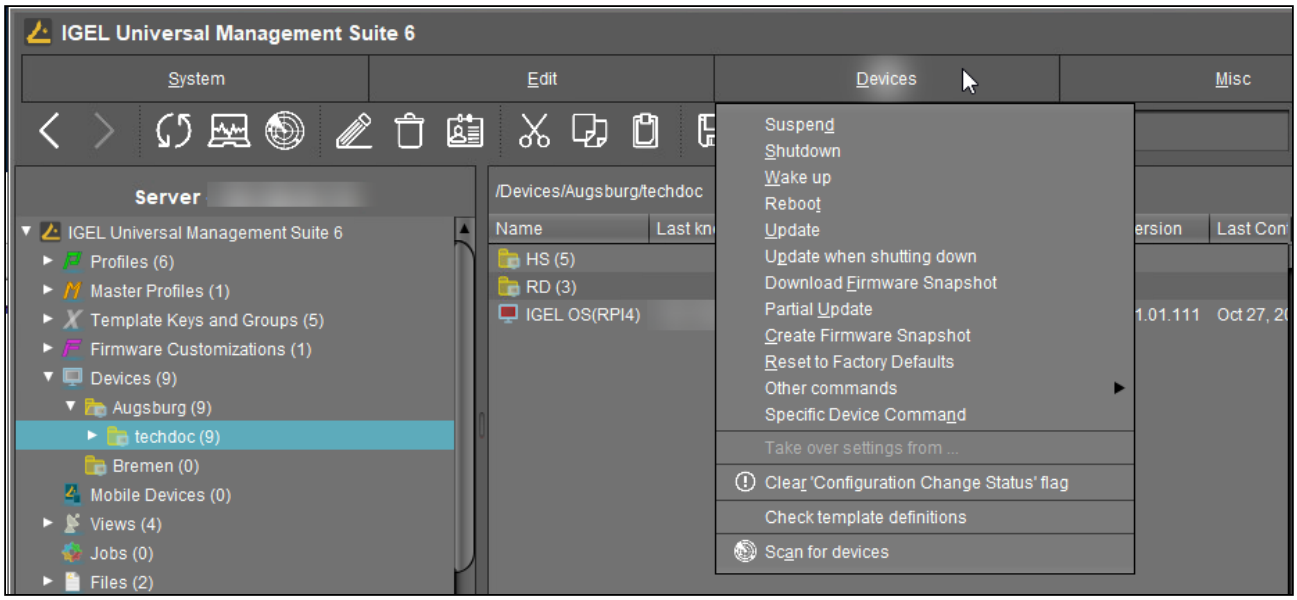
Cut: Allows you to cut a data object and copy it to the clipboard.

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.

> See also (11.10-en) Reset to Factory Defaults.

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 (see page 639).
- **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 (11.10-en) Jabra Xpress (IGEL OS).
- **Start Login Enterprise Launcher**: Starts Login Enterprise Launcher if it has been configured, see (11.10-en) How to Login Enterprise Launcher in IGEL OS.

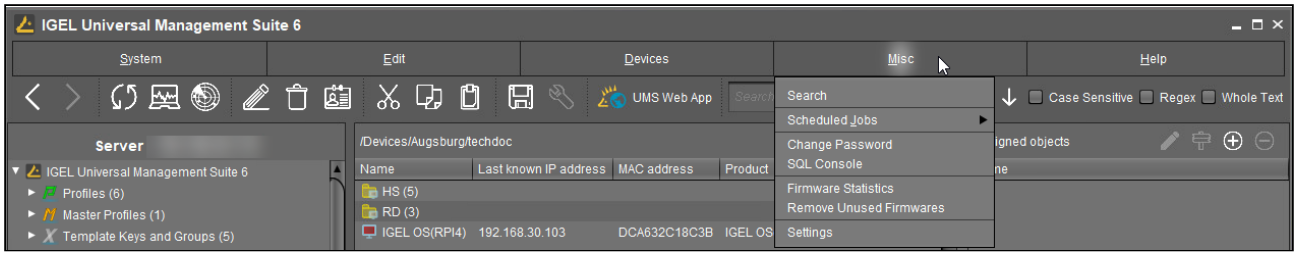
Take over settings from...: Sends profile settings to the device on a one-off basis.

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 758). For general information on template profiles, see Template Profiles in the IGEL UMS (see page 746).

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 861) 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.

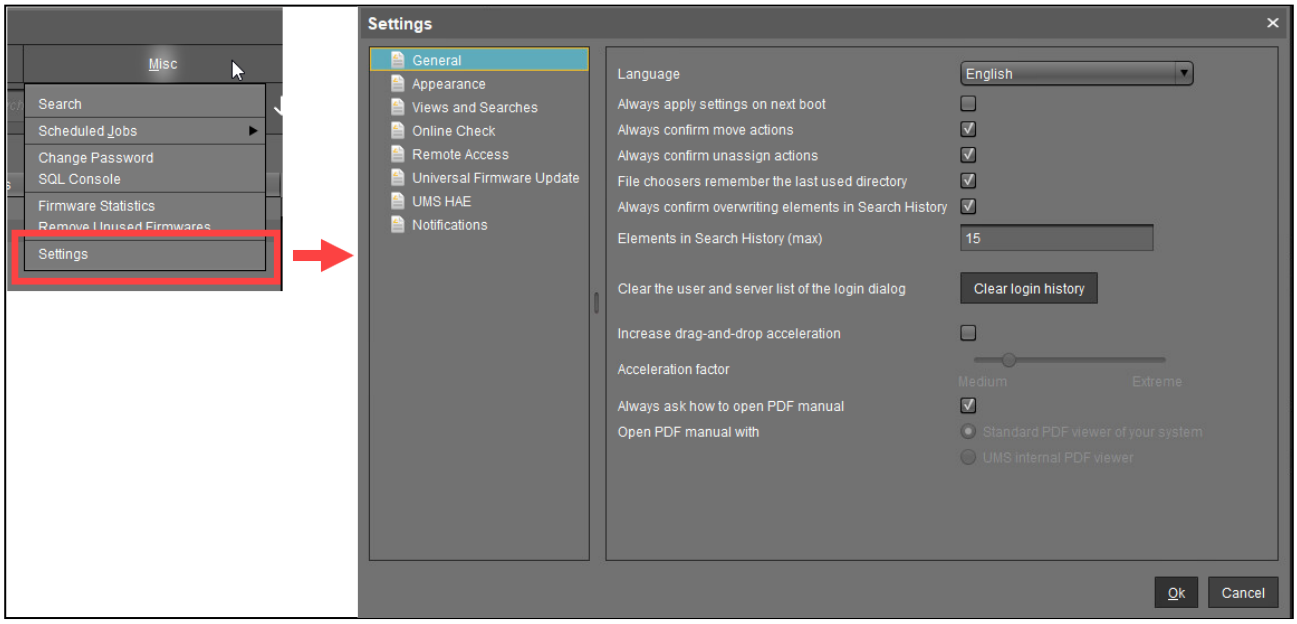
Firmware Statistics: A list of firmware versions registered in the database with filter function.

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 856).

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 776). (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 776).

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 (see page 1154).

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 (see page 1387) 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**.

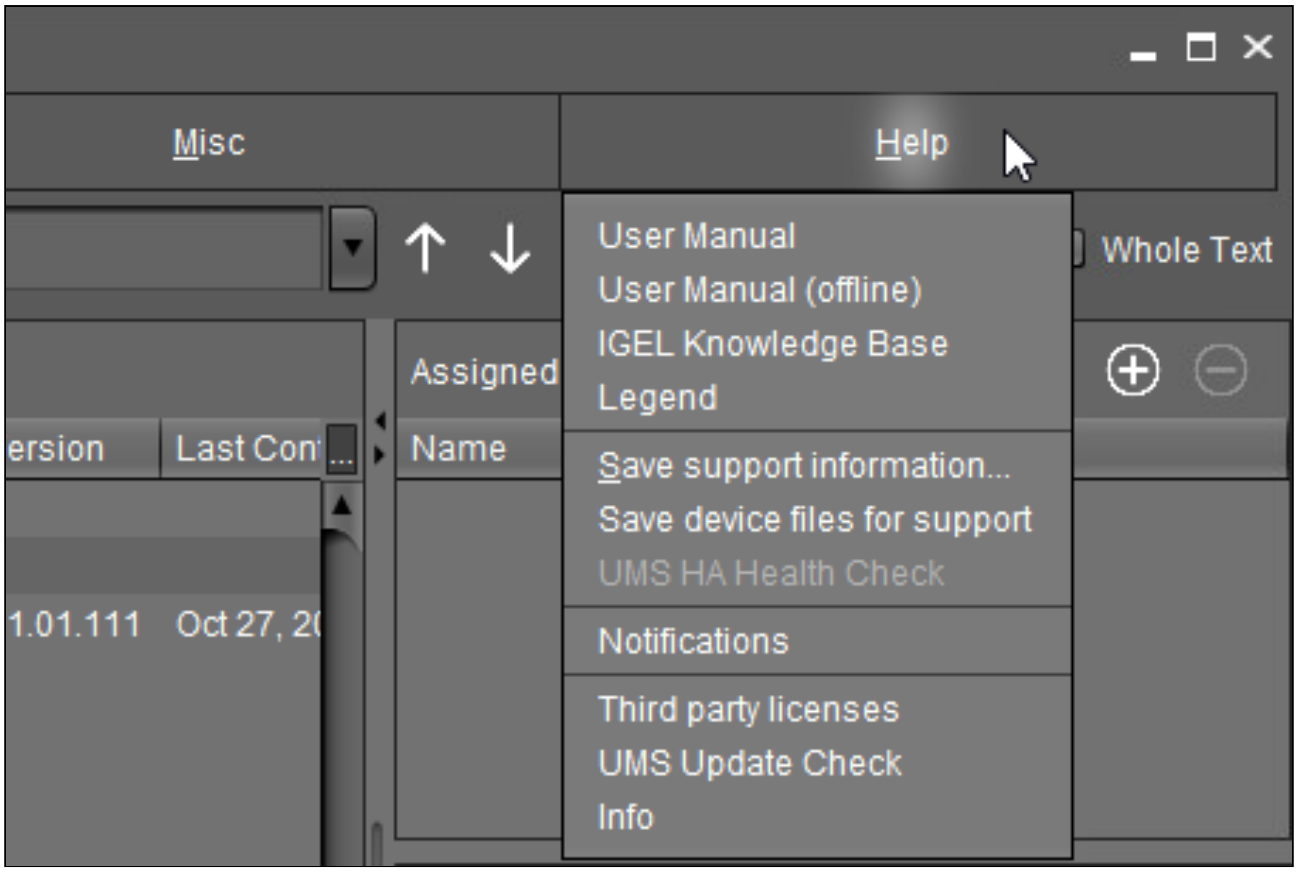
Show following notifications for the current user or group
Possible options:

- **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 (see page 640).

Help

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



User Manual: Link to the manual on the IGEL KB.

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

IGEL Knowledge Base: Link to further online documentation on IGEL KB.

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 1032).

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

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 (see page 1420).

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 695): Create and organize standard profiles.
- Priority Profiles (see page 744): Create and organize priority profiles.
- Template Keys and Groups (see page 746): Keys and values for use in template profiles.
- Firmware Customizations (see page 764): Customize the user interface to suit your corporate design.
- Devices - Managing Devices in the IGEL UMS (see page 776): Organize managed devices.
- **Shared Workplace users** (see page 817): Assign specific profiles to AD users.
- Views - Filtering for Devices in the IGEL UMS (see page 818): Create configurable list views for devices.
- Jobs - Sending Automated Commands to Devices in the IGEL UMS (see page 847): Define scheduled tasks, e.g. firmware updates.
- Files (see page 1123): Registering files for transfer to devices.
- Universal Firmware Update in the IGEL UMS (see page 856): Allows you to download the current firmware versions for distribution to devices.
- Search History in the IGEL UMS (see page 861): Saved search queries.
- Recycle Bin (see page 864): 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

	Open the IGEL UMS Web App (see page 1154).
	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 695).
- **Priority Profiles**: Name, description, profile ID, etc. See Priority Profiles in the IGEL UMS (see page 744).
- **Template Profiles**: Name and description of template keys and value groups. See Template Profiles in the IGEL UMS (see page 746).
- **Firmware Customizations**: Name, use case, and configuration parameters of a firmware customization. See Firmware Customizations in the IGEL UMS (see page 764).
- **Devices**: System information, license and monitor information, features, etc. See Devices - Managing Devices in the IGEL UMS (see page 776) and View Device Information in the IGEL UMS (see page 778).

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 in the IGEL UMS (see page 817).
- **Views**: Name, rule, matching devices, etc. See Views - Filtering for Devices in the IGEL UMS (see page 818).
- **Jobs**: Job info, schedule, execution results, etc. See Jobs - Sending Automated Commands to Devices in the IGEL UMS (see page 847).
- **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 1123).
- **Universal Firmware Update**: Firmware update settings and version, download status, etc. See Universal Firmware Update in the IGEL UMS (see page 856).
- **Search History**: Name, rule, matching devices, etc. See Search History in the IGEL UMS (see page 861).
- **Recycle Bin**: Name and type of the deleted object, its deletion date, etc. See Recycle Bin - Deleting Objects in the IGEL UMS (see page 864).

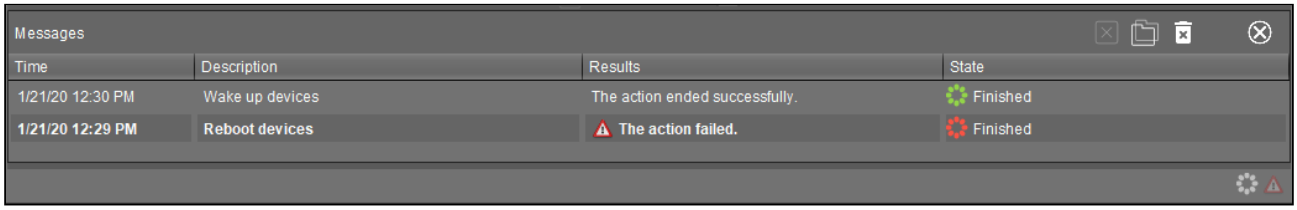
UMS Administration

- **Server**: Information regarding the service executed, requests, failed and waiting requests. See Server - View Your IGEL UMS Server Information (see page 870).
- **Load Balancer**: Information regarding the service executed, requests, failed and waiting requests. See Load Balancer - View Your IGEL UMS Load Balancer Information (see page 873).
- **Licenses**: License summary, registered licenses. See Licenses (see page 883).
- **Certificate Management**: Signature algorithm, key, status of the certificates, etc. See Certificate Management in the IGEL UMS (see page 895).
- **Device Attributes**: Device attributes such as name, type, etc. See Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879).
- **Administrative Tasks**: List with tasks, execution history. See Administrative Tasks - Configure Scheduled Actions for the IGEL UMS (see page 920).
- **Proxy Server**: Name, host, port, etc. See Proxy Server Configuration in the IGEL UMS (see page 967).
- **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 - Distributing Firmware in the IGEL UMS (see page 979).
- **Wake-on-LAN**: Wake-on-LAN configuration parameters. See Wake on LAN Configuration in the IGEL UMS (see page 981).
- **Active Directory / LDAP**: Active Directory / LDAP domains. See Active Directory / LDAP (see page 984).
- **Remote Access**: Secure VNC connection, graphics settings, etc. See Remote Access Configuration in IGEL UMS (see page 985).
- **Logging**: Log message settings, logging event settings. See Logging in the IGEL UMS (see page 987).
- **Mail Settings**: Mail settings, recipient for administrative task result and service emails. See Mail Settings (see page 993).
- **UMS Features**: Activating recycle bin, template profiles, priority profiles, etc. See UMS Features (see page 998).

Messages in the IGEL UMS Console

The **Messages** window area contains information regarding the successful or unsuccessful execution of commands.

An unsuccessfully executed command will be marked in the message list with a warning symbol and a red **State** symbol. A warning symbol will also flash in the status bar of the UMS Console until the user selects the message.



→ Click or double-click the message in order to view the relevant details.

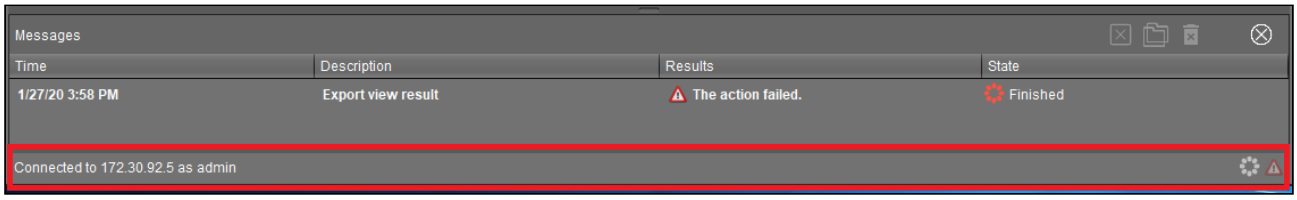
→ Click to delete messages you have already dealt with or wait until the message window is automatically reset when you close the UMS Console.

→ You can change the size of the message window using the middle slider or hide it altogether with a button .

To open the **Messages** window area again, click in the status bar of the UMS Console (or if messages about the unsuccessful command execution have not yet been selected).

Status Bar in the IGEL UMS Console

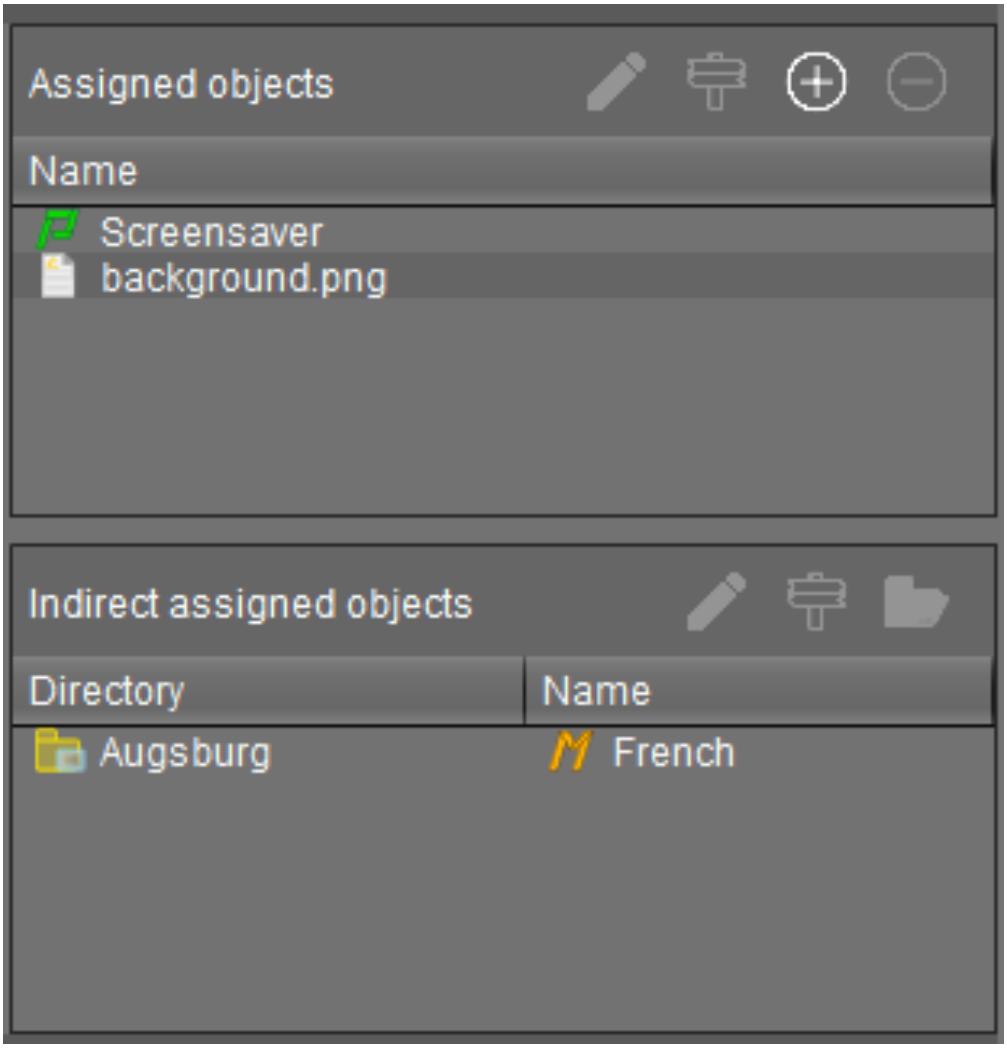
The **status bar** shows the name of the UMS Server currently connected and the user who is logged in to the UMS Console. The symbol at the bottom right indicates the status of the message window. For example, it signals when new warning messages are present. These can be seen here even if the message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



Assigned Objects in the IGEL UMS Console

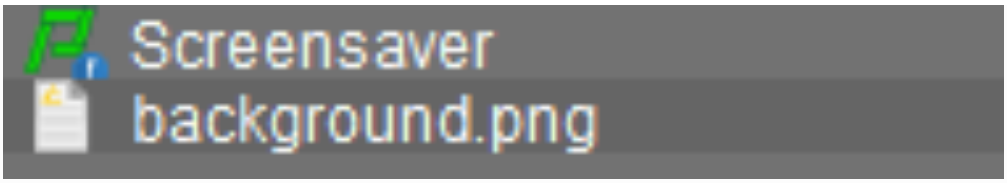
To ensure that you can quickly tell directly and indirectly assigned objects apart, the **Assigned objects** area is subdivided into two parts:

- Directly assigned objects have been assigned to an individual device, folder or profile.
- Indirectly assigned objects have been "inherited" via the file structure.



→ Double-click an object in the assignment area in order to directly edit it.

Assigned objects with configuration changes not yet transferred to the device are marked with an exclamation mark:


Screensaver
background.png

Context Menu in the IGEL UMS Console

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 672).

Search for Objects in the IGEL UMS Console

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

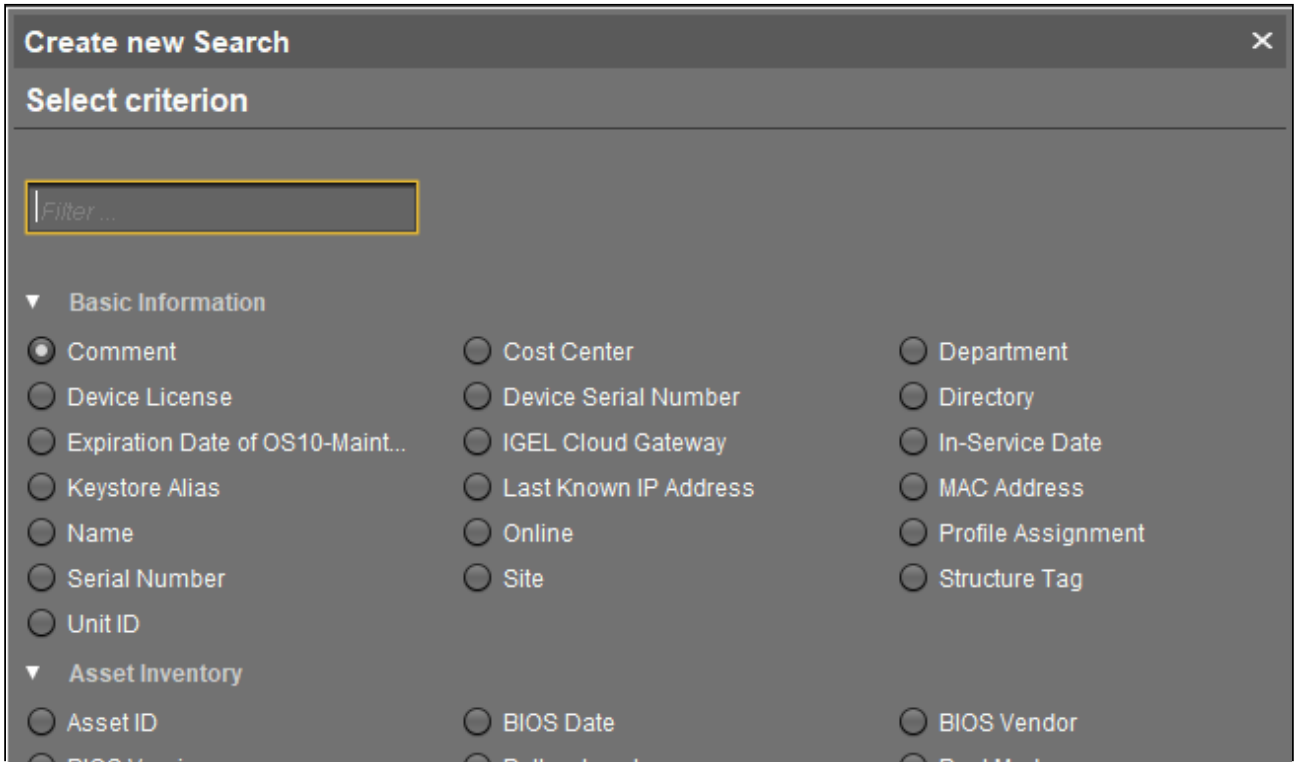
- **Quick Search**
- **Search function**
- **View**

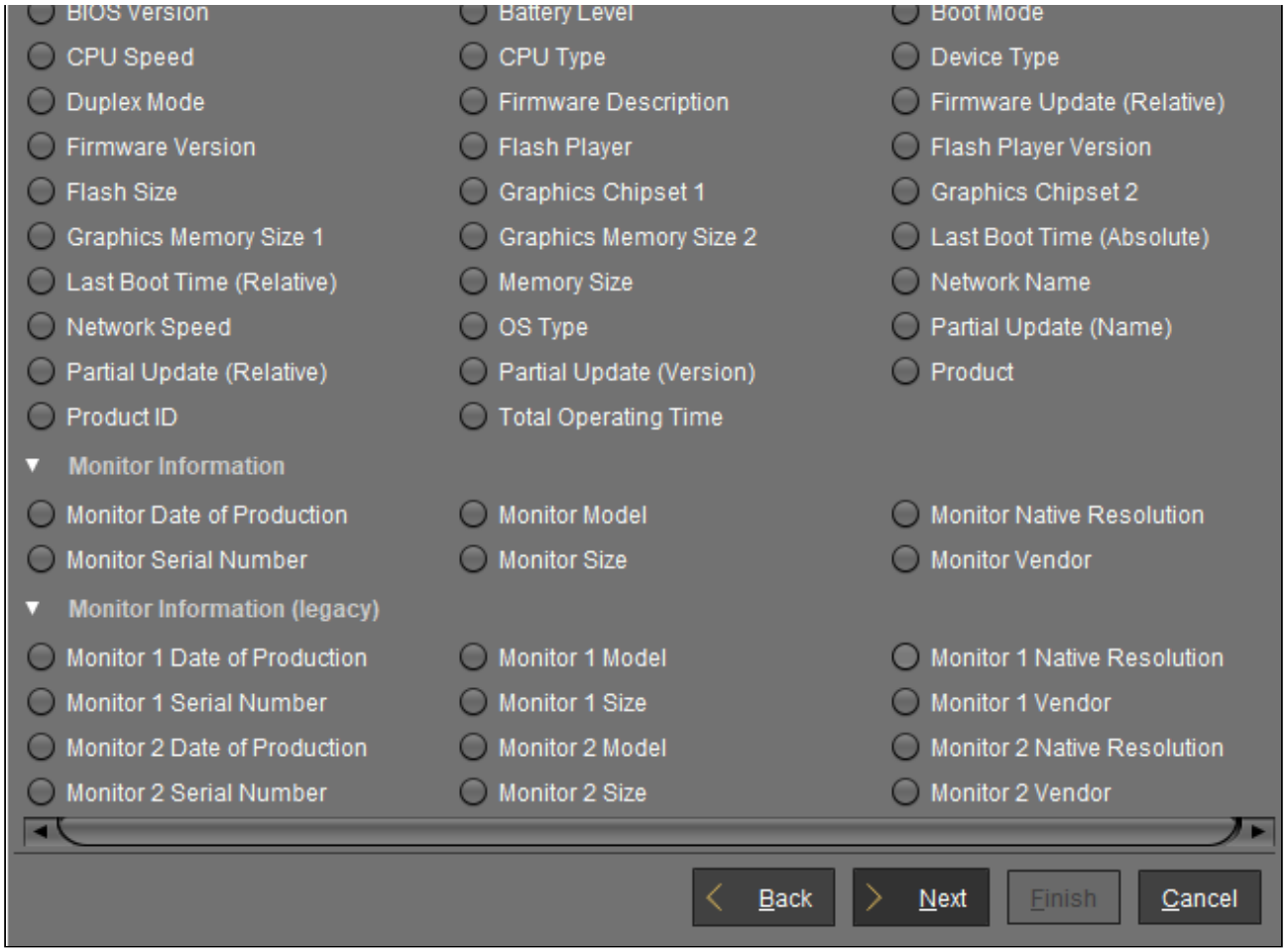
Quick Search

The **Quick Search** in the symbol bar (see page 684) 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 861) in the structure tree and can therefore be processed or reused easily.





Views

Views (see page 818) 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 847).

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 846) and Assign Objects to the Devices of Views or Device Searches (see page 950).

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.
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 (see page 1239).

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).

Menu path: **UMS Console > Profiles**

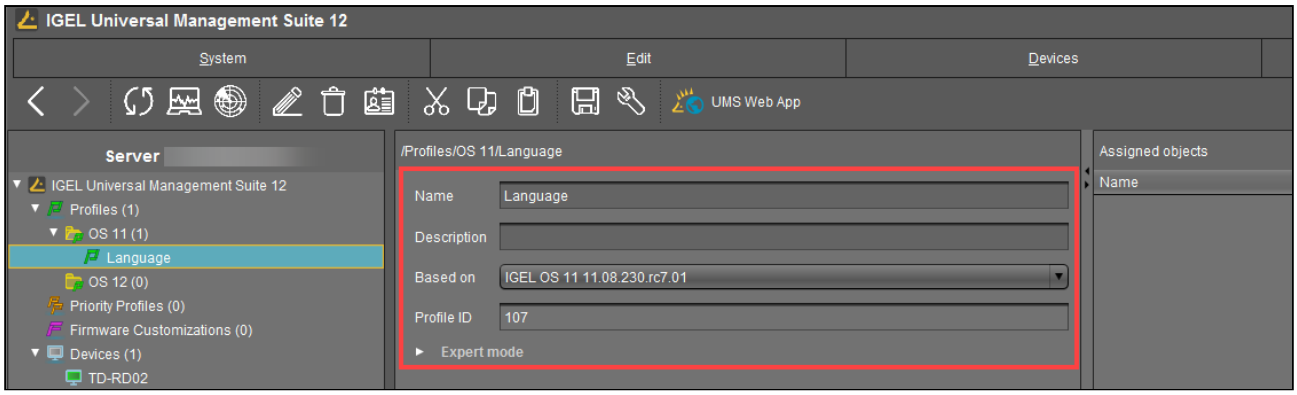
When Is It a Good Idea to Use Profiles?

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.

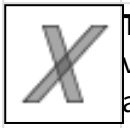
Information on a profile is shown in the content panel.



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:

	**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 743). If you use Shared Workplace (see page 1427), 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 732) and Prioritization of Profiles in the IGEL UMS (see page 728).
	**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 746) chapter. If you deploy Shared Workplace (see page 1427), notice that template profiles cannot be used.
	**Priority profiles** can overwrite the settings of standard profiles and have their own authorizations, see Priority Profiles in the IGEL UMS (see page 744). 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 734).

- Choosing the Right Profile (see page 698)
- Configuration Levels (see page 699)
- Using Profiles (see page 700)
- Prioritization of Profiles in the IGEL UMS (see page 728)

- Effectiveness of Settings (see page 743)

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 700) chapter, you can find out how to set up and assign profiles.

In the Template profiles (see page 746) chapter, you can also find out how to create profiles with variable values.

In the Prioritization of Profiles in the IGEL UMS (see page 728) 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 744) 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 (see page 1431) and Parameters Configurable in the User Profile (see page 1435).

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 728) 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 701).

Using Profiles

In this chapter, you can learn the following:

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 (see page 1252).

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).

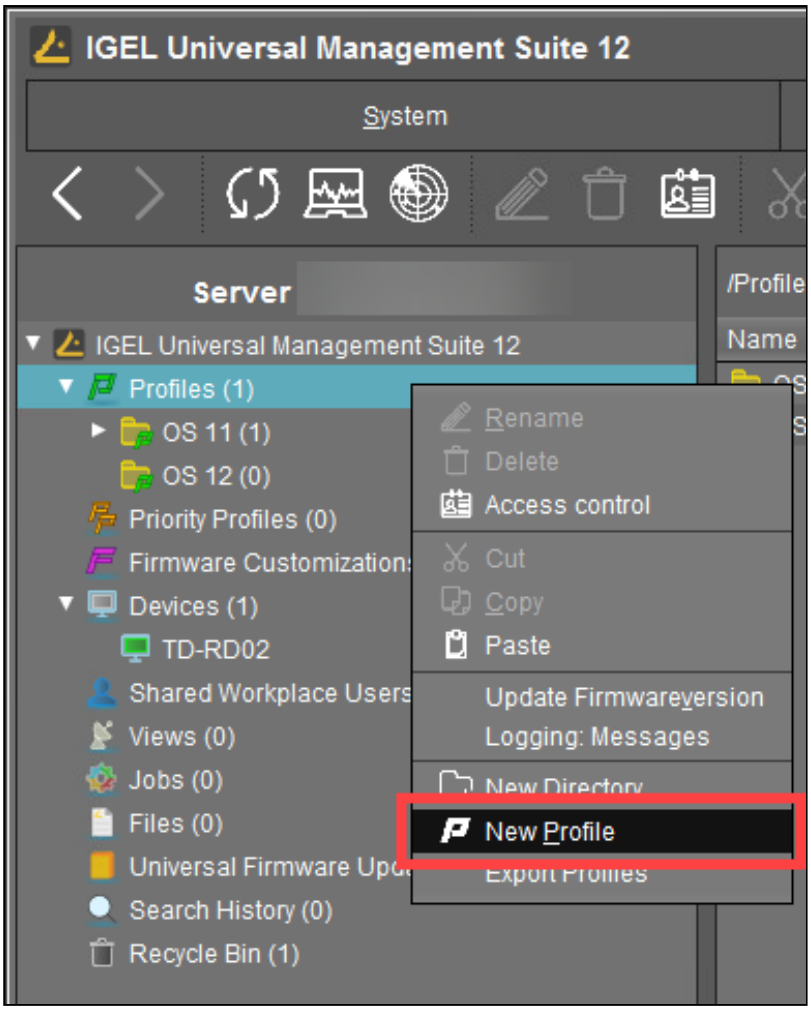
To ensure that you can use all new features of IGEL OS:
→ Update your UMS to the current version.
→ For all relevant OS 11 profiles (see page 701), set **Based on** to the appropriate firmware version.
→ For OS 12 profiles (see page 1252), note the following: An OS 12 profile configures ALL versions of an app, unless a specific version is set under **Show Versions**.

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

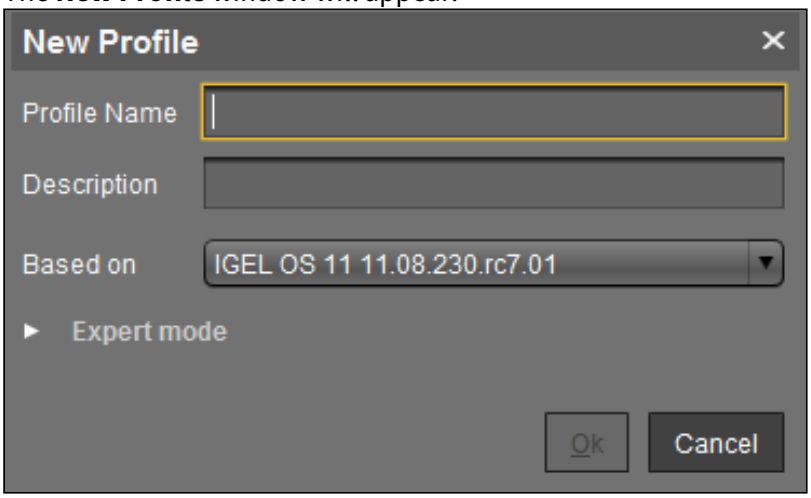
How to Create a Profile

To create a new profile, proceed as follows:

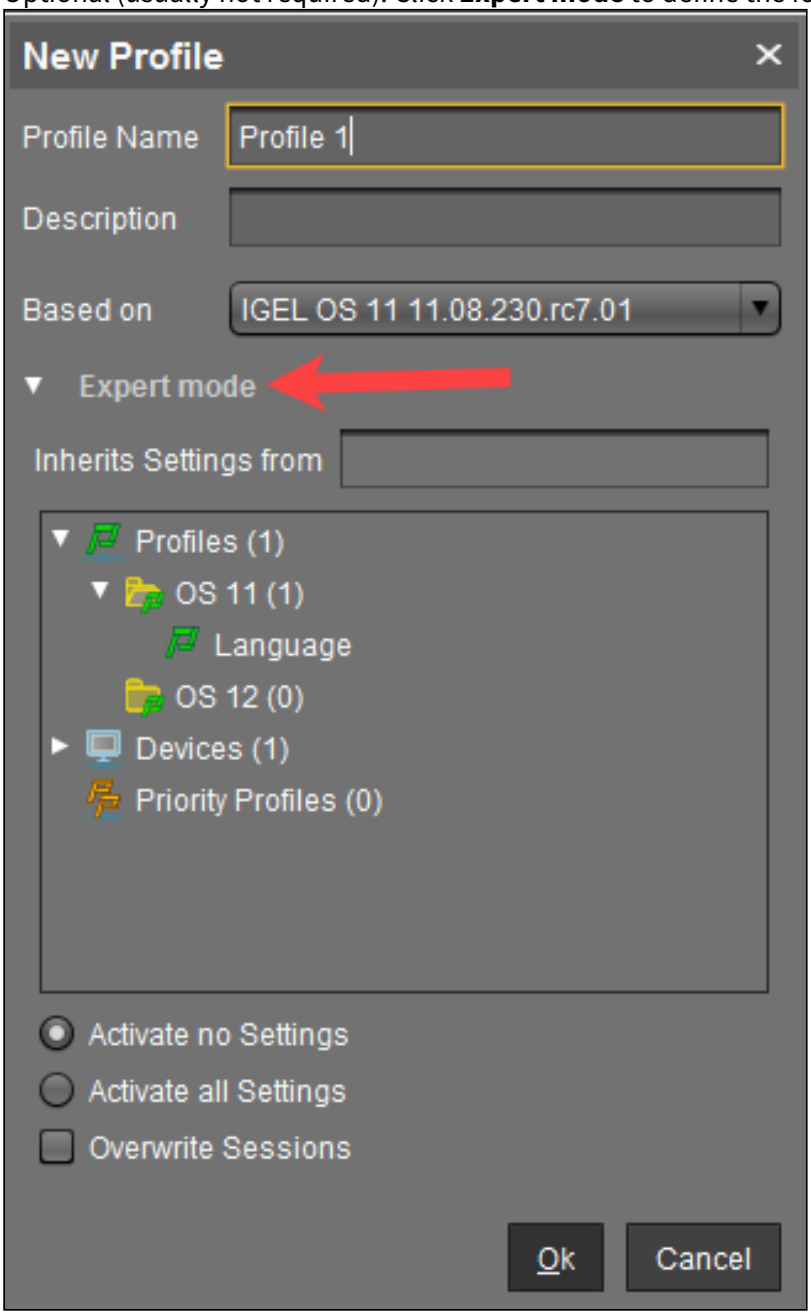
1. In the UMS Console, click **Profiles > [context menu] > New Profile** or **System > New > New Profile**.
   Alternatively, you can import a previously created profile. See Exporting and Importing Profiles (see page 719).



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.

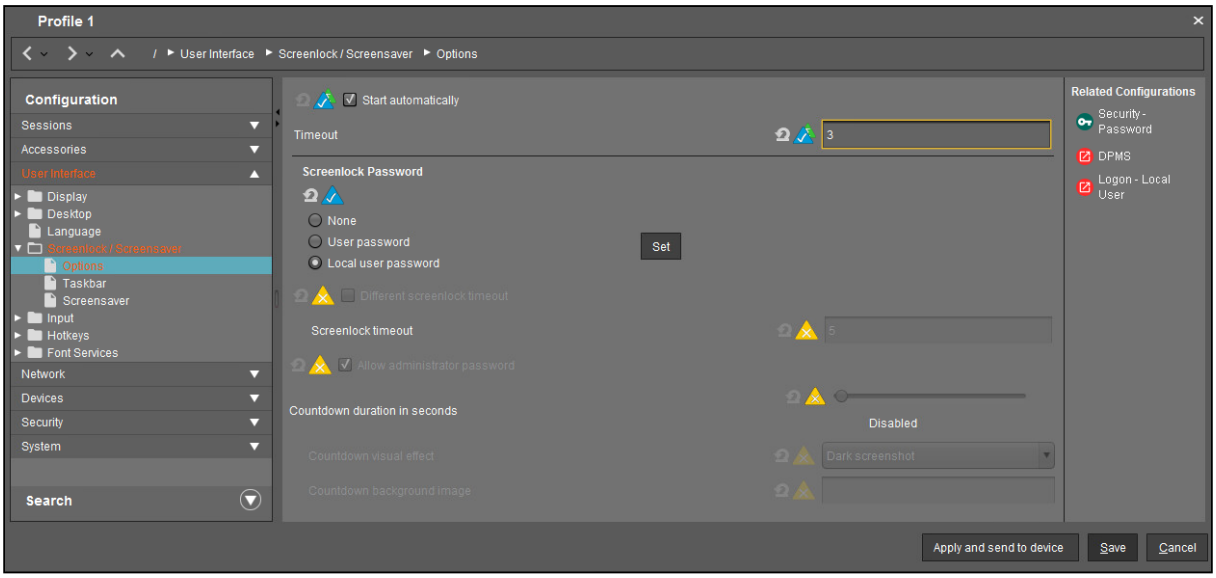
IMPORTANT! Before changing the default settings here, inform yourself about the possible consequences, see "New Profile: Expert Mode" below. **Activate all settings** will block all settings in the local Setup! **Overwrite sessions** should be activated only in exceptional cases! With this option, you can override free instances of all other profiles.

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

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 746)):
   - 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 707).

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.

> ℹ 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

> ℹ 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 699).

☑ 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.

> ℹ 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 744) 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=Ml522x3qqn0

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.

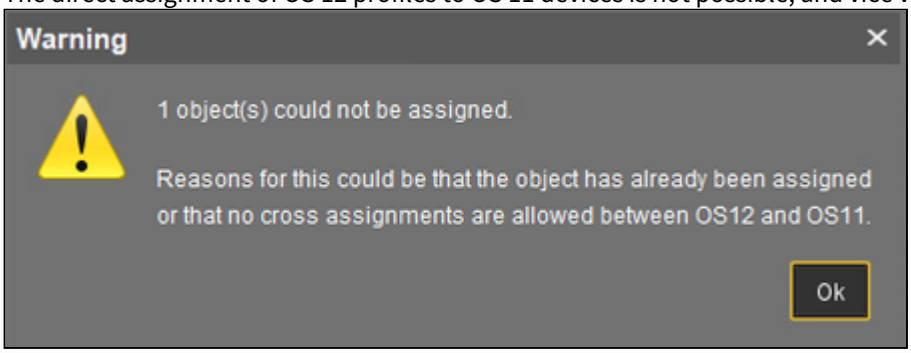
Direct and Indirect Assignment of Objects in the IGEL UMS
Objects in the IGEL UMS can be assigned directly or indirectly:

- 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 729).
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.

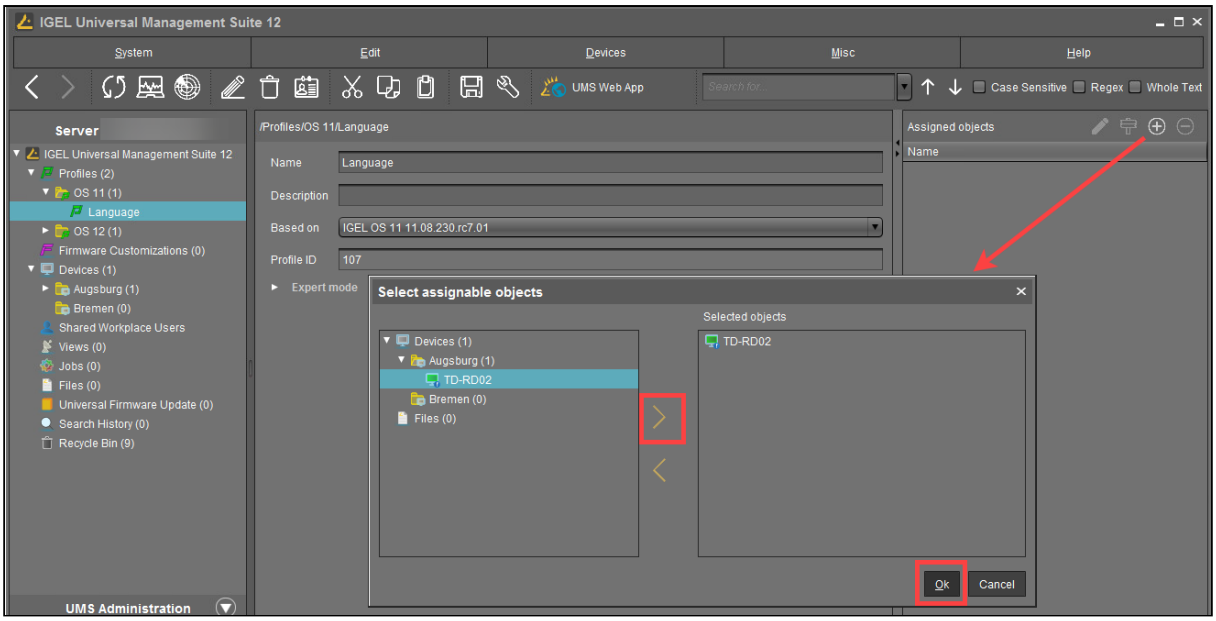
The direct assignment of OS 12 profiles to OS 11 devices is not possible, and vice versa:



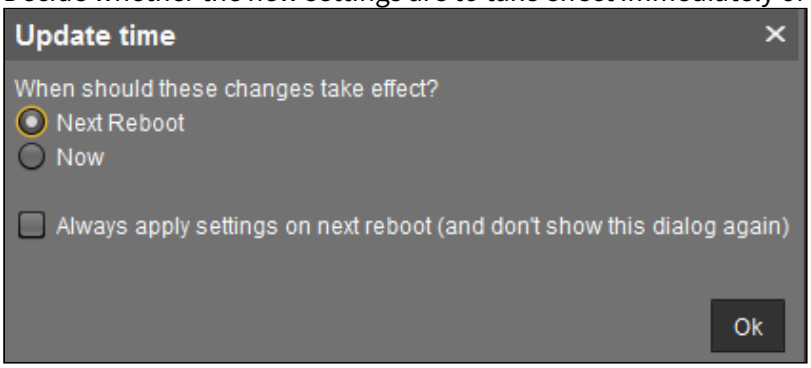
If you assign an OS 12 profile to an OS 11 device indirectly, i.e. via a directory structure, the OS 12 profile is NOT regarded for the OS 11 device (and vice versa).

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.



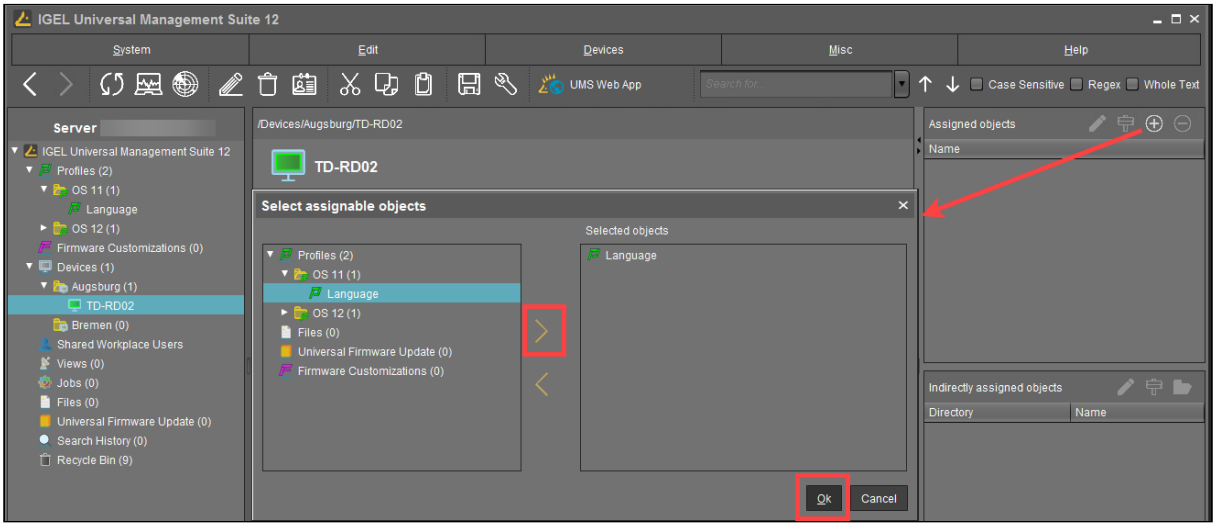
Bear in mind that users who are working may be disturbed if changes take effect immediately.

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

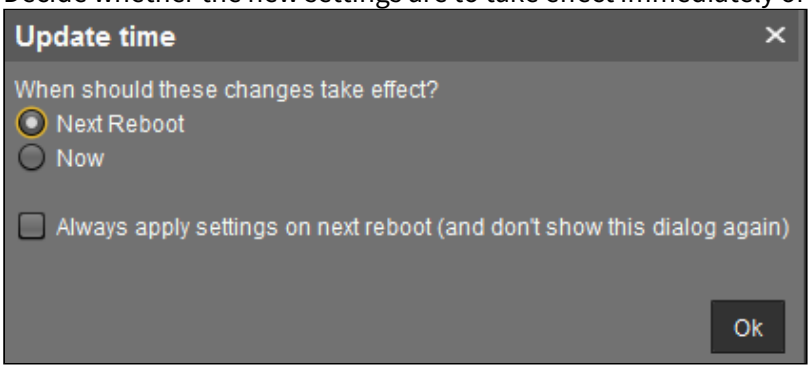
How to Assign a Profile: Starting from the Device / Device Directory

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**.

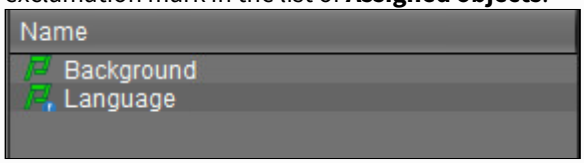


5. Decide whether the new settings are to take effect immediately or at the next reboot of the device.



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**.

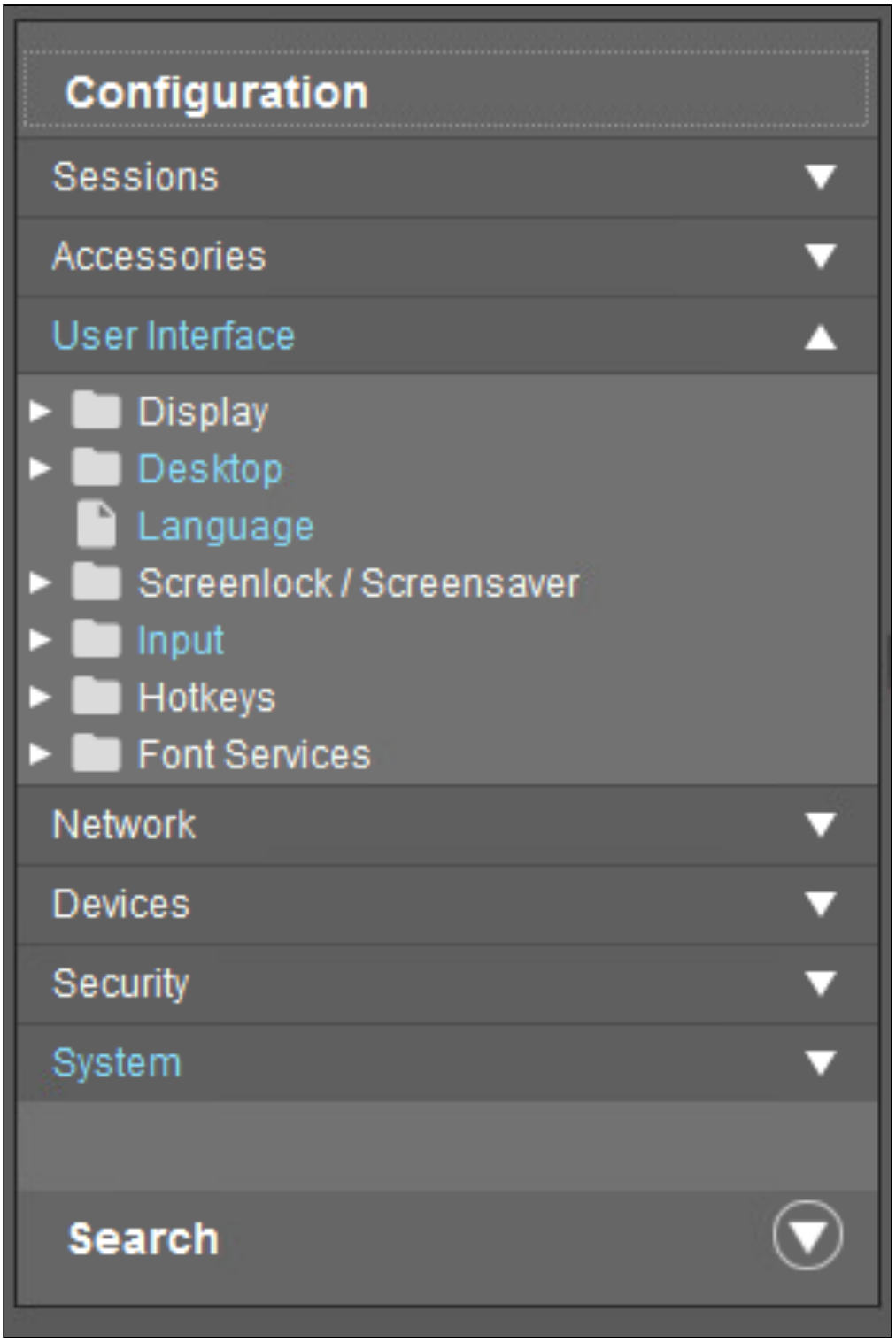


How to Check Profiles in the IGEL UMS

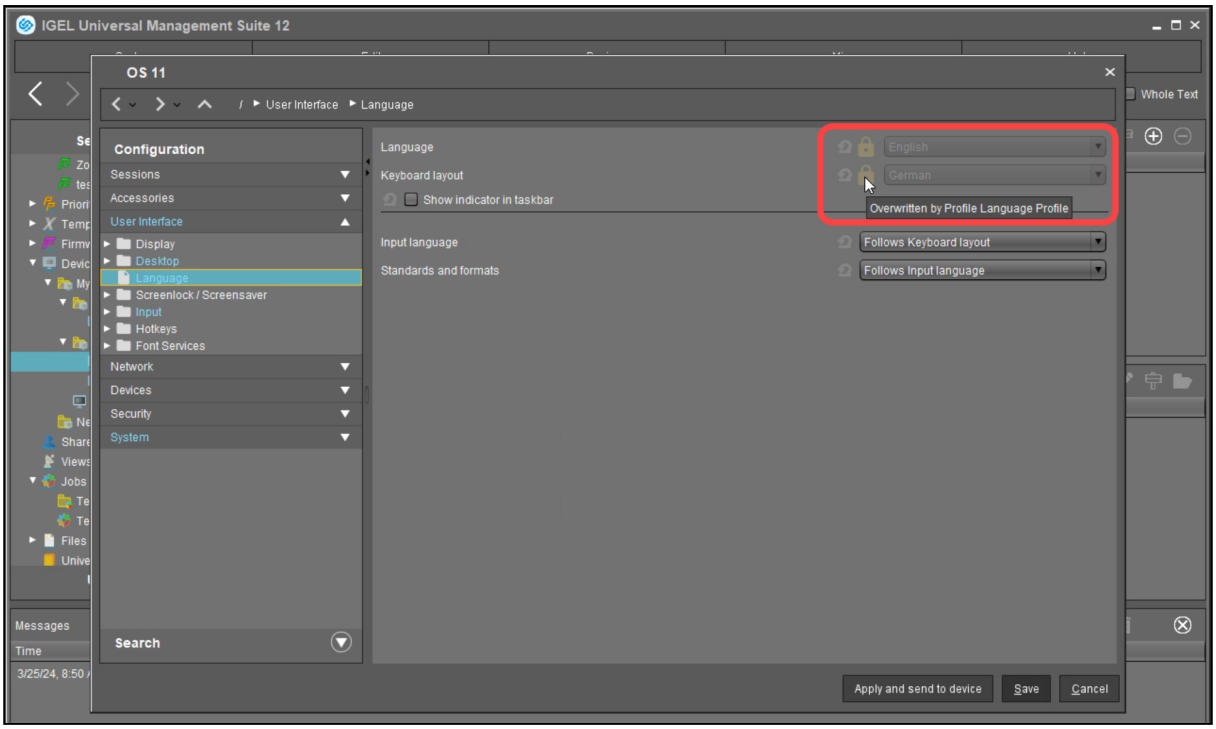
If you have assigned a profile to a device in the IGEL Universal Management Suite (UMS), you can check the results as follows. In the IGEL UMS Web App, you can do it as described in How to Check which Profiles Define Parameters in the IGEL UMS Web App (see page 1268).

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.

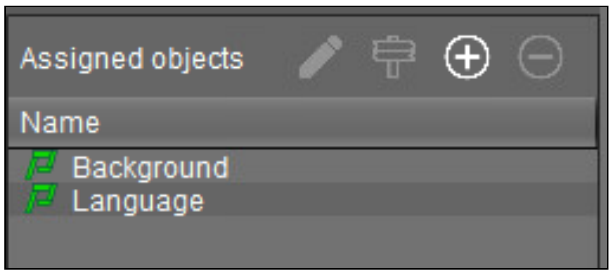


A lock symbol will be shown in front of each setting configured via an assigned profile. The value that you have specified in the profile will be shown. You cannot change the setting here.



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.



→ 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

How to Edit 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**

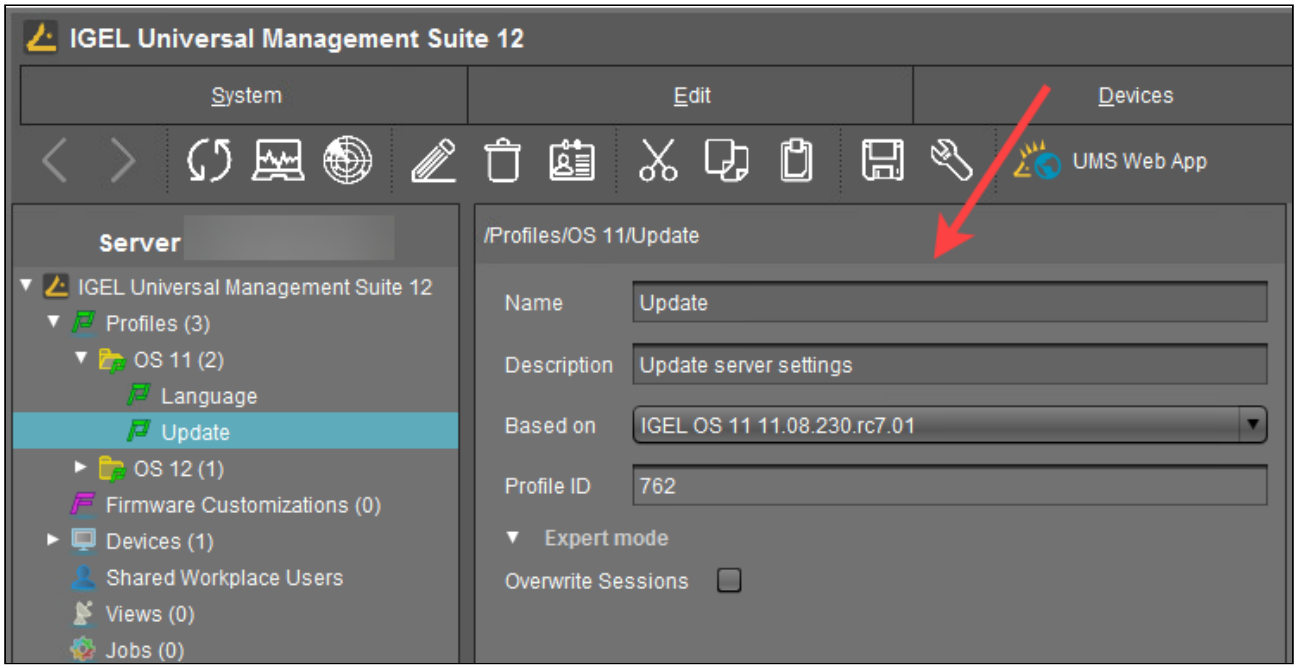
How to Edit Description Data of a Profile

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.

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

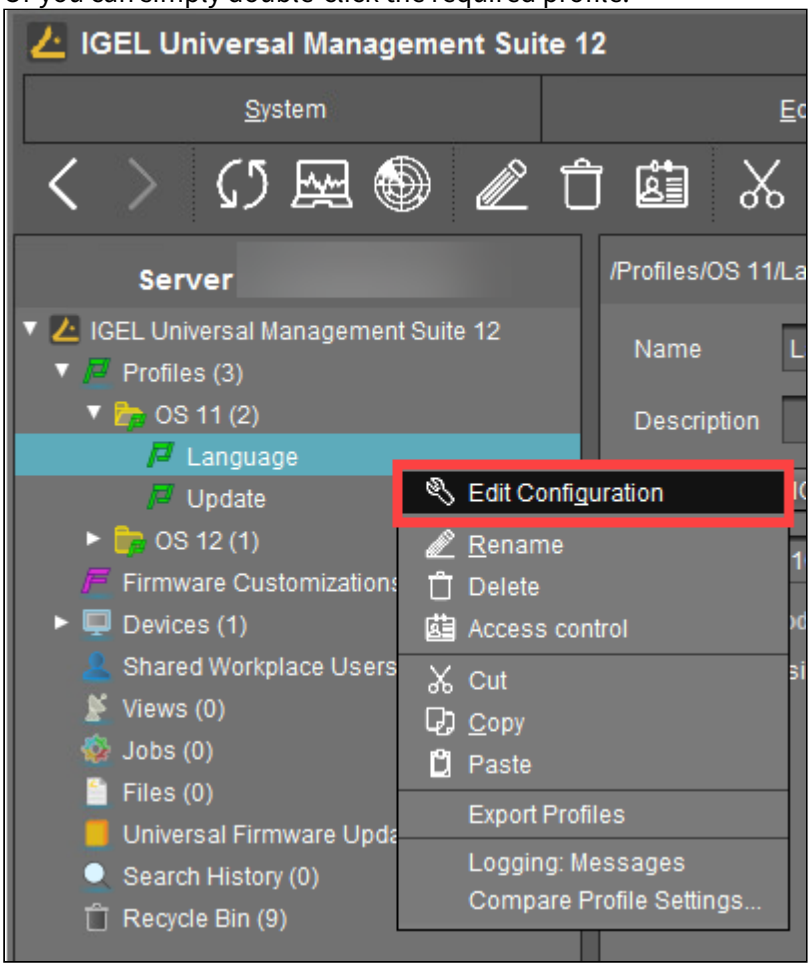


3. To save the changes, click or **Edit > Save description**.
   The data are now updated in the database.

How to Edit the Profile Configuration

To edit the profile configuration, proceed as follows:

1. 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.

2. 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 746)):
-  - 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.

How to Remove Assigned Profiles from a Device in IGEL UMS

You can remove assigned profiles from a device or a device directory in the IGEL Universal Management Suite (UMS).

Starting from the profile

1. Select a profile in the navigation tree.
2. Select an object in the **Assigned Objects** area.
3. Click  .

Starting from the device

1. Select a device or a device directory in the navigation tree.
2. Select an assigned profile from the list in the **Assigned Objects** area.
3. Click  .

This profile will now no longer affect the individual device(s) in the directory. The overwritten value for the settings is reset to the value which was valid before the profile was assigned.

> Only directly assigned profiles can be removed. Indirectly assigned profiles can only be removed where they are assigned directly, that is the directory.

Deleting Profiles

If you would like to delete a profile, select it in the UMS navigation tree and perform one of the following options:

→ In the symbol bar, click on **Delete**  .

→ Press the [Del] button on your keyboard.

→ Right-click on the profile and select the **Delete** option from the context menu.

The same applies to directories too. These are deleted along with all sub-directories and profiles.

> If you delete a profile, it will be removed for every device or every device directory to which it was assigned. The profile values no longer affect the device settings. In addition, all settings for the profile from the database will be deleted.

If the recycle bin is active, the deleted profile will be stored there and you may recover it if you need to.

Exporting and Importing Profiles

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 803).

> 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 (see page 1269).

Exporting a Profile and Firmware

To export an individual profile, proceed as follows:

1. Right-click the profile.
2. Select the command **Export Profile.**

To export a number of profiles in one file (ZIP archive), proceed as follows:

1. Highlight the desired profiles using the [Ctrl] and [Shift] keys.
2. Select **System>Export>Export Profile.**
   The **Export Profiles** window will open.

3. Select the requested profiles in the column **Include**.
4. Confirm by clicking **OK**.
5. Select the destination file.

The firmware information can be exported to an archive along with the profile data. This allows importing to a *UMS* installation without the relevant firmware being registered. This can now be imported together with the profile.

The profiles are converted into the XML format. Make sure that you do not make these files public if the source profiles contain passwords or other confidential data!

Importing a Profile and Firmware

To import an individual profile, proceed as follows:

1. Click **System > Import > Import Profiles**.
2. Select the `XML` file or archive containing your profile(s).

   The **Import Profiles** dialog window will appear. This shows the name and firmware version of each profile configuration contained in the file you have selected.
3. Uncheck one of the boxes in the left row of the table to exclude the relevant profile from the import process.

> During the import, you can retain the original directory path of the profile. Alternatively, the profile can be placed in the main directory.

A dialog window shows whether all the selected profiles were imported.
An item of firmware from an archive which was previously not present in the database will automatically be imported together with the corresponding profile.

- Importing Profiles with Unknown Firmware (see page 723)

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 744).

> It is not possible to copy IGEL OS 12 profiles via the UMS Console. Use the **Duplicate** function in the UMS Web App, instead, see Configuration - Centralized Management of Device Settings in the IGEL UMS Web App (see page 1239).

Menu path: **UMS Console > 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.

> 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 744).

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.

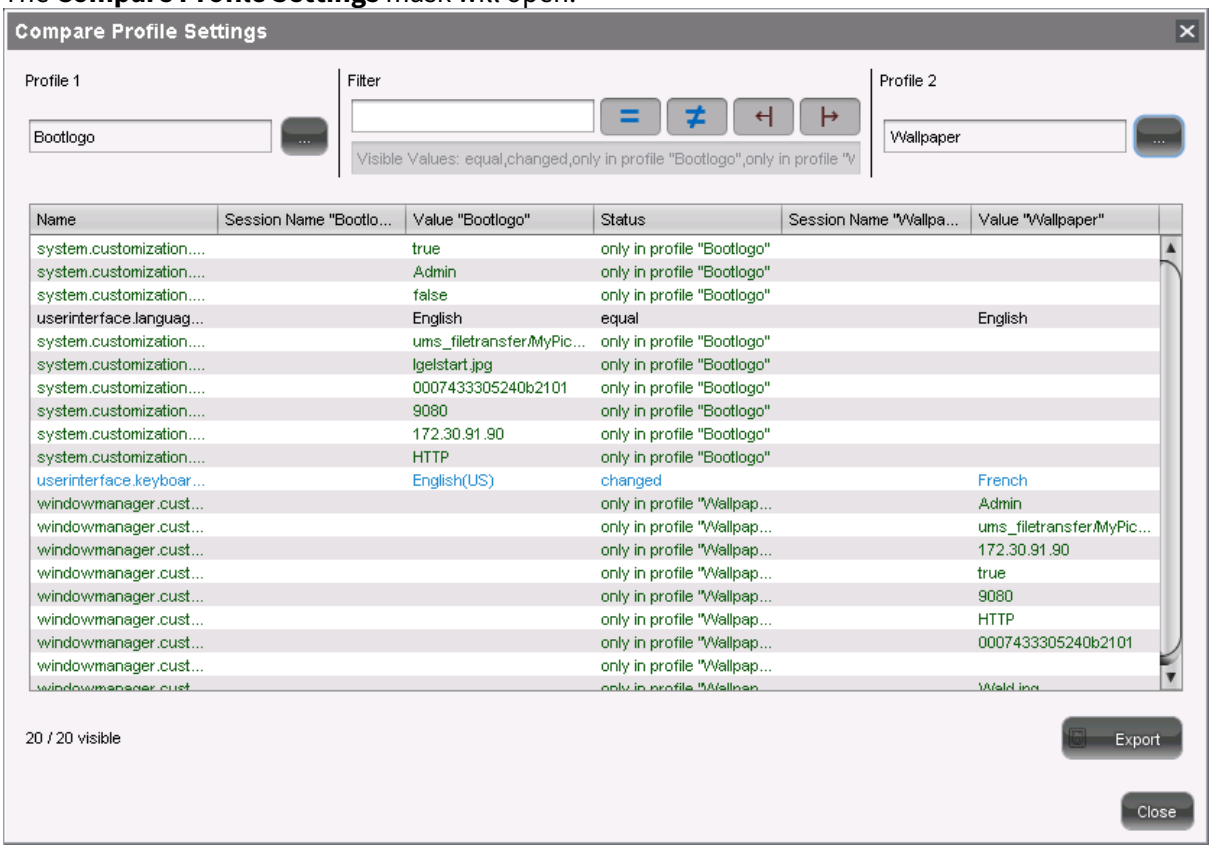
Comparing Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can use a function which makes it easy to compare profiles with each other.

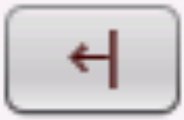
Menu path: **UMS Console > Profiles**

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.



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 732).

The procedure for setting up and configuring profiles is described in Use profiles (see page 700). This chapter mainly looks at priorities – which profile overrides which one and when.

Order of Effectiveness

The priority of profiles is symbolized by "LEDs" below. The more red lights, the higher the priority of the profile.

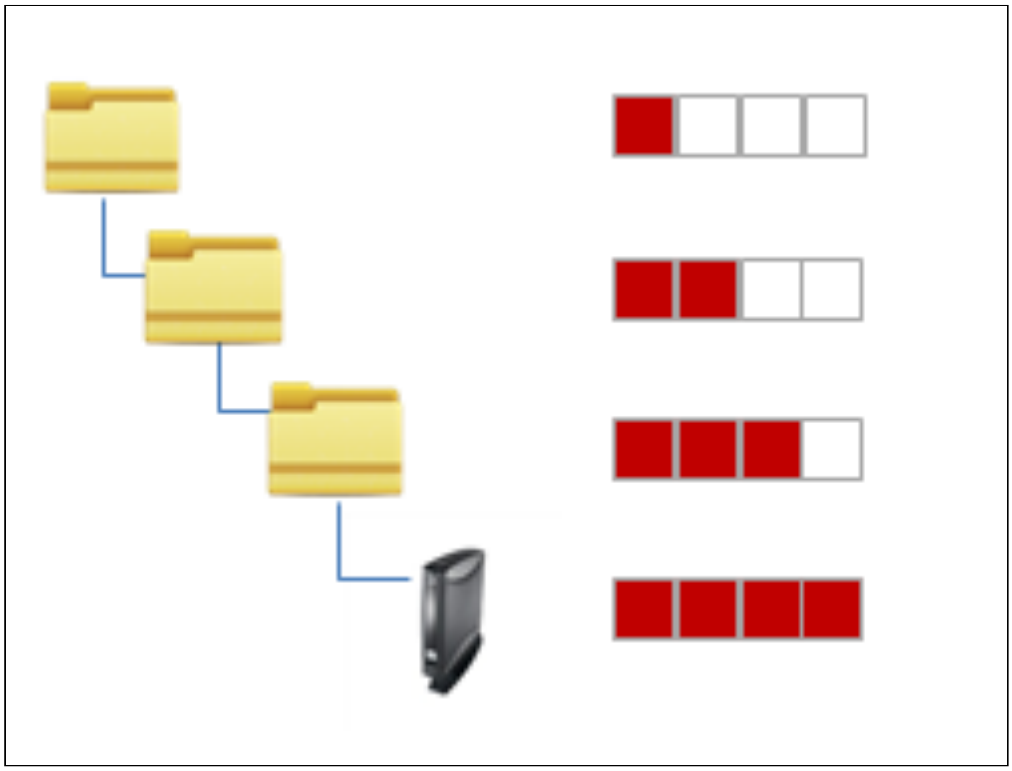
Order of Effectiveness of Profiles

In order to be able to manage the effectiveness of different profile types, you need to understand the order of priority. Various profiles that overlap like stencils can be assigned to a device. What happens if two profiles specify a different value for a setting? Which one has more weight?

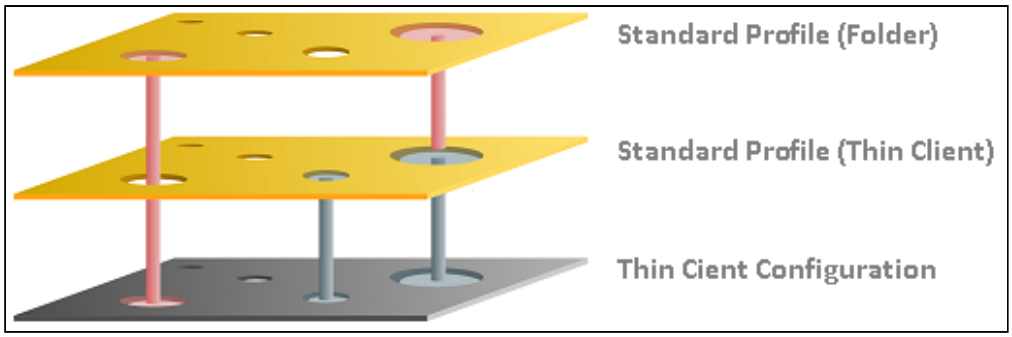
Avoid competing settings in a number of profiles. If possible, set up one profile per setting, e.g. a profile for language settings, one for a left-handed mouse, etc.

The following rules apply to competing settings in various profiles:

Rule: The closer the standard profile is to the device in the directory tree, the higher its priority.



The priority rule only plays a role if the same parameter value is different in two profiles. The following graphic shows that there are specified values in both profiles which have an effect on the device. Only the parameter on the right is set by both profiles. In this case, the value of the bottom profile has priority because it is closer to the device.



Rule: In the event that the same settings are specified a number of times, the profiles with higher priority override other profiles. The effectiveness of settings which are specified in one profile only does not change.

See the following example (see page 731).

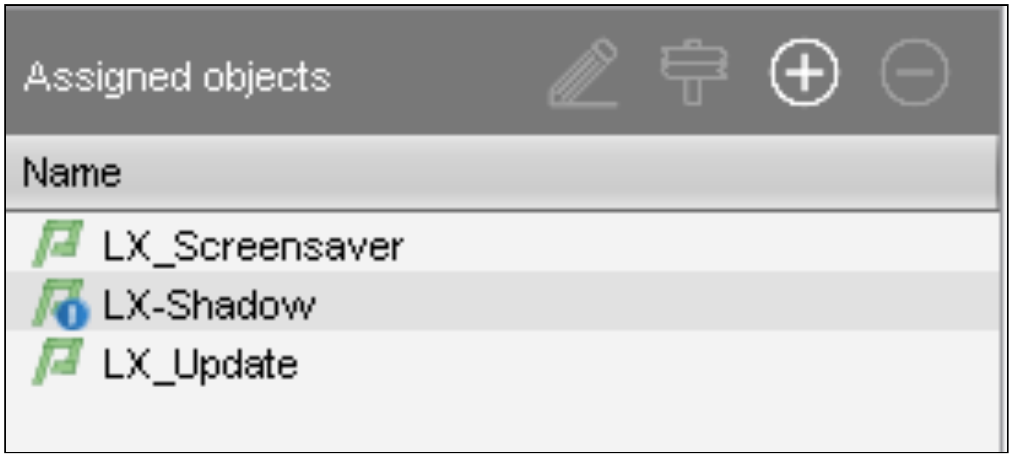
Rule: If several profiles are assigned on an equal basis, the newer profile with the higher profile ID has priority.

> In order to read out the ID of a profile, point to a profile in the list of assigned profiles with the mouse pointer. A tooltip with the profile ID will be shown.

Rule: The priority rule only applies to general settings. If a number of sessions are set up, they will not be overridden. They will exist alongside each other because free instances are added.

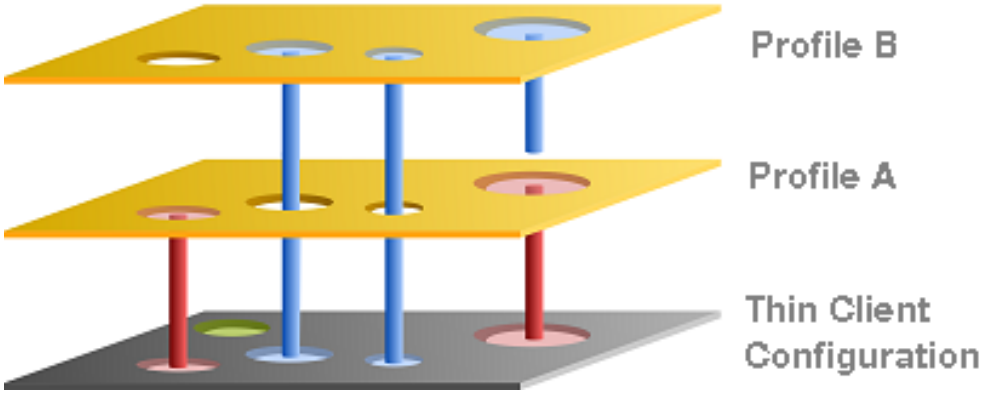
The lists of directly or indirectly assigned profiles are sorted according to the order of priority. Within a directory level, the profile which is higher up in the list thus has a higher priority.

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



Example – Standard Profiles

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

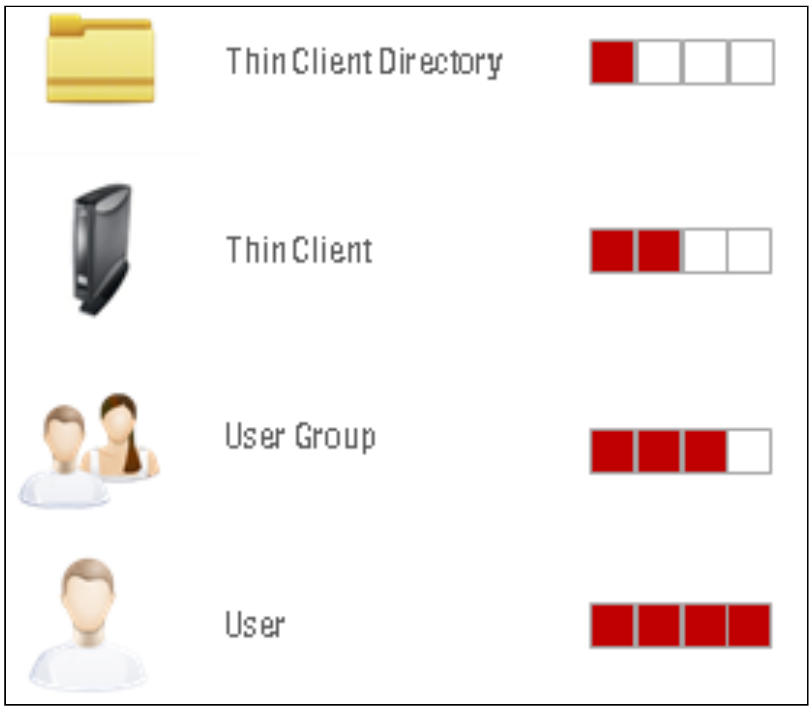
In IGEL Shared Workplace (see page 1427), you can use profiles to configure user settings. For further information, see the guide IGEL Shared Workplace - Assigning a User Profile (see page 1431).

⚠ Template profiles and template keys (see page 746) cannot be used if Shared Workplace is deployed.

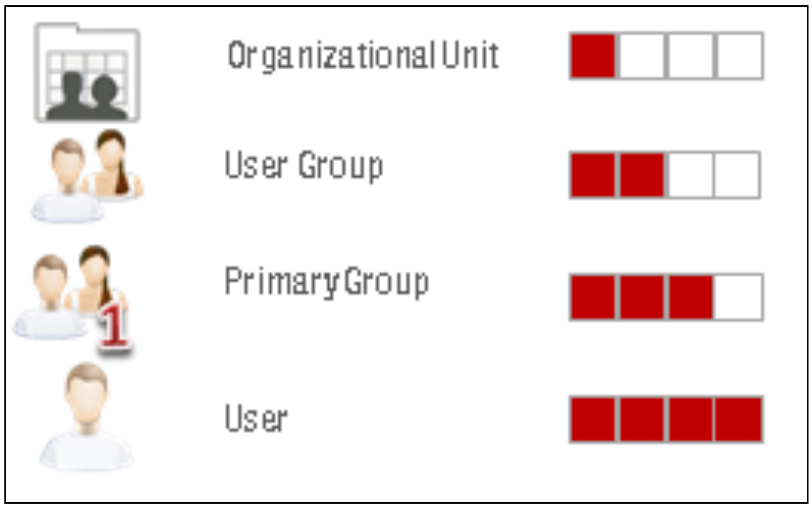
Rule: Profiles that are assigned to users have a higher priority than those that are assigned to devices. This applies to standard profiles and priority profiles.

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:

- user-specific profiles have a higher priority than device-specific profiles
- the profiles closer to the user/device have a higher priority



- primary groups have a higher priority than other groups
- other groups have a higher priority than the organizational unit



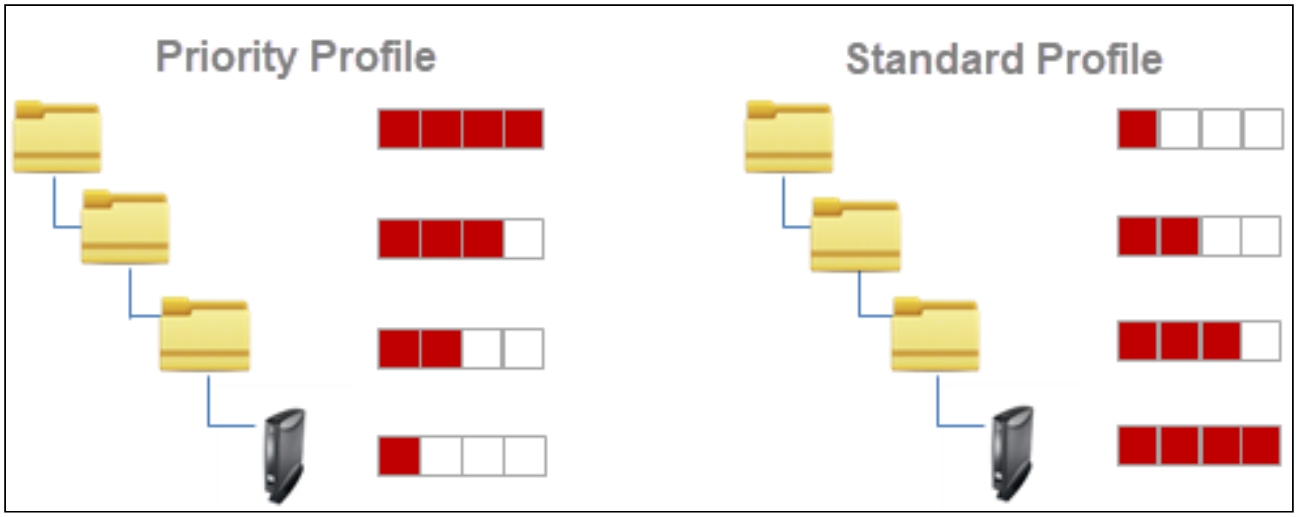
Rule: Profiles that are assigned to an object are prioritized in descending order according to profile ID (highest ID = highest priority).

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:

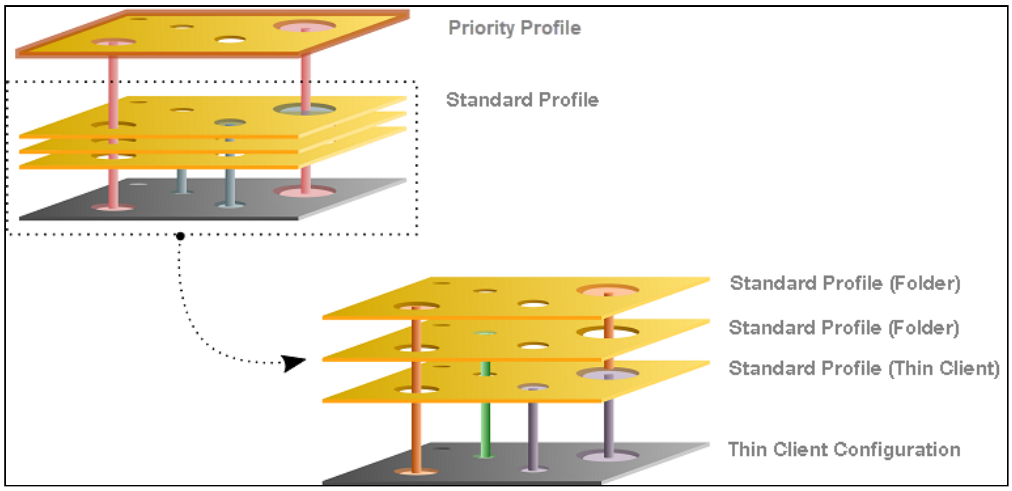


The following applies to priority profiles:

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

Rule: Priority profiles override all standard profiles.

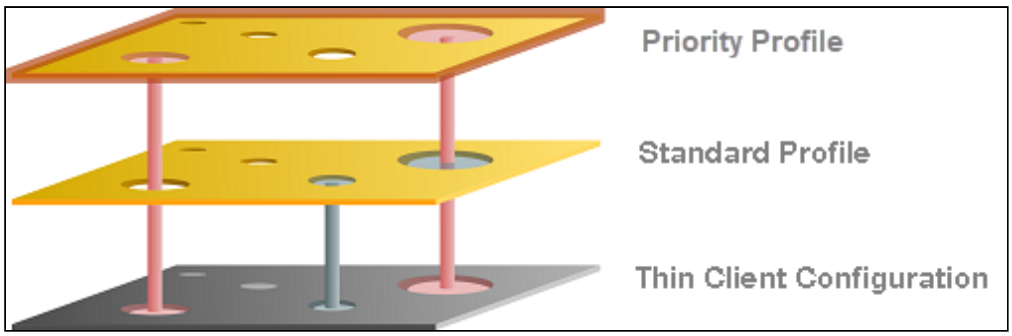
The following graphic shows that the priority profile setting overrides that of the standard profiles if the same parameter is pre-populated. Settings that are not double-populated are effective without restriction.



- Example – Priority Profiles (see page 736)
- Example – Priority and Various Standard Profiles (see page 737)
- Priority Profiles in IGEL Shared Workplace (see page 738)

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).

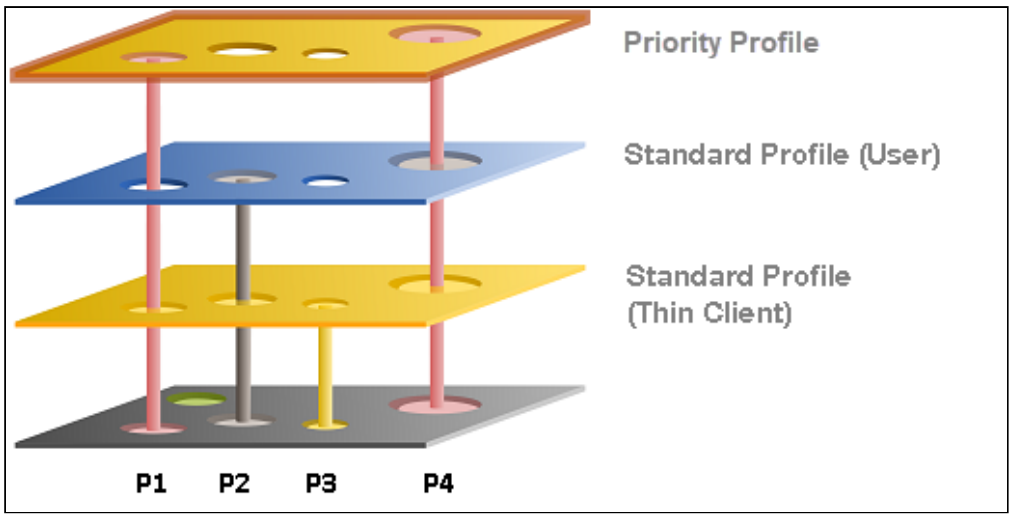
The settings that arrive at the device are:

- 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.

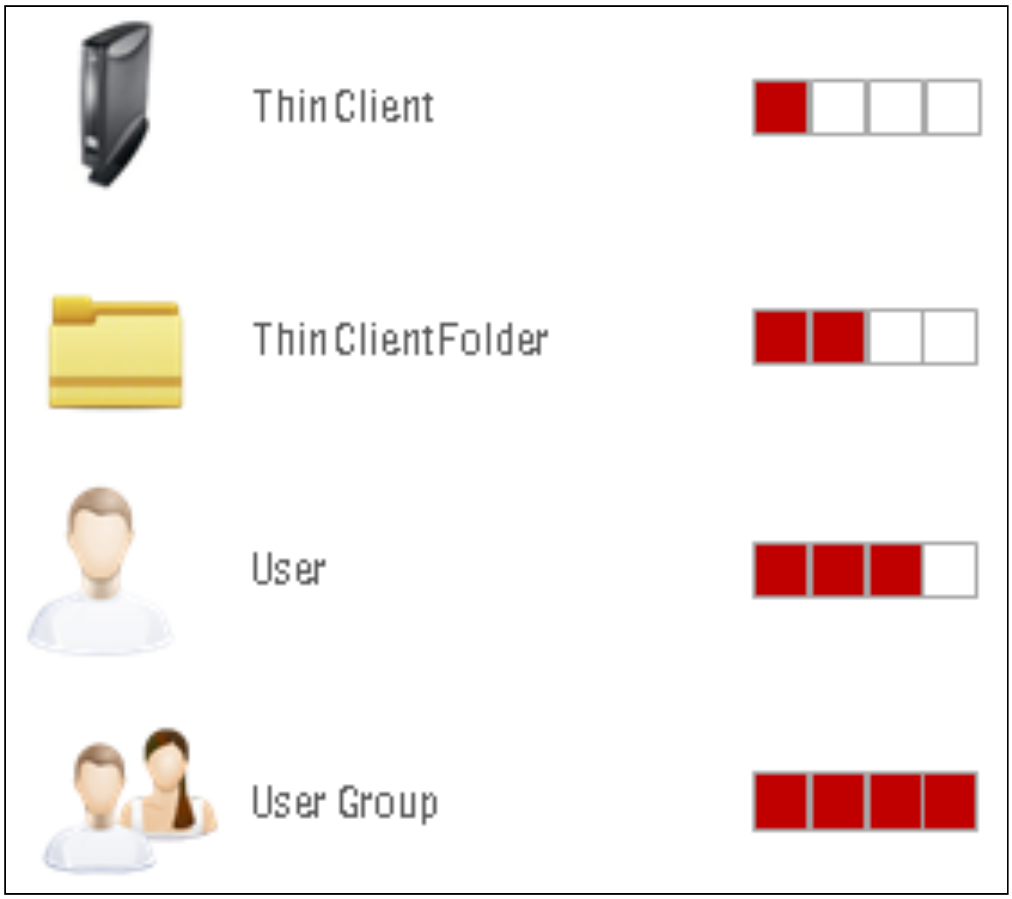
The settings that arrive at the device are:

- 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)

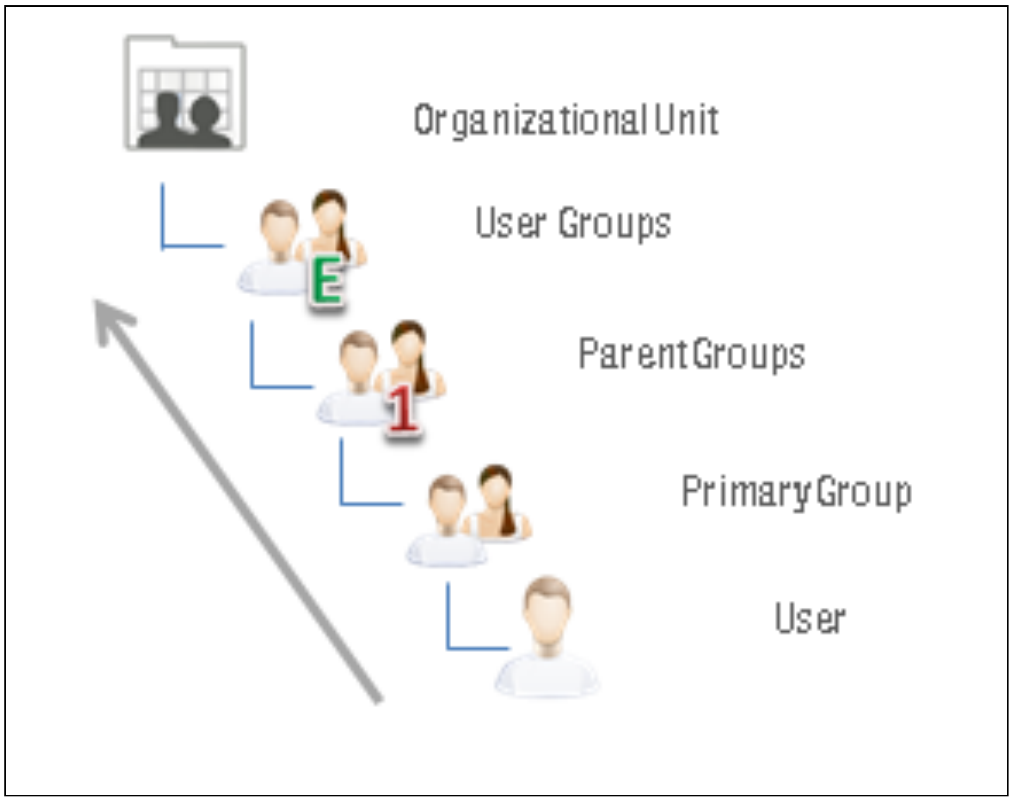
Priority Profiles in IGEL Shared Workplace

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.

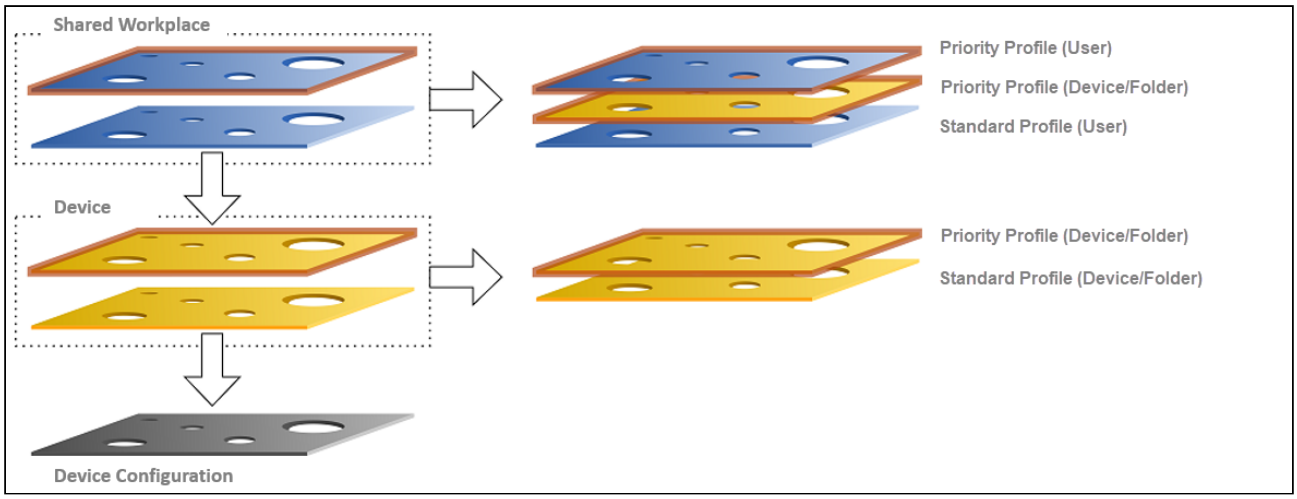


Higher priority	than...
user-specific profiles	device-specific profiles
further away from the user/device	closer to the user/device



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 731).
- 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 699) 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

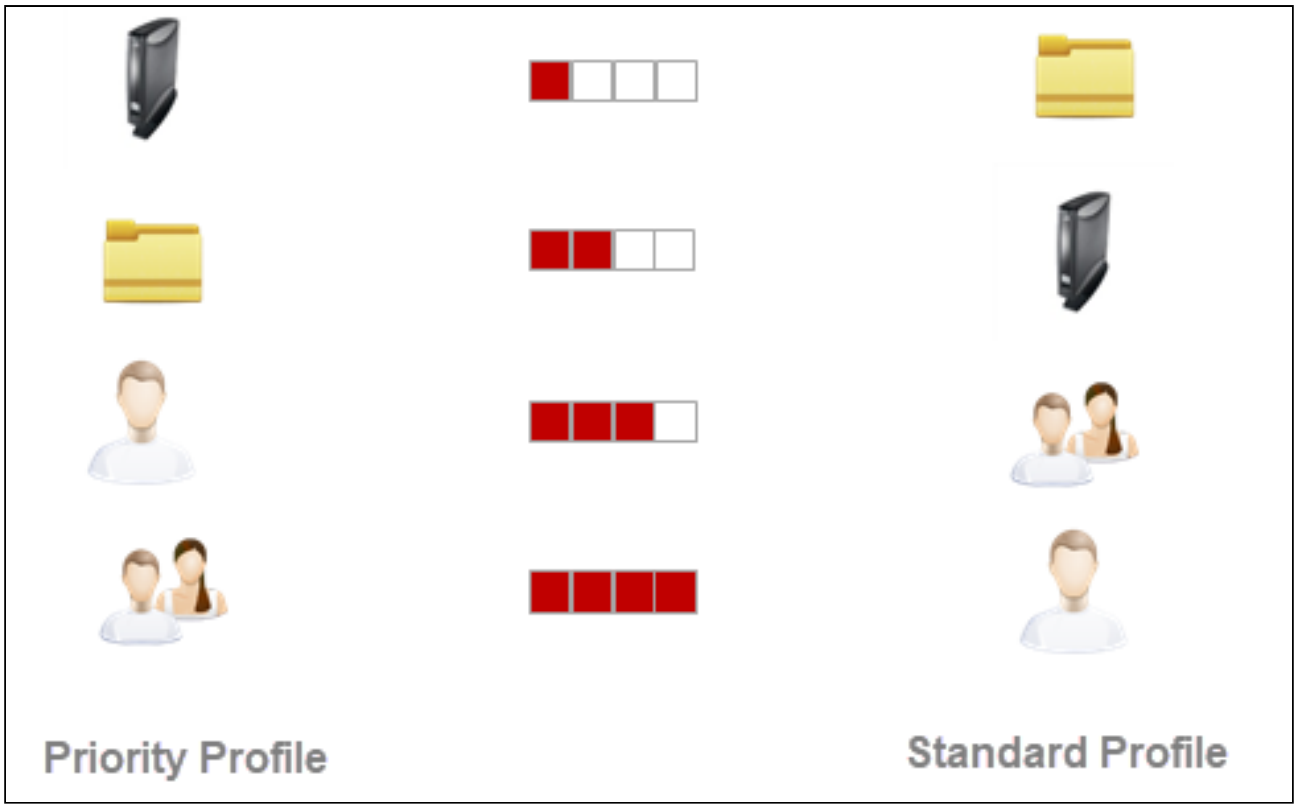
- The closer the standard profile is to the device, the higher its priority.

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.

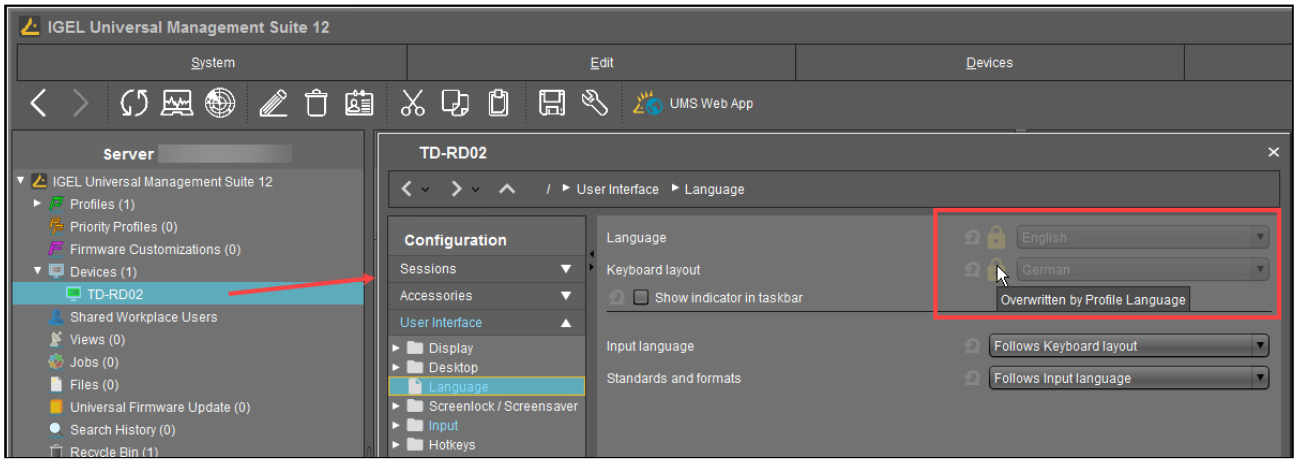


For information on the prioritization of firmware customizations, see Firmware Customizations in the IGEL UMS (see page 764).

For information on the prioritization of Universal Firmware Updates, see Precedence of IGEL UMS Profiles and Universal Firmware Updates (see page 619).

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.

> 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.

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.

Starting from IGEL UMS version 12.07.100. the feature is only available with specific UMS Licenses. For details, see IGEL OS Editions[139].

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 734).
- 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.

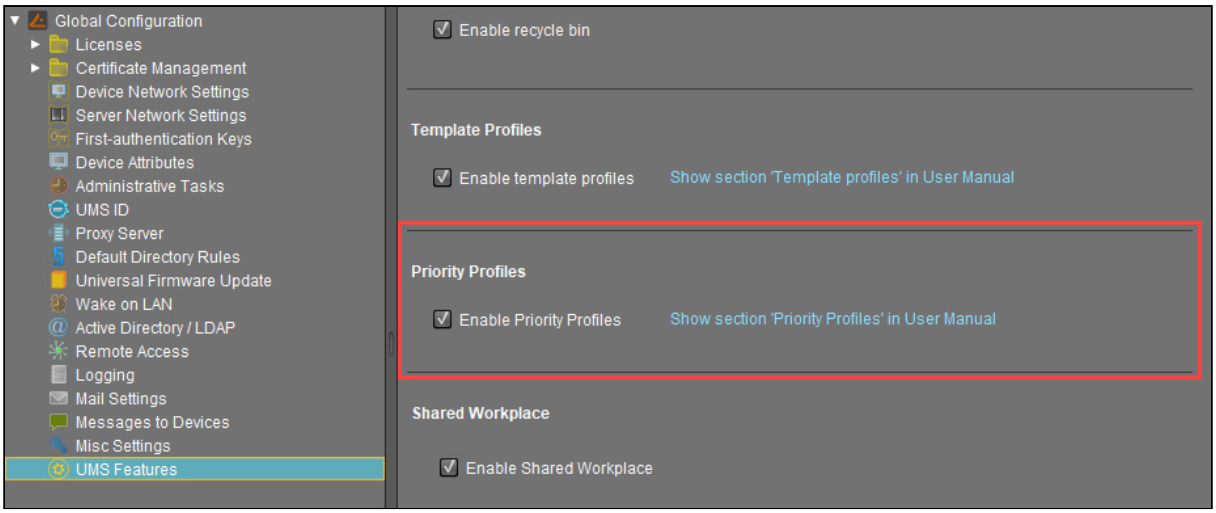
How to Enable Priority Profiles

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**.

139. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions



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 701).

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 (see page 1347) .

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 749).

For information on how to use template profiles in the UMS Web App, see How to Use Template Profiles in IGEL UMS Web App (see page 1272).

Starting from IGEL UMS version 12.07.100. the feature is only available with specific UMS Licenses. For details, see IGEL OS Editions[140].

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.

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 (see page 1427) 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 699). The unnecessarily large number of profiles is also difficult to manage in the long term.

Solution

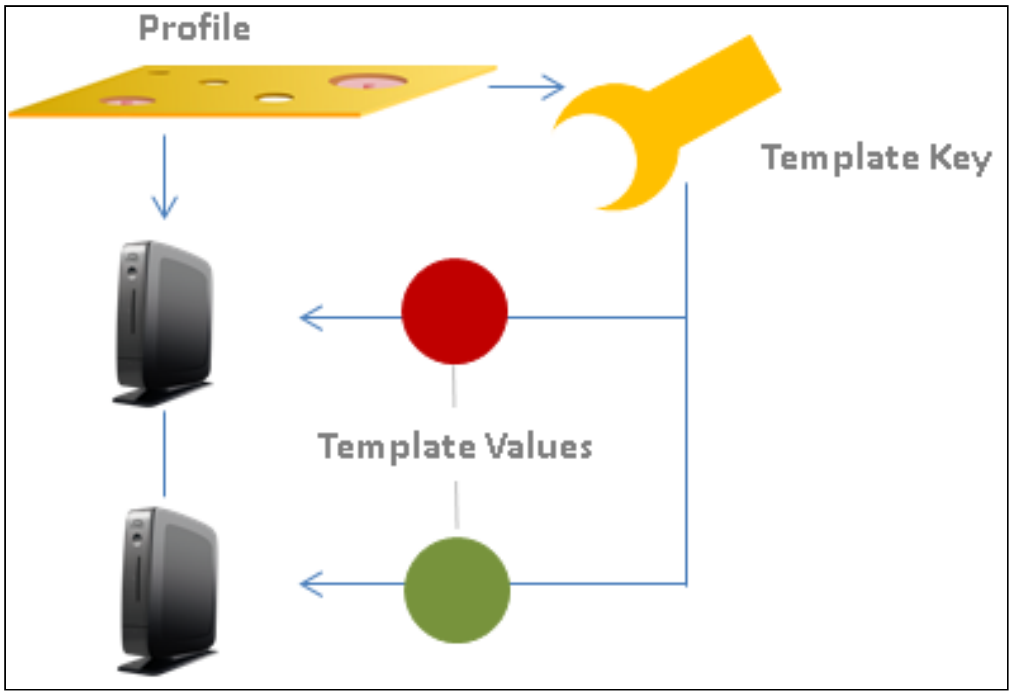
The use of a single template profile offers greater flexibility. This contains all data for the browser session which are common to the devices as well as placeholders, so-called template keys (see page 751). The template keys contain

140. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions

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

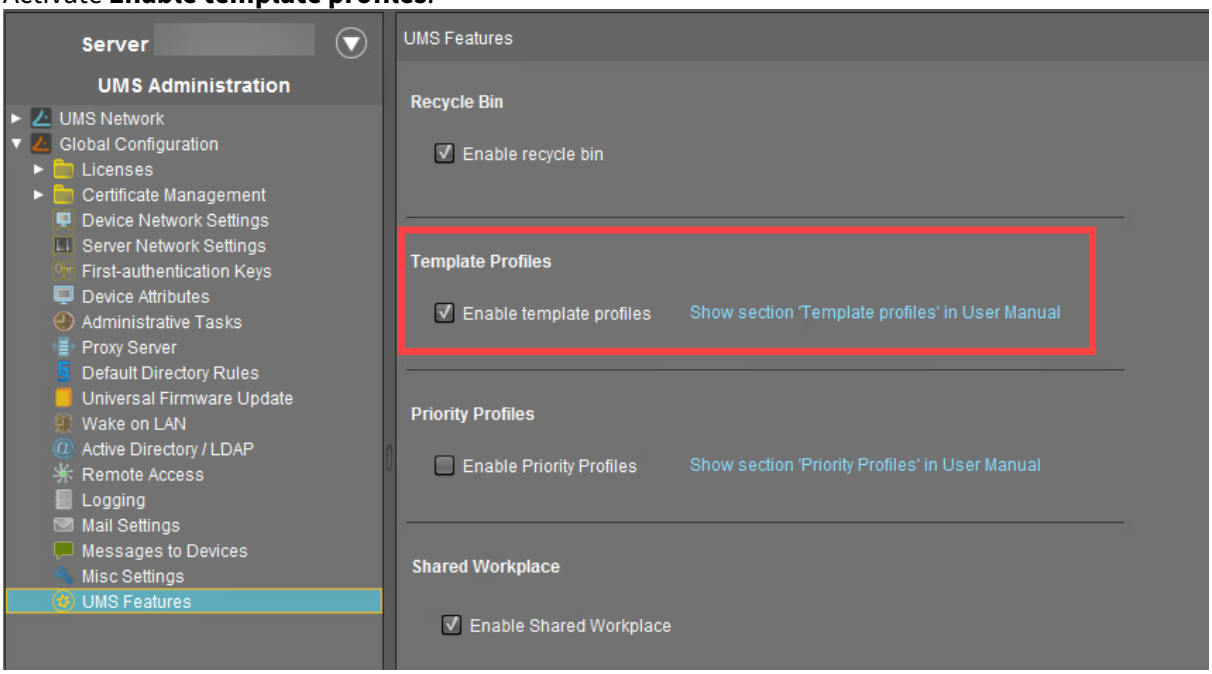
- How to Activate Template Profiles in the IGEL UMS (see page 749)
- How to Create Template Keys and Values (see page 751)
- How to Use Template Keys in Profiles (see page 756)

How to Activate Template Profiles in the IGEL UMS

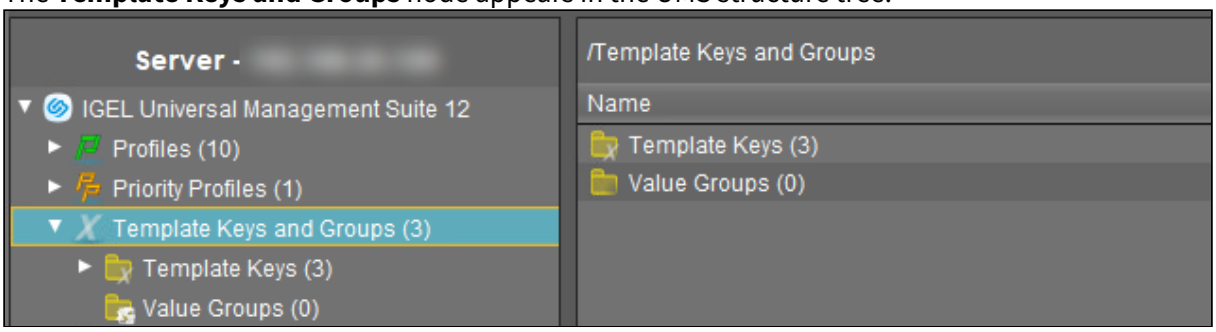
If you would like to use the template profiles function in the IGEL Universal Management Suite (UMS), you must enable it first through the UMS Console or the IGEL UMS Web App.

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

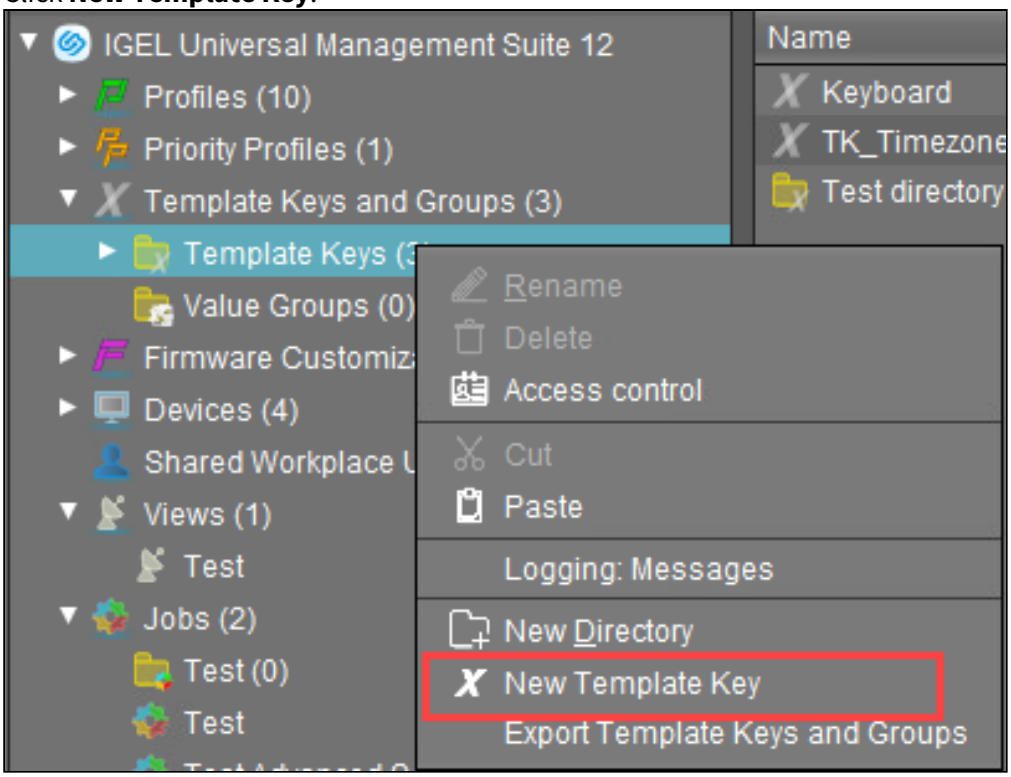
1. In the UMS Web App, go to the **Network > Settings** area.
2. Go to the **UMS Features** tab.
3. Activate **Enable template profiles**.

For more information, see Network Settings in the IGEL UMS Web App (see page 1347).

How to Create Template Keys and Values

To create template keys and values, proceed as follows:

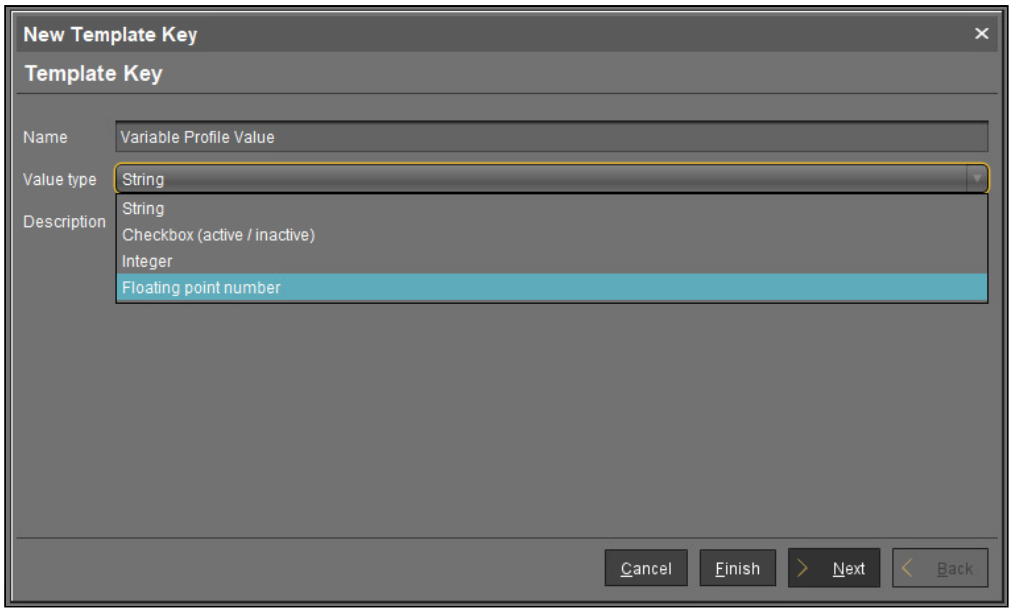
1. Open the context menu for the **Template Keys** folder.
2. Click **New Template Key**.



> Alternatively, this function is also accessible via the menu **System>New>New Template Key**, the focus must be on the **Template Keys** node.

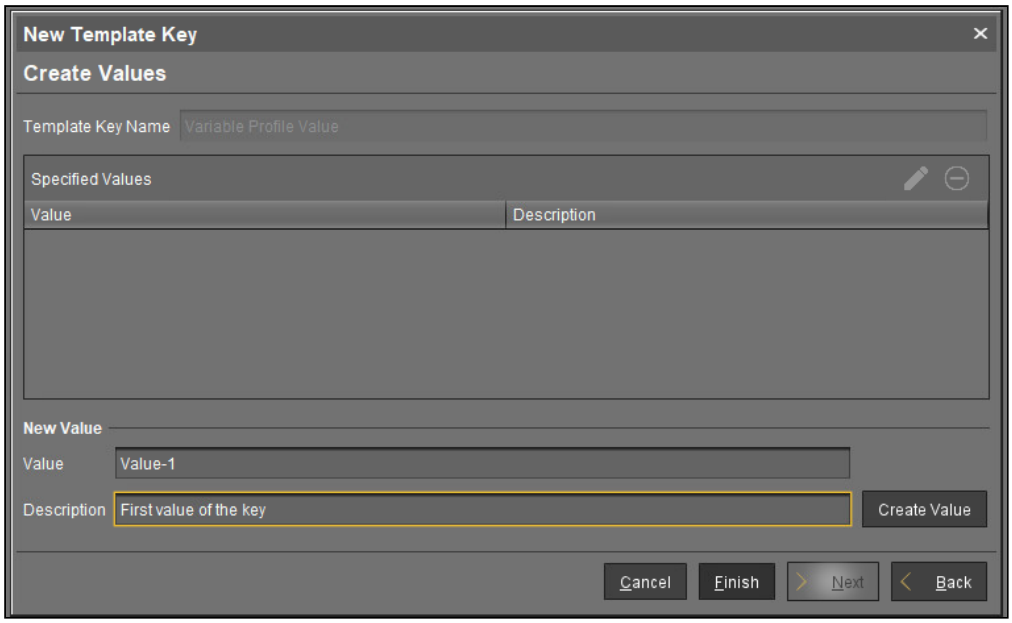
An assistant will guide you through the steps for creating a new template key:

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. Click **Next**.



To specify the first value of the key, proceed as follows:

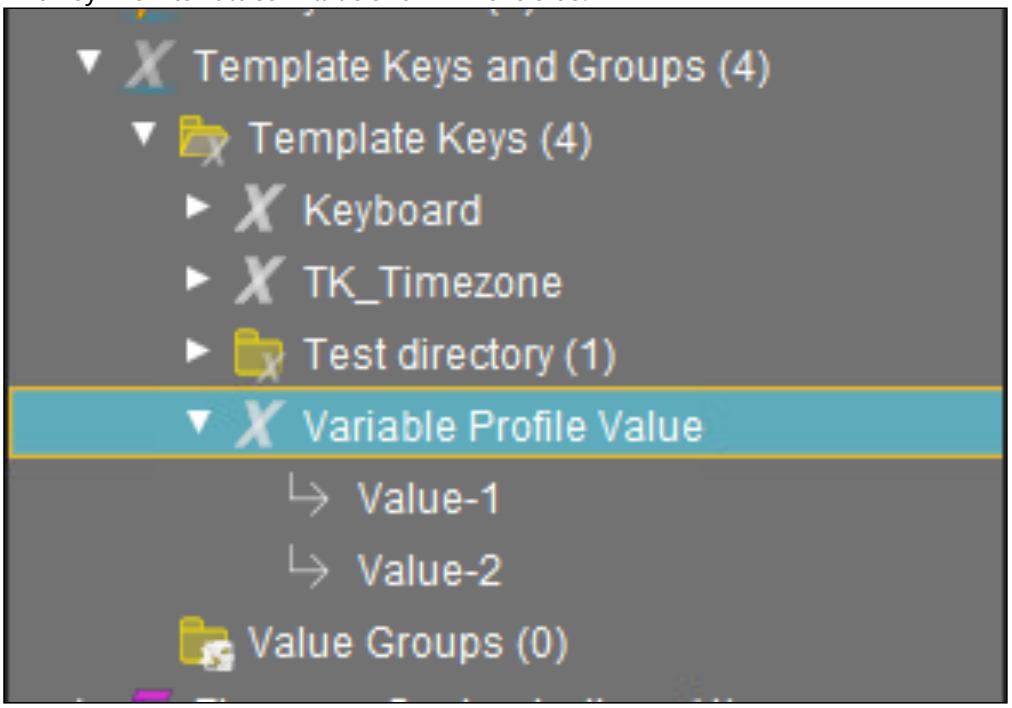
6. Enter the desired parameter value in the **Value** field.
7. Optionally, add a **description** of the value.
8. Click **Create Value**.



To specify further values for the key, proceed as follows:

9. Change the entries under **Value** and **Description**.
10. Click again on **Create Value**.

11. Click **Finish** to save the key with its values once you have created all desired values.
    The key with its values will be shown in the tree:



> The recommended workflow is to create template keys and values from the profile configuration (see page 754).

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:

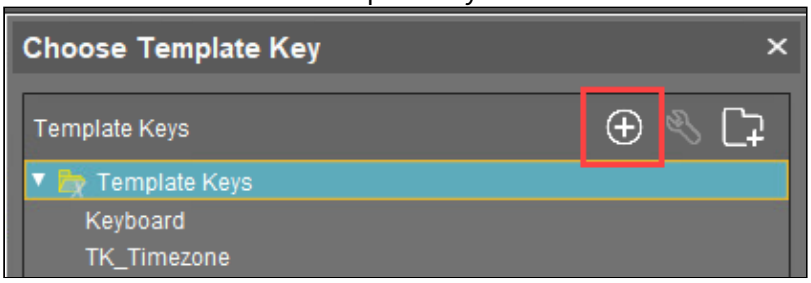
- How to Create Template Keys and Values (see page 751)
- How to Use Template Keys in Profiles (see page 756)

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 becomes 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.

> Certain parameters cannot be configured with template keys and only offer the option *inactive* or *active*. This applies for example to passwords or parameters which depend on other configuration settings.

5. Click on the **selection symbol** in order to select a template key.
6. Click **Add** to create a new template key.



An assistant will guide you through the steps for creating a new template key:

7. Give a **name** for the key.

> The **value type** for the key is stipulated by the parameter.

8. Optionally, give a **description** of the key.

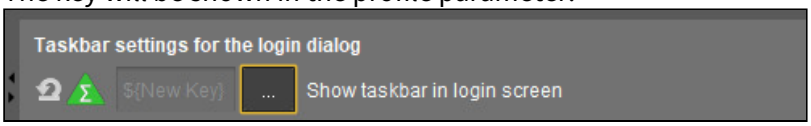
9. Click **Next**.

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 **Create Value**.

   > In the case of parameters with a fixed value range such as selection menu or checkbox, the available options will be provided for selection. Click on **Add all** to create values for each entry in the value range or **Create Value** to add selected entries only.

4. Click **Finish** to save the key with its values.
5. Click **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:  .

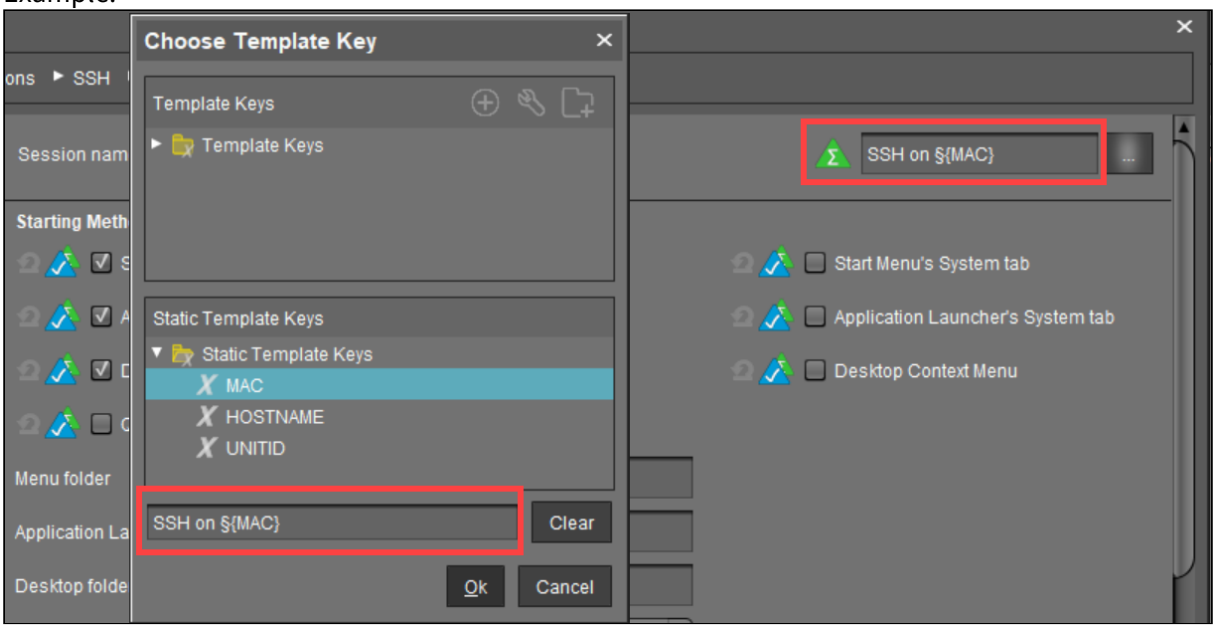
How to Use Template Keys in Profiles

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
- **SERIALNUMBER**: Serialnumber 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 – marked with the icon:  .

> The meaning of the icons can be found under **UMS Console > Help > Legend**.

> 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 754).
7. Click on **OK**.
8. **Save** the template profile.
9. You can also combine template keys:

Profiles which use at least one template key in the configuration are labeled with a special symbol in the structure tree:

How to Assign Template Profiles and Values to the Devices in the IGEL UMS

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:

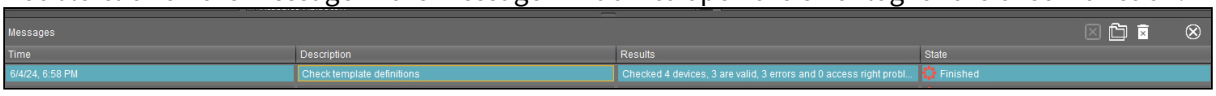
1. Select a **template profile** and assign it in the usual manner to a group of devices or a device directory. For details, see Assigned Objects in the IGEL UMS (see page 690) and Assign Objects to the Devices of Views or Device Searches in the IGEL UMS (see page 950).
2. Select a **value** for each **template key** used in the profile.
3. Assign the relevant values to the corresponding devices.

4. Assign further key values to further devices. Several values for various keys can also be assigned collectively ([Shift]and [Ctrl] keys).

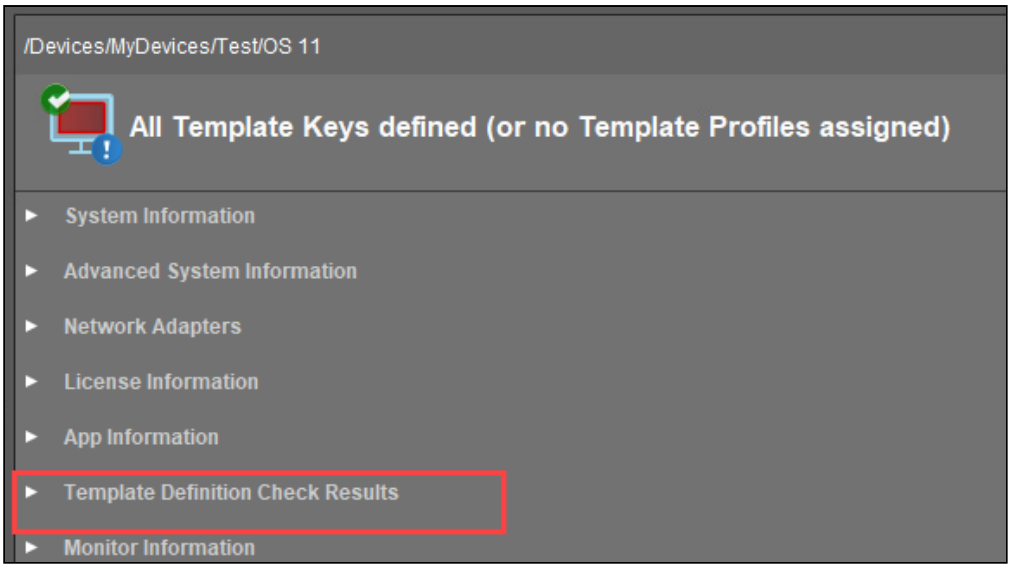
> Each device must then have an assigned value for each key in the assigned profiles.

To check that template profiles and values have been assigned correctly, proceed as follows:

1. Click on **Devices** in the top menu bar.
2. Select **Check the Template Definitions**.
   The selected and checked devices are flagged according to the result:
   -  - all template keys are defined
   -  - missing template keys
3. Double-click on the message in the message window to open the error log for the check function:



   Or click on a device and the results of the check will be shown under **Template Definition Check Results**.



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.

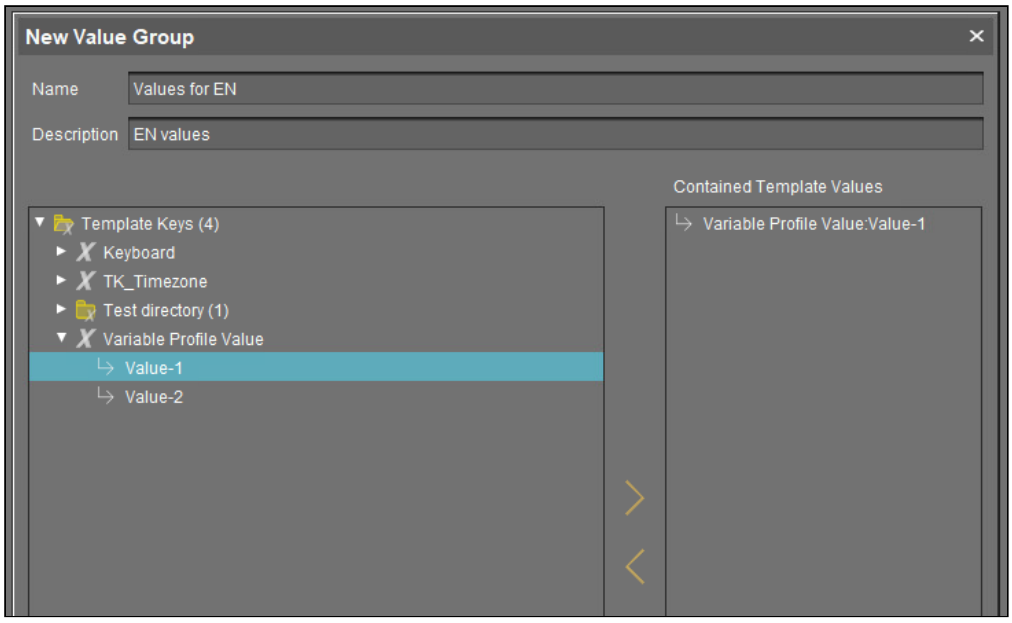
How to Create Value Groups from Template Keys

In value groups, logically associated values from various template keys can be brought together and assigned together to devices.

If for example you have various profiles which are to receive country-specific settings via template keys and value assignments, all values for a country / a language can be grouped in a value group. When such a group is assigned, a device also receives all values for its country / its language contained in it.

To create a group, proceed as follows:

1. Create a template profile with keys and values.
2. Click on **System>New>New Value Group** in order to create a new value group.
3. Enter a **Name** and **Description** for the group.
4. Select the desired values from each key, multiple selections are possible.



5. Confirm your settings by clicking on **OK**.
6. Create further groups.
7. Assign the template profile to all devices.
8. Assign the appropriate group in each case to the devices.
9. Highlight the **Devices** tree node.
10. Click on **Devices>Check the Template Definitions** in order to check the definitions.
    The result is shown in the message window.

After the next restart or a manual transfer, the devices will receive the new session data with shared and country-specific profile settings.

The advantage of this method is that you only need to add further key values to the relevant value group in the future in order to assign these to the site's devices. In addition, a better overview is possible if there are a large number of template keys and values.

How to Export Template Keys and Value Groups in the IGEL UMS

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 **Next** and select a save location.
5. Click **Done**.
   The template keys and value groups will be saved in a ZIP archive.

How to Import Template Keys and Value Groups in the IGEL UMS

You can import template keys and value groups. In order for this to be possible, the template keys which are to be imported must not yet exist in the UMS database. Each template key has a unique name which may only be used once in a UMS database.

To import template keys and value groups, proceed as follows:

1. In the navigation tree, highlight the directory in which the template keys and value groups are to be placed.

   > If you would like to import template keys and value groups in a single step, please note the following: If a directory below **Template Keys** is selected, the template keys will be placed in the selected directory and the value groups in the **Value Groups** directory. If a directory below **Value Groups** is selected, the value groups will be placed in the selected directory and the template keys in the **Template Keys** directory.

2. Go to **System** > **Import** > **Import Template Keys and roups**.
3. Select the file with the template keys and value groups and click on **Open**.
   The **Template keys and value groups** window will open.
4. In the **Import** column, select the template keys and value groups that are to be imported.
5. With the **Create path relative to the directory currently selected** option, specify whether the directory structure of the imported template keys and value groups is to be retained:
   ☑ The directory structure of the imported template keys and value groups will be retained, i.e. the exported subdirectories will be restored. (default)
   ☐ The directory structure of the imported template keys and value groups will be ignored, i.e. all template keys and value groups will be placed on the highest directory level.
6. Click on **OK**.
   Once all template keys and value groups have been imported, a confirmation will be shown.
   If not all template keys and value groups could be imported, the template keys and value groups for which the import failed will be shown.

Corporate Identity Customizations in the IGEL UMS

> The function was formerly known as Firmware Customizations. It was renamed with the introduction of the function to the UMS Web App with UMS 12.05.100. For more information, see How to Use Corporate Identity Customizations in IGEL UMS Web App (see page 1279) .

You can customize the user interface of your IGEL OS devices to suit your corporate design using the Corporate Identity Customization (CIC) 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.

> The management of CICs is synchronized between the UMS Web App and UMS Console. If you create a CIC either in the UMS Web App or in the UMS Console you can later edit it both in the UMS Web App and UMS Console, except for CICs with multiple use cases. Multi-use CICs are only editable in the UMS Web App.

Menu path: **UMS Console > Corporate Identity Customizations**

Mode of Action

A CIC can be assigned to a device (both OS 11 and OS 12) or a device directory.

CICs 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 728).

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 CIC assigned directly to the device has a higher priority than one which is assigned to the device directory. If both CICs have the same priority, the CIC with the higher ID will be effective.

> In order to obtain the ID of a CIC, move the mouse pointer over the relevant object in the structure tree.

- How to Create Corporate Identity Customization in the IGEL UMS Console (see page 765)
- How to Export Corporate Identity Customizations in the IGEL UMS Console (see page 774)
- How to Import Corporate Identity Customizations in the IGEL UMS (see page 775)

How to Create Corporate Identity Customization in the IGEL UMS Console

You can customize the user interface of your IGEL OS devices to suit your corporate design using the Corporate Identity Customization (CIC) function in the IGEL Universal Management Suite (UMS). For more information, see Corporate Identity Customizations in the IGEL UMS (see page 764).

To create a CIC, proceed as follows:

1. Right-click **Corporate Identity Customization** in the structure tree.
2. Select **Create New Corporate Identity Customization** in the context menu.
   The **Corporate Identity Customization Details** dialog window will appear.
3. Give a **Name** to this CIC.
4. Select a **Use case**. The following can be selected:

- Start Button (see page 766)
- Start Menu (see page 767)
- Taskbar Background (see page 768)
- Screensaver (see page 769)
- Screensaver (Custom Partition) (see page 770)
- Bootsplash (see page 772)
- Background Image (see page 773)

5. Click **Next**.
   The **Corporate Identity Customization Assignment** dialog appears with use case specific settings.
   The settings can be enabled or disabled:

	The parameter is inactive and will not be configured by the CIC.
	The parameter is active and the set value will be configured by the CIC.

Exception: The file path for screensaver (custom partition) cannot be disabled.

6. Highlight one or more directories or devices and click > in order to assign the CIC.
7. Click **Finish**.

The CICs created are listed in the structure tree under the **Corporate Identity Customization** node. If you click on a CIC, the associated files and assigned objects will be shown.

The files used in a CIC are marked with a  .

If you want to delete a file marked with  , you must first remove it from the associated CIC.

Start Button

Corporate Identity Customization Details

- **Name**: Name of the Corporate Identity Customization
- **Use case**: “Start button”
- **Image**: Name of the selected image file
    - **Choose file**: All files registered in the UMS in a suitable format (*.png, *ico) and for which your have authorizations are shown here.
    - **Upload file**: Select a file from a local directory or from the UMS Server.
    - **Clear**: Deletes the image file shown under **Image**.

Corporate Identity Customization Assignments

Assignment of the devices for which the customizations are to apply.

Start Menu

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Start menu”
- **Image**: Name of the selected image file
    - **Select file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
    - **Upload file**: Select a file from a local directory or from the UMS server.
    - **Delete**: Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Taskbar Background

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Taskbar background”
- **Image**: Name of the selected image file
    - **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
    - **Upload file**: Select a file from a local directory or from the UMS server.
    - **Clear**: Deletes the image file shown under **Image**.

Firmware Customization Assignment

Assignment of the device for which the customizations are to apply.

Screensaver

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Screensaver”
- **Image**: Name of the selected image files
  - **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
  - **Upload file**: Select a file from a local directory or from the UMS server.
  - **Clear**: Deletes the image file shown under **Image**.
- **Display mode**: Type of display.
  Possible options:
  - next to each other small
  - next to each other medium
  - centered in the middle
  - cut
- **Screen mode**:
  - One image per monitor
  - One image for all monitors (stretched if necessary)
- **Display time**: Time in seconds that an image is shown before it switches. (default: 10)
- **Start**
  Possible options:
  - Start screensaver automatically
  - Do not start screensaver automatically
- **Start time**: Time in minutes until the screensaver starts. (default: 5)
- **Background color**: (default: black)
  - **Choose color**: Color selection according to color spaces
    Possible color spaces:
    Swatches
    HSV
    HSL
    RGB
    CMYK

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Screensaver (Custom Partition)

Firmware Customization Details

- **Name**: Name of the firmware customization
- **Use case**: “Screensaver (custom partition)”
- **Images**: Names of the selected image files
  - **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here. You can select a number of images here.
  - **Upload file**: Select a file from a local directory or from the UMS server.
  - **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 your have authorizations are shown here.
  - **Upload file**: Select a file from a local directory or from the UMS server.
  - **Clear**: Deletes the image file shown under **Image**.

For the bootsplash, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

- **Horizontal position**: Horizontal position of the bootsplash. (default: 50%)
- **Vertical position**: Vertical position of the bootsplash. (default: 50%)
- **Progress horizontal position**: Horizontal position of the progress bar. (default: 90%)
- **Progress vertical position**: Vertical position of the progress bar. (default: 90%)

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

Background Image

Firmware Customization Details

- **Name**: “Background image”
- **Use case**: “Background image”
- **Background monitor 1-8**: Name of an image file for up to 8 monitors
  - **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
  - **Upload file**: Select a file from a local directory or from the UMS server.
  - **Clear**: Deletes the image file shown under **Background monitor 1-8**.

For the background image, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

Firmware Customization Assignment

Assignment of the devices for which the customizations are to apply.

How to Export Corporate Identity Customizations in the IGEL UMS Console

You can export Corporate Identity Customizations (CICs) into data containing all necessary settings and files.

⚠ Multi-use CICs cannot be exported.

To export CICs, proceed as follows:

1. If you would like to preselect CICs, highlight the desired CICs or directories in the navigation tree.
2. Go to **System** > **Export** > **Export Corporate Identity Customizations**.
   In the **Export Corporate Identity Customizations** window, the previously selected CICs or all available CICs will be shown.
3. In the **Export** column, select the CICs that you want to export.
4. Click on **Next** and select a save location.
5. Click on **Finish**.
   The exported data will be saved in a ZIP archive.

How to Import Corporate Identity Customizations in the IGEL UMS

You can import Corporate Identity Customizations (CICs). The imported data contain not only the settings but also all required files.

To import CICs, proceed as follows:

1. Highlight the directory where the CICs are to be placed.
2. Go to **System** > **Import** > **Import Corporate Identity Customizations**.
3. Select the file with the CICs and click **Open**.
   The **Import Corporate Identity Customizations** dialog will open.
4. In the **Import** column, select the CICs 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 CICs is to be retained:
   ☑ The directory structure of the imported CICs will be retained, i.e. the exported subdirectories will be restored. (default)
   ☐ The directory structure of the imported CICs will be ignored, i.e. all CICs will be placed on the highest directory level.
6. Click **OK**.
   Once all CICs have been imported, a confirmation will be shown.
   If not all CICs could be imported, the CICs for which the import failed will be shown.

Devices - Managing Devices in the IGEL UMS

In the **Devices** area of the IGEL Universal Management Suite (UMS) Console, you can manage endpoint devices registered on the UMS Server. All devices registered on the UMS Server are shown.

For details on device management in the IGEL UMS Web App (see page 1154), see Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App (see page 1176).

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.**

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 672).

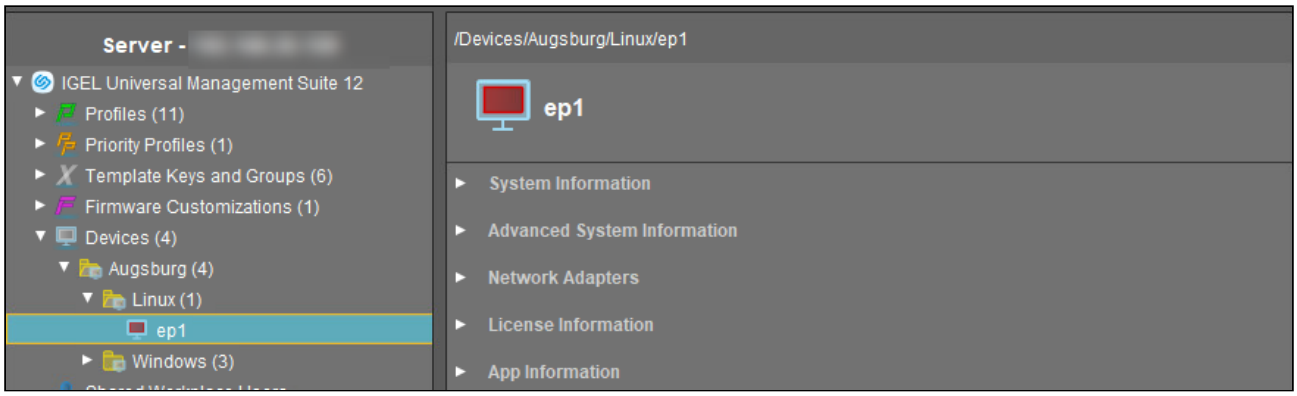
- View Device Information in the IGEL UMS (see page 778)
- Managing Devices (see page 786)
- Configuring Devices in the IGEL UMS (see page 795)
- Exporting and Importing Device Data in the IGEL UMS (see page 798)
- Sending Messages to Devices in the IGEL UMS (see page 804)
- Accessing Devices via Secure Terminal (Secure Shell) in the IGEL UMS (see page 806)
- Shadowing - Observe IGEL OS Desktop via VNC (see page 810)

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 (see page 1176) .

Menu path: **Devices > [Directories] > [Name of the device]**



For details on icons for an IGEL OS device, see Devices - Managing Devices in the IGEL UMS (see page 776) .

→ 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]**: Here you can find the attributes added under **UMS Administration > Global Configuration > Device Attributes** or through the **UMS Web App**. For details, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879) and How to Manage Custom Device Attributes in the IGEL UMS Web App (see page 1219) .

Advanced System Information

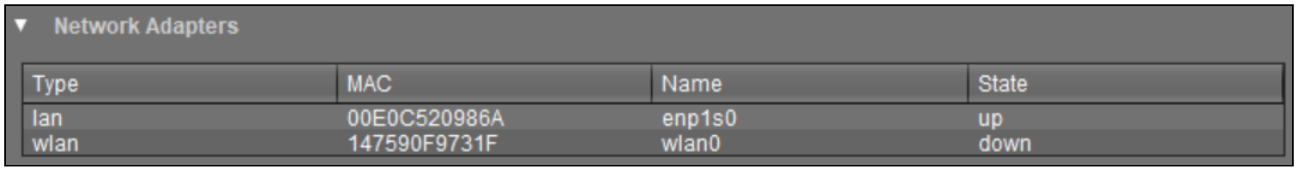
- **Unit ID**
- **MAC address**
- **Last IP**
- **Product**
- **Product ID**
- **Version**: Version of the operating system
- **Firmware description**
- **Connected to**: Shows for an IGEL OS 12 device to which device connector it is connected. If the device is connected through a reverse proxy, it is also shown here.
- **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 in the IGEL UMS (see page 543) .
- **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 *IGEL OS > IGEL OS Creator > UDC 3 How-Tos > Setting up UDC3 on Mobile Devices > 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 Devices (see page 422).

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:

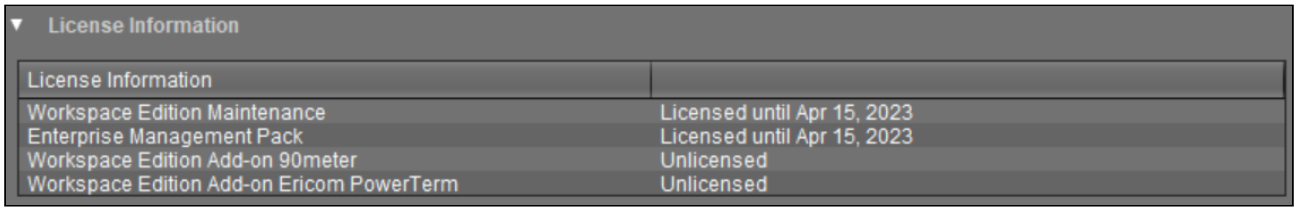
- **Type**: Type of the network adapter
- **MAC**: MAC address of the network adapter
- **Name**: Name of the corresponding network interface
- **State**: State of the network adapter as sent by the endpoint device, for example: **down**, **up** (the network adapter is connected to a network, not necessarily the same network as the UMS).



Read Out Network Adapter Data via API
You can read out network adapter information via a REST interface. For details, see *IGEL Management Interface V3 > IMI API V3 Reference > Resources > Device*.

License Information

In this area, the licenses available for the device are listed.

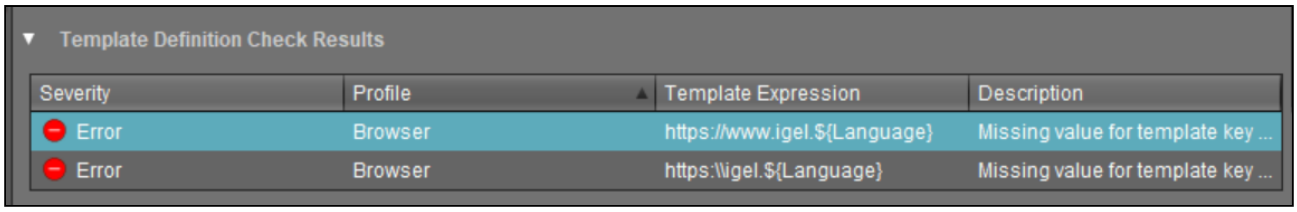


Template Definition Check Results

In this area, you see the results of the check if template profiles and values have been assigned correctly, see How to Assign Template Profiles and Values to the Devices in the IGEL UMS (see page 758) . For general information on template profiles, see Template Profiles in the IGEL UMS (see page 746) .

The following information is shown.

- **Severity**
- **Profile**
- **Template expression**
- **Description**



Monitor Information

- **Monitor 1**
  - **Vendor**
  - **Model**
  - **Serial Number**
  - **Size**
  - **Native Resolution**
  - **Date of Manufacture**
- **Monitor 2**
  - **Vendor**
  - **Model**
  - **Serial Number**
  - **Size**
  - **Native Resolution**
  - **Date of Manufacture**
- Further monitors, if applicable...

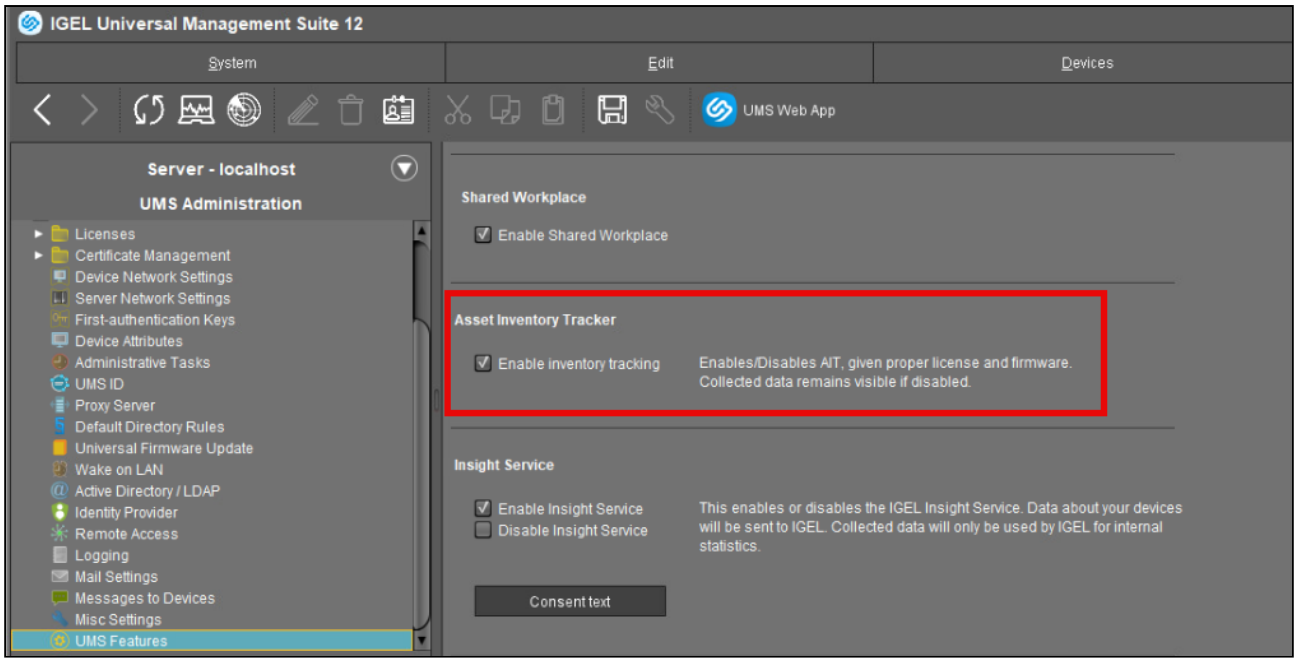
Asset Inventory

With the Asset Inventory Tracker (AIT) function, you find information about peripherals connected to an endpoint device. For IGEL OS 12 devices, the feature is avaible as of UMS 12.08.100 or higher and IGEL OS version 12.6.1 or higher.

License Required
To activate and use the AIT feature with IGEL OS 12 devices, a valid Enterprise UMS license or evaluation license is required. See IGEL Software Licenses for IGEL OS and IGEL UMS[141] and IGEL OS Editions[142].
For IGEL OS 11 devices, a valid license from the IGEL Enterprise Management Pack (EMP) is required.
When the license expires, the feature is no longer available, i.e. devices will no longer send updated asset information to the UMS. For information on license deployment, see IGEL Software Licenses How-Tos.

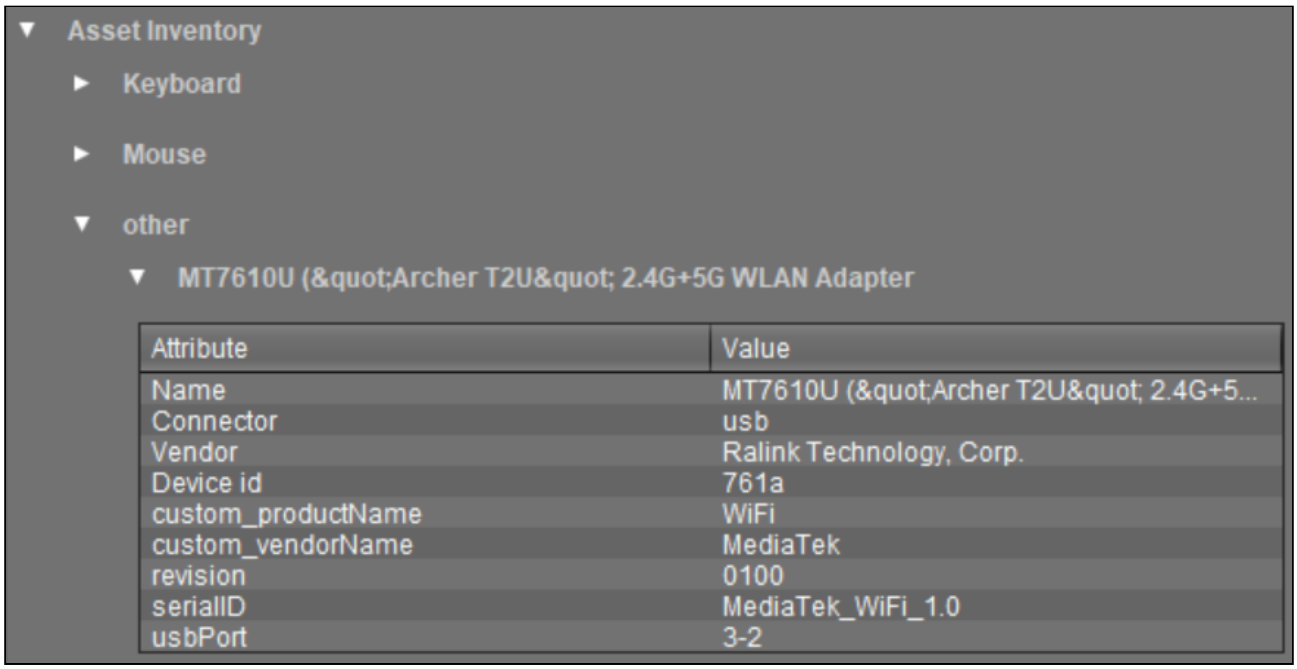
The Asset Inventory Tracker can be activated or deactivated under **UMS Console > UMS Administration > Global Configuration > UMS Features > Enable inventory tracking**.

141. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums
142. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions



The connected peripherals can be viewed both in the UMS Console and in the **UMS Web App > Devices > [name of the device] > Peripherals**, see Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App[143].

The peripherals are sorted according to categories, e.g. keyboard, mouse, Bluetooth, etc. A device can belong to more than one category and, accordingly, may be shown a number of times.

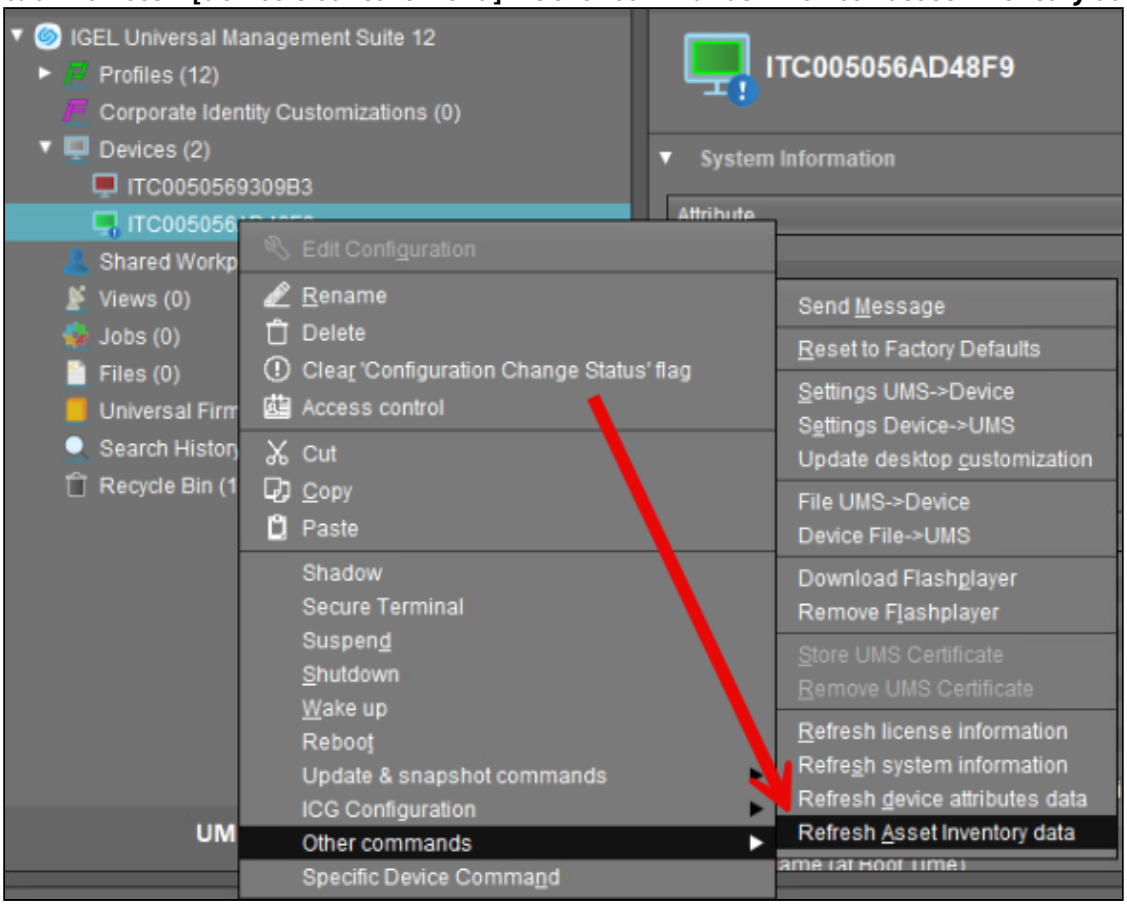


143. https://kb.igel.com/en/universal-management-suite/current/devices-view-and-manage-your-endpoint-devices-in-t

Asset information includes details on the vendor, product, connector, etc. and is saved every time a peripheral is connected to or removed from an endpoint that supports the feature.

→ To refresh the asset information:

- click **Refresh** button in the symbol bar
  or
- click **Devices > [device's context menu] > Other commands > Refresh asset inventory data**



Note that the asset information (but not asset history) is removed when

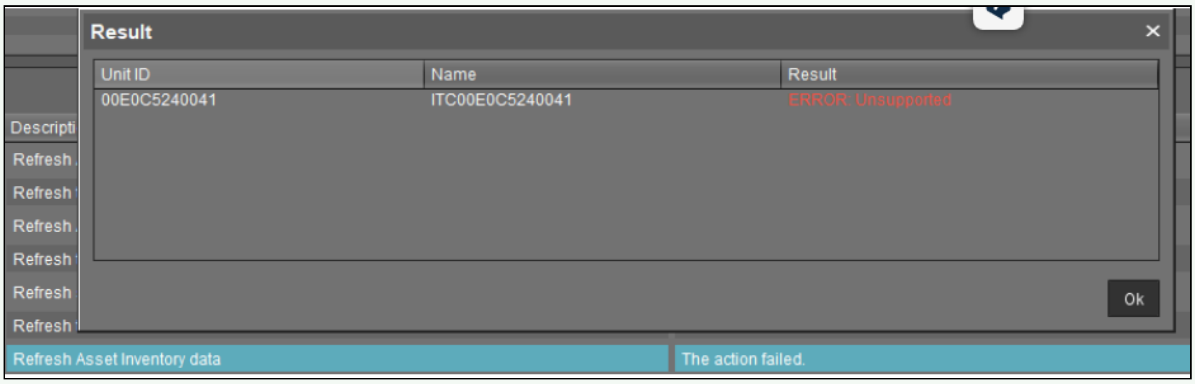
- a peripheral is disconnected from the endpoint
- an endpoint is reset to factory defaults
- an endpoint is deleted from the UMS

→ To delete the asset history (i.e. events that are sent when a peripheral is plugged in or unplugged), create an administrative task under **UMS Console > UMS Administration > Global Configuration > Administartive Tasks > Delete asset information history**; see Delete Asset Information History as an Administrative Task in IGEL UMS[144]. For general information on administrative tasks, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS[145].

144. https://kb.igel.com/en/universal-management-suite/current/delete-asset-information-history-as-an-administrat
145. https://kb.igel.com/en/universal-management-suite/current/administrative-tasks-configure-scheduled-actions-f

Read Out Asset Data via API
With a valid license (see page 781), you can read out asset information as well as the asset history via IGEL Management Interface (IMI). For details, see Asset Information[146].

If you are unable to retrieve the asset information and the license is valid, try to restart the endpoint device.



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**

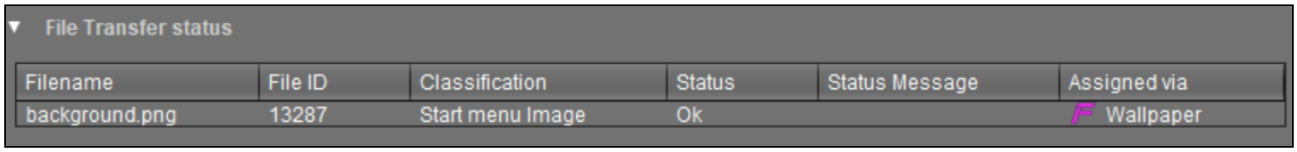
File Transfer Status

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:

146. https://kb.igel.com/en/igel-management-interface/current/asset-information

- **Filename**
- **File ID**
- **Classification**: The classification assigned when the file is uploaded, or the use case of the firmware customization or the description of the profile.
- **Status** - possible values:
  - **OK**
  - **Error**
  - **unknown**
- **Status Message**
- **Assigned via**: For directly assigned files, the file name is displayed here. Otherwise, the name of the profile or of the firmware customization will be displayed.



User Login History

Specific types of user login can be logged in the UMS.

The user logins are logged if the following options are enabled:

- device or profile: **System > Remote management > Options > Log login and logoff events** checkbox
- UMS: **UMS Administration > Misc Settings** (see page 996) **> 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.

- How to Create a Device Directory in the IGEL UMS (see page 787)
- How to Copy a Device Directory in the IGEL UMS (see page 789)
- How to Import a Device Directory in the IGEL UMS (see page 790)
- How to Delete a Directory in the IGEL UMS (see page 792)
- How to Move Devices in the IGEL UMS (see page 793)
- How to Assign Firmware Updates to Devices in the IGEL UMS (see page 794)

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 695) 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

How to Create a Device Directory in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can create as many directories and sub-directories as you want in order to group the devices together. When you create sub-directories, the devices organized in it form sub-groups of a group.

> A device that is unequivocally identified by its MAC address can only be stored in a single directory, i.e. only as a member of a single group.

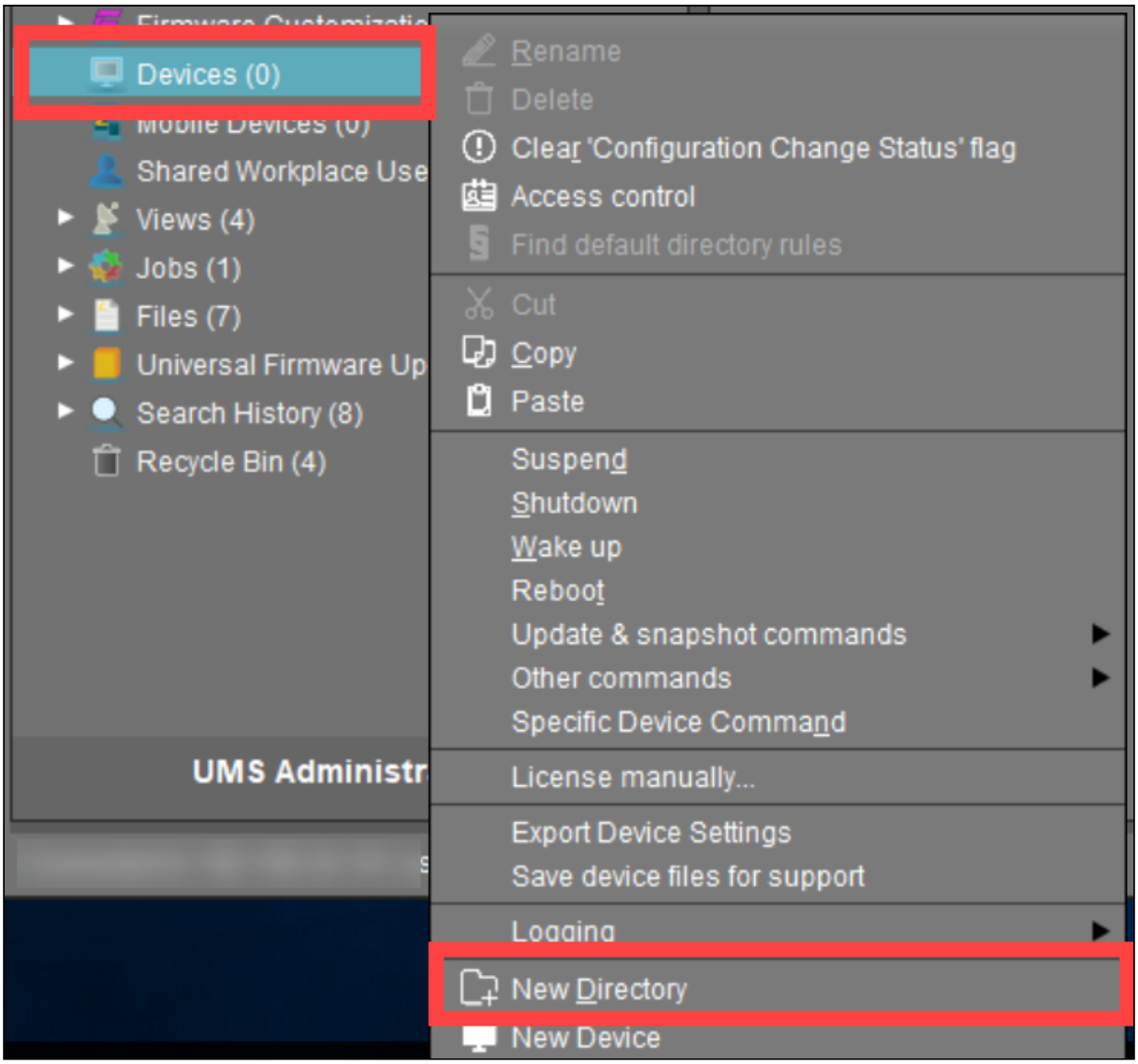
Alternatively, you can import a directory structure, see Importing a Directory (see page 790).

For details on how to create a directory in the IGEL UMS Web App (see page 1154), see Creating a Directory Structure in the IGEL UMS Web App (see page 1234).

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 969).

How to Copy a Device Directory in the IGEL UMS

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.

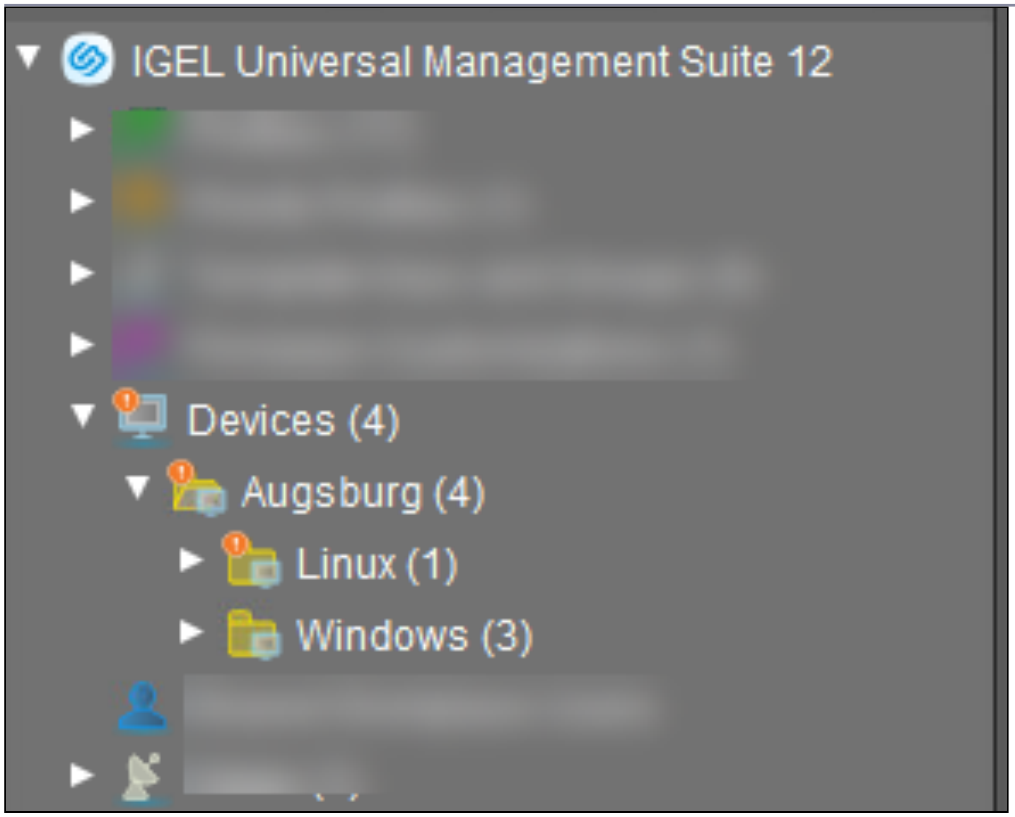
For details on how to copy a directory in the IGEL UMS Web App (see page 1154), see Copying a Device Directory in the IGEL UMS Web App (see page 1236).

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.

How to Import a Device Directory in the IGEL UMS

If you are planning a complex directory structure, you do not need to set it up in a step-by-step manner in the UMS Console. Instead, you can create a `.csv` file (e.g. with a spreadsheet program) in which you determine the directory structure and then import the structure from this list.

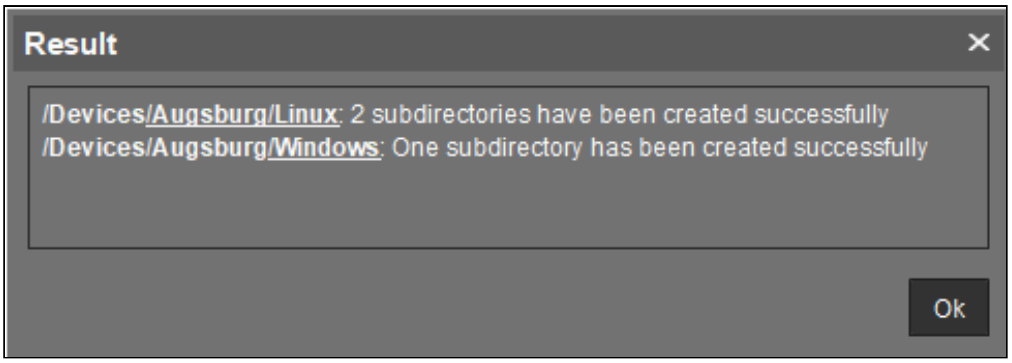


The tree structure shown above is based on the following file:

```
Devices; Augsburg; Linux
Devices; Augsburg; Windows
```

To import a directory structure from a `.csv` file, proceed as follows:

1. Select **System > Import > Import Directories** from the main menu.
   The **Import Directories** window will appear.
2. Click **Open File** in order to load a `csv` file.In the first column, you must specify one of the default master directories. In this way, you can also import directory structures for profiles, tasks, views or files.
3. Click **Import Directories** in order to create the directory structure.
   A window showing the result of the import will appear. Any newly created directories will be underlined.


Result
/Devices/Augsburg/Linux: 2 subdirectories have been created successfully
/Devices/Augsburg/Windows: One subdirectory has been created successfully
Ok

How to Delete a Directory in the IGEL UMS

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**.

How to Move Devices in the IGEL UMS

Drag-and-drop is the easiest way of moving devices from one directory to another. For details on how to move devices in the IGEL UMS Web App (see page 1154), see Moving Devices in the IGEL UMS Web App (see page 1235).

To move devices:

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**.

How to Assign Firmware Updates to Devices in the IGEL UMS

There are various options for assigning a registered firmware update to a device.

> Assigning a firmware update will not trigger the update process, only the information required for the update will be transferred to the device. After the assignment, you also need to launch the update process to update the devices.

Assign the Firmware Update

Direct assignment:

- using drag & drop
- using **Assigned Objects** in the device view

Indirect assignment:

- via a device directory

> If you are using a Windows-based device, refer to the chapters Snapshots and Partial Update in the Windows 10 IoT manual.

Launch the Update Process

To launch the update process manually:

1. Right-click on the device in the UMS structure tree.
2. From the context menu, select **Update & snapshot commands > Update** or **Update when shutting down**.

To launch the update process through a job:

1. Right-click on **Jobs** in the UMS structure tree.
2. Select **New Scheduled Job** from the context menu.
3. Enter a **Name**.
4. As **Command**, select **Update**, or **Update on Boot**, or **Update when shutting down**.
5. Complete the setup procedure for the job, see Job Configurations and Execution Results (see page 850).
6. Assign the job to devices or directories, see Assigning Objects to a Job (see page 855).

Configuring Devices in the IGEL UMS

You can configure a device via the UMS in the following ways:

- 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.
- Via a profile: You assign part-configurations to the device via a profile.
- 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`.

How to Copy a Session in the IGEL UMS

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 Device Data in the IGEL UMS

You can export and import data for devices. The settings and parameters are saved in an XML format.

How to Export Firmwares in the IGEL UMS

You can export the data for specific firmware versions from the IGEL Universal Management Suite (UMS). 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.

How to Import Firmwares in the IGEL UMS

You can import the configuration data for specific firmware versions to the IGEL Universal Management Suite (UMS). 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.

How to 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.

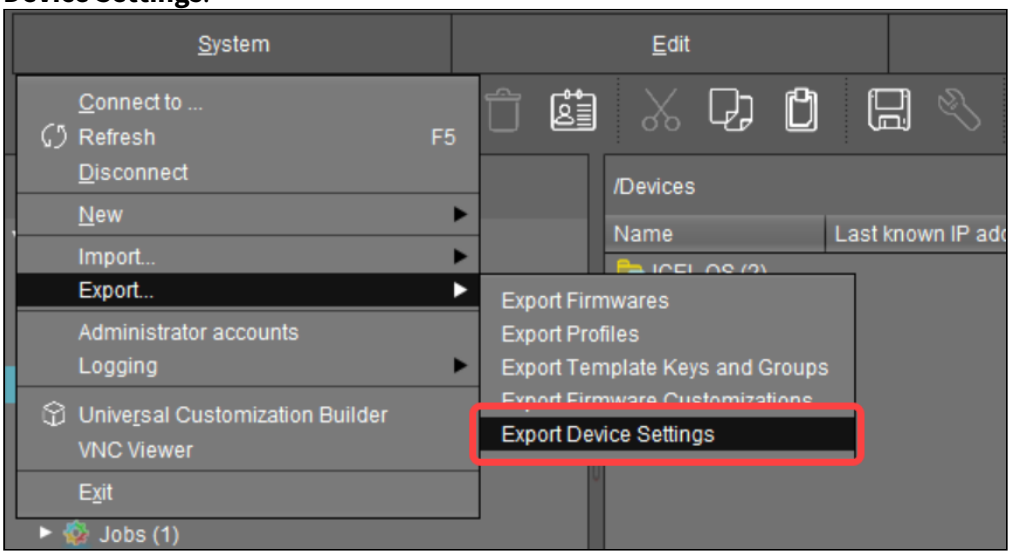
Exporting device settings can be necessary for support purposes (see *IGEL OS > IGEL OS Articles > Miscellaneous > Exporting the Local Configuration of the IGEL OS Device*) or if you want, for example, to import them later as a profile (see How to Import Devices as Profiles in the IGEL UMS (see page 803)) and, by using the compare profile settings (see page 726) 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 (see page 1226).

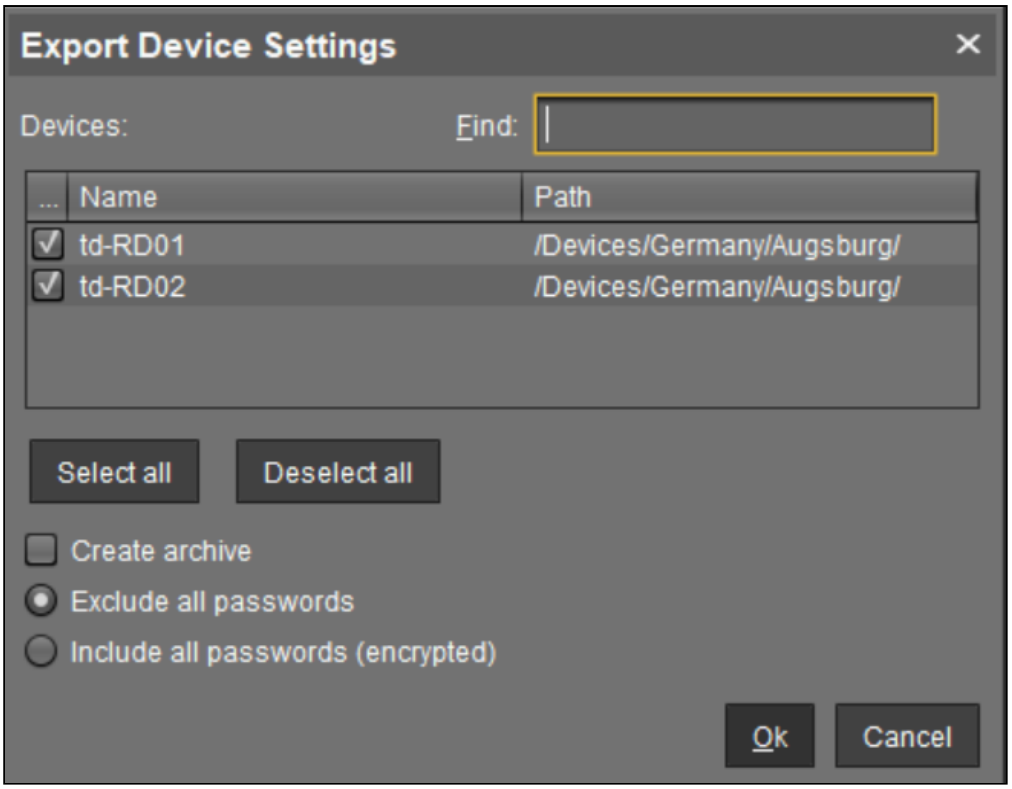
If you want to export / import purely profiles, see Exporting and Importing Profiles (see page 719).

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 How to Import Devices as Profiles in the IGEL UMS (see page 803)), 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**.

How to Import Devices as Profiles in the IGEL UMS

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 801).

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.

Sending Messages to Devices in the IGEL UMS

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 995).

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 (see page 1192).

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**.

> 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 995):

- {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.

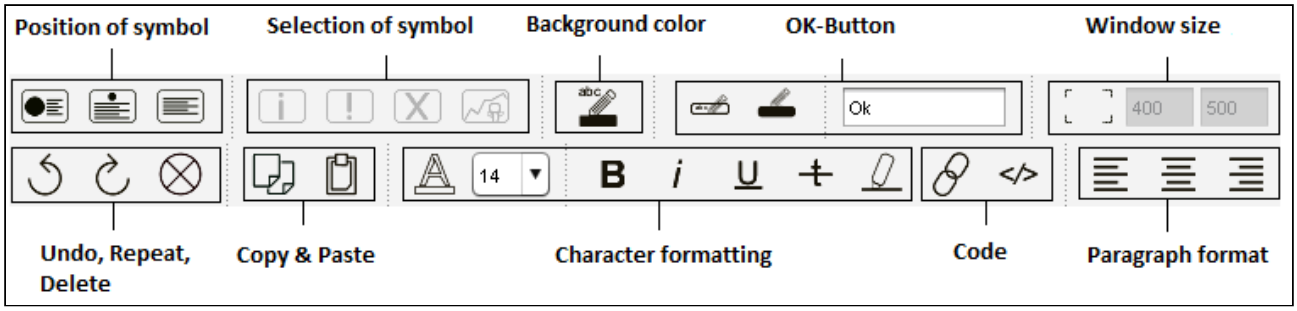
> In order to save templates, the user will need to write rights on the **Messages to Devices** (see page 995) node.

In order to format the text, you can either use the integrated toolbar or you can create HTML snippets using an expert tool and insert them using copy and paste.

> A message may have up to 7,000 characters including the formatting elements.

Message Editor

Menu path: **Structure tree > Devices > [Directories] > [Name of the device] > Other Commands > Send Message**



Accessing Devices via Secure Terminal (Secure Shell) in the IGEL UMS

You can establish a secure terminal connection to devices with IGEL Linux v5.11.100 or higher or IGEL OS 10.01.100 or higher.

You can allow access via the secure terminal for all registered devices. To do this, enable the **UMS Administration > Global Configuration > Remote Access > Enable secure terminal globally**.

To enable access for a single device:

1. In IGEL Setup, go to **System > Remote Access > Secure Terminal**.
2. Enable **Secure Terminal**.

Configuring the Secure Terminal in IGEL UMS

With the following settings, you can configure and manage access to devices via a secure terminal in the IGEL Universal Management Suite (UMS).

- **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[147].
  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.
- **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**.

147. http://www.chiark.greenend.org.uk/~sgtatham/putty/

☑ 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

How to Use the Secure Terminal in the IGEL UMS

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**.

For shadowing, **remote access** rights are required. See Object-Related Access Rights (see page 1016).

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 (see page 1224).

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

How to Launch a VNC Session in the IGEL UMS

> **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 *IGEL* VNC Viewer.

You can specify the following parameters as options:

Preferred Coding	The coding used when sending image data from the device to your PC. The coding option **Tight** is particularly useful in a network with a low bandwidth. It contains two additional parameters: • **Compression level**: The higher the compression, the longer the computing operation takes! • **JPEG quality**: If you select **Off**, no JPEG data will be sent.
Use Draw Rectangle Method	This option improves performance. However, artifacts may be encountered.
Color Depth	8 or 24 bits per pixel

Update Period	Time period between two updates. A longer time period reduces network traffic, but the update may not be seamless. Please note: An update query will be sent as soon as you move the mouse or enter a key in the VNC Viewer. This event will be passed on to the remote host.
Save Properties as Standard Values	Saves the current settings as standard values for future VNC sessions.

External VNC Viewer

> **Limitations for Special Characters**
>
> Some special characters might not be transmitted through the VNC connection. The processing of special characters depends on the following factors:
> - Keyboard layout configured on the VNC client and on the VNC server
> - VNC viewer in use: An external viewer and the internal viewer behave differently.
> - Firmware version of the endpoint device
> - 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 *IGEL OS > IGEL OS Articles > Security > Secure Shadowing (VNC with TLS/SSL).*

> **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[148] via plain VNC protocol.

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:

148. https://kb.igel.com/endpointmgmt-12.04.120/en/external-vnc-viewer-126851694.html

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 985).

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 in the IGEL UMS

IGEL Shared Workplace is an optional, licensed feature of the IGEL OS firmware. It allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters.

You will find the complete documentation here: Shared Workplace (see page 1427).

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 - Filtering for Devices in the IGEL UMS

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.

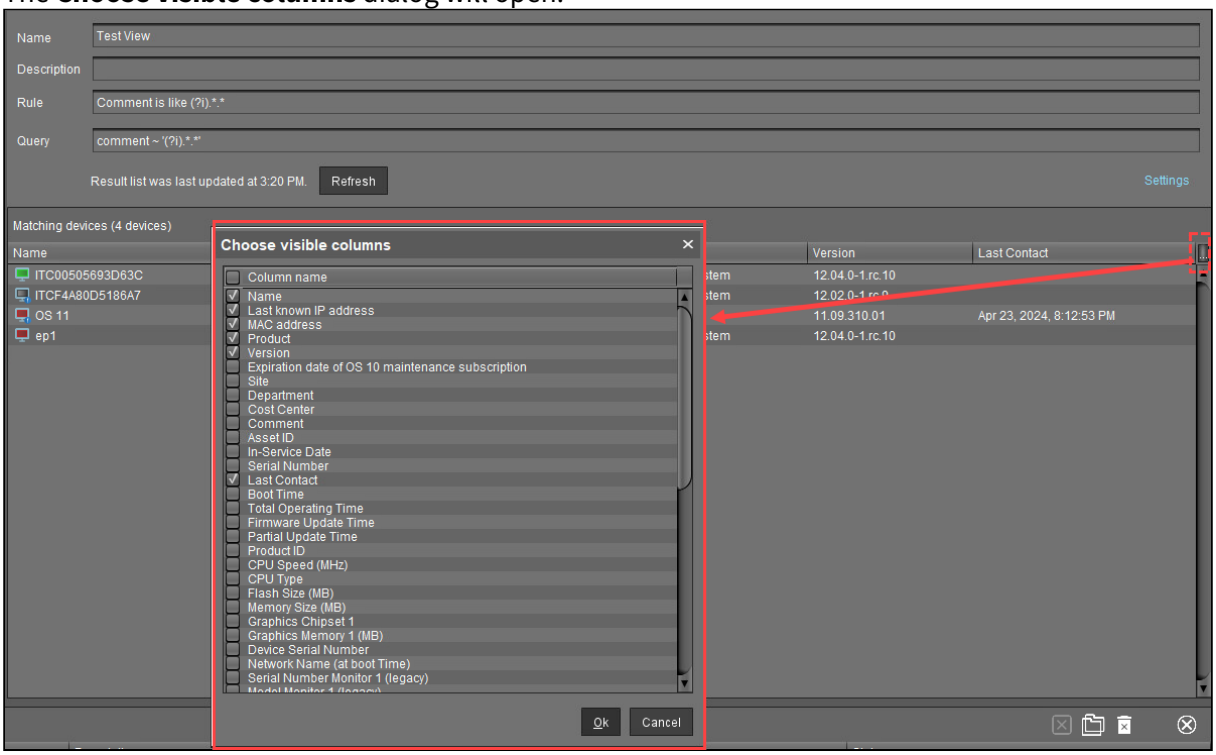
The **Search** feature of the UMS Web App is a successor to views in the UMS Console. It does not currently include all the criteria that are available for views but the range of the criteria will constantly be expanded. See Search for Devices in the IGEL UMS Web App[149]

You can use a view to define a scheduled job for a specific selection of devices, e.g. a firmware update. For more on jobs, see Jobs - Sending Automated Commands to Devices in the IGEL UMS (see page 847).

Configure the Displayed Information

In views, device information is displayed in a table format. 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.

149. https://kb.igel.com/en/universal-management-suite/current/search-for-devices-in-the-igel-ums-web-app

Related Articles

- How to Create a New View in the IGEL UMS (see page 820)
- How to Save the View Results List in the IGEL UMS (see page 841)
- How to Copy a View Directory in the IGEL UMS (see page 842)
- How to Copy a View in the IGEL UMS (see page 843)
- How to Send a View as Mail in the IGEL UMS (see page 844)
- How to Assign Objects to a View in the IGEL UMS (see page 846)

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 818). 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 678).

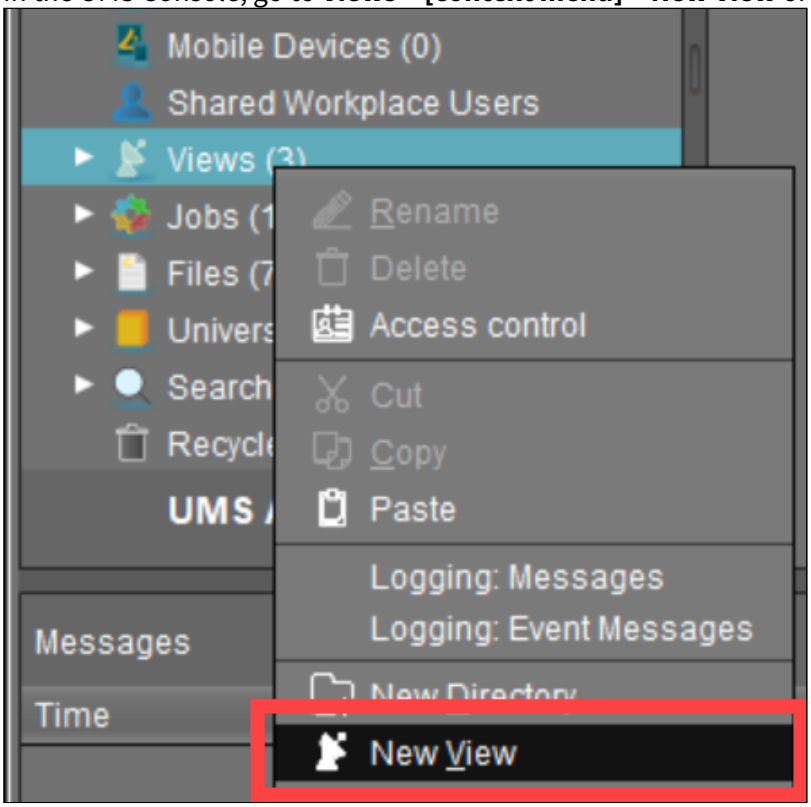
Menu path: **Views > [Context Menu] > New View**

> 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

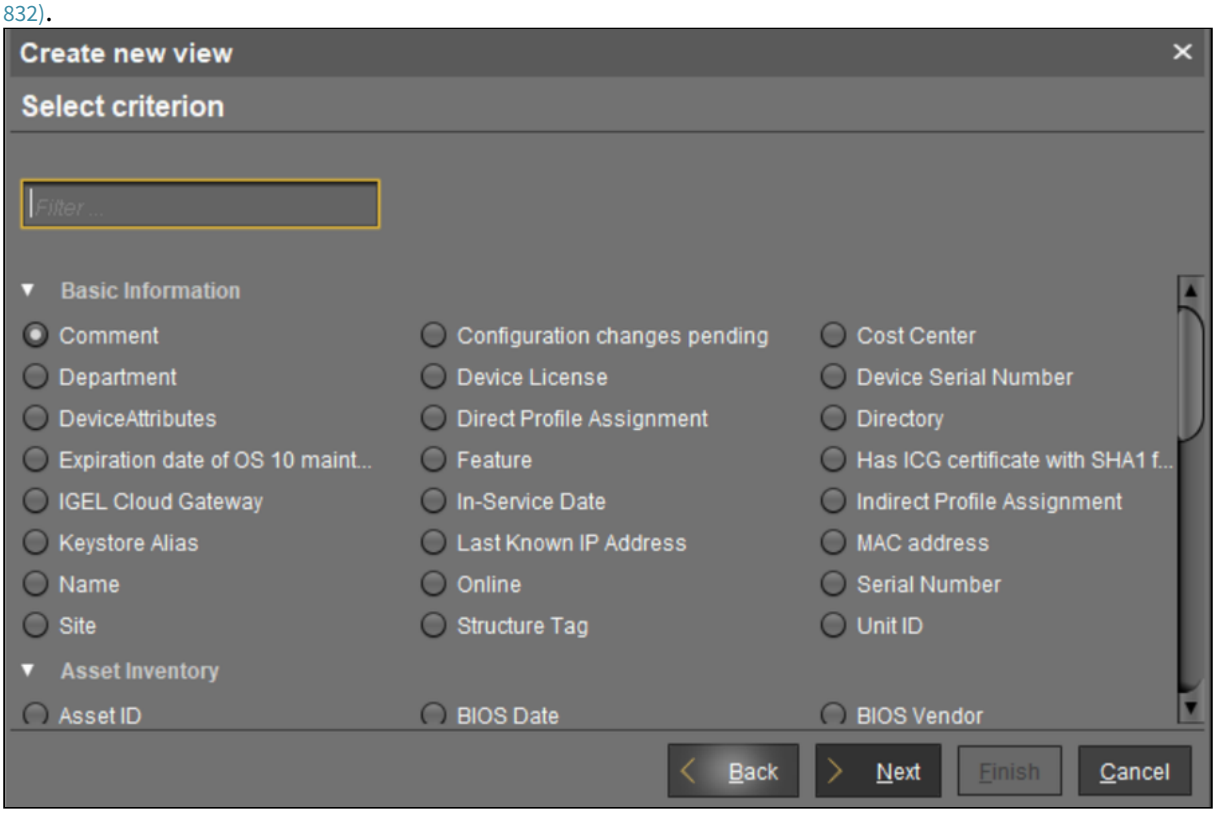
Typically, you create a view as follows:

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 832).



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 Pattern[150] in the Oracle documentation.

150. https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

☐ 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.

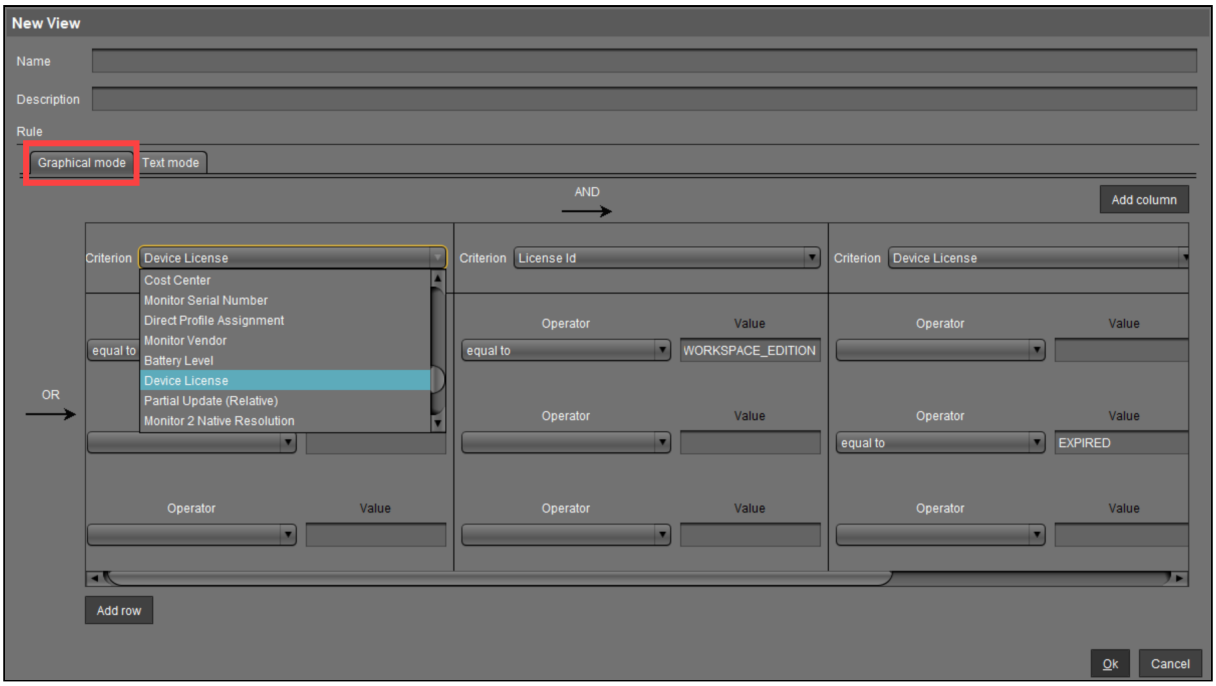
How to Create a View: Expert Mode

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.
2. Click **Expert mode**.
   The **New View** window will open.
3. Select **Graphical mode**.

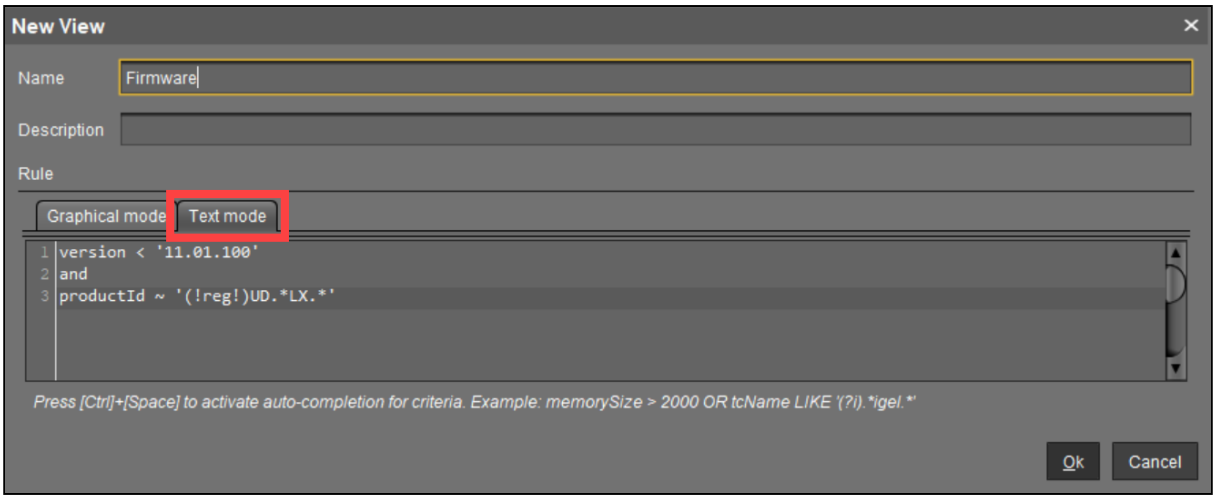


4. Give a **Name** and a **Description**.
5. Under **Criterion**, select a parameter.
   You will find a list of all available search parameters under Possible Search Parameters (see page 832).
6. Select an **Operator** and define the **Value**. The list of operators can vary depending on the selected 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 824) 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**.

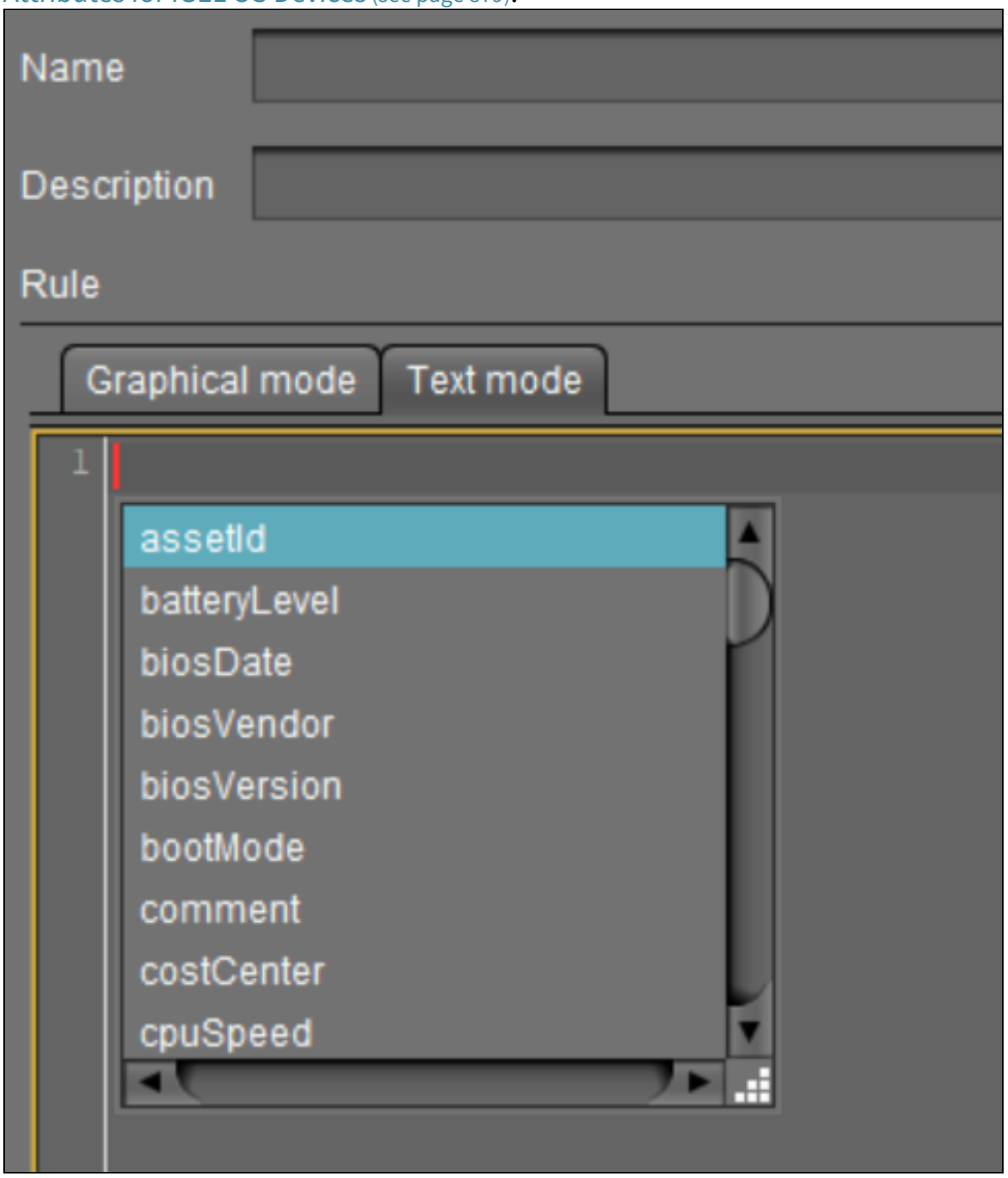
Queries in Text Mode of Views: Expression Parts

- 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'.

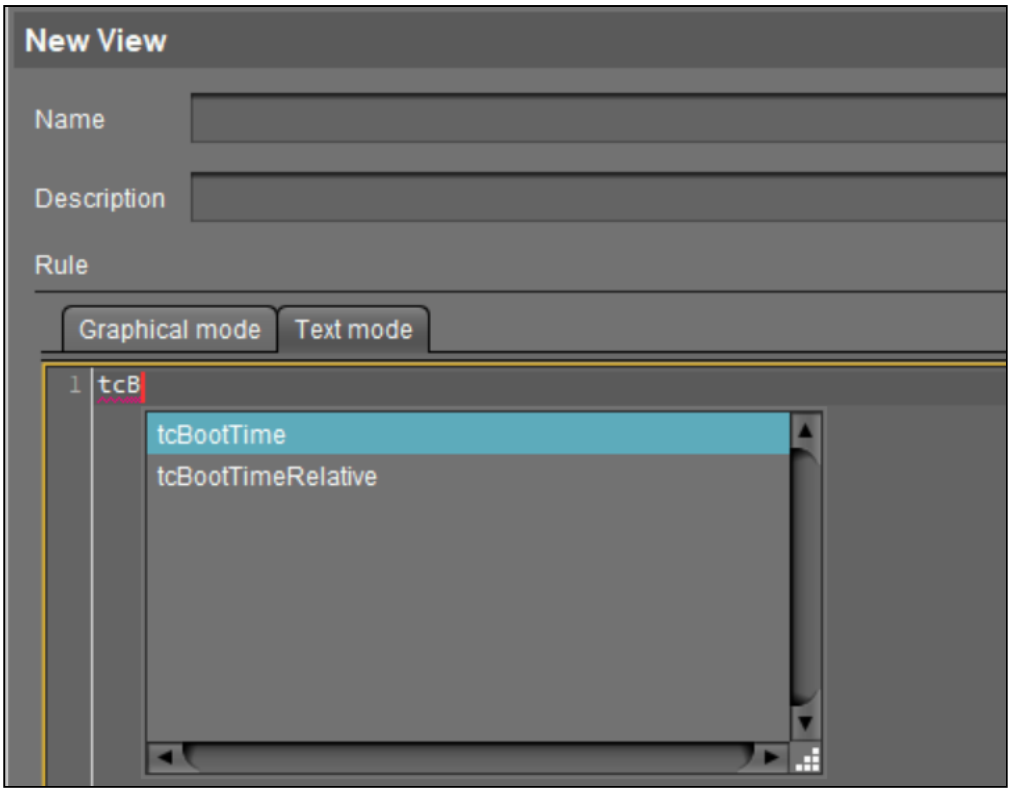
Criterion

- Possible criteria and their internal identifiers can be found under Text Mode of Views: Matrix of Possible Criteria and Operators.
- [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 879).

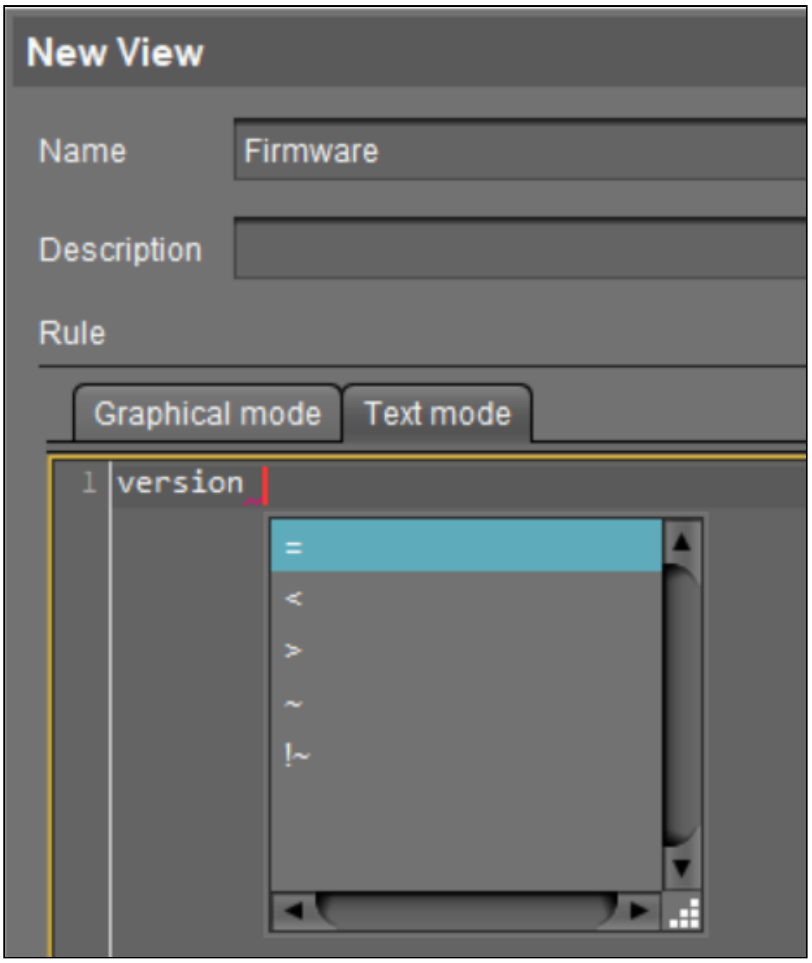


- Auto-completion also works when a criterion is entered only partially. It will then show only criteria matching the already entered fragment. If only one criterion matches the fragment, it will be completed without showing the popup window.

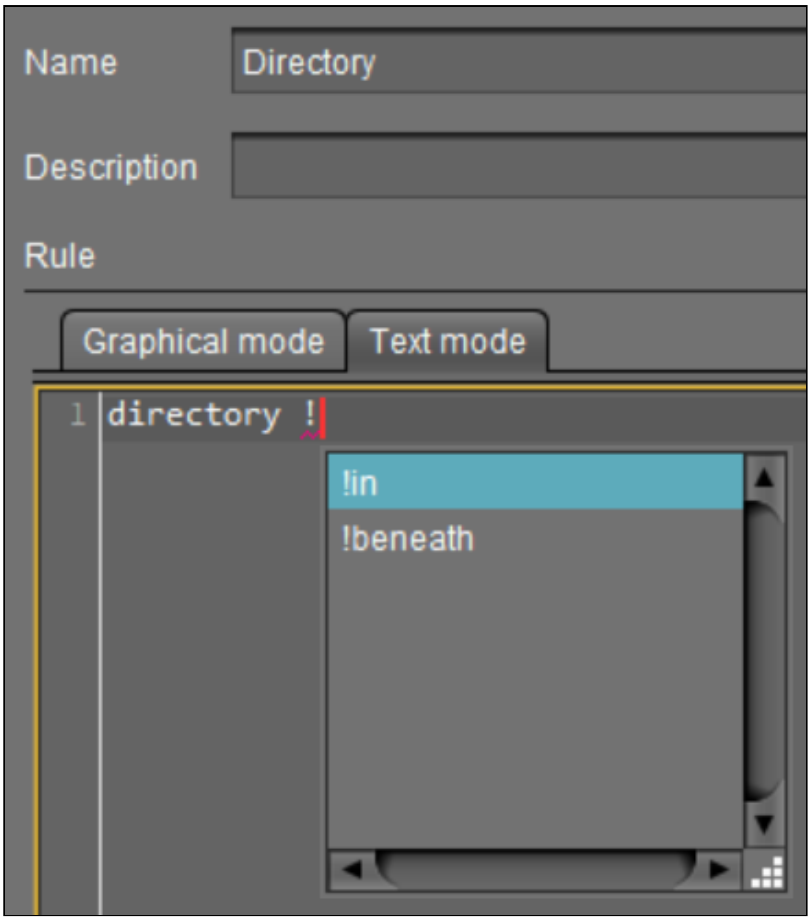


Operator

- For the list of operators possible for the criterion entered, see Text Mode of Views: Matrix of Possible Criteria and Operators.
- [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	

Operator	Pattern(s)			
not beneath	!beneath	!Beneath	!BENEATH	
is true	= true			
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 879):

```
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 Pattern[151] 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`

151. https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

```
tcName ~ '(!reg!)igel[0-9A-F]+'
```

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 820).

Basic Information

- **Comment**
- **Configuration changes pending**
- **Connected via Reverse Proxy**: for more information on a reverse proxy, see IGEL Universal Management Suite Network Configuration (see page 265) and Useful IGEL UMS Features for Managing Reverse Proxy Connected Devices (see page 348) .
- **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 778).
- **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 778).
- **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 778).
- **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 778).
- **[Name of the Device Attribute]**. For details on device attributes, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879).

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 in the IGEL UMS (see page 543))
- **Last contact time (relative)** (see Monitoring Device Health and Searching for Lost Devices in the IGEL UMS (see page 543))
- **Memory Size**
- **Network Name**
- **Network Speed**
- **OS Type**
- **Partial Update (Name)**
- **Partial Update (Relative)**
- **Partial Update (Version)**
- **Product**
- **Product ID**
- **Total Operating Time**

Onboarding User Information

Information provided by the Identity Provider used in the IGEL Onboarding Service configuration, see (en) Initial Configuration of the IGEL Onboarding Service (OBS) .

- **Onboarding User Mail Domain**
- **Onboarding User Name**

- **Onboarding User Role**

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 678) 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						
CPU Speed	cpuSpeed		x	x								
CPU Type	cpuType	x	x	x	x	x						
Comment	comment	x	x	x	x	x						
Configuration changes pending	tcConfigChange										x	x
Cost Center	costCenter	x	x	x	x	x						
Department	department	x	x	x	x	x						
Device License	licenseInfo	x										
Device Serial Number	deviceSerialNumber	x	x	x	x	x						
Device Type	deviceType	x	x	x	x	x						
Direct Profile Assignment	profile2TCAssignment	x				x						
Directory	directory						x	x	x	x		
Duplex Mode	duplexMode	x										
Expiration date of OS 10 maintenance subscription	subscriptionExpirationDate	x	x	x								
Feature	tcFeature	x				x						
Firmware Description	customFirmwarename	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
Firmware Update (Relative)	tcFwupdateTimeRelative		x	x								
Firmware Version	version	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						
Graphics Chipset 2	graphicsChipset2	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						
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	keystoreAlias	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						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
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						
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						

Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Monitor 2 Vendor	monitor2Vendor	x	x	x	x	x						
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						
Serial Number	serialNumber	x	x	x	x	x						
Site	site	x	x	x	x	x						
Structure Tag	umsStructuralTag	x	x	x	x	x						

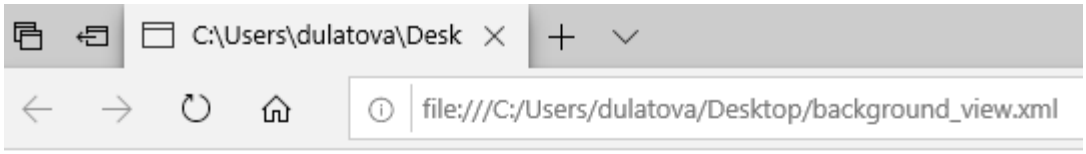
Criterion name	Internal identifier	equal to	less than	greater than	like	not like	in	not in	beneath	not beneath	is true	is false
Total Operating Time	totalUsagetime		x	x								
Unit ID	unitId	x	x	x	x	x						
[Name of the Device Attribute]	Identifier specified under **UMS Administration > Global Configuration >** Device Attributes > UMS internal identifier (see page 879)	x	x	x	x	x						

How to Save the View Results List in the IGEL UMS

The results of a view can be saved in four file formats: XML, HTML, XSL-FO, and CSV.

→ Select **Save as...** in the context menu of a view in order to save the current view results.

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 678).

How to Copy a View Directory in the IGEL UMS

You can copy a view directory and paste it in any directory.

To copy a view directory, proceed as follows:

1. Menu path: **Structure Tree > Views**.
2. Click on the view directory that you want to copy.
3. Open the context menu for the directory and select **Copy**.
4. 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.
5. 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.

How to Copy a View in the IGEL UMS

You can copy a view and paste it in any view directory in the IGEL Universal Management Suite (UMS).

To copy a view, proceed as follows:

1. Go to **Structure Tree > Views**.
2. Click on the view that you want to copy.
3. Open the context menu for the view and select **Copy**.
4. 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.
5. 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.

How to Send a View as Mail in the IGEL UMS

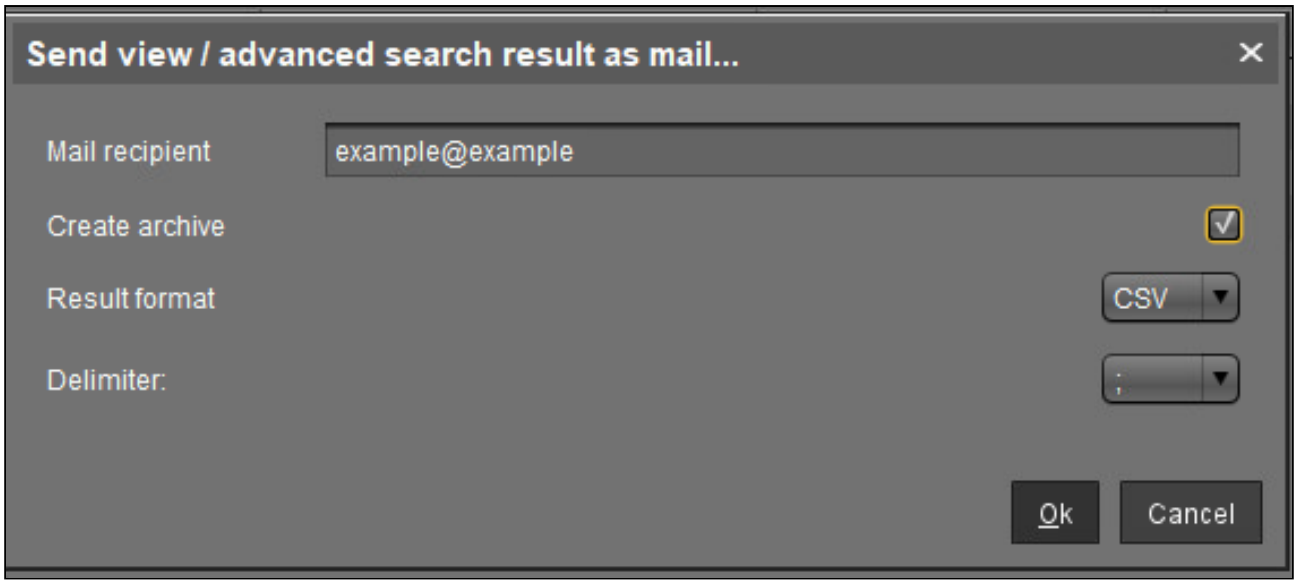
You can send the results of a view created in the IGEL Universal Management Suite (UMS) by email in several formats and to multiple recipients at a time.

Emails can only be sent if you have configured appropriate mail settings (see page 993) under **UMS Administration > Global Configuration > Mail Settings**.

You can also send views automatically and regularly as an administrative task (see page 944).

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. Check the **Create archive** box to send the view as a zip file.
5. Under **Result format**, select the format in which the view is to be sent.
6. If the CSV format is selected, under **Delimeter** you can select the type of delimeter to be used in the file.


Send view / advanced search result as mail...
Mail recipient
example@example
Create archive
Result format
CSV
Delimiter:
;
Ok
Cancel

How to Assign Objects to a View in the IGEL UMS

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 950).

Using the same principle, you can assign objects to devices that you have filtered via a search (see page 861).

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 678).

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 1016).
- **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 in the IGEL UMS (see page 1024).
- **Execute Job**: Executes the job immediately.

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 in the IGEL UMS

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 850) and Commands for Jobs (see page 849).
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 850).
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 855).
   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 (see page 1164).
5. Click **Finish** to save the Job.

Commands for Jobs in the IGEL UMS

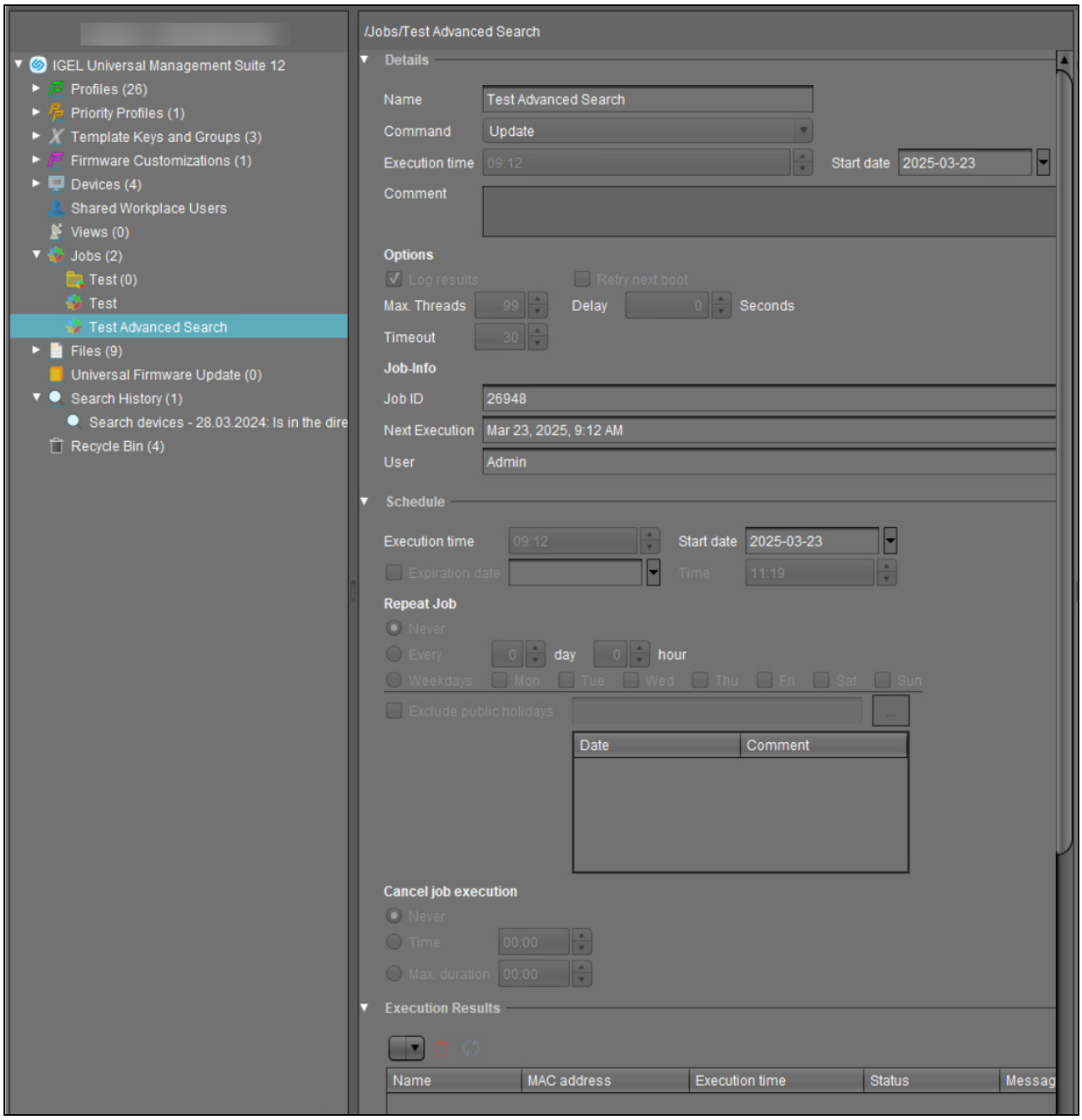
Here you find information on the commands that you can define for a job in the IGEL Universal Management Suite (UMS).

- **Update**
  - IGEL OS 12: Triggers the activation of the assigned app version for IGEL OS 12 devices. For details when the **Update** command is required, see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334).
  - IGEL OS 11 or earlier: Executes the firmware update with the existing settings, see also Universal Firmware Update (see page 979).
- **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 Sending Messages to Devices in the IGEL UMS (see page 804).
- **Partial Update**: Executes the partial update with the existing settings (WES).
- **Update desktop customization**: Updates the desktop background and the boot logo.
- **BIOS - Get settings**: Gets the current BIOS settings from the device. See *IGEL OS > IGEL OS Articles > BIOS Tools > BIOS Tools for Selected HP Devices*.
- **BIOS - Set password**: Sets a password for the BIOS. See *IGEL OS > IGEL OS Articles > BIOS Tools > BIOS Tools for Selected HP Devices*.
- **BIOS - Set settings**: Deploys the changed BIOS settings to the device. See *IGEL OS > IGEL OS Articles > BIOS Tools > BIOS Tools for Selected HP Devices*.
- **BIOS - Trigger update**: Triggers a BIOS update. See *IGEL OS > IGEL OS Articles > BIOS Tools*.
- **Deploy Jabra Xpress package**: Installs a Jabra Xpress (IGEL OS). See *IGEL OS > IGEL OS Reference Manual > Devices > Unified Communications > Jabra > Jabra Xpress.*
- **OS 11 Upgrade**: Upgrades devices from IGEL OS 10 to IGEL OS 11. For details, see *IGEL OS > IGEL OS Articles > Update and Upgrade > Upgrading from IGEL OS 10 to IGEL OS 11 > Upgrading UDC3 Devices from IGEL OS 10 to IGEL OS 11 > Mass Deployment Using a Scheduled Job.*
- **Start Login Enterprise launcher**: Starts Login Enterprise Launcher if it has been configured, see *IGEL OS > IGEL OS Articles > Login Enterprise Configuration > Login Enterprise Launcher in IGEL OS.*
- **Update the firmware of an attached HP G5 Dock**
- **Upgrade to IGEL OS12**

Job Configurations and Execution Results in the IGEL UMS

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]



Details

Name
Name of the job.

Command
Command which is executed for all assigned devices. For more information, see Commands for Jobs (see page 849).

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

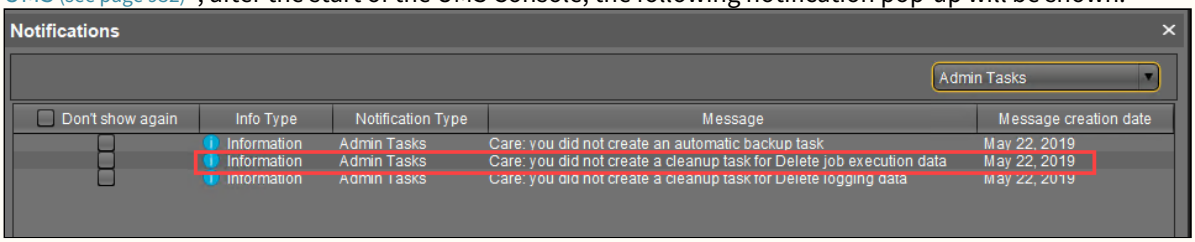
Job ID
Internal job number which cannot be changed. This field is empty if a job is new.

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 as an Administrative Task in the IGEL UMS (see page 932)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Schedule

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).

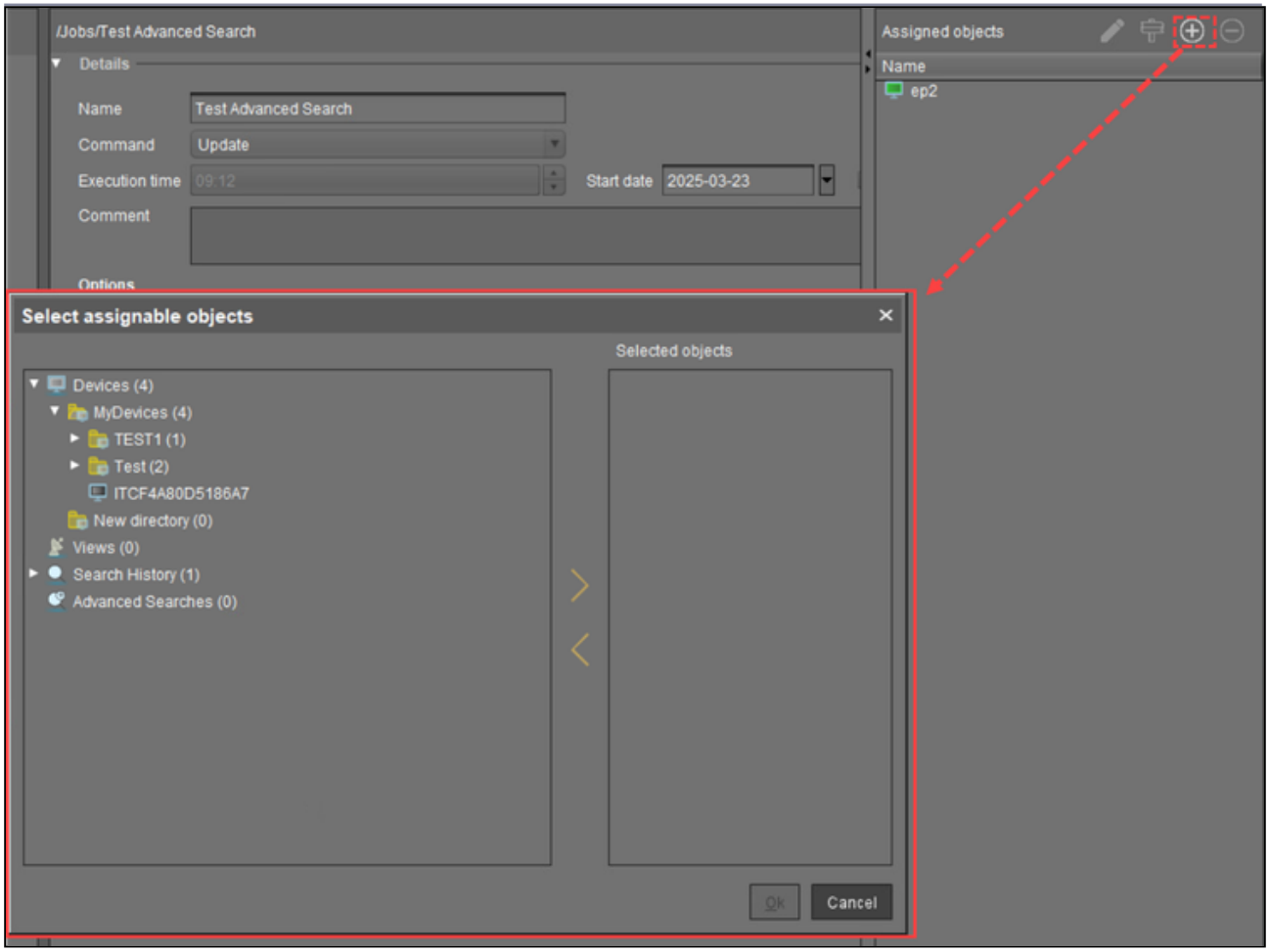
The job execution status is also displayed for the devices:

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 in the IGEL UMS

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.

Universal Firmware Update in the IGEL UMS

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 857)
- **Snapshot -> Universal Firmware Update**
- **Firmware archive (zip file) -> Universal Firmware Update**
- **Access control**. See Access Rights (see page 1010).

When you select **Snapshot -> Universal Firmware Update** or **Firmware Archive (zip file) -> Universal Firmware Update**, you can choose one of the following options:

- **How to Import Firmwares to the IGEL UMS** (see page 800): 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 859): Registers a Windows Embedded Standard snapshot as a Universal Firmware Update.
- **Firmware archive (zip file) -> Universal Firmware Update** (see page 860): 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 How to Assign Firmware Updates to Devices in the IGEL UMS (see page 794).

ℹ 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 2 (see page 979).
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? (see page 514).

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=XflN_BEyDZc

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.

Menu path: **Server - [UMS Server address] > Universal Firmware Update >** [context menu] **> Check for new firmware updates**

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.

> 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.

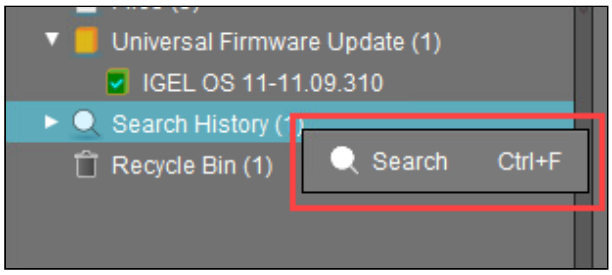
Display name: Names for displaying the updates in the UMS.

WebDAV target directory: Directory in which the update is saved in order to distribute it to the devices.

Search History in the IGEL UMS

All search queries are saved here as individual objects and can be edited further via the context menu.

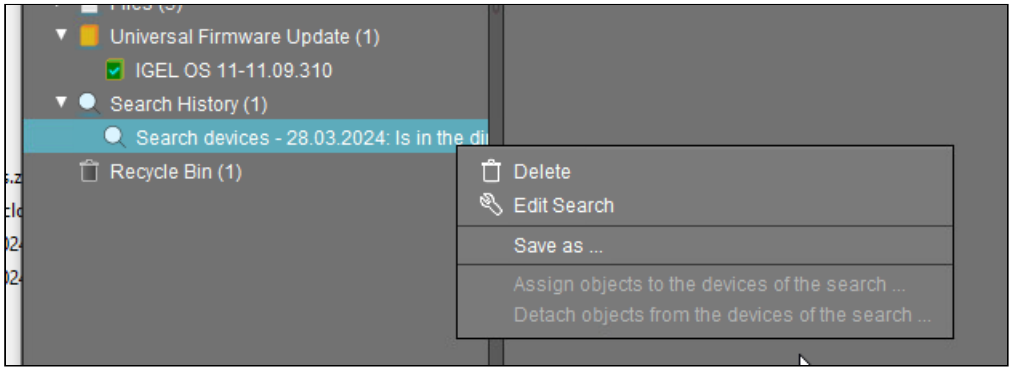
Menu path: **Structure Tree > Search History**



→ Click **Search** in the context menu to start a new search. You can search for:

- Devices
- Profiles
- Views

Context Menu of a Search Query



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 820). 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 How to Assign Objects to a View in the IGEL UMS (see page 846) .
- **Detach objects from the devices from the search...**: Removes the assigned objects.

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 822). 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 How to Assign Objects to a View in the IGEL UMS (see page 846).
- **Detach objects from the devices from the search...**: Removes the assigned objects.

Recycle Bin - Deleting Objects in the IGEL UMS

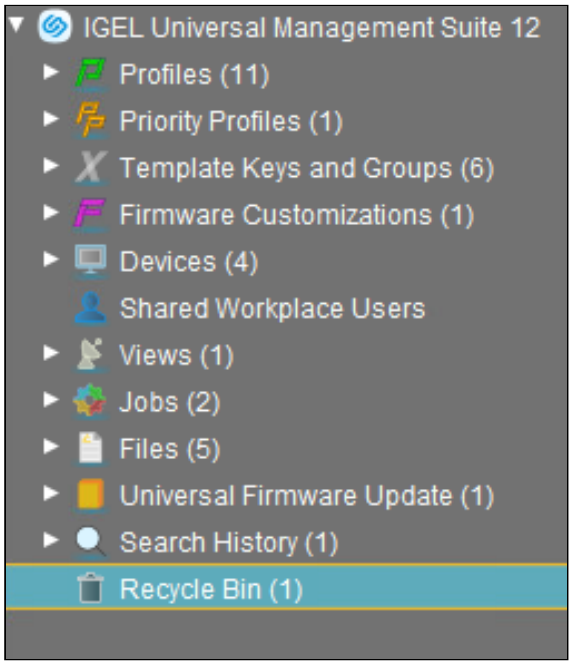
In the IGEL Universal Management Suite (UMS), items are sent to the recycle bin when deleted by default.

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 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 (see page 533).

The recycle bin is also available in the UMS Web App, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356) .

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.

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.

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.

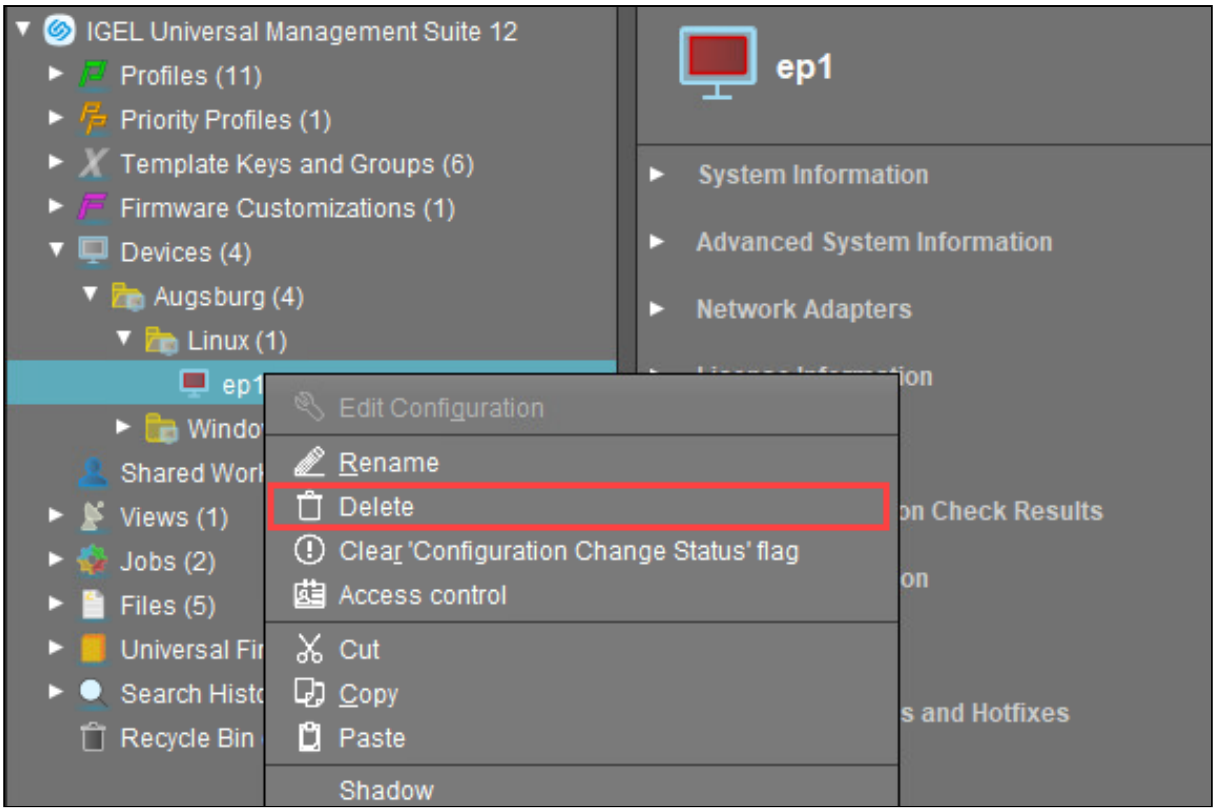
Virtually all elements from the UMS structure tree can be moved to the recycle bin: Devices, profiles, views, jobs, files and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) can only be deleted permanently. Search history elements can 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

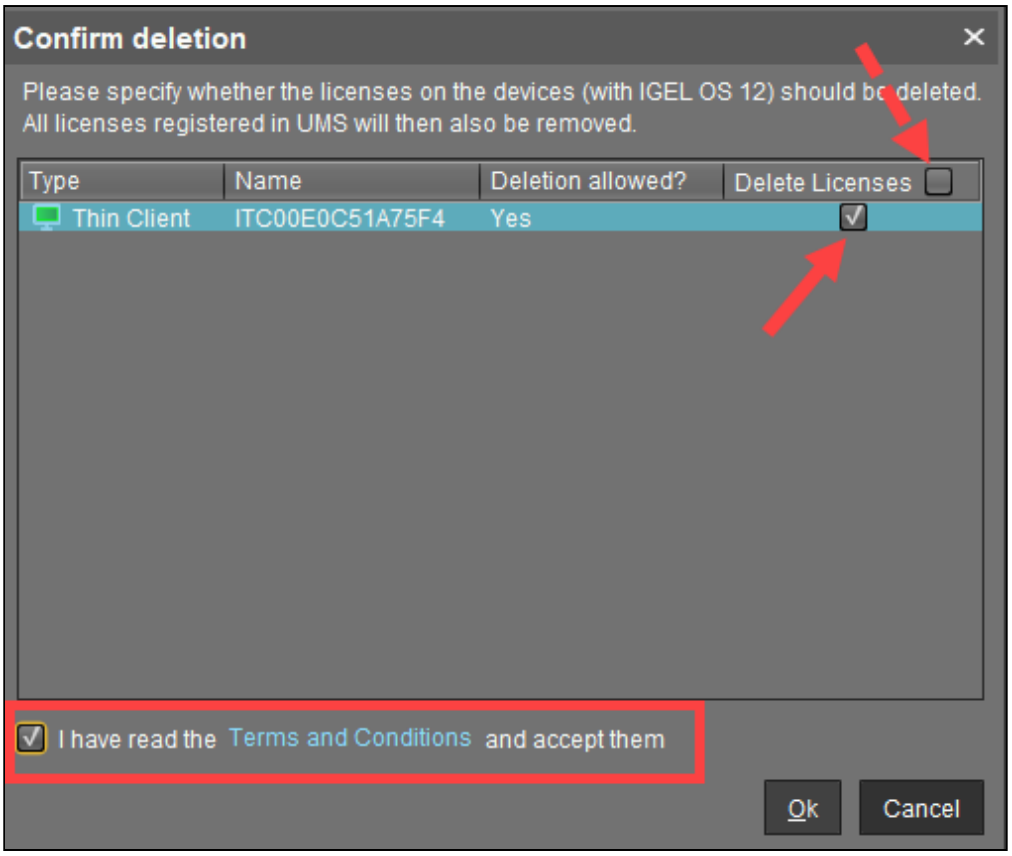
To delete devices in the UMS:

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 - Managing the Network in the IGEL UMS

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

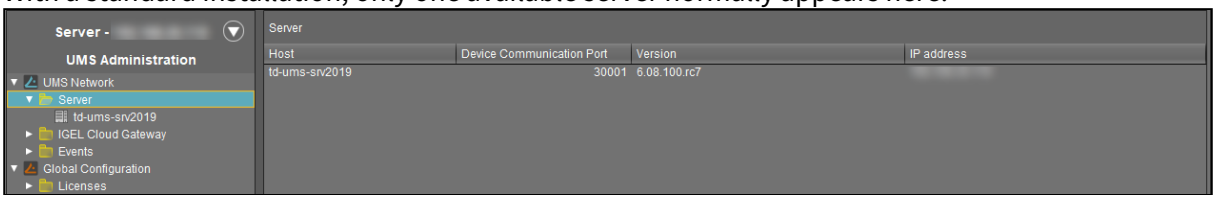
In the **Server** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all servers that belong to your UMS installation. For an individual server, additional details such as process information, service status, statistical data, etc. are available. You can also define here the Public Address and Public Web Port for your UMS Server.

Menu path: **UMS Console > UMS Administration > UMS Network > Server**

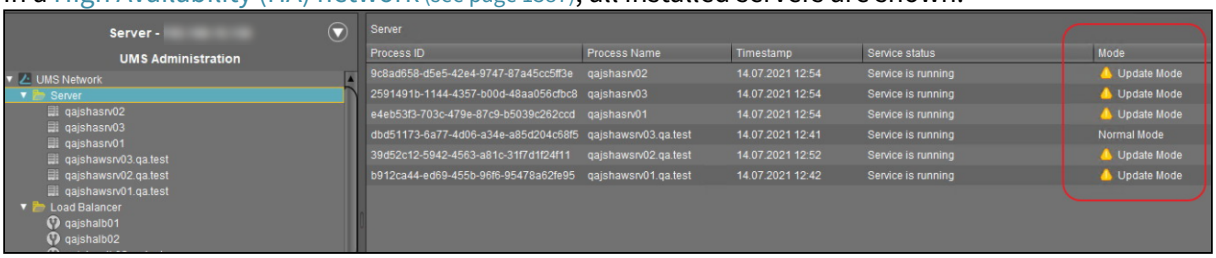
Server Node in the IGEL UMS

The **Server** node lists all servers belonging to the UMS installation:

- With a standard installation, only one available server normally appears here.



- In a High Availability (HA) network (see page 1387), all installed servers are shown.



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 How to Update a UMS HA Installation: Without Downtime of the Servers (see page 1414) . 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:

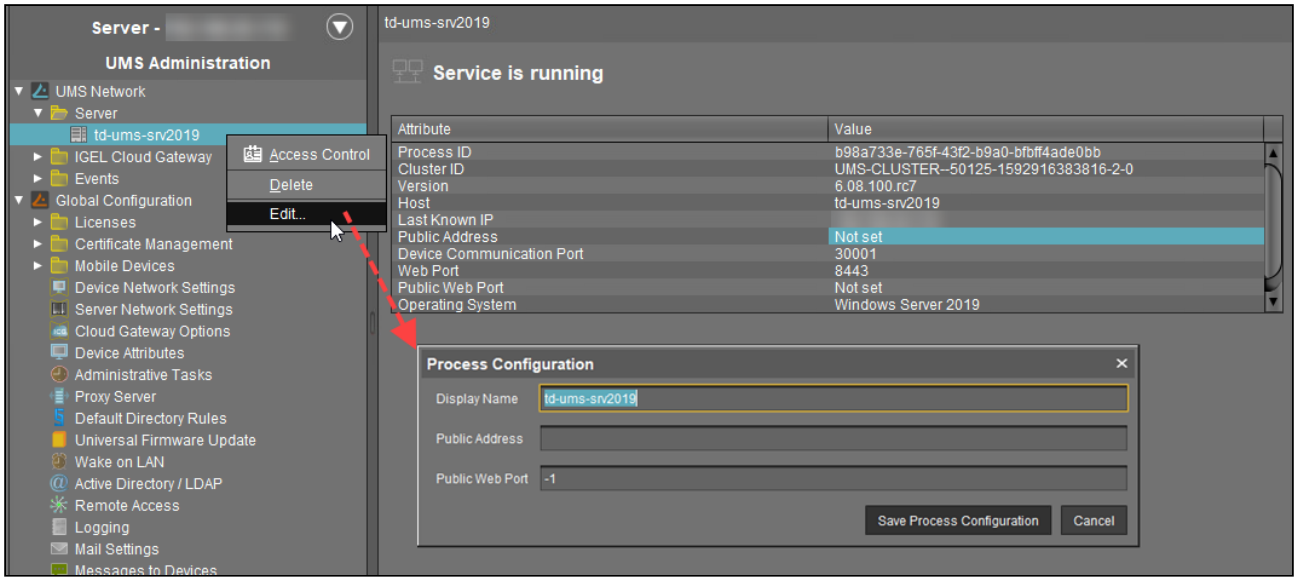
	The server is online.
	The server is offline.

	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.



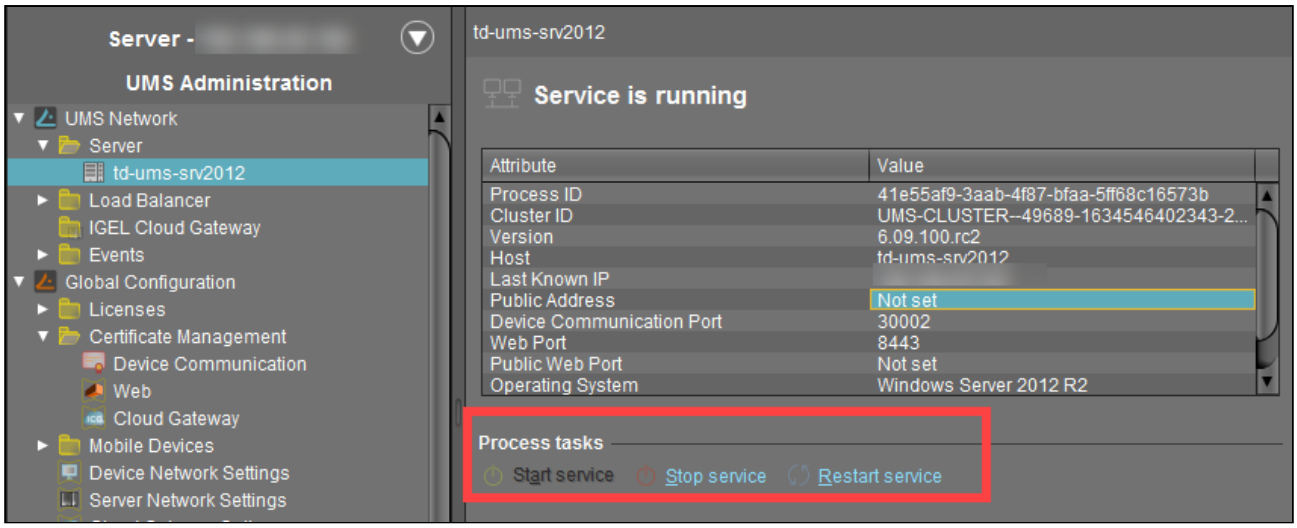
If set, the **Public Address** and **Public Web Port** will be used

- 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 1123)) and Universal Firmware Updates (see Universal Firmware Update in the IGEL UMS (see page 856))
- 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? (see page 514), incl. the section "Connection Data Used during the Update")
- for the automatically generated web certificates, see Web (see page 899)
- for HTTPS requests from devices if no **Cluster Address** is set (see Server Network Settings in the IGEL UMS (see page 909))

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:

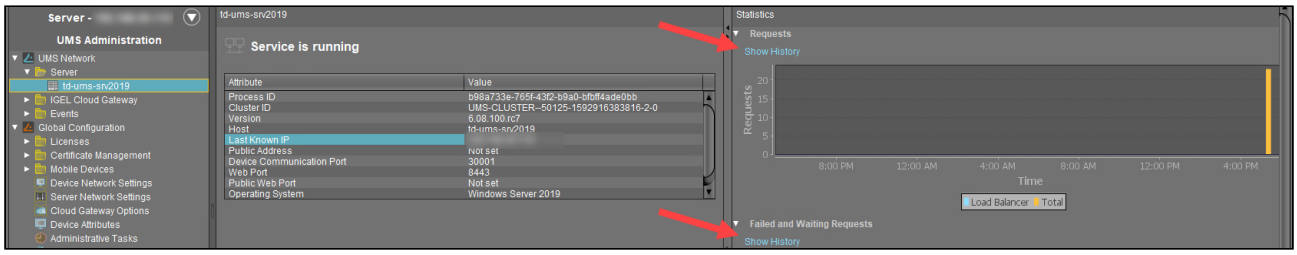


For how you can start or stop services, see also IGEL UMS HA Services and Processes (see page 1425).

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.



Load Balancer - View Your IGEL UMS Load Balancer Information

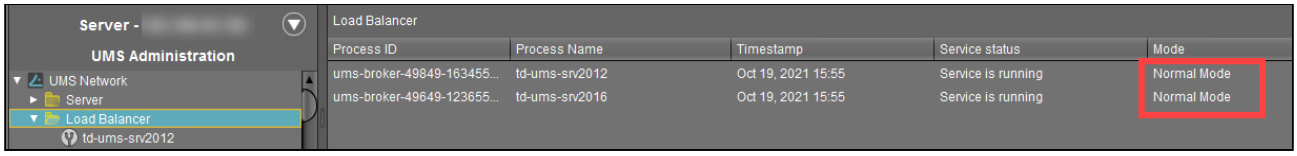
In the **Load Balancer** node of the IGEL Universal Management Suite (UMS) Console, you can find basic information on all load balancers that belong to your UMS installation. For an individual load balancer, additional details such as process information, service status, statistical data, etc. are available.

Menu path: **UMS Administration > UMS Network > Load Balancer**

"Load Balancer" Node in the IGEL UMS

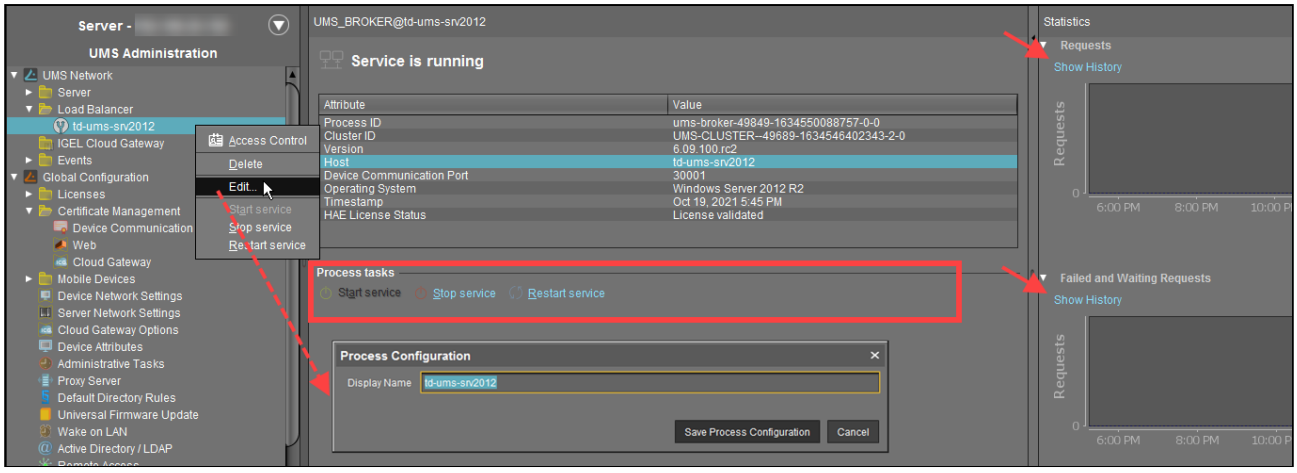
The **Load Balancer** node is visible in the UMS structure tree and active only if you have installed a UMS High Availability network with **UMS Load Balancer** activated. See IGEL UMS High Availability (HA) (see page 1387).

The **Load Balancer** node lists all load balancers belonging to the UMS installation:



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 (see page 1420).

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 (see page 1425).

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 - Managing an ICG Connection in the IGEL UMS

You can connect the IGEL Universal Management Suite (UMS) to one or more IGEL Cloud Gateways (ICG).

For details of how to set up all components for a connection to ICG, see (12.05-en) IGEL Cloud Gateway Installation and Setup .

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway**

	Restart IGEL Cloud Gateway Restarts the selected ICG.
	Install a new IGEL Cloud Gateway with the ICG Remote Installer See (12.05-en) IGEL Cloud Gateway Installation and Setup .
	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 (12.05-en) How to Update the IGEL Cloud Gateway .
	Update the keystore of the selected IGEL Cloud Gateway with the Update Keystore Wizard For renewing the end certificate, see (12.05-en) How to Renew a Signed Certificate for the ICG . For exchanging the root certificate, see (12.05-en) How to Exchange 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. If you remove an IGEL Cloud Gateway from the UMS database, you can not add it to the UMS database again. In most cases, it is preferable to uninstall the IGEL Cloud Gateway and then reinstall it using the ICG Remote Installer.
	Edit the settings of the selected IGEL Cloud Gateway
	Navigate to the ICG instance view

	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 Configuration in the IGEL UMS (see page 967)
  - **Use selected proxy server**: Select a proxy server from the list

IGEL Cloud Gateway (Instance) in the IGEL UMS

Here, you will find information regarding a configured gateway and can establish or disconnect the connection.

Menu path: **UMS Administration > UMS Network > IGEL Cloud Gateway > [Display Name]**

	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 in the IGEL UMS

Menu path: **UMS Administration > Global Configuration**

Under **Global Configuration**, you can regulate administrative tasks (see page 920), integrate user data from the Active Directory (see page 984), set up Universal Firmware Updates (see page 979) and manage licenses (see page 883).

Managing Device Attributes for IGEL OS Devices in the IGEL UMS

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 778) .

The additional attributes can also be used in:

- Searches in the Search for Objects in the IGEL UMS Console (see page 693) and the Search for Devices in the IGEL UMS Web App (see page 1164)
- Views - Filtering for Devices in the IGEL UMS (see page 818)
- Default Directory Rules (see page 969)

You can also manage custom device attributes in the IGEL UMS Web App. For details, see How to Manage Custom Device Attributes in the IGEL UMS Web App (see page 1219) .

Menu path: **UMS Administration > Global Configuration > Device Attributes**

Global Overwrite Rule

> This parameter is relevant for devices with IGEL OS 11.07 or higher.

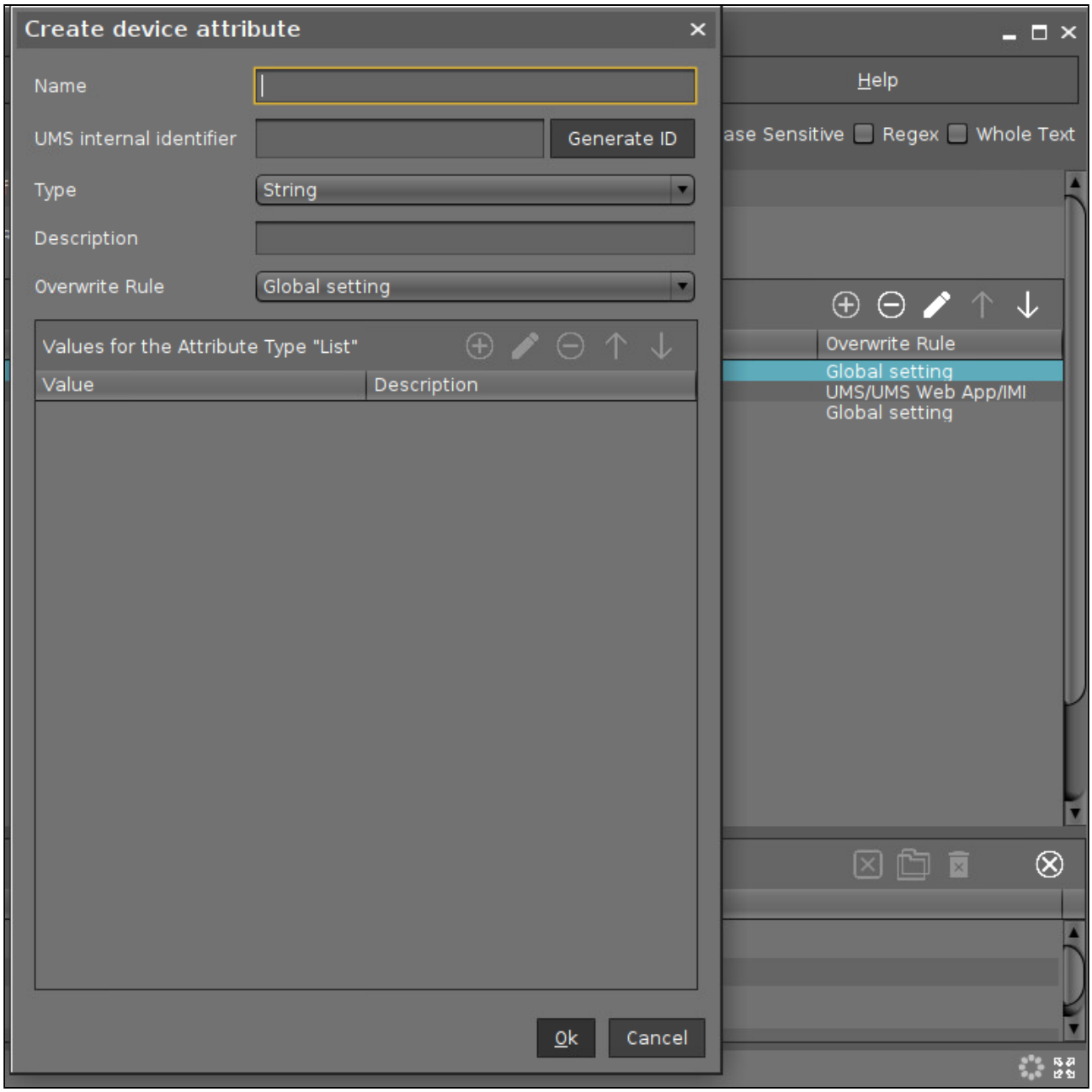
Defines the default overwrite rule for those device attributes whose overwrite rule is set to **Global setting**. The overwrite rule defines how the values of device attributes can be set and changed.

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 How to Manage IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You (see page 553) .
- **All**: Both the UMS and the devices can set and change the values of the device attributes. New values overwrite older values.

Set a Device Attribute

→ Click on  to set up a new device attribute:



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 820)) 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.

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:

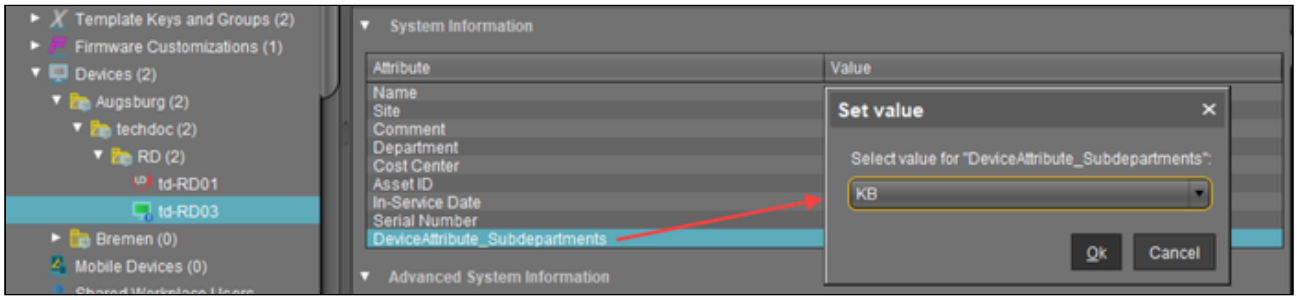
- **String**: A sequence of letters, numbers, and special characters is expected.
- **List**: A list of values is provided for selection. These values are specified as shown below:
  Values for the Attribute Type "List"
  - **Value**: Name of the predefined value
  - **Description**: Optional description 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.



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 How to Manage IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You (see page 553) .

- **All**: Both the UMS and the devices can set and change the values of this device attribute. New values overwrite older values.

Default Directory Rule

Device attributes used in default directory rules are marked with a check mark.

Device attributes used in default directory rules cannot be deleted.

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 884)
- Device Licenses (see page 886)
- Deployment - Deploying Licenses through the IGEL UMS (see page 888)

UMS Licenses

In this area, you are given an overview of the availability and status of UMS licenses.

Menu path: **UMS Administration > Global Configuration > Licenses > UMS Licenses**

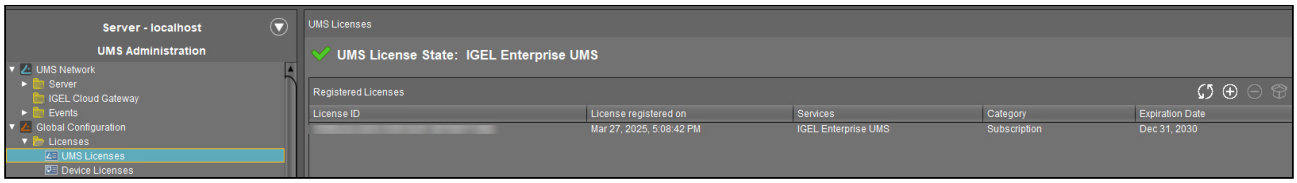
UMS License State

At the top, you can see the state of the UMS license. For example, if the license is active, you can see a green checkmark, or, when the license is about to expire, you can see the remaining days till expiration.

Starting from version 12.07.100, the UMS needs to have a UMS License. The License level defines the accessible feature set of the UMS. The license level is shown here (for example, **IGEL Enterprise UMS**).

For more information, see IGEL Software Licenses for IGEL OS and IGEL UMS[152] .

Registered Licenses



In the columns of the table view, you can see:

- **License ID**: Identification number of the license
- **License registered on**: Point in time when the license was registered in the UMS
- **Services**: Licensed service, e.g. IGEL Enterprise UMS
- **Category**: Shows whether a license is an evaluation license or a license included in a subscription
- **Expiration Date**: End date of the license period

Action Buttons

Retrieve UMS License from License Portal

Functions as **Retrieve UMS License from license portal** described in https://kb.igel.com/en/universal-management-suite/current/settings-change-server-settings-in-the-igel-ums-ad .

152. https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums#IGELSoftwareLicensesforIGELOSandIGELUMS-IGELUMSLicenses

	**Add license file** Functions as **Activate new UMS license** described in https://kb.igel.com/en/universal-management-suite/current/settings-change-server-settings-in-the-igel-ums-ad .
	**Delete license**
	**Show content of the license file**

Device Licenses

Menu path: **UMS Administration > Global Configuration > Licenses > Device Licenses**

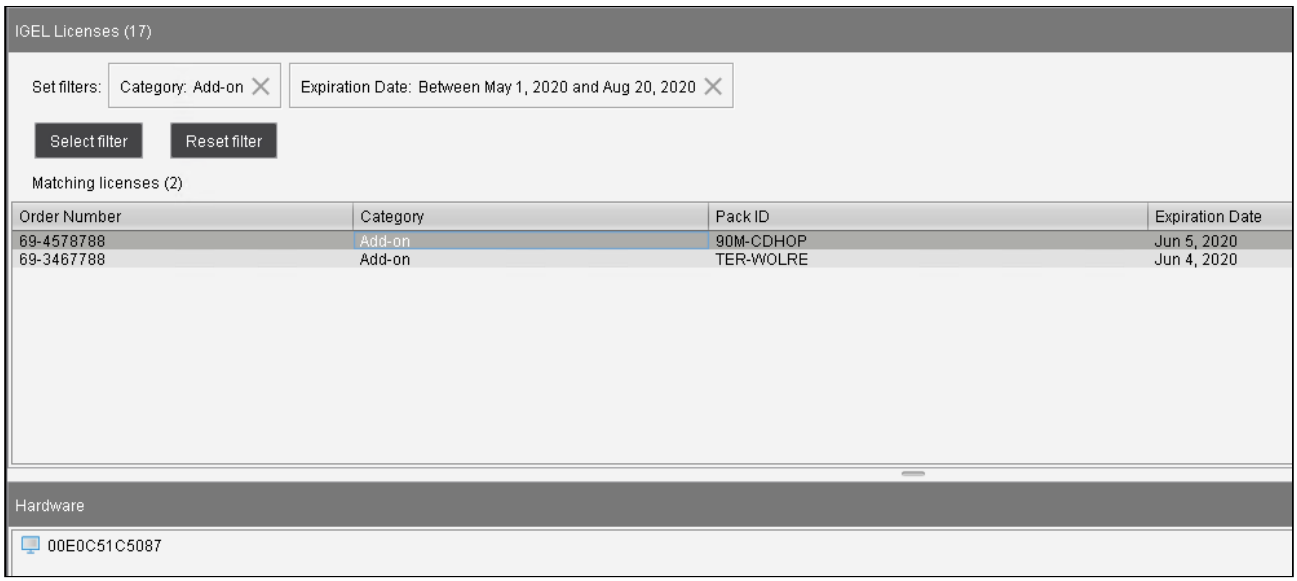
IGEL Licenses

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

To avoid registering the same device license several times, the UMS checks if the device license already exists in the database during the registration. If so, the license cannot be registered again and an error message is displayed.

Select Filter / Reset Filter



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

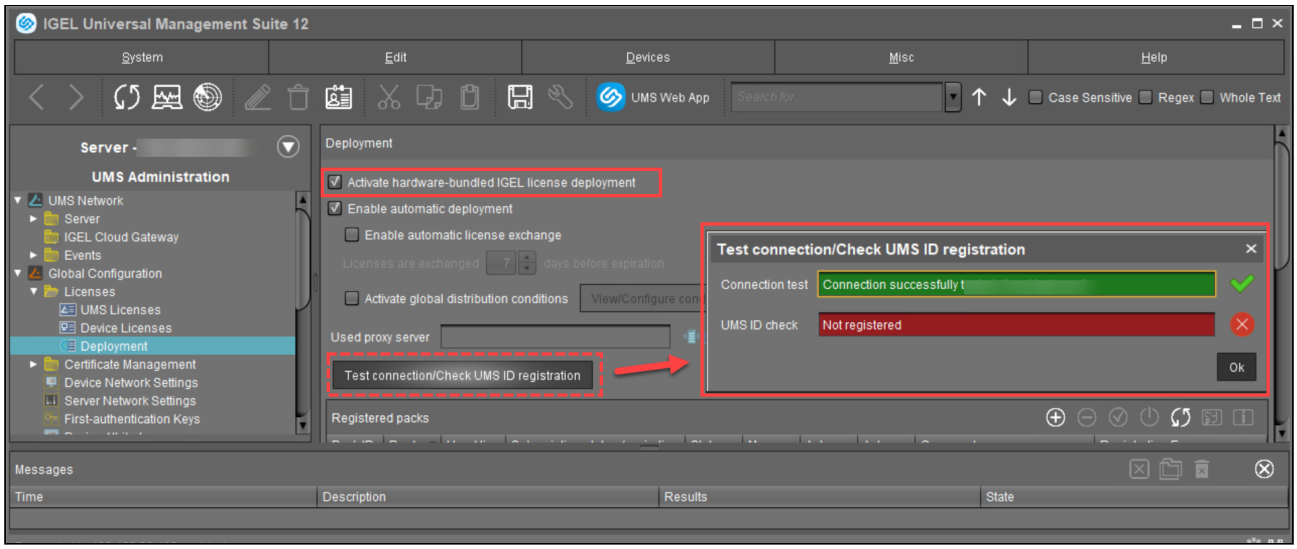
Here, you can enable and configure the automatic deployment of licenses by the IGEL Universal Management Suite (UMS). The automatic license deployment includes licenses for OSC/UDC3, UMA and UD Pocket. Once commercially available, the UMS can also deploy hardware-bundled IGEL licenses automatically.

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.

> 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)

> 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

> As of UMS 12, demo licenses for IGEL OS 12 and IGEL OS 11 devices are also supported by Automatic License Deployment.

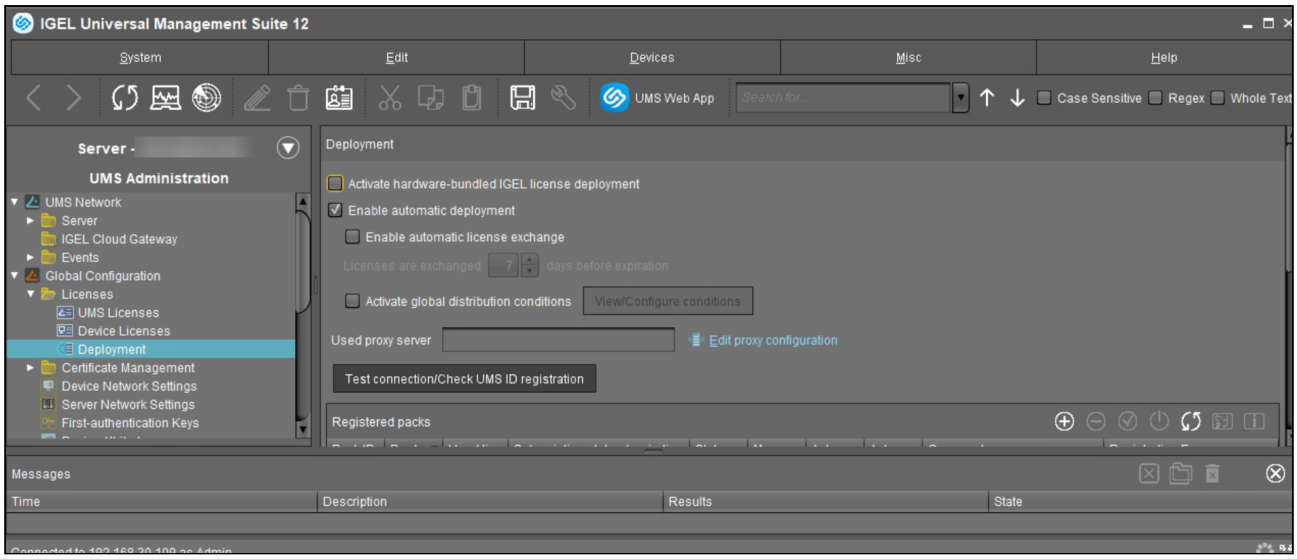
Automatic license deployment requires a connection between the UMS and the IGEL license server as well as the IGEL update server. This connection can be established via a proxy.

For details about the process of automatic license deployment, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD)*

> If a number of Product Packs for which suitable and non-allocated licenses are available, a selection will be made in accordance with the following criteria:
>
> - The Product Pack with the most allocated licenses will be used first.
> - Product Packs with an earlier registration date will be used before Product Packs with a later registration date.

As soon as a license is registered in the UMS, the UMS stores the license and adds a license download link to the device settings. After that, the UMS sends the settings to the devices. When the devices have received their settings, they download the licenses and reboot. After the reboot, all licensed features are available on the devices.

> For further information about setting up and using automatic license deployment, see *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > 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

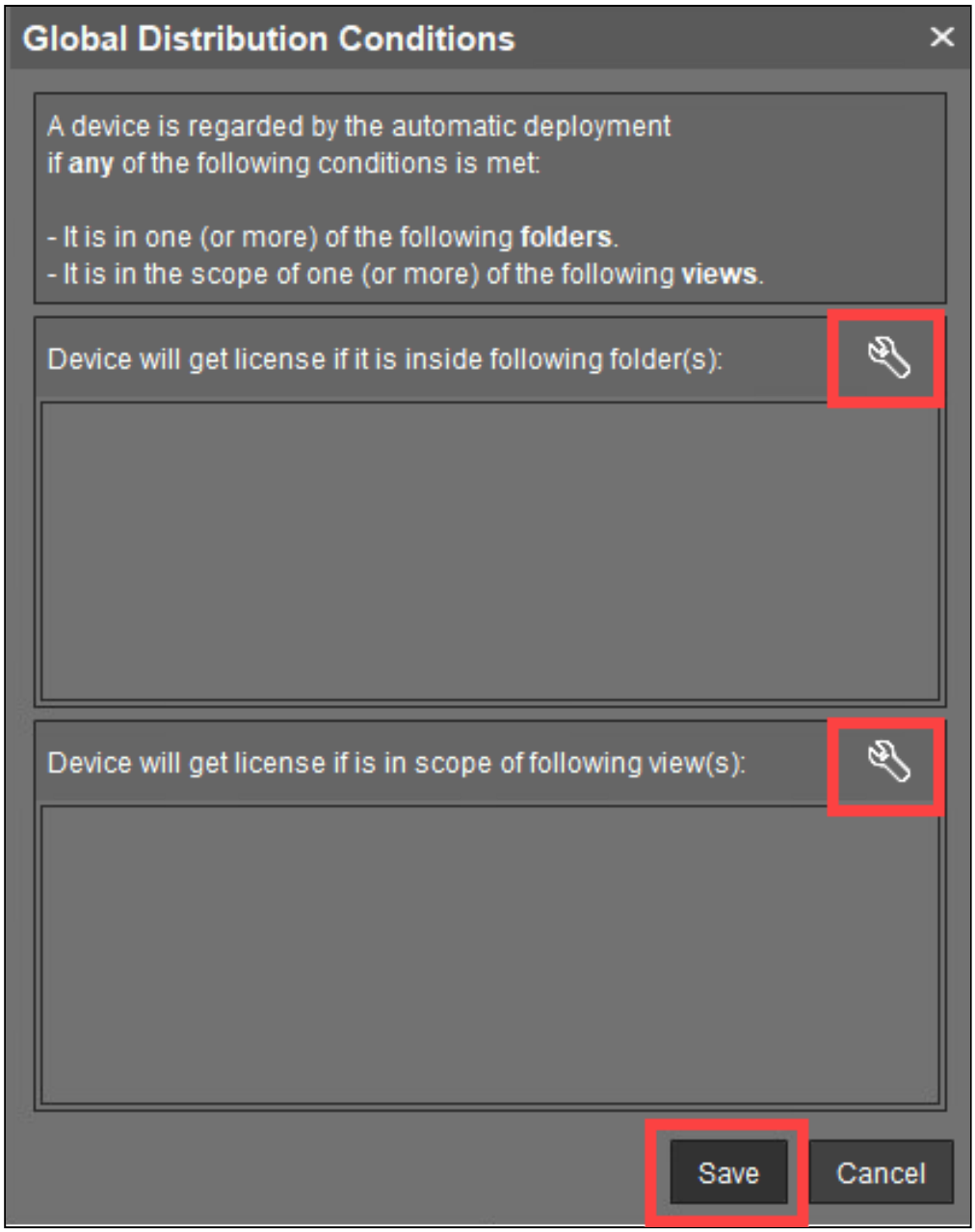
☑ Only devices that fulfill the conditions defined under **View / Configure conditions** are considered for the automatic license deployment. These conditions apply globally to the automatic license deployment. However, you can still configure pack-specific distribution conditions (see "Registered Packs" below).

> **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 (see page 1342).

Under **UMS Administration > Global Configuration > Proxy Server**, one or more proxies must be configured; see Proxy Server (see page 967).

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 967) 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 *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) > Configuring the Distribution Conditions.*

	Show Product Pack details: • **Attribute**: Shows the attributes of a Product Pack. • **Licensed hardware**: Shows all devices licensed with the Product Pack belonging to the entry.

The following information is shown:

- **Pack ID**: ID of the Product Pack
- **Product**: Product pack type
- **Used licenses**: Licenses currently in use
- **Subscription status (expiration date/validity 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 *IGEL Subscription and More > IGEL Software Licenses Articles > IGEL Software Licenses How-Tos > Deploying Licenses > Setting up Automatic License Deployment (ALD) > 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 in the IGEL UMS

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 Certificates in the IGEL UMS

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 Certificates in the IGEL UMS

Here, you can manage the certificates through the IGEL Universal Management Suite (UMS) for communication via the Web Port (default: 8443).

Menu path: **UMS Administration > Global Configuration > Certificate Management > Web**

Overview

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 Troubleshooting: Browser Displays a Security Warning (Certificate Error) when Opening the UMS Web App (see page 564)
- If you need to use an alternative certificate chain instead of the pre-installed one, see How to Use Your Own Certificates for Communication over the Web Port (Default: 8443) in IGEL UMS[153]

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 How to Use Your Own Certificates for Communication over the Web Port (Default: 8443) in IGEL UMS[154].

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.

153. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication
154. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication

 - 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.

 - Show the content of the selected certificate.

 - 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.

 - 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 How to Use Your Own Certificates for Communication over the Web Port (Default: 8443) in IGEL UMS[155].

155. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication

Cloud Gateway Certificates in the IGEL UMS

Here, you can manage the certificates for the communication between the IGEL Cloud Gateway (ICG) and the endpoint devices.

Menu path: **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**

For details of how to set up all components for a connection to the ICG, see *IGEL Cloud Gateway* > *ICG Manual* > *IGEL Cloud Gateway Installation and Setup*.

Use

- *IGEL Cloud Gateway* > *ICG Manual* > Administration > *How to Exchange the Root Certificate for ICG*
- *IGEL Cloud Gateway* > *ICG Manual* > Administration > *Renewing a Signed Certificate for the 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

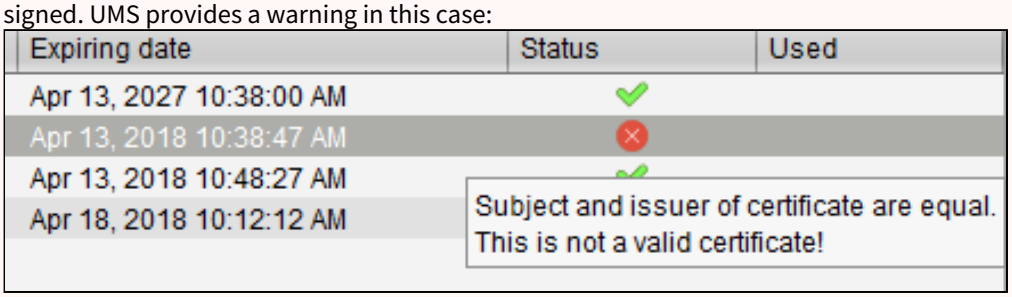
Display name: Name in the certificate (common name, CN).

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:



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.

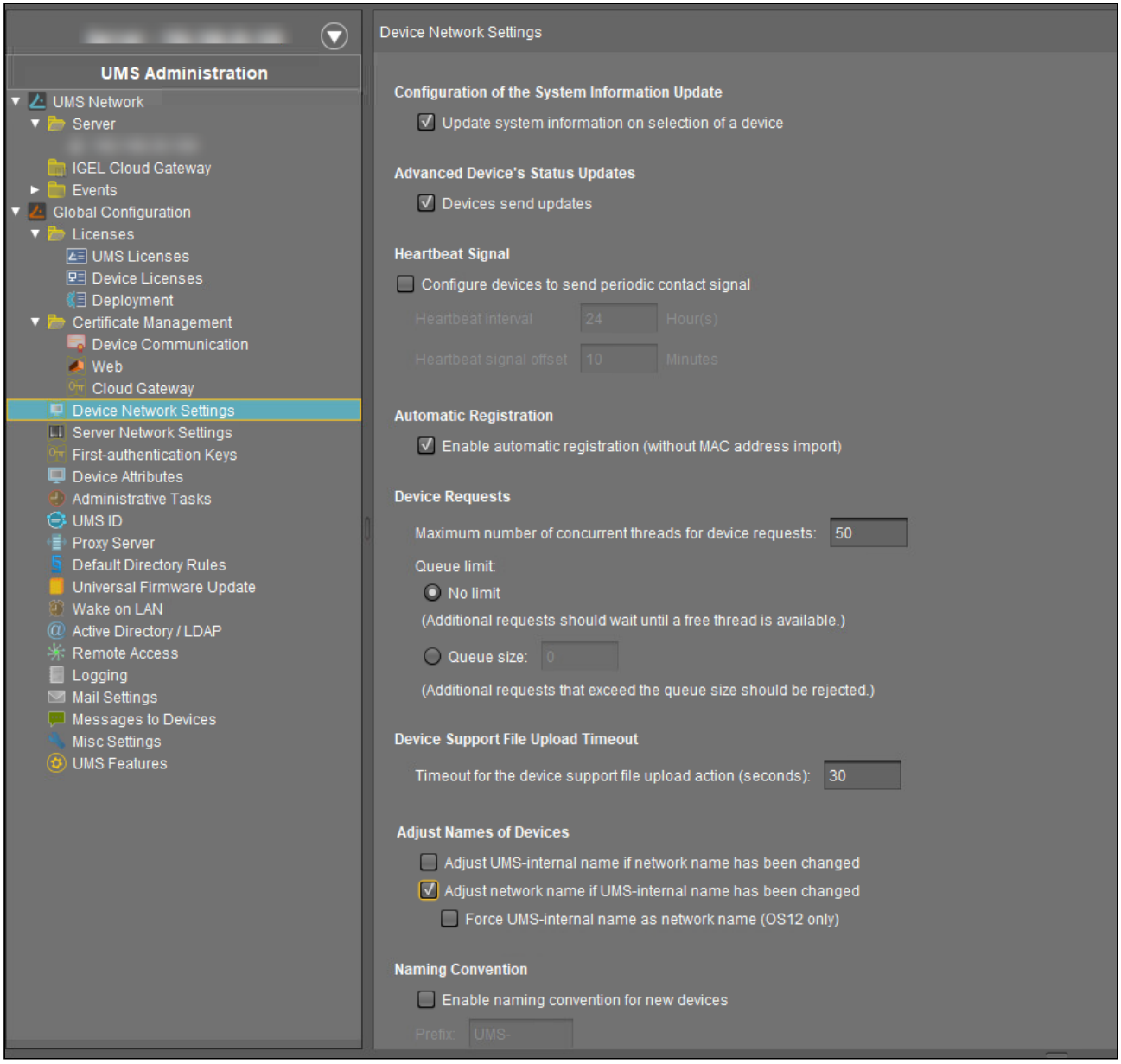
Export certificate: Exports certificate file.

Show certificate content: Shows the content of the certificate in a text window.

Device Network Settings for the IGEL 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 778).

☑ 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 the **Heartbeat interval**.

☐ The devices do not send a regular heartbeat signal. (Default)

Heartbeat interval

The interval between each heartbeat signal. The value can be defined in hours (from 1 to 5000). (Default: 24)

For more information, see Monitoring Device Health and Searching for Lost Devices in the IGEL UMS (see page 543).

Heartbeat signal offset

The heartbeat signal will have a random delay between 0 and the value specified here. The value is defined in minutes. The minimum value is 5, the maximum is one third of the defined heartbeat interval. (Default:10)

This is to avoid overloads which might occur when large amounts of devices send their heartbeat signals simultaneously.

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 1143).

☑ 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) (see page 1387).

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)

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)

Force UMS-internal name as network name (OS12 only)

The parameter is only visible if the **Adjust network name if UMS-internal name has been changed** parameter is enabled and the **Adjust UMS-internal names if network name has been changed** parameter is disabled. The setting is only valid for OS 12 devices.

☑ The network name of OS 12 devices is set to the UMS-internal name. The setting on the device gets overwritten and changing the network name on the OS 12 device gets blocked.

☐ Name adjustments are made according to the **Adjust network name if UMS-internal name has been changed** parameter. Changing the network name on the OS 12 device is possible. (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)

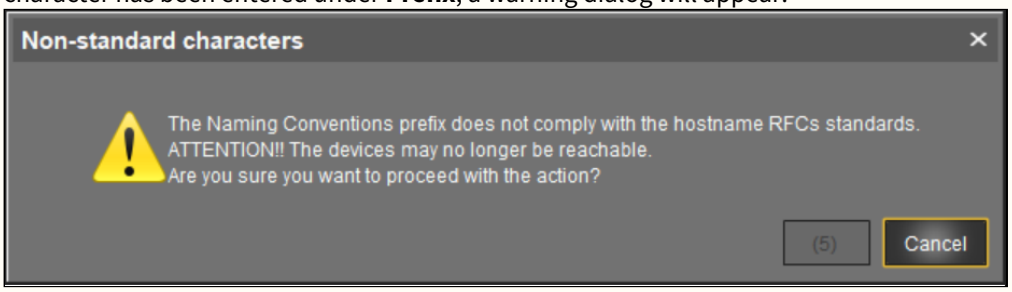
Prefix

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

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

> Note for UMS 12.02.120 or Higher
>
> This setting is only available if the **Identifier** is set to **Sequential Number**.

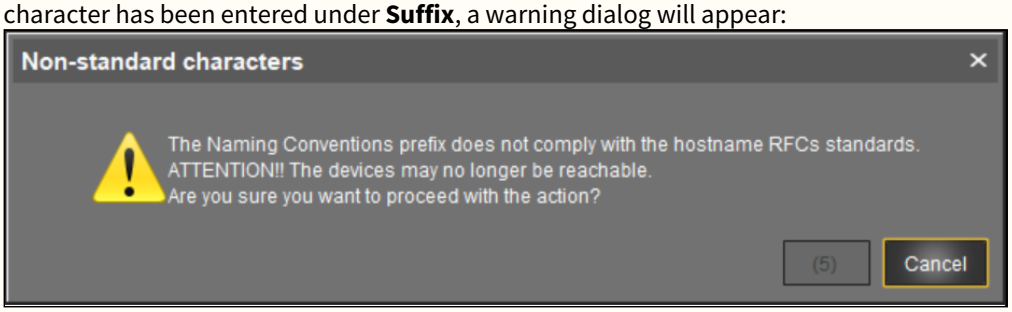
A minimum number of digits for the sequential number added to the prefix. The digits not allocated will be filled with zeros. Examples: If **2** is selected, the consecutive number of the first device will be **01**, if **3** is selected, the consecutive number will be **001**, and so on.

> If the number of devices exceeds the value defined here, the numbering will simply continue without an error occurring.

Suffix

> 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.

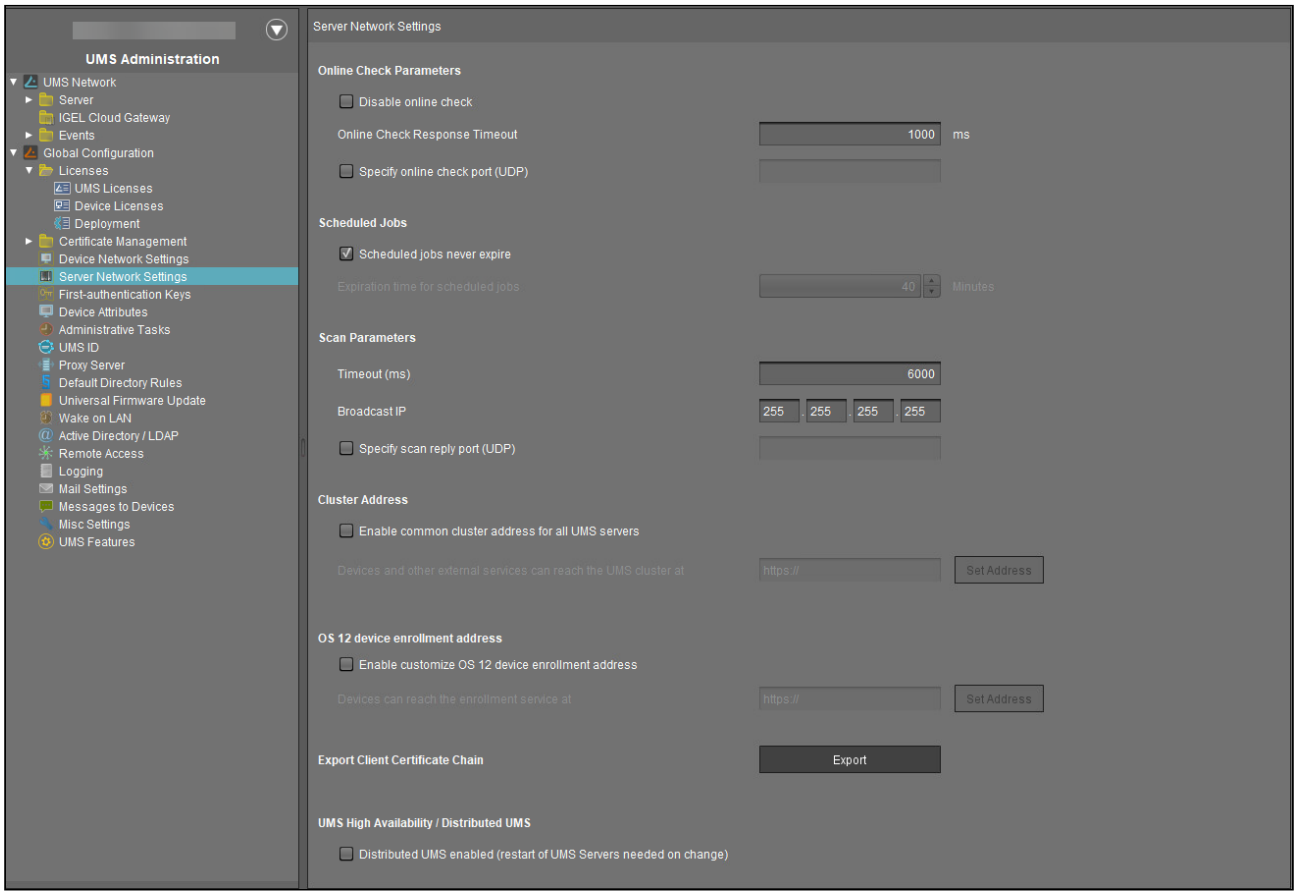
Rename and renumber all devices

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**



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 870).

- The Cluster Address is only for communication via the web server port (see page 1038) (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 (see page 265).

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.

As a best practice, only use lowercase letters in the **FQDN**. Using capital letters might lead to authentication issues or connection issues from OS 12 devices due to case sensitivity.

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

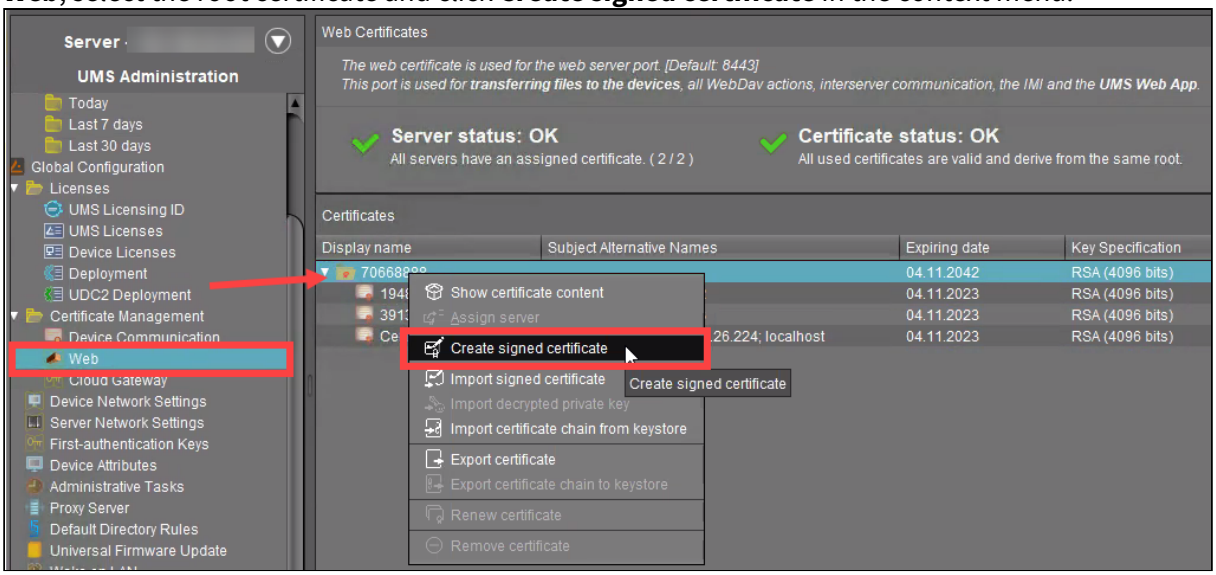
Configure a Web Certificate for All Servers...

If you have a UMS HA or Distributed UMS installation and configured the **Cluster Address**, you must define a web certificate for all servers:

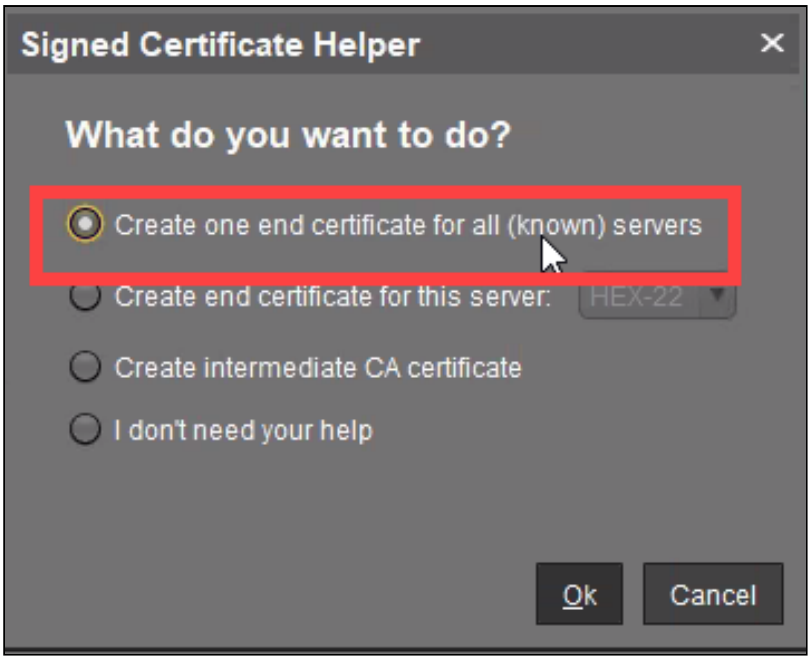
- The certificate must contain the cluster address and all server addresses
- The certificate must be assigned to all servers

To define a web certificate for all servers, proceed as follows:

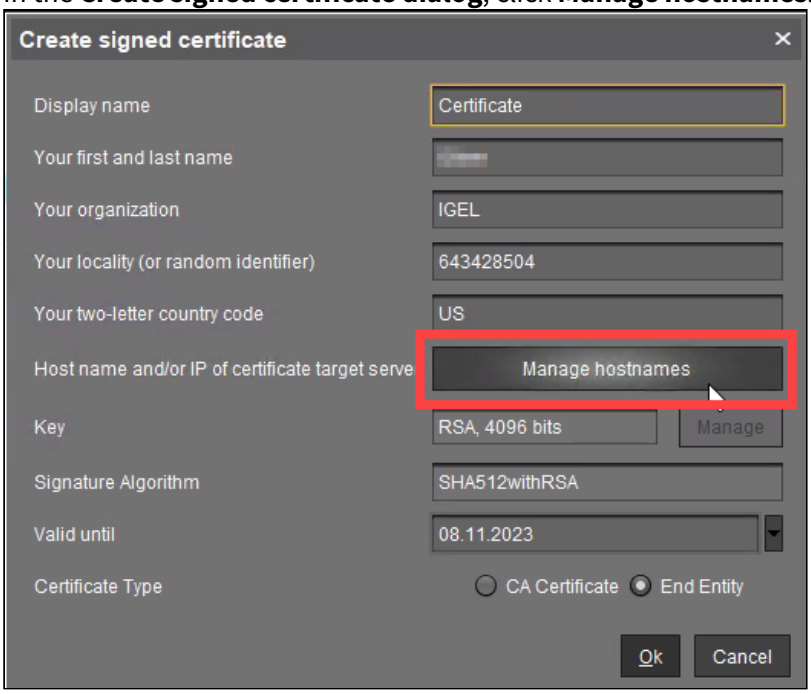
1. In the **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**, select the root certificate and click **Create signed certificate** in the context menu.



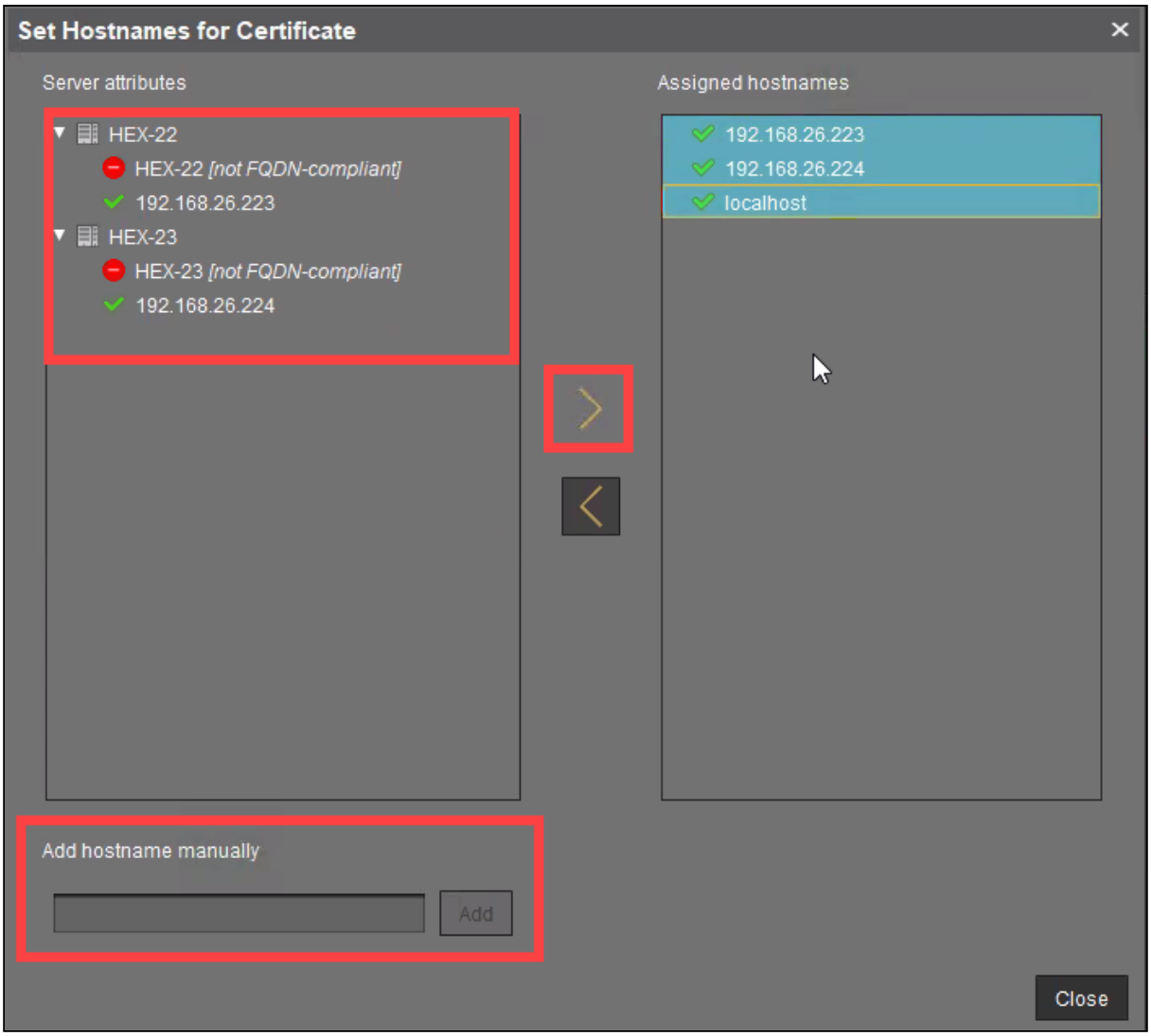
2. In the **Signed Certificate Helper** dialog, select **Create one end certificate for all (known) servers**.



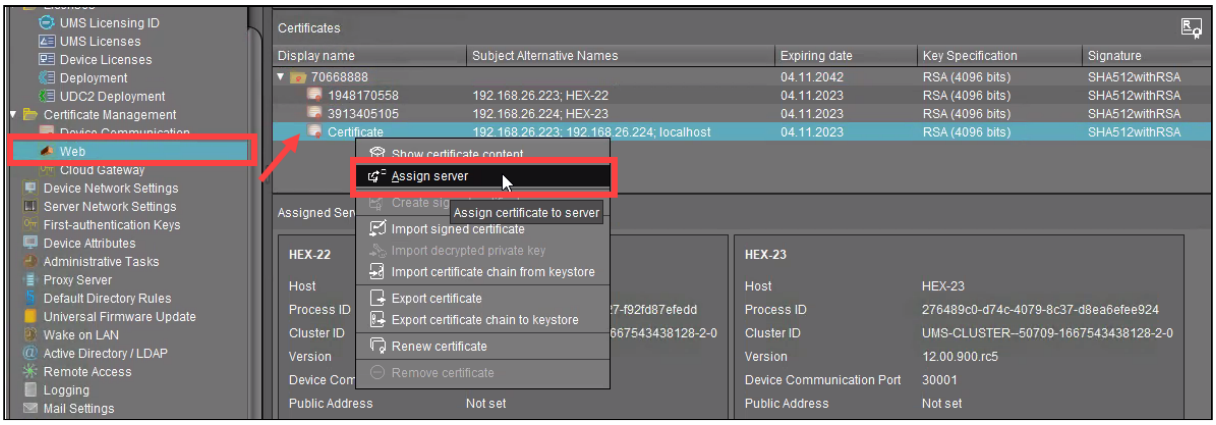
3. In the **Create signed certificate dialog**, click **Manage hostnames**.



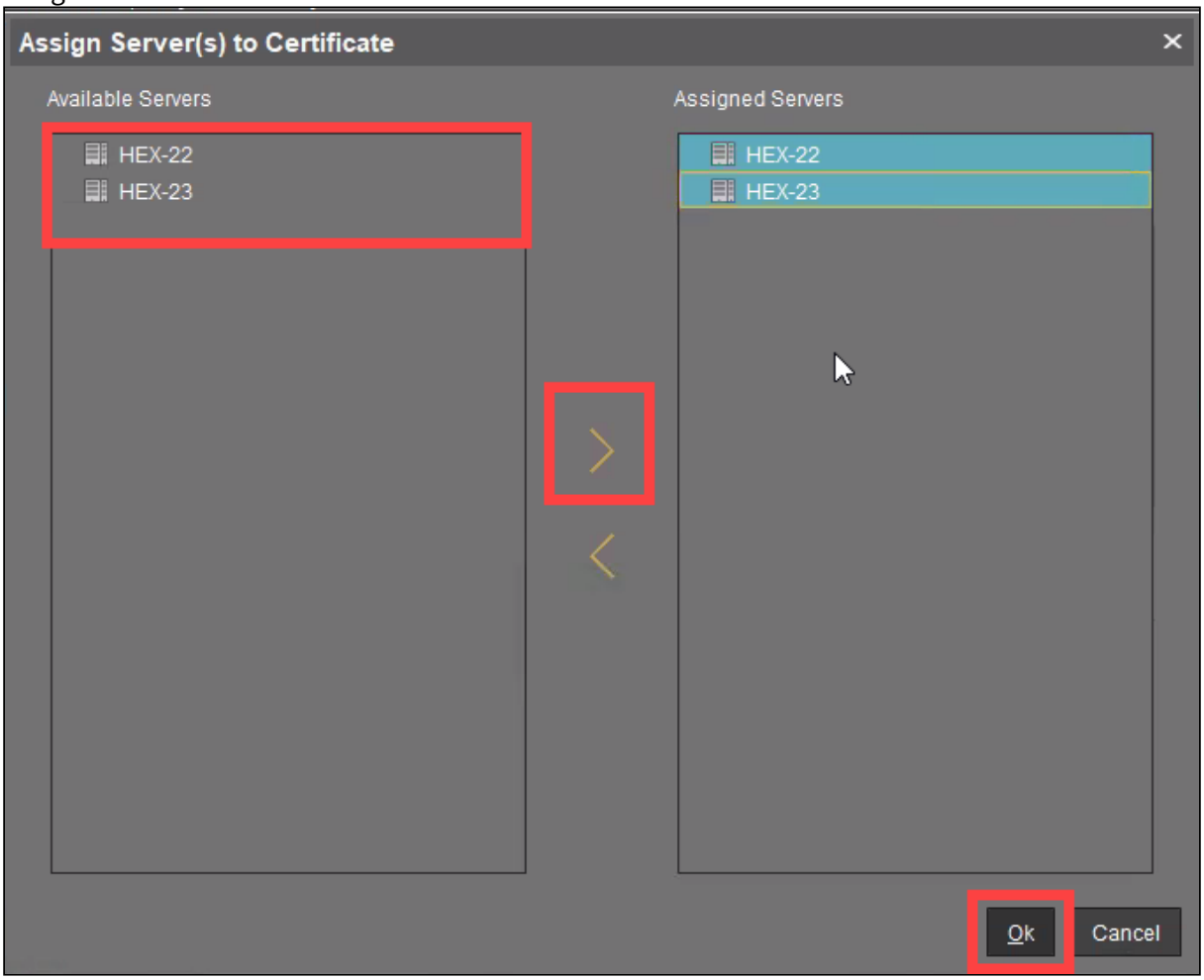
4. In the dialog **Set Hostnames for Certificate**, check if Cluster Address, "localhost", all IP addresses, and FQDNs (Fully Qualified Domain Names) under which your servers are reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname 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.



7. Assign the certificate to all servers.



OS 12 Device Enrollment Address

> 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 (see page 316).

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.

> You need the Client Certificate Chain to configure the reverse proxy / external load balancer. For more information, see IGEL Universal Management Suite Network Configuration (see page 265).

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 in the IGEL UMS

You can use first-authentication keys to onboard IGEL OS 12 devices in the IGEL Universal Management Suite (UMS). For more information, see the documentation Onboarding IGEL OS 12 Devices[156].

You can also create and edit first-authentication keys in the UMS Web App, see How to Manage First-Authentication Keys in the IGEL UMS Web App[157].

Menu path: **UMS Administration > Global Configuration > First-authentication Keys**

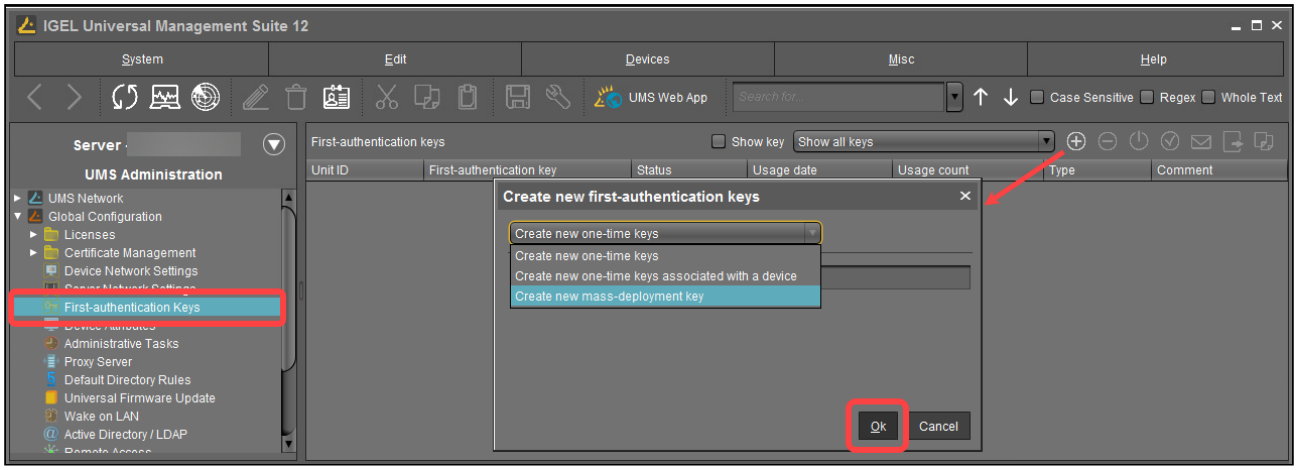
Menu Buttons

	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.

156. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices
157. https://kb.igel.com/en/universal-management-suite/current/how-to-manage-first-authentication-keys-in-the-ige

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.

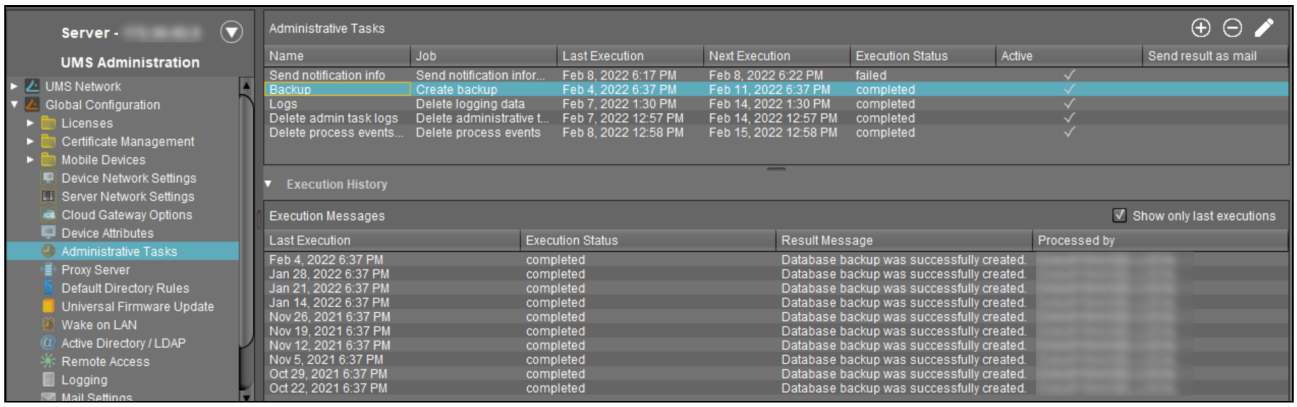
> It is not possible to create more than one first-authentication key with the same password.

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 1056)), 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 225) and IGEL UMS Maintenance Tasks (see page 221).

Menu path: **UMS Administration > Global Configuration > Administrative Tasks**



How to Create an Administrative Task

To create an administrative task, proceed as follows:

1. Click on  .
2. In the **Create Administrative Task** dialog, configure the necessary settings. What settings are available depends on the chosen **action**. The settings are spread over a number of pages. You can switch between these by clicking on **Next** and **Back**.
   The following actions are available:

- Create Data Backup as Administrative Task in the IGEL UMS (see page 922)
- Remove Unused Firmwares as an Administrative Task in the IGEL UMS (see page 925)
- Delete Logging Data as an Administrative Task in the IGEL UMS (see page 928)
- Delete Job Execution Data as an Administrative Task in the IGEL UMS (see page 932)
- Delete Administrative Task Execution Data as an Administrative Task in the IGEL UMS (see page 935)
- Delete Process Events as an Administrative Task in the IGEL UMS (see page 938)
- Delete Devices as an Administrative Task in the IGEL UMS (see page 941)

- Export View or Advanced Search Result via Mail as an Administrative Task in the IGEL UMS (see page 944)
- Save View or Advanced Search Results in the File System in the IGEL UMS (see page 947)
- Assign Objects to the Devices of Views or Device Searches in the IGEL UMS (see page 950)
- Detach Assigned Objects from Devices of Views or Device Searches as an Administrative Task in IGEL UMS (see page 953)
- Delete Asset Information History as an Administrative Task in IGEL UMS (see page 956)
- Send Notification Information via Email as an Administrative Task in the IGEL UMS (see page 959)
- Cleanup Device Licenses as an Administrative Task in the IGEL UMS (see page 962)

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 as Administrative Task in the IGEL UMS

→ 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 993).

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.

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

The **Server Assignment** settings page is displayed only if you deploy High Availability or Distributed UMS (see page 13) environment.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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**.

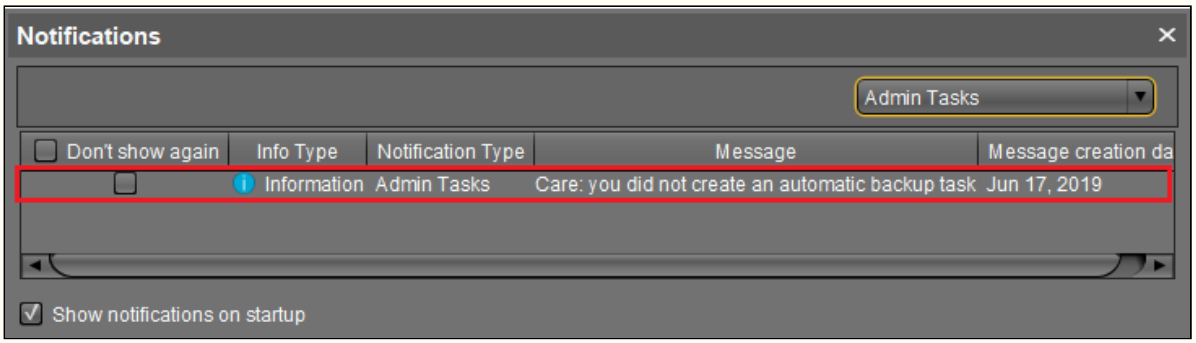
Exclude public holidays

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 672).

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 for data backup (see, Create Data Backup as Administrative Task in the IGEL UMS (see page 922)), the following notification pop-up will be shown after the start of the UMS Console:



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 as an Administrative Task in the IGEL UMS

You can define the removal of unused firmware as an administrative task. The deletion helps with performance optimization, see Performance Optimizations in IGEL UMS.

The first firmware that was registered in your UMS installation can not be removed.

The **Remove Unused Firmwares** administrative task currently applies **only to IGEL OS 11 firmware packages**. It does **not remove unused IGEL OS 12 apps** from the UMS cache directory:

```
/opt/IGEL/RemoteManager/rmguiserver/persistent/ums-appproxy/files
```

For app cleanup, you can use the **Enable automatic cleanup of unused versions** option described in Configuring Global Settings for the Update of IGEL OS Apps[158].

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.

158. https://kb.igel.com/en/universal-management-suite/current/configuring-global-settings-for-the-update-of-igel

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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.

Expiration
Point in time as of which the task will no longer be repeated.

Delete Logging Data as an Administrative Task in the IGEL UMS

You can define the deletion of Universal Management Suite (UMS) message and event logs as an administrative task[159]. The deleted logs are exported as a backup file into a selected folder as part of the administrative task.

Running this administrative task helps with performance optimization, see Performance Optimizations in IGEL UMS (see page 225).

The logs for Secure Shadowing (see page 815) as well as performance logs (see page 988) are not deleted as a result of this administrative task.

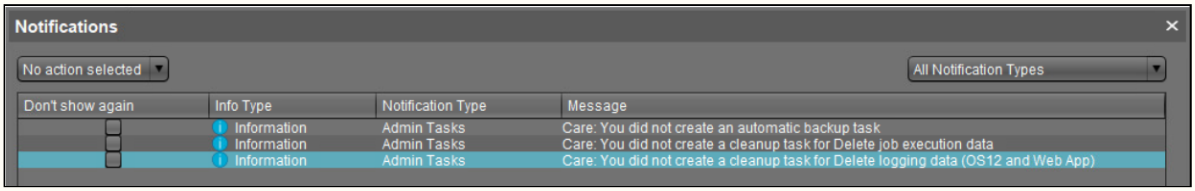
Menu path: **UMS Administration > Administrative Tasks >** Dialog "**Create Administrative Task**" **>** Action "**Delete logging data (OS12 and Web App)**" / "**Delete logging data (OS11 and Console)**"

Updates Starting from UMS 12.09.110

- **Delete logging data** was renamed to **Delete logging data (OS11 and Console)** - which deletes the log message and event messages related to the UMS Console and to OS 11 device management.
- **Delete logging data (OS12 and Web App)** was added as a new administrative task to delete messages related to the UMS Web App and to OS 12 device management.

The configuration of the two administrative tasks, **Delete logging data (OS12 and Web App)** and **Delete logging data (OS11 and Console)**, is almost the same. The information in this article applies to both.

Administrative Task Notification
If you have not set an administrative task for deleting logging data, the following notification pop-up will be shown after the start of the UMS Console.



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**.

General Window

In the **General** dialog window, you can define the following parameters.

159. https://kb.igel.com/en/universal-management-suite/current/administrative-tasks-configure-scheduled-actions-f

Name

Name for the task.

Action

- To delete log message and event messages related to the UMS Console and to OS 11 device management. select **Delete logging data (OS11 and Console)**.
- To delete log message and event messages related to the UMS Web App and to OS 12 device management, select **Delete logging data (OS12 and Web App).**

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 993).

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

In the **Configuration** dialog window, you can define details of the action through the following parameters.

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`

Logging message deletion settings (OS11 and Console) / Logging message deletion settings (OS12 and Web App)

The parameter is named differently depending on the selected administrative task, but it is used the same way.

- **Keep no more than [number] messages**: When this administrative task is executed, the oldest log entries of OS 11 devices and the UMS Console 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

This paramater is only available under the **Delete logging data (OS11 and Console)** administrative task.

- **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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Delete Job Execution Data as an Administrative Task in the IGEL UMS

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 225).

For more information on Jobs, see Jobs - Sending Automated Commands to Devices in the IGEL UMS (see page 847).

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 993).

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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**.

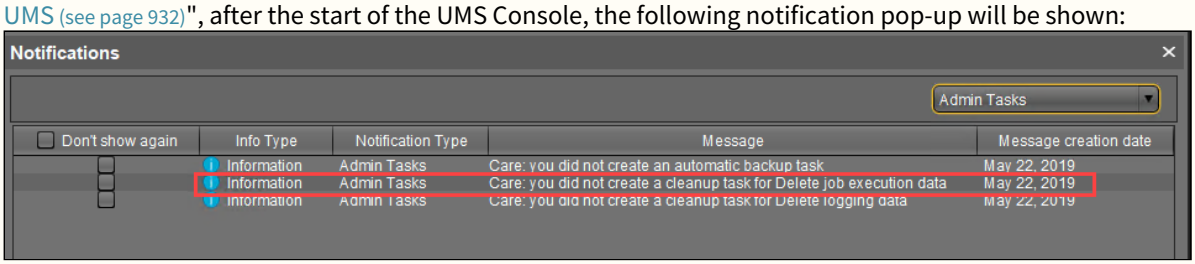
Exclude public holidays

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 672).

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 as an Administrative Task in the IGEL UMS (see page 932)", after the start of the UMS Console, the following notification pop-up will be shown:



Only users with read permission for administrative tasks can see this notification. You can set the rights under **Edit** > **Access control**.
You can manage the display settings under **Misc > Settings > Notifications**.
You can find the notifications under **Help > Notifications**.

Delete Administrative Task Execution Data as an Administrative Task in the IGEL UMS

You can define an administrative task to delete of the results of a (see page 920)dministrative tasks. The deletion helps with performance optimization, see Performance Optimizations in IGEL UMS (see page 225).

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 993).

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_admin_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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Delete Process Events as an Administrative Task in the IGEL UMS

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 225).

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 993).

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_process_events_.xml`.

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Delete Devices as an Administrative Task in the IGEL UMS

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 (see page 1164).

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 993).

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Export View or Advanced Search Result via Mail as an Administrative Task in the IGEL UMS

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 (see page 1164) .

> In order for emails to be sent, the UMS mail settings must be correct. Further information can be found under Mail Settings (see page 993).

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 993).

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 ";".

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)

Result format

Data format in which the results are sent as a mail attachment.
Possible options:

- **XML**
- **HTML**
- **CSV**

Delimeter

Defines the type of the delimeter used in the file for the CSV result format.

Server Assignment

> The **Server Assignment** settings page is displayed only if you deploy High Availability or Distributed UMS (see page 13) environment.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

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 UMS

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 920). For more information on the advanced search in the UMS Web App, see Search for Devices in the IGEL UMS Web App (see page 1164) .

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 993).

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.

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)

Result format

Data format in which the results are sent as a mail attachment.
Possible options:

- **XML**
- **HTML**
- **CSV**

Delimeter

Defines the type of the delimeter used in the file for the CSV result format.

Schedule

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Assign Objects to the Devices of Views or Device Searches in the IGEL UMS

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 page 1164).

See also the instructions in How to Assign Objects to a View in the IGEL UMS (see page 846).

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 993).

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Detach Assigned Objects from Devices of Views or Device Searches as an Administrative Task in IGEL UMS

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 How to Assign Objects to a View in the IGEL UMS (see page 846).

For general information on administrative tasks, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS (see page 920).

For more information on the advanced search in the UMS Web App, see Search for Devices in the IGEL UMS Web App (see page 1164).

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 993).

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.

In the **Server Assignment** dialog window you can configure the following.

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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Delete Asset Information History as an Administrative Task in IGEL UMS

When you use Asset Inventory Tracker[160] (AIT), you should periodically delete asset history as a part of performance optimization, see Performance Optimizations in IGEL UMS[161].

The administrative task **Delete asset information history** helps you to delete asset history, i.e. a log of events that are sent to the UMS when a peripheral is plugged in to the endpoint or unplugged.

This administrative task deletes only asset history, but NOT the current asset information (which is displayed for the selected endpoint in the **UMS Console > Devices > Asset Inventory** and in the **UMS Web App > Devices > Peripherals** if the AIT is activated and license requirements are met).

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 993).

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

160. https://kb.igel.com/en/universal-management-suite/current/view-device-information-in-the-igel-ums#ViewAssetInformation
161. https://kb.igel.com/en/universal-management-suite/current/performance-optimizations-in-igel-ums

☑ 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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Send Notification Information via Email as an Administrative Task in the IGEL UMS

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 (see page 640).

For general information on administrative tasks, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS (see page 920).

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 993).

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 (see page 640).
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

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

Cleanup Device Licenses as an Administrative Task in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can define an administrative task to cleanup expired or duplicated device licenses from your UMS database.

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 **Cleanup device licenses (expired licenses and/or license duplicates)**

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 993).

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 expired licenses
☑ All expired device licenses are deleted.

☐ The task will not delete expired licenses. (Default)

Delete license duplicates
☑ All duplicated device licenses are deleted.

☐ The task will not delete duplicated licenses. (Default)

Schedule

In the **Schedule** dialog window you use the following options to schedule task execution.

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 672).

Expiration
Point in time as of which the task will no longer be repeated.

UMS ID

The UMS ID is essentially a certificate of your IGEL Universal Management Suite (UMS) server. It is used, for example, for the communication of your UMS with the IGEL Cloud Services and the IGEL License Portal (ILP). The UMS ID consists of a public/private key pair. In the UMS ID area of the UMS Console, you can see details on the UMS ID and export the public key of the UMS ID as a `.crt` file.

Menu path: **UMS Administration > Global Configuration > UMS ID**

What is the UMS ID Used For?

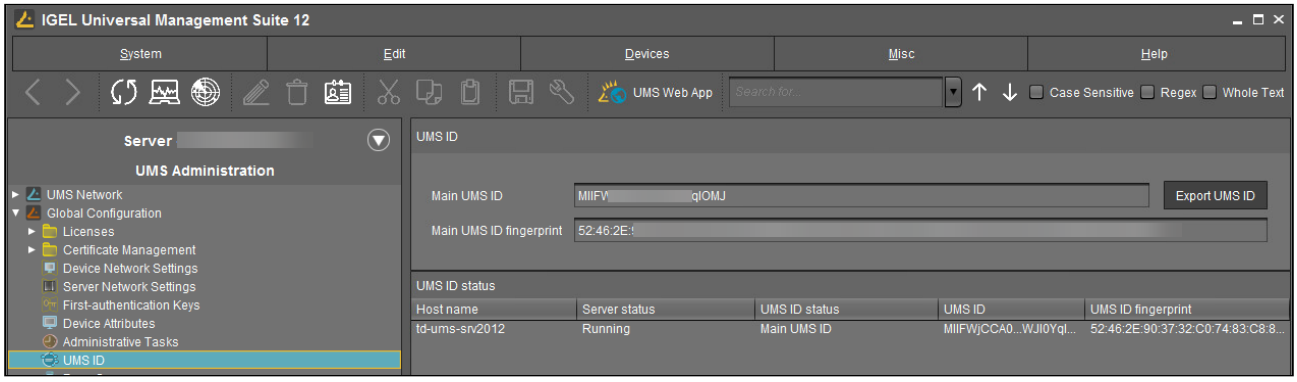
If registered in the ILP, the UMS ID allows for using Automatic License Deployment (ALD) without the need to handle an ALD Token with each purchase. The registration of the UMS ID is done by uploading the exported certificate file to the ILP, as described in Setting up Automatic License Deployment (ALD) .

The UMS ID is also used for communication with the IGEL Cloud Services. To enable the communication, you need to register the UMS in the IGEL Customer Portal. For details, see Registering the UMS[162].

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 example, during migration. For details, see Transferring or Registering the UMS ID[163].

For the backup options of the UMS ID, see UMS ID Backup in the IGEL Administrator (see page 1043) or IGEL UMS Administrator Command-Line Interface (see page 1079).

UMS ID in the UMS Console



Main UMS ID
The UMS ID used for communication with the ILP and IGEL Cloud Services. The first and last 10 characters are displayed.

162. https://kb.igel.com/en/how-to-start-with-igel/current/registering-the-ums
163. https://kb.igel.com/en/universal-management-suite/current/transferring-or-registering-the-ums-id

The UMS ID is generated upon each UMS Server installation. Therefore, if you have a 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 below.

Export UMS ID
Export the UMS ID as a `.crt` file. You need this file for registration in the ILP and IGEL Customer Portal. For details, see How to Export the UMS ID[164].

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 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`

164. https://kb.igel.com/en/universal-management-suite/current/how-to-export-the-ums-id

If the restart was unhelpful, the UMS ID has to be synchronized manually, see How to Manually Synchronize the UMS ID (see page 521) .

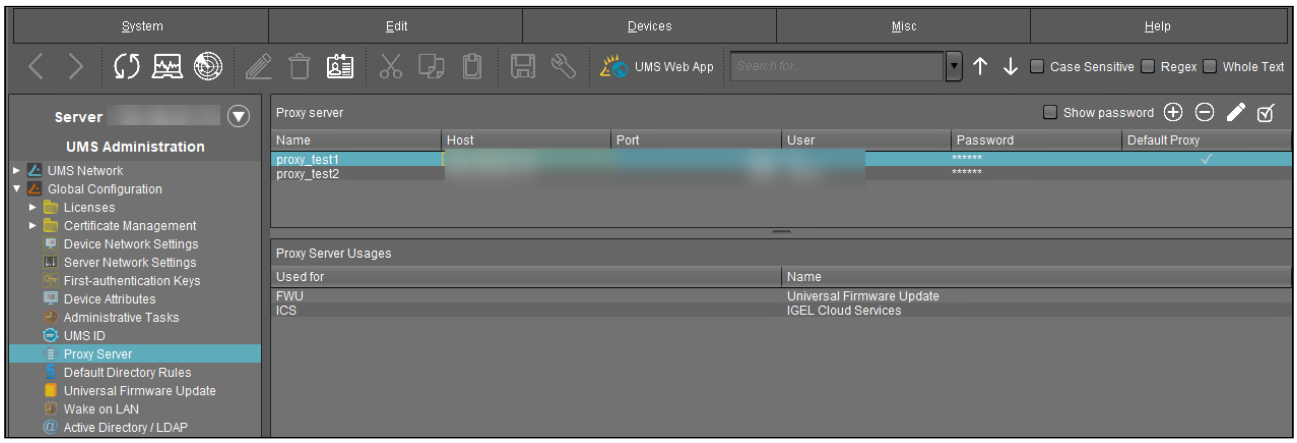
UMS ID
The UMS ID currently used on the server. The first and last 10 characters are displayed.

UMS ID fingerprint
The SHA-256 fingerprint of the UMS ID.

Proxy Server Configuration in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can configure proxy servers.

Menu path: **UMS Console > UMS Administration > Global Configuration > Proxy Server**



In this area, you can add and configure proxy servers in order to use them in the following scenarios:

- IGEL Cloud Gateway - Managing an ICG Connection in the IGEL UMS (see page 875)
- 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 888), 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 (see page 1342))
- Universal Firmware Update - Distributing Firmware in the IGEL UMS (see page 979) (if configured, this proxy is also used for UMS update check (see page 680))

> 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

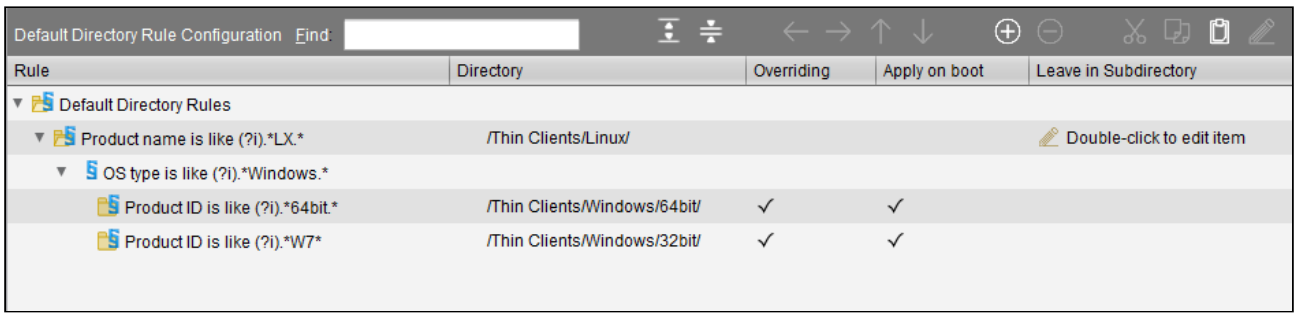
Rules for default directories are used to automatically classify devices into specific directories during registration. These directories can be linked to profiles which are then assigned to the devices contained. As a result, you can automatically configure the devices during registration (zero touch deployment).

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

See also the following how-tos for further information:

- Creating a Default Directory Rule (see page 971)
- Using Structure Tags with IGEL OS 11 Devices (see page 422)

→ Go to **UMS Administration > Global Configuration > Default Directory Rules**.
The user interface looks like this:



When you open a UMS database from an older version with UMS *Version 5.03.100* or newer for the first time, the default directory rules will automatically be converted into the new structure. Rules for the IP range will be split into two rules (IP greater than and IP less than).

- Symbol Bar (see page 970)
- How to Create a Default Directory Rule (see page 971)
- Finding Default Directory Rules (see page 974)
- How to Apply Default Directory Rules (see page 975)
- Editing a Rule (see page 976)
- Combining Conditions (see page 977)
- Using the Netmask (see page 978)

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:

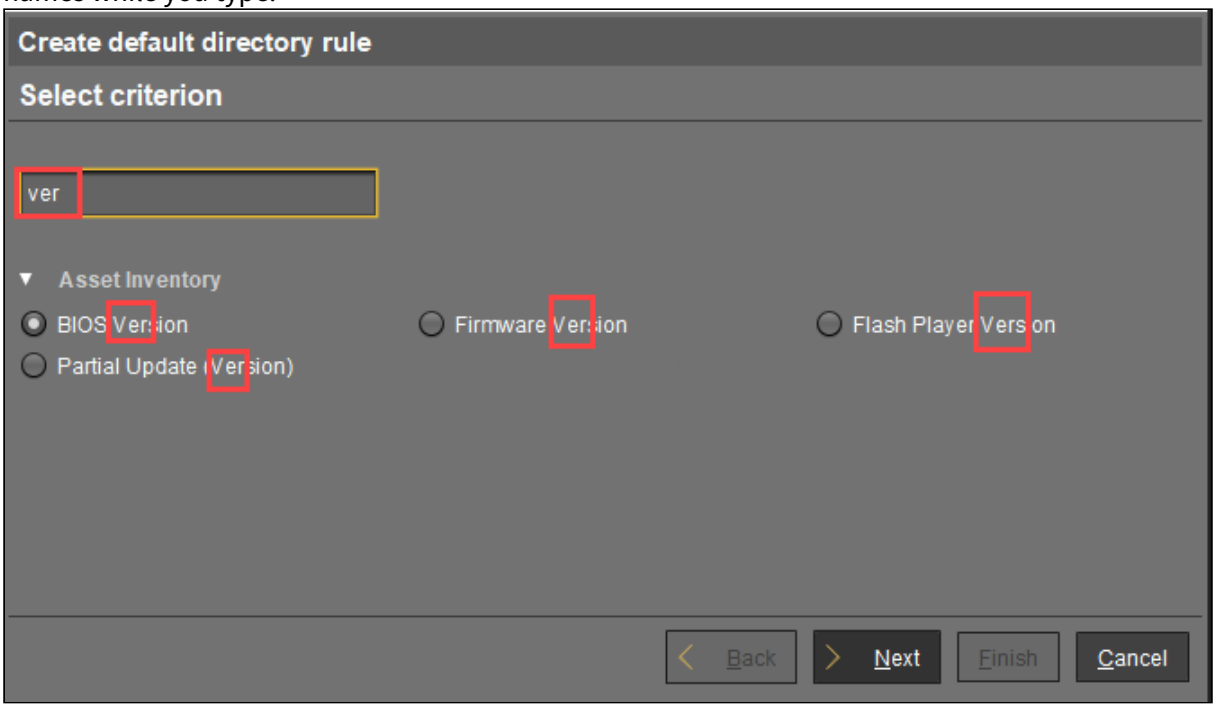
The symbols are as follows (in the correct order):

	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

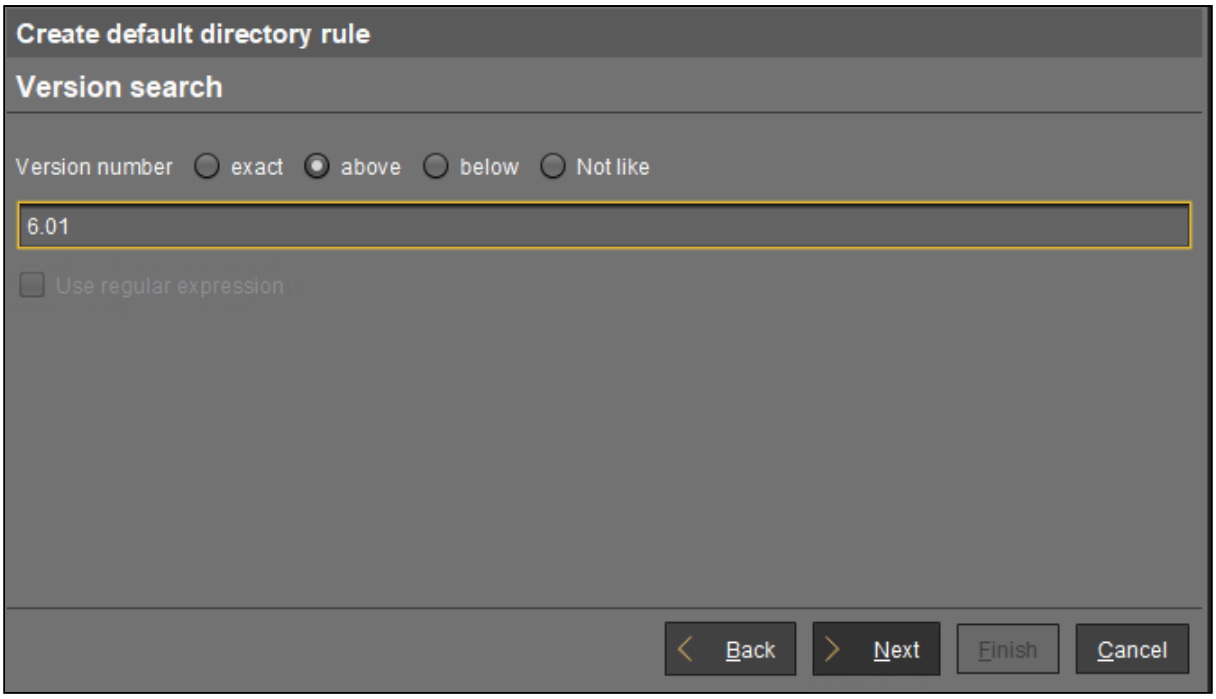
How to Create a Default Directory Rule

Menu path: **UMS Administration > Global Configuration > Default Directory Rules**

1. Click on the ⊕ symbol.
2. The **Create Default Directory Rule** dialog will open.
3. Select a **criterion**. To help you, a search field narrows down the selection to matching parameter names while you type.

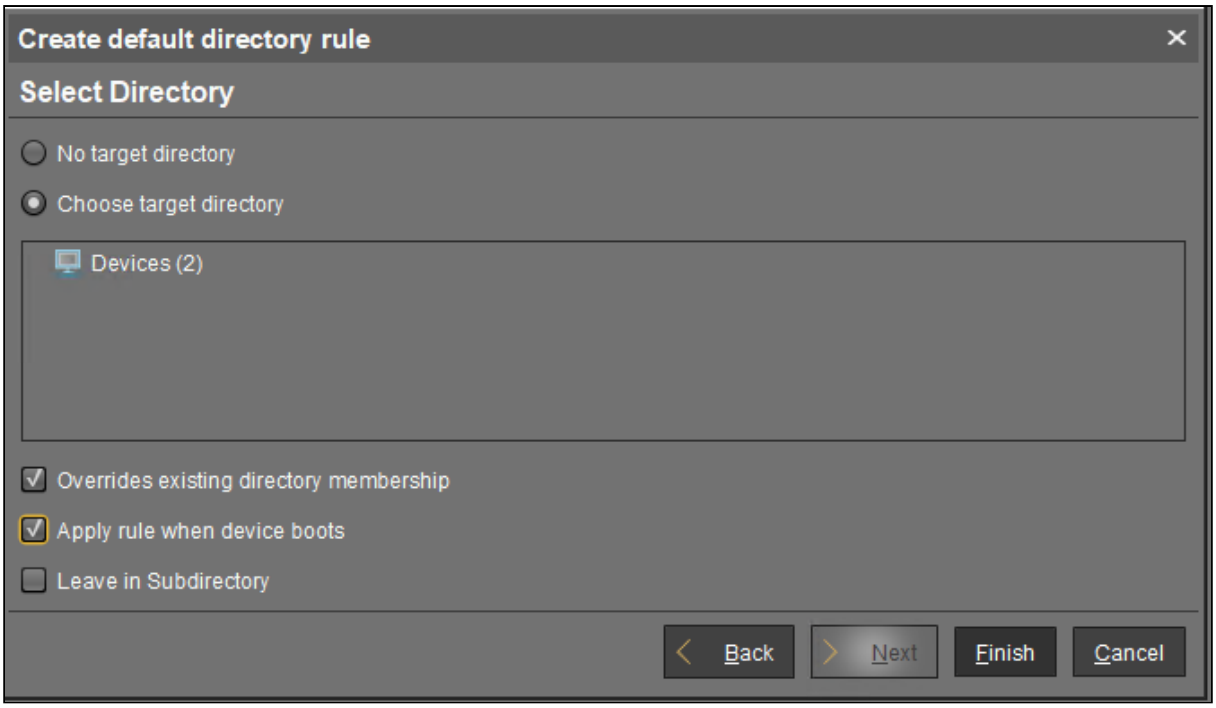


4. Specify the comparative value and comparative operator for the criterion.



If you create a rule which contains a range (from - to), this will automatically be converted into a pair of rules linked with AND (from AND to). This applies for example to date or IP ranges.

5. Select a target directory (must already exist) or select the **No target directory** option.
   With the **Choose target directory** option, you have the following further options:
   - **Overides existing directory membership**
     ☑ A previously registered device is re-registered in the target directory.
   - **Apply rule when device is booting**
     ☑ The rule is applied not only when registering but also each time the devices boot.
   - **Leave in Subdirectory**
     ☑ A device will not be moved if it is already in a subdirectory of the target directory.

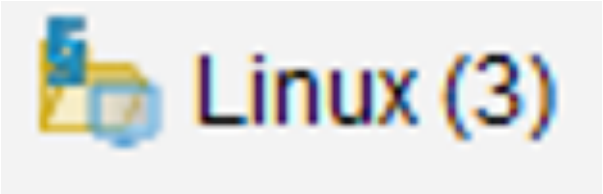


6. Finish creating the rule by clicking on **Finish**.

The order of the rules is important. Generally speaking, the default directory rules tree is worked through from top to bottom for each device. If the criterion of a rule applies and it has a target directory, its children rules will be scrutinized. If none of the children rules apply, the device will be moved to the target directory of the rule above. If however one of the children rules applies and it has a target directory, this child rule will be taken as a new starting rule and the search will begin again. If an applicable rule does not have a target directory, its children rules will be scrutinized.

Finding Default Directory Rules

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.

How to Apply Default Directory Rules

The rules can be applied regardless of new clients being imported or existing clients booting:

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.

Editing a Rule

→ In the rule overview, double-click on a row...

- in the **Rule** column in order to edit the **Criterion**, **Operator** and **Value**.
- in the **Directory** column in order to change or remove the target directory.
- in the **Overiding**, **Apply on boot** or **Leave in subdirectory** column in order to change these options (see page 971).

Combining Conditions

In the UMS, you can combine the conditions of directory rules using AND and OR links.

→ Indent a rule using → in order to create an AND link with the condition of the superordinate rule:

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.

Example: In the illustration, devices whose **product ID** contains `64bit` OR `W10` are moved to the `/devices/Windows/64bit/` directory.

> You can move rules and groups of rules using drag and drop or by copying and pasting with the help of the symbol bar.

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

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.

Menu path: **UMS Administration > Global Configuration > Universal Firmware Update**

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

⚠ Starting from UMS 12.04.100, the Apache FTP Library is used. In this library, implicit SSL is deactivated by default. As a result, FTP connections over implicit SSL are not supported.
For details, see: https://mina.apache.org/ftpserver-project/configuration_ssltls_support.html .

Host: Hostname of the server

Port: Port number. (Default: 21 for FTP and FTPS, 22 for SFTP)

User name: Name of the user

Password: User password

Directory: Path of the FTP server

ℹ 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:

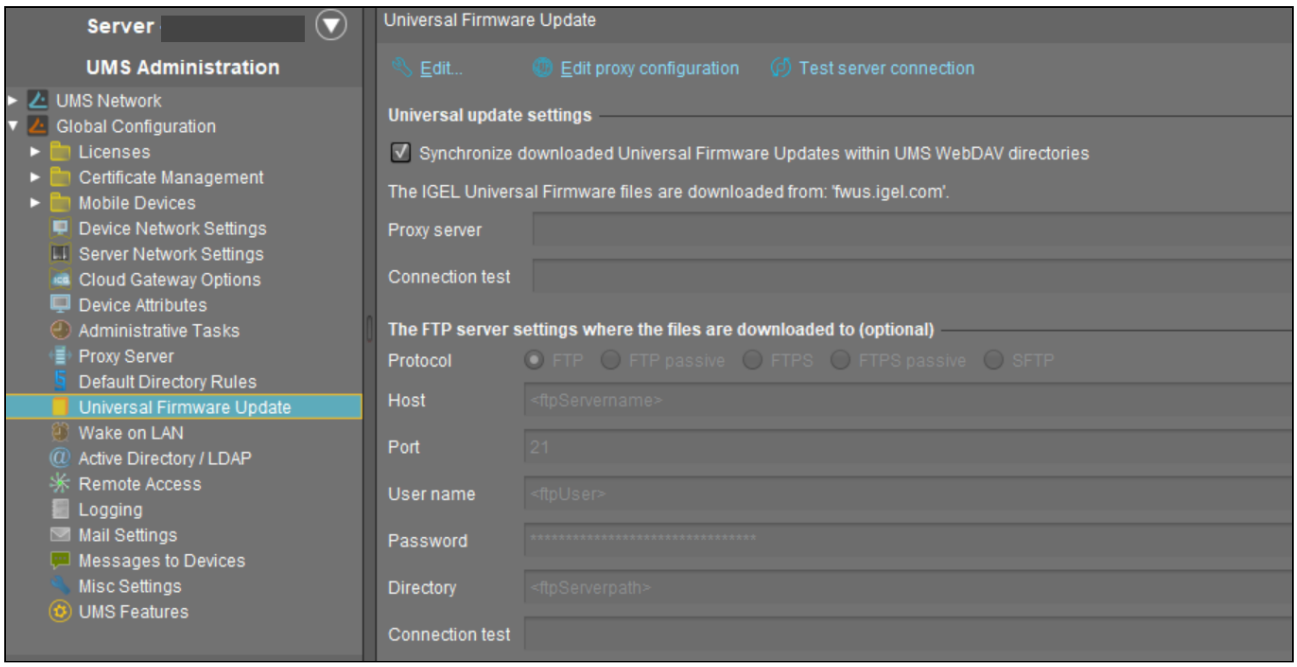
- **No proxy server**: Direct connection to the configured server.
- **Use default proxy server**: Use the proxy server which is configured as default in Proxy Server. (see page 967)
- **Use selected proxy server**: Select a proxy server from the list.

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? (see page 514).

☐ The Universal Firmware Updates are not synchronized between the HA servers.



Further information regarding the Universal Firmware Update can be found under Universal Firmware Update in the IGEL UMS (see page 856).

Wake on LAN Configuration in the IGEL UMS

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 IGEL 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. For details, see the articles under How to Deploy a Wake on LAN Proxy for Distributed Environments in IGEL (see page 506) .

> To use the feature, you need to use UMS version 5.02.100 or higher and devices running IGEL OS version 5.09.100 or higher.
> To use the feature with IGEL OS 12 devices, you need to use UMS version 12.06.100 or higher and IGEL OS version 12.5.1 or higher.

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.

   > 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.

> 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 in the IGEL UMS

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**.

Menu path: **UMS Administration > Global Configuration > Active Directory / LDAP**

For detailed instructions see the articles under How to Integrate Active Directory in IGEL UMS (see page 600).

Remote Access Configuration in IGEL UMS

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)

> **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 814) 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 the IGEL UMS

In this area, you can specify the logging behavior of the IGEL Universal Management Suite (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 (see page 1353).

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.

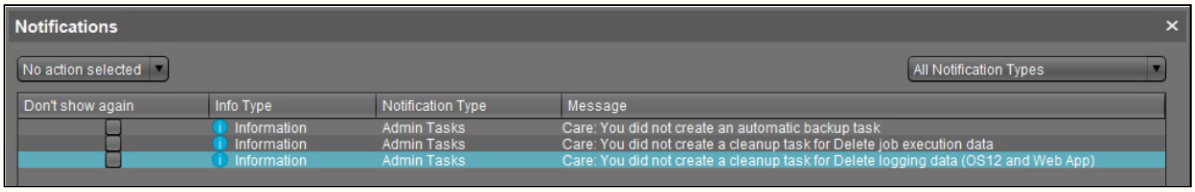
☐ Actions initiated by a device will not be logged.

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 for deleting logging data, the following notification pop-up will be shown after the start of the UMS Console.



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 990).

☐ 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 1032).

☐ The monitoring is disabled. (Default)
In the case of High Availability (see page 1387) 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

> 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:

- How to Send a View as Mail in the IGEL UMS (see page 844)
- Export view result as mail (see page 944)
- Export results of the following administrative tasks as mail:
  - Database backup (only for embedded DB) (see page 922)
  - Remove unused firmwares (see page 925)
  - Delete logging data (see page 928)
  - Delete job execution data (see page 932)
  - Delete Devices as an Administrative Task in the IGEL UMS (see page 941)
  - How to Assign Objects to a View in the IGEL UMS (see page 846)
- Mailing of one-off passwords for IGEL Cloud Gateway (ICG)
  If you would like to use Gmail for sending mails, see How to Configure the IGEL UMS to Send Emails via Gmail (see page 648).

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.

> 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 804).

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 in IGEL UMS

This article describes the parameters under **Misc Settings** in the IGEL Universal Management Suite (UMS).

Menu path: **UMS Administration > Global Configuration > Misc Settings**

User Login History

Enable user login history

☑ Recording of the user login activity is enabled. (Default)

> Events are only logged if the **Log login and logoff events** parameter under **System > Remote management > Options** is enabled for the device (for example, via profile).

Add last device users to quick search

☑ The user who logged in last will be added.

Add only still logged-in users

☑ Only users who are currently logged in will be added. (Default)

> In the event of configuration changes, the page will need to be reloaded by clicking on  in order for the settings to be applied.

> 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 778).
> - 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 (see page 1176).

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 (see page 640).

☐ 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.

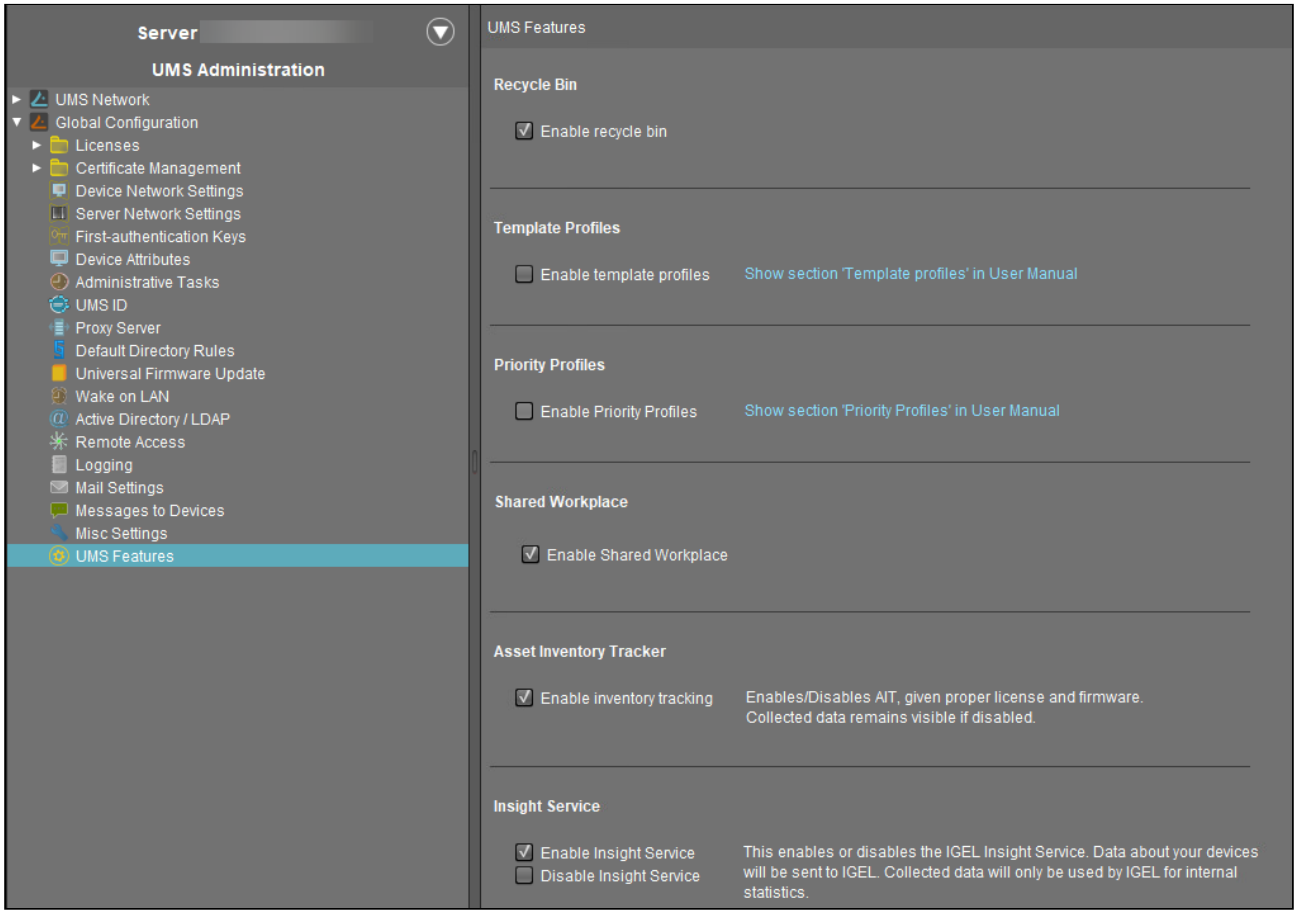
A notification will be created when the free disk space is below [...] GB: When the free disk space is below this value, a warning will be created.

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 Feature**



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)

> 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 864).

Template Profiles

Enable template profiles

☑ Template profiles are enabled. For information on template profiles, see Template Profiles in the IGEL UMS (see page 746).

☐ 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 744).

☐ Priority profiles are disabled. (Default)

Shared Workplace

Enable Shared Workplace

☑ IGEL Shared Workplace (SWP) (see page 817) is enabled. (Default)

Licensed Feature

This feature requires a valid license from the IGEL Enterprise Management Pack.

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

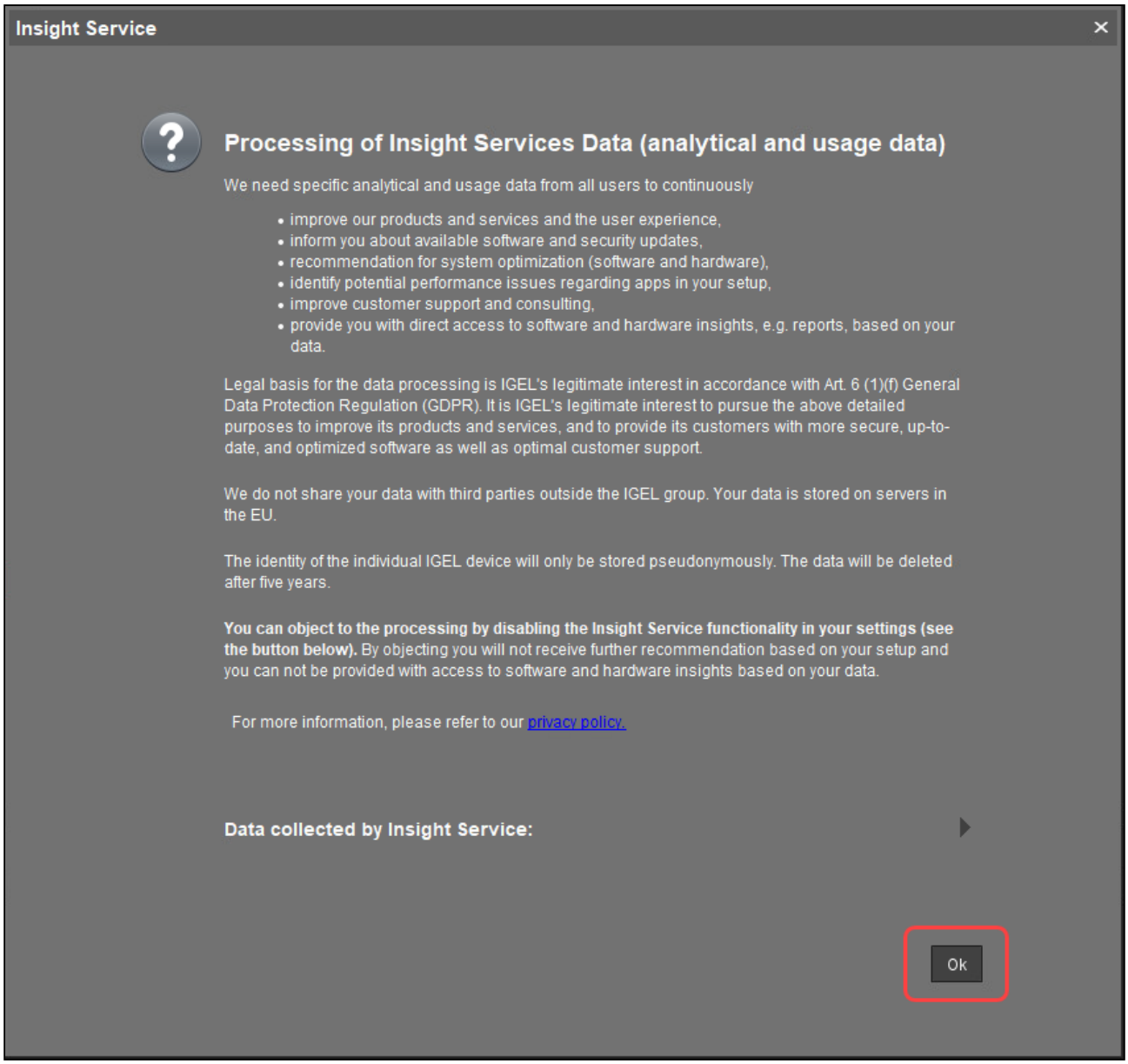
Enable inventory tracking

☑ Inventory tracking (see page 781) is enabled. (Default)

Insight Service

Enable Insight Service

☑ Enables IGEL Insight Service if you accept the privacy policy in the consent dialog by clicking **Ok**. When you activate the IGEL Insight Service, IGEL collects specific analytical and usage data listed under **Data collected by Insight Service**. For details, see (en) IGEL Insight Service .



Disable Insight Service

☑ Disables IGEL Insight Service.

Consent text

Click to display the content of the consent dialog.

Identity Provider Configuration in IGEL UMS

You need to configure the Identity Provider (IdP) client and map IdP roles to user groups to enable Single Sign-On (SSO) for your IGEL Universal Management Suite (UMS). This article helps with configuring an IdP client using the IGEL UMS Console.

You can also configure the IdP client in the IGEL UMS Web App, see How to Configure an Identity Provider Client in the IGEL UMS Web App (see page 1373) .

Prerequisites

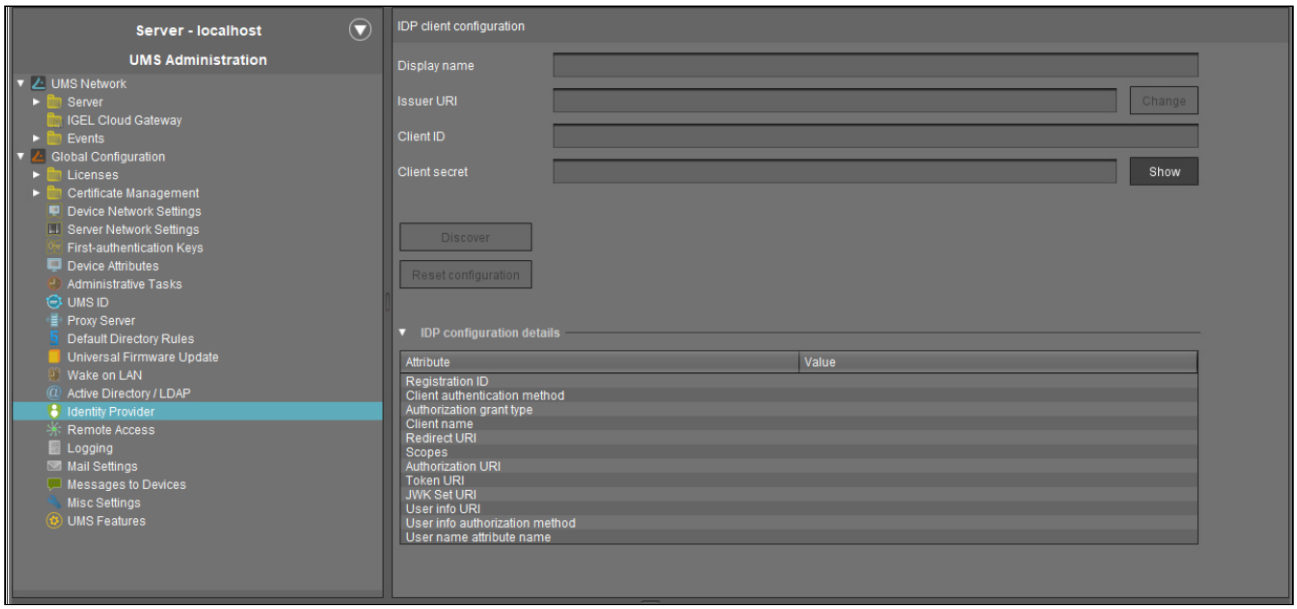
- You need to have an application configured for the IGEL UMS in your IdP. For details, see How to Set Up UMS Login with SSO (see page 139) .

Permission Requirement

- The **Identity Provider** node is read-only for users with read permission for the node. It is only editable for users with write permission for the **Identity Provider** node. The permission can be set through the UMS Console structure tree. For details, see Access Rights in the Administration Area (see page 1022) .

Configuring the IdP Cient

1. In the UMS Console go to **UMS Administration > Global Configuration > Identity Provider.**



2. Enter the details to configure the IdP client:

- **Display name**: The name of your IdP client configuration, that will be displayed in UMS (e.g., “Okta SSO” or “Ping Configuration”).
- **Issuer URI**: The URL provided by your IdP (e.g. “https://auth.pingone.eu/…”).
- **Client ID**: The Client ID provided by your IdP.

- **Client secret**: The secret key provided when you registered your application with the IdP. Click **Show** to toggle visibility if needed.

3. After filling in all fields, click **Discover** to save the configuration and create the connection with the IdP.

- If the discovery is successful, the discovery data gets added to the **IdP configuration details** collapsible list.
- If an error occurs during the discovery process, an alert dialog is shown and the form is reset and configuration is deleted.

After the client is configured, you can map IdP roles to users and user groups either in the UMS Console or in the UMS Web App, see Administrator Accounts in the IGEL UMS (see page 1007) or How to Map Identity Provider Roles in the IGEL UMS Web App (see page 1376) .

4. You can click **Reset configuration** to clear the data and start over.

⚠ All users who log in through the configured IdP will not be able to access the UMS after the reset.

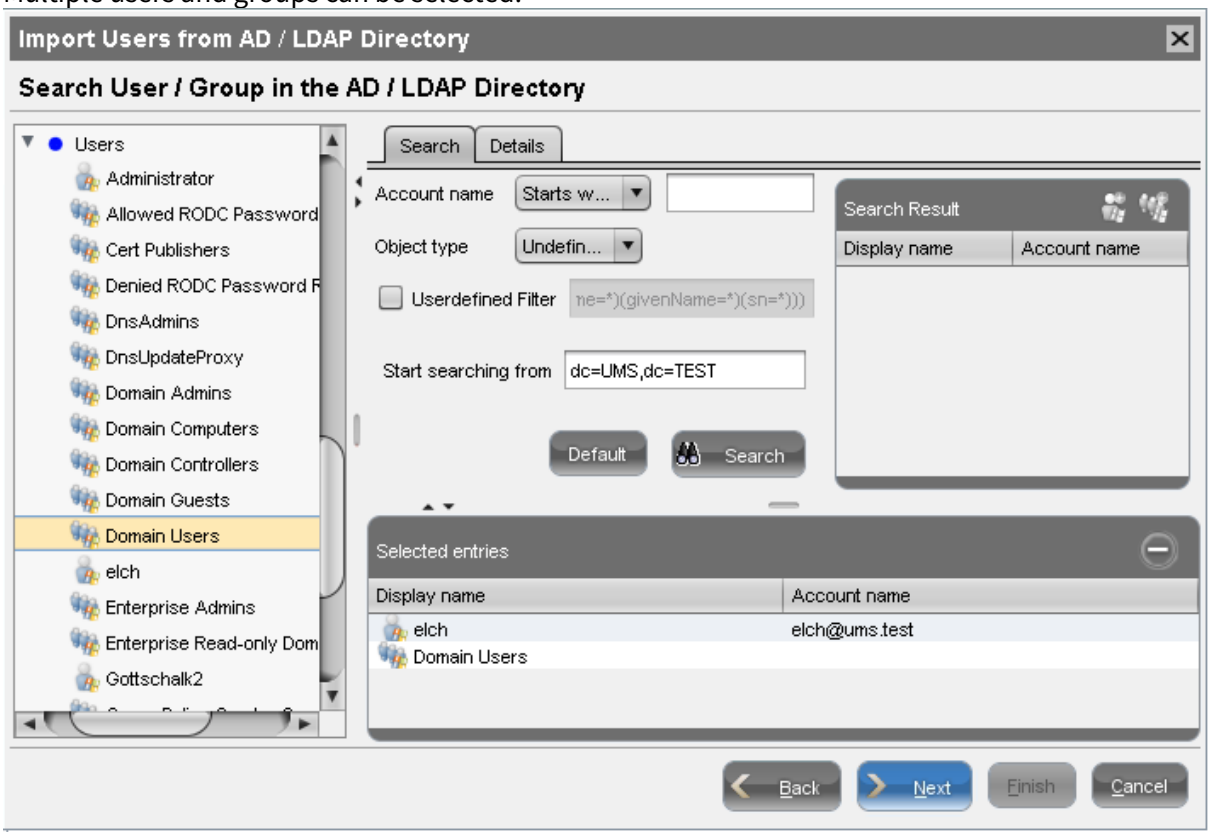
Importing Active Directory Users

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 984). When importing user accounts, only connected ADs are available for selection.
3. Click on **Continue**.
   The Active Directory browser will open.
4. Select individual users or groups from the navigation tree of your AD.
   The highlighted users/groups can be added to or removed from the selection to be imported via the context menu or using drag and drop. The users/groups found in the **Found AD Accounts** hit list can be transferred to the **Selected Accounts** list using the symbols.
   Multiple users and groups can be selected.



As an alternative to navigating in the navigation tree, you can also highlight and add users or groups to the selection via the **Search** function.

5. Click on **Continue** to start the import.
   A confirmation window will appear.

Once a user has been successfully imported, this action cannot be undone. A UMS administrator set up by mistake must be deleted manually via the administrator account management system. The *IGEL* UMS uses the **account** as the name of the AD user imported.

Searching in the Active Directory

The options in the AD navigation tree have the following meanings:

Account name: Allows you to search on the basis of account names of parts thereof

Object type: Allows you to restrict a search to users or groups

User-defined filter: Filter criteria in accordance with the RFC-2254 standard

Start searching from	Element within the tree where the search begins
Default	Resets all search options to the standard values
Search	Starts the specified search

The context menu allows the following actions to be performed on items in the list of hits:

- **Add user**
- **Add group**
- **Start searching from**
- **Details...**

Under **Details**, you can once again bring up the properties of the objects selected for import and remove objects prior to the import if necessary.

Import Results List

Once the import is complete, a results window will appear.

This shows how many accounts were ignored during the import and which ones were imported successfully. If a user account already exists in the UMS, this AD account will be skipped during the import.

Administrator Accounts in the IGEL UMS

To access the UMS Console / UMS Web App (see page 661), you can create and manage administrator accounts in the IGEL UMS or you can import UMS administrator accounts from a linked Active Directory. You can also create user groups for easier management.

In the IGEL UMS Web App, you can do the same in the **User Management** area, see User Management and IdP Management in the IGEL UMS Web App (see page 1362) .

Menu path: Menu bar **> System > Administrator accounts**

Access rights to objects, actions and features within the IGEL UMS are attached to the administrator accounts and user groups through permissions. The matrix of these permissions create the effective rights of a user, see Effective Rights in IGEL UMS (see page 1010) .

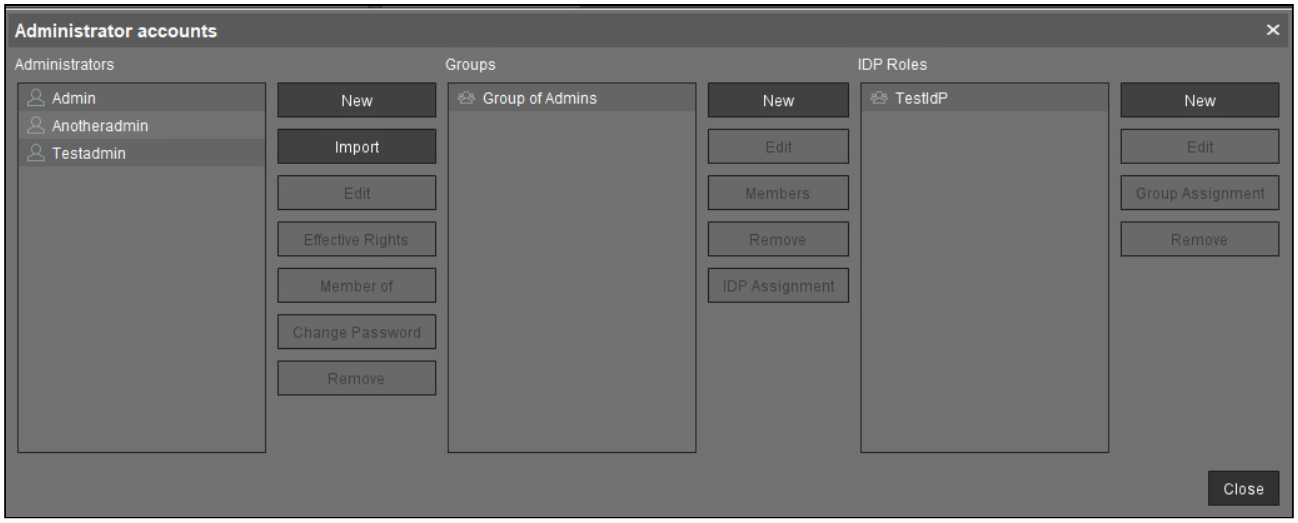
The rights of the UMS superuser that was created during the installation (see IGEL UMS Installation under Linux (see page 17) or IGEL UMS Installation under Windows (see page 48)) cannot be restricted. The UMS superuser always has full access rights in the UMS.

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 (see page 1155).

Administrator Accounts Dialog

To manage the IGEL UMS administrator accounts go to **System > Administrator accounts** in the menu bar.



The administrator accounts dialog is organised in columns:

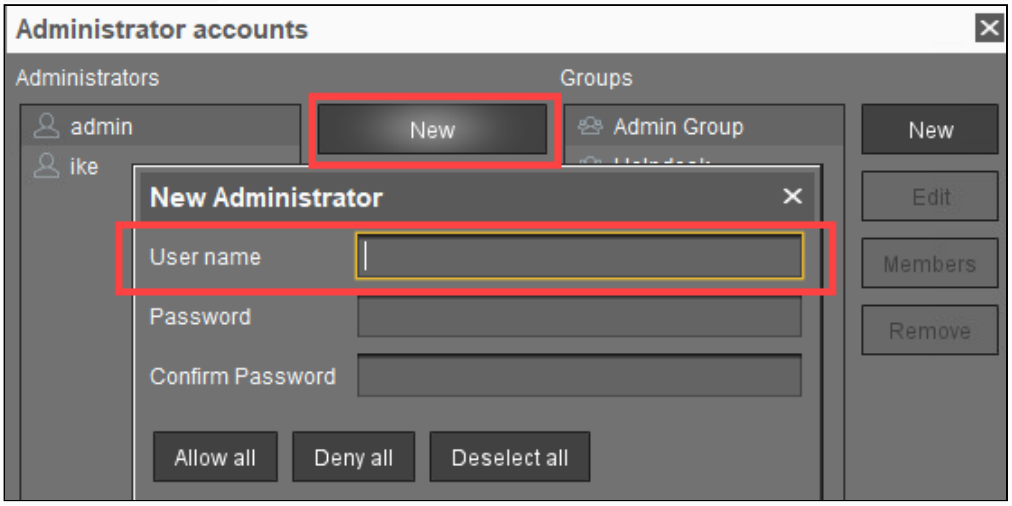
- All user accounts are listed in the left-hand column under **Administrators**.
- All configured groups are listed under **Groups**.
- All configured IdP roles are listed under **IDP Roles**.

Options to Manage Administrator Accounts

To the right of each column, you will find the associated options.

- Click **New** to create a new administrator a new group or a new IdP role. For more on IdP roles, see How to Map Identity Provider Roles in the IGEL UMS Web App (see page 1376) .

The following characters are not allowed for user names of UMS administrators: `"/ \ [ ] : ; | = , + * ? < >`

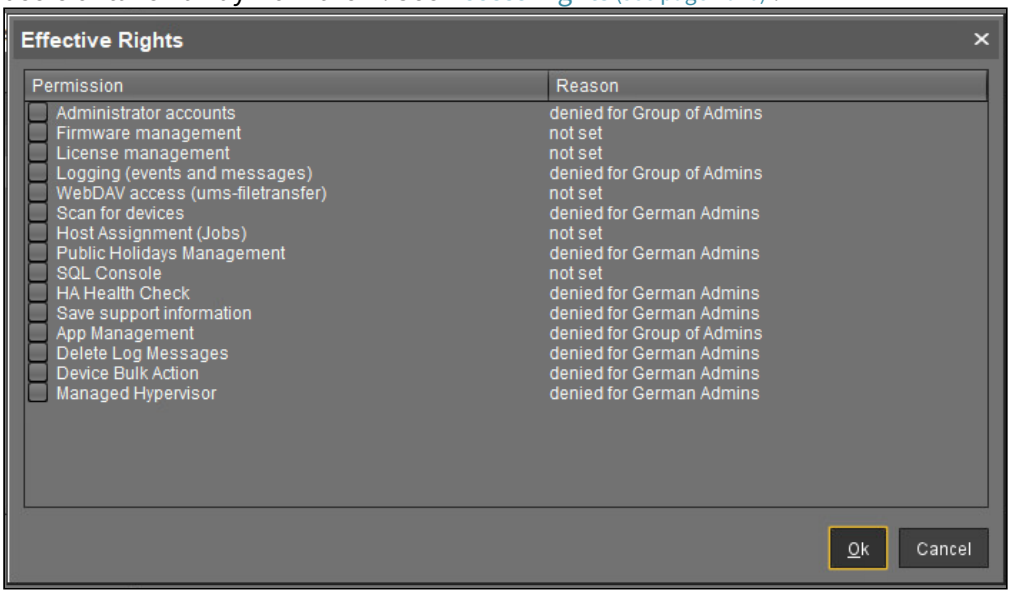


- Click **Import** to import a user from the AD/LDAP directory.
  - **Domain**: Domain in which the AD/LDAP service runs
  - **User**: Name of the user
  - **Password**: Password of the user

This procedure requires an AD/LDAP connection. For further details, see Importing Active Directory users (see page 1003).

- Click **Edit** to edit the selected user, group, or role.
- Click **Remove** to delete the selected entry.
- Click **Change Password** to change the password of user accounts.
- Click **Member of** to show group memberships of the selected user.
- Click **Members** to see details on the members who make up a selected group.

- Click **Effective Rights** to get an insight into the rights that were directly or indirectly granted to users or taken away from them. See Access Rights (see page 1010) .



- Click **IDP Assignment** to assign IdP roles to groups.
- Click **Group Assignment** to assign groups to IdP roles.

Effective Rights in IGEL UMS

The effective rights of a user in the IGEL UMS are the result of:

- General rights which can be granted /denied through permissions to a user directly, or indirectly through group membership, see General Administrator Rights in IGEL UMS (see page 1013) .
- Access rights to objects in the structure tree, see Object-Related Access Rights (see page 1016).
- Access rights to the nodes within the UMS Administration area of the UMS Console, see Access Rights in the Administration Area (see page 1022).

Since the same permission settings are used for individual administrators and groups, the description of the configuration of right applies equally to administrators and groups.

Permission Precedence

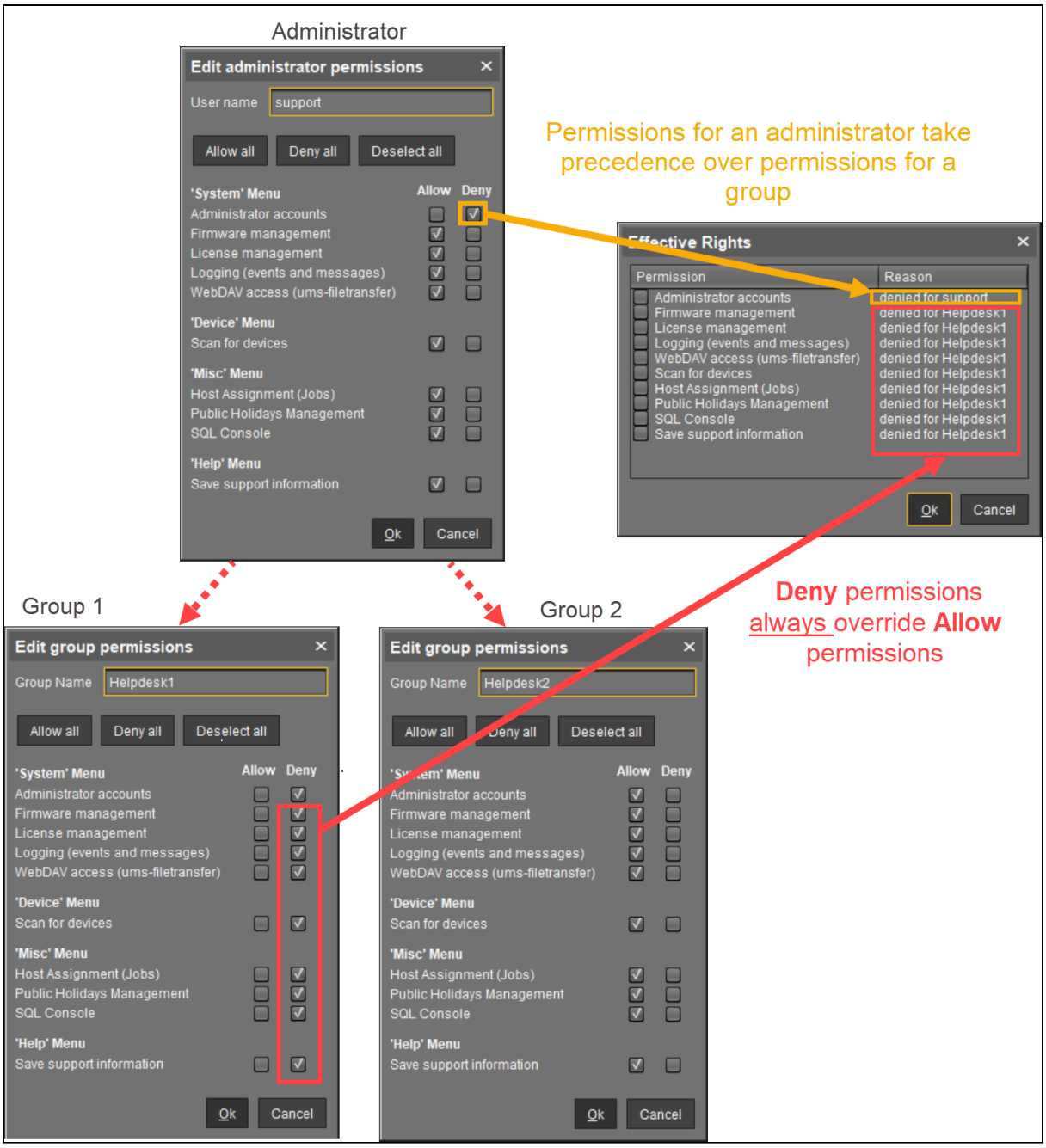
The indirect rights given to an administrator on the basis of their group membership can be changed further for each administrator in the group, keeping the following in mind:

- Permissions that were granted directly have precedence over those granted indirectly.
- The withdrawal of permissions always overrides the granting of permissions.

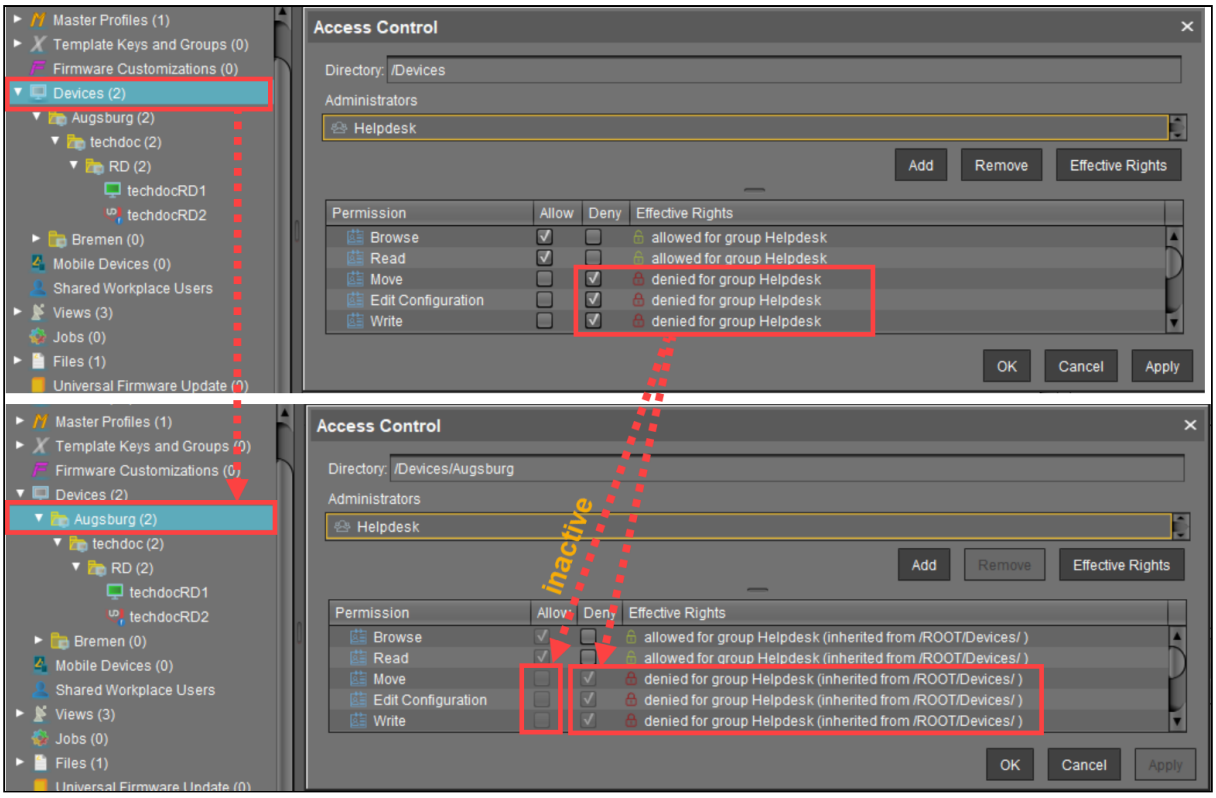
Examples

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.



- 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.


Master Profiles (1)
Template Keys and Groups (0)
Firmware Customizations (0)
Devices (2)
Augsburg (2)
techdoc (2)
RD (2)
techdocRD1
techdocRD2
Bremen (0)
Mobile Devices (0)
Shared Workplace Users
Views (3)
Jobs (0)
Files (1)
Universal Firmware Update (0)
Access Control
Directory: /Devices
Administrators
Helpdesk
Add
Remove
Effective Rights
Permission
Allow
Deny
Effective Rights
Browse
Read
Move
Edit Configuration
Write
allowed for group Helpdesk
denied for group Helpdesk
OK
Cancel
Apply
Directory: /Devices/Augsburg
inactive
allowed for group Helpdesk (inherited from /ROOT/Devices/)
denied for group Helpdesk (inherited from /ROOT/Devices/)

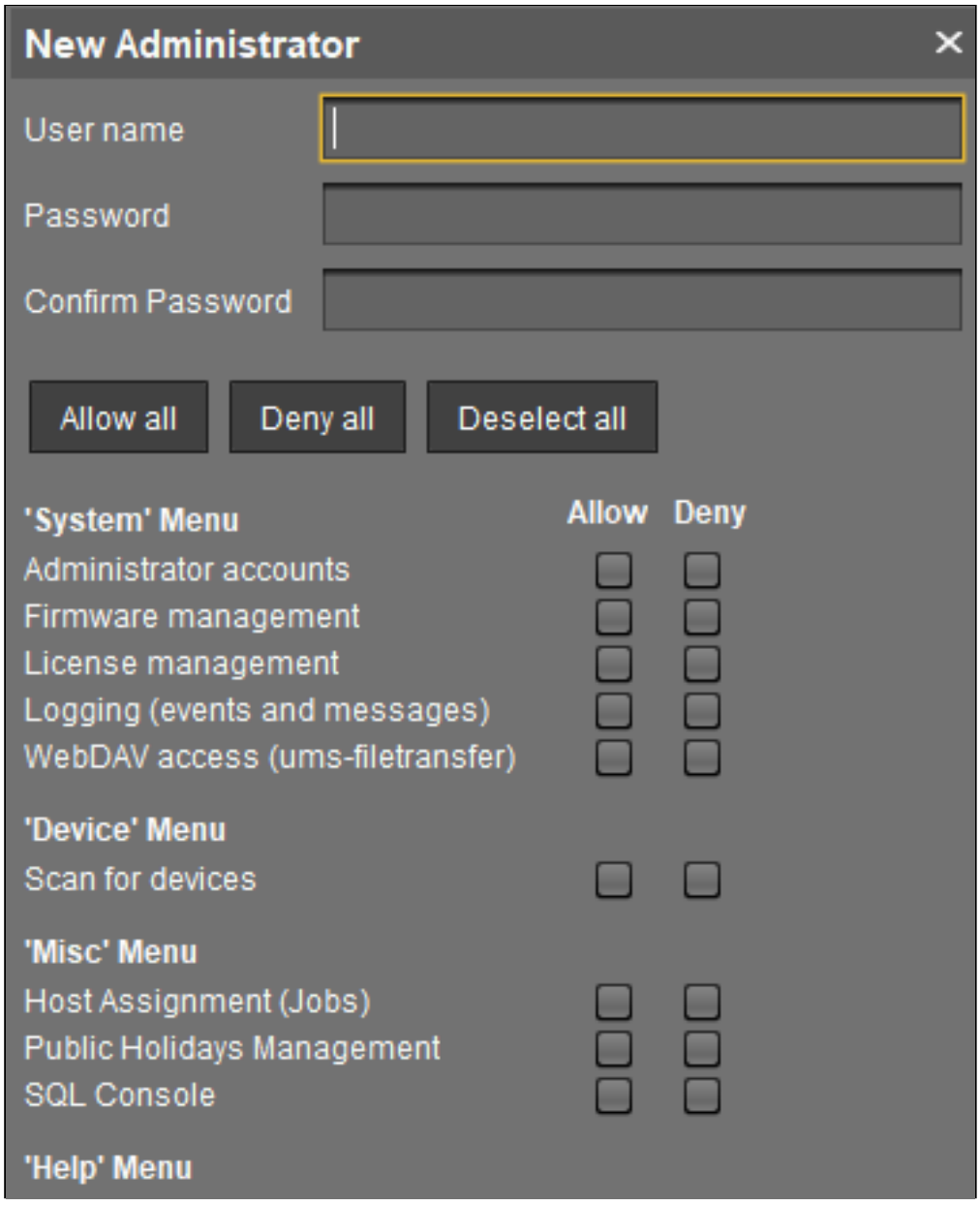
General Administrator Rights in IGEL UMS

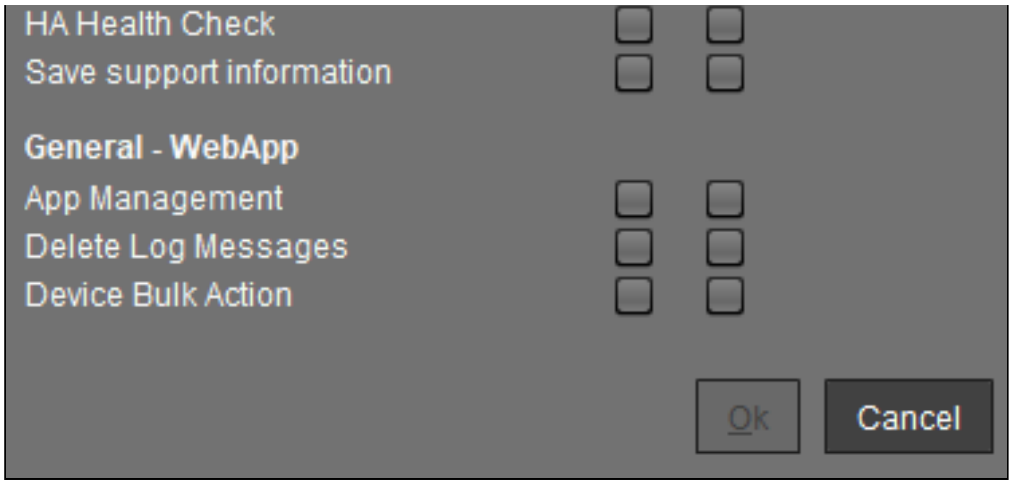
An administrator can grant others general administrator rights and take away those rights through permission assignment in the IGEL Universal Management Suite (UMS). These permissions are called administrator permissions or global permissions.

This article describes permission management in the UMS Console. For details on how to manage permissions in the UMS Web App, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .

Menu path: Menu bar **> System > Administrator accounts**

Below, you will find a list of permissions that can be given to individual administrators or groups under **System > Administrator accounts > New** or **Edit**. Each permission has three possible states: not set, **Allow** or **Deny**.





'System' Menu

Administrator accounts

☑ The management of permissions can be performed: administrators and groups, as well as their rights, can be added and edited.

Administrator accounts permission should only be granted to users who are to have full access to all objects and actions in the UMS!

Firmware management

☑ Firmware versions can be imported, exported, and removed from the database.

License management

☑ IGEL firmware licenses can be allocated to devices.

Logging (events and messages)

☑ The event and message log may be viewed if **Logging** is enabled.

WebDAV access (ums-filetransfer)

☑ The user is authorized to add, modify, and delete files in the directory `/ums_filetransfer/`.

'Devices' Menu

Scan for devices

☑ The network can be scanned for devices, for example, if they are to be registered on the UMS Server.

'Misc' Menu

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** (see page 1420) 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.

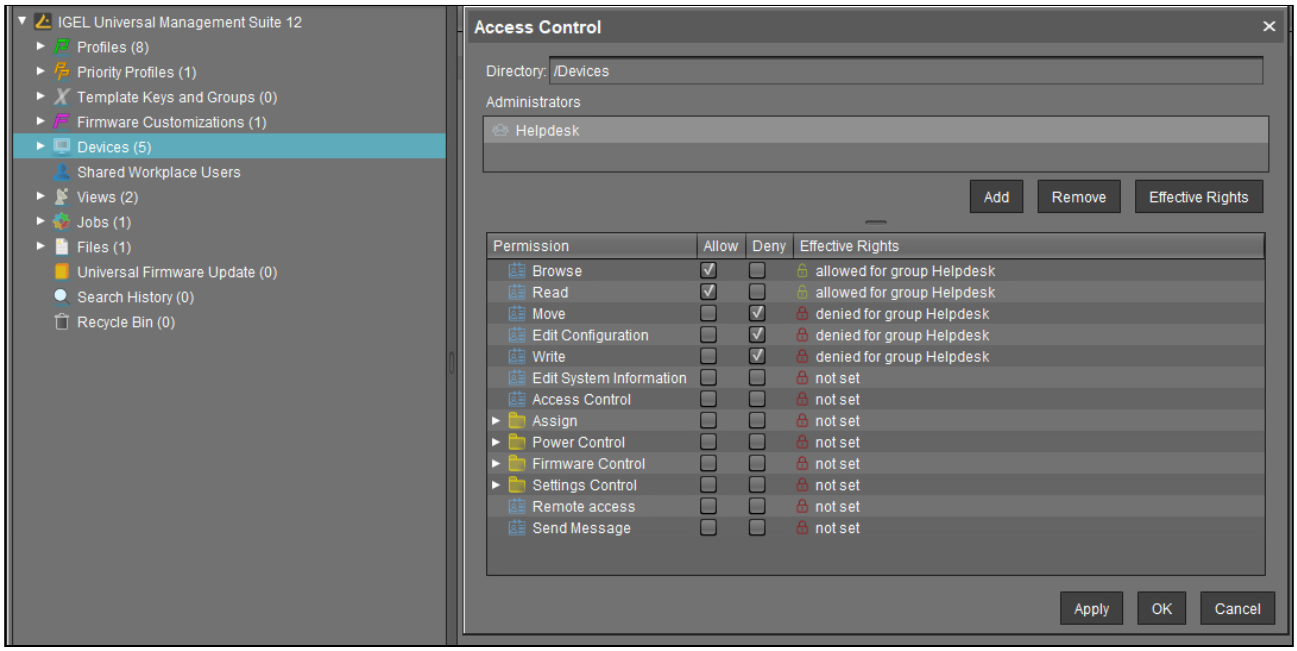
⚠ This only applies to the UMS Web App; bulk actions can still be performed from the UMS Console.

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**

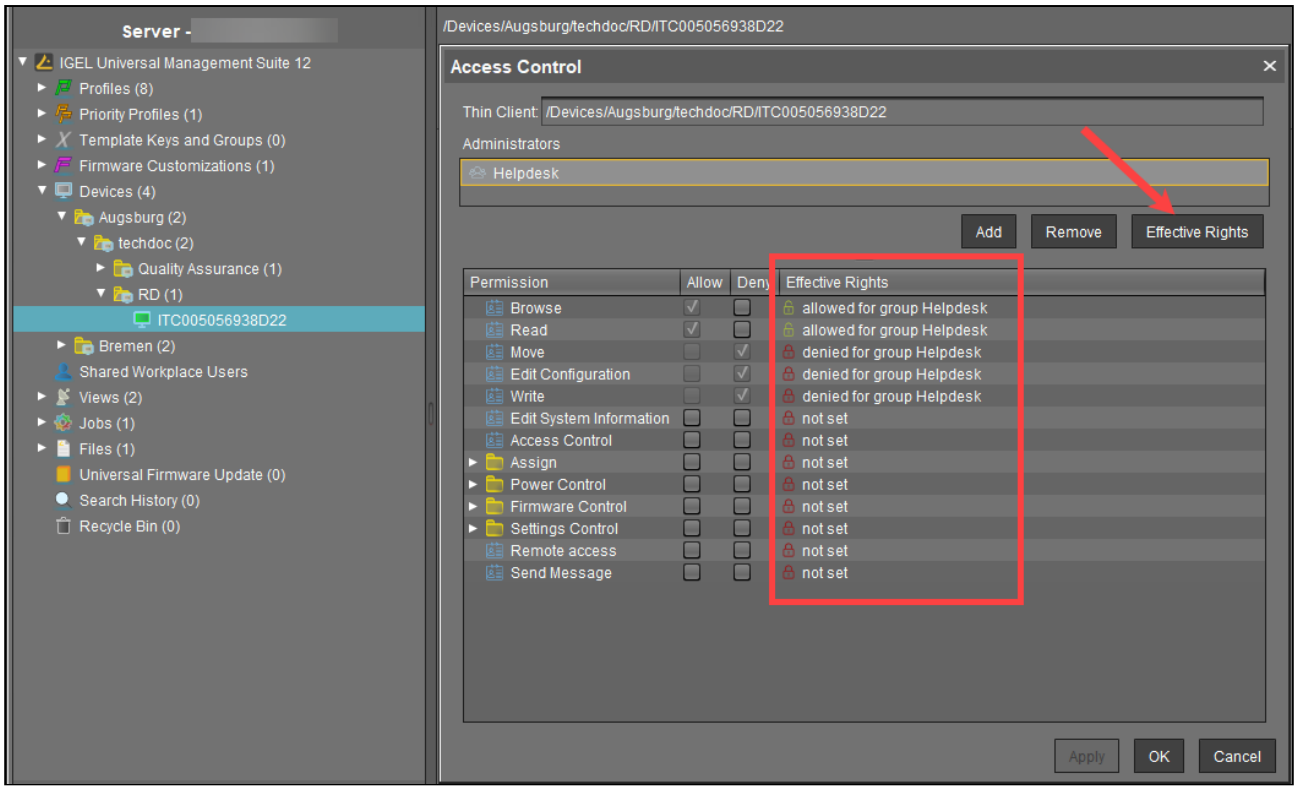


The above list contains all object-related permissions available in the UMS structure tree. Only one selection is available for each selected object. For example, a view cannot be assigned updates and cannot be shut down.

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.


Server -
IGEL Universal Management Suite 12
Profiles (8)
Priority Profiles (1)
Template Keys and Groups (0)
Firmware Customizations (1)
Devices (4)
Augsburg (2)
techdoc (2)
Quality Assurance (1)
RD (1)
ITC005056938D22
Bremen (2)
Shared Workplace Users
Views (2)
Jobs (1)
Files (1)
Universal Firmware Update (0)
Search History (0)
Recycle Bin (0)
/Devices/Augsburg/techdoc/RD/ITC005056938D22
Access Control
Thin Client: /Devices/Augsburg/techdoc/RD/ITC005056938D22
Administrators
Helpdesk
Add
Remove
Effective Rights
Permission
Allow
Deny
Effective Rights
Browse
allowed for group Helpdesk
Read
allowed for group Helpdesk
Move
denied for group Helpdesk
Edit Configuration
denied for group Helpdesk
Write
denied for group Helpdesk
Edit System Information
not set
Access Control
not set
Assign
not set
Power Control
not set
Firmware Control
not set
Settings Control
not set
Remote access
not set
Send Message
not set
Apply
OK
Cancel

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:

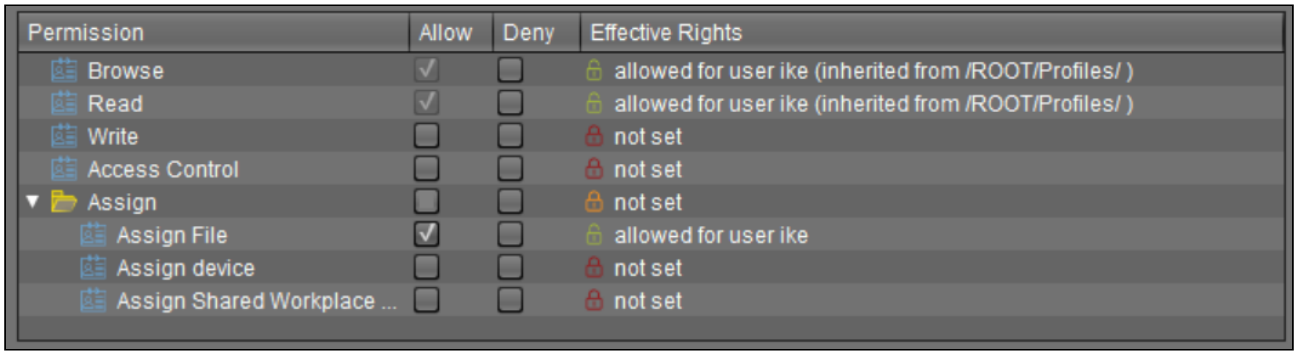
- **Browse**
- **Read**
- **Assign** on both sides

> **Write** permission is not required directly for the assignment of objects.

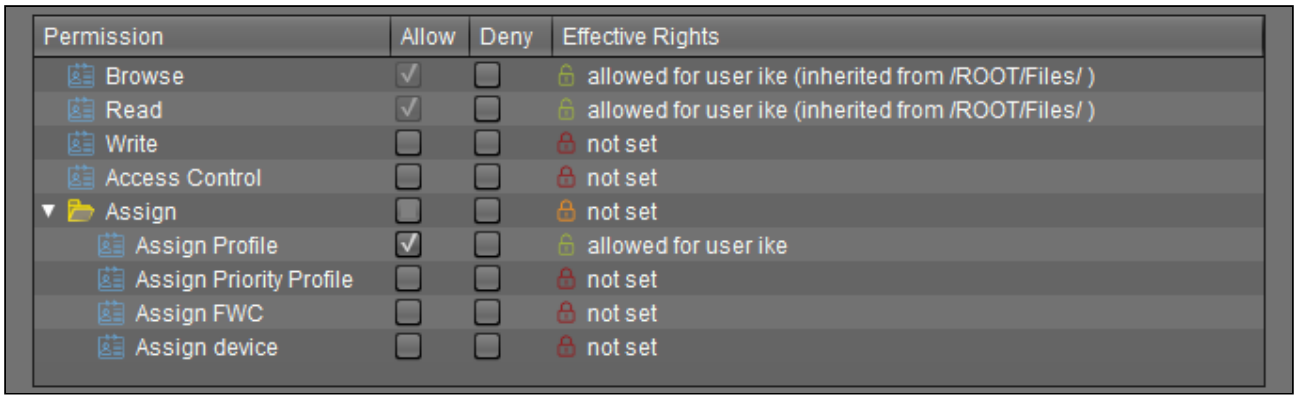
Example 1: Assigning a File to a Profile

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



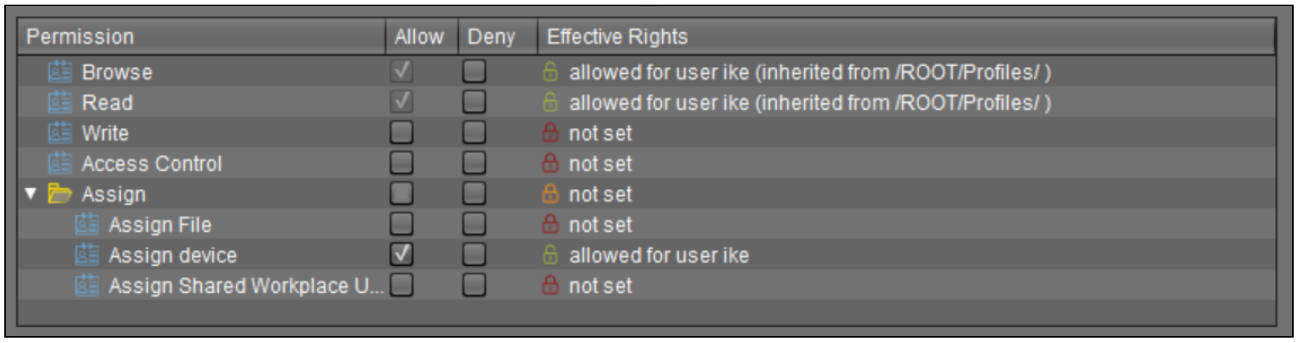
Permissions on the File



Example 2: Assigning a Device to a Profile

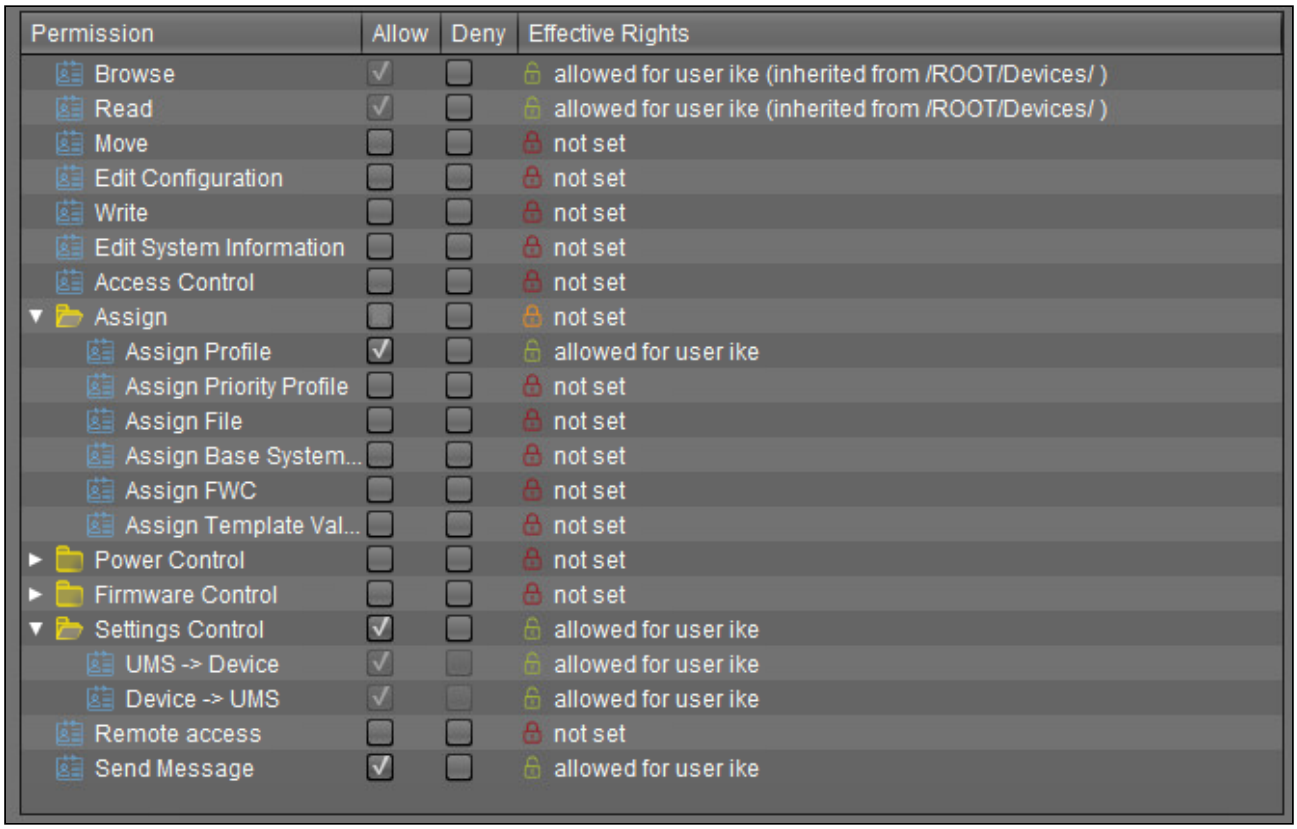
A user can only assign a device to a profile or delete this assignment. He cannot make any changes to the device or profile, i.e. he cannot rename, delete the device or profile, or edit their configuration.

Permissions on the Profile



Permission	Allow	Deny	Effective Rights
Browse	☑	☐	allowed for user ike (inherited from /ROOT/Profiles/)
Read	☑	☐	allowed for user ike (inherited from /ROOT/Profiles/)
Write	☐	☐	not set
Access Control	☐	☐	not set
▼ Assign	☐	☐	not set
Assign File	☐	☐	not set
Assign device	☑	☐	allowed for user ike
Assign Shared Workplace U...	☐	☐	not set

Permissions on the Device



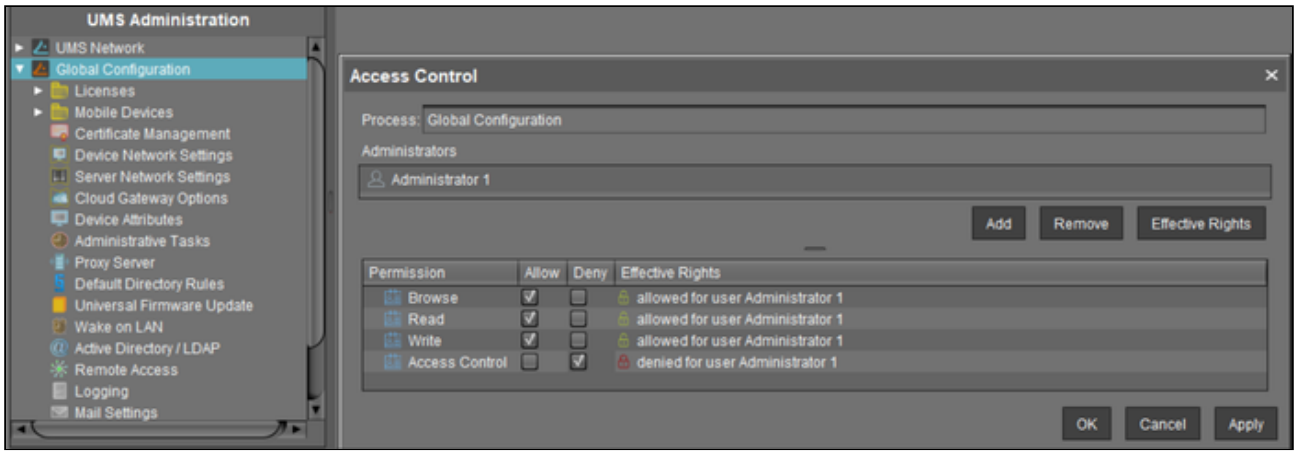
Permission	Allow	Deny	Effective Rights
Browse	☑	☐	allowed for user ike (inherited from /ROOT/Devices/)
Read	☑	☐	allowed for user ike (inherited from /ROOT/Devices/)
Move	☐	☐	not set
Edit Configuration	☐	☐	not set
Write	☐	☐	not set
Edit System Information	☐	☐	not set
Access Control	☐	☐	not set
▼ Assign	☐	☐	not set
Assign Profile	☑	☐	allowed for user ike
Assign Priority Profile	☐	☐	not set
Assign File	☐	☐	not set
Assign Base System...	☐	☐	not set
Assign FWC	☐	☐	not set
Assign Template Val...	☐	☐	not set
▶ Power Control	☐	☐	not set
▶ Firmware Control	☐	☐	not set
▼ Settings Control	☑	☐	allowed for user ike
UMS -> Device	☑	☐	allowed for user ike
Device -> UMS	☑	☐	allowed for user ike
Remote access	☐	☐	not set
Send Message	☑	☐	allowed for user ike

Access Rights in the Administration Area

In the **UMS Administration** area of the UMS Console, you can grant or deny general rights **Browse**, **Read**, and **Write**, as well as **Access Control** for administrator accounts. Permissions should only be granted to users who will actually perform administrative tasks on the UMS.

You can change the permission settings after selecting a tree node in the following ways:

- via **Access control** in the context menu
- via the **Access control** symbol in the symbol bar
- via the menu item **Edit > Access control**



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	

User Logs in the IGEL UMS

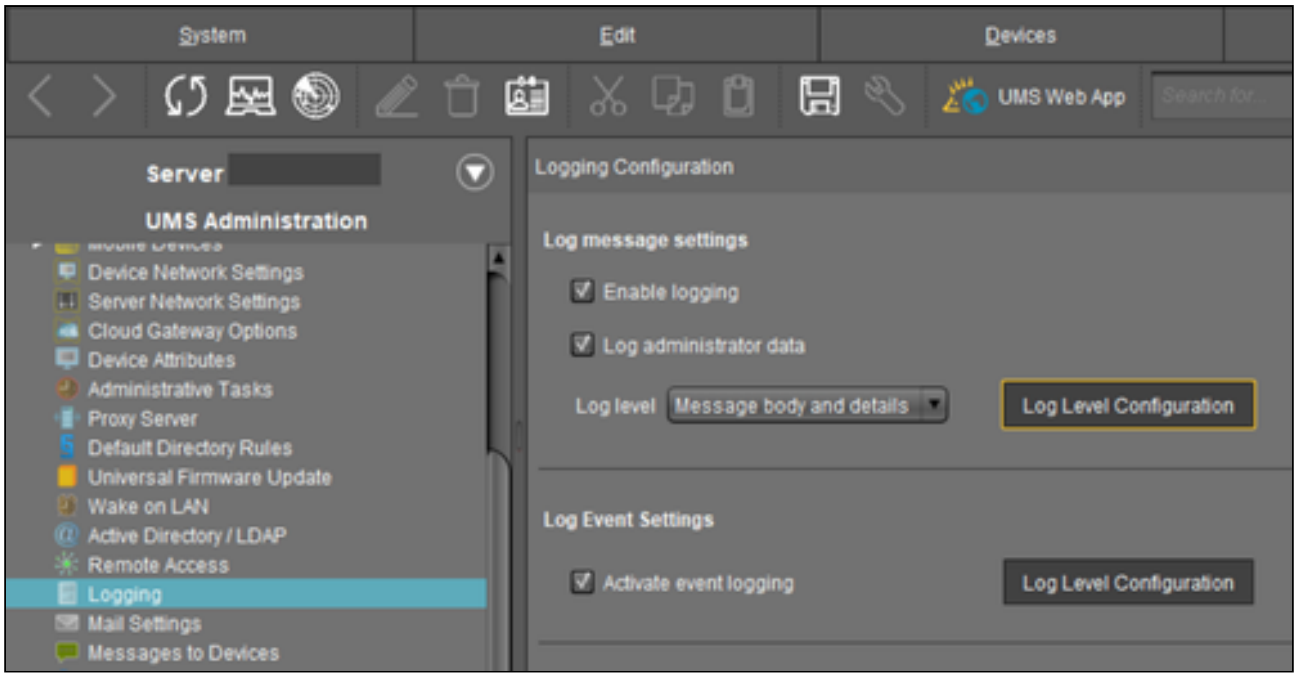
The logging system is used by the UMS and the registered devices in order to record all changes to the database. Only successful actions are logged. You will not find details of any errors in the log file of the UMS GUI Server.

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 987).



- **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

---

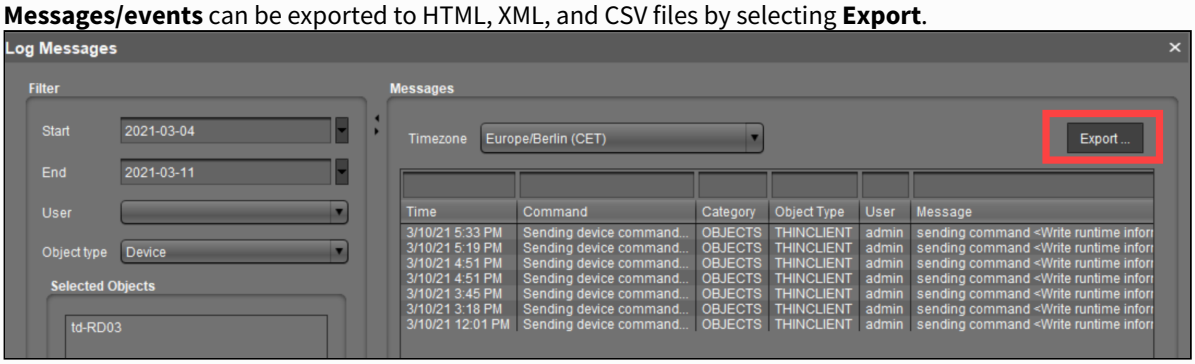
- Logging Dialog Window: Setting a Filter (see page 1026)

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**.

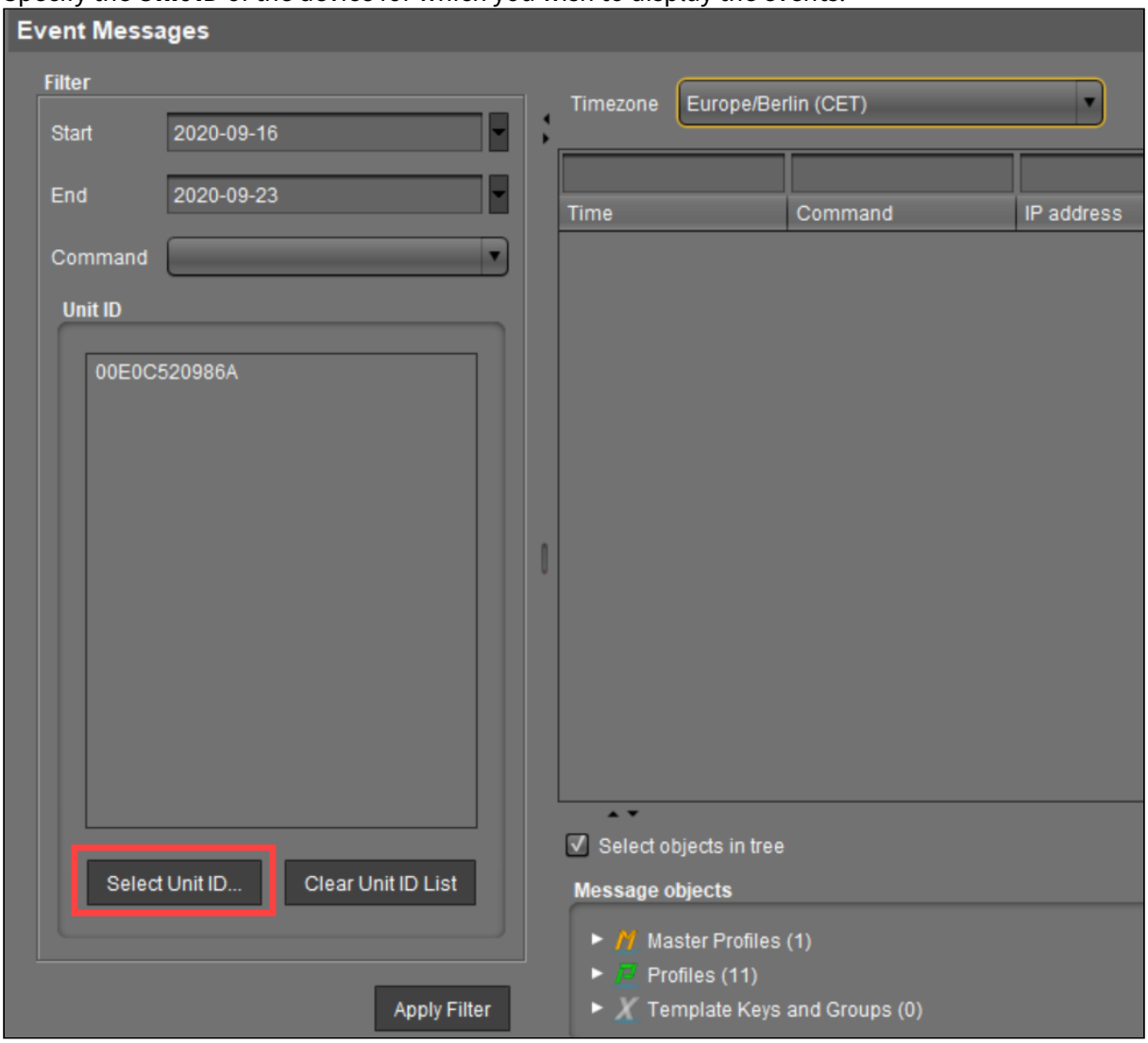


- Setting a Filter for Events (see page 1027)
- Filter for Messages (see page 1028)
- Setting a Filter for Categories (see page 1029)
- Notes (see page 1030)

Setting a Filter for Events

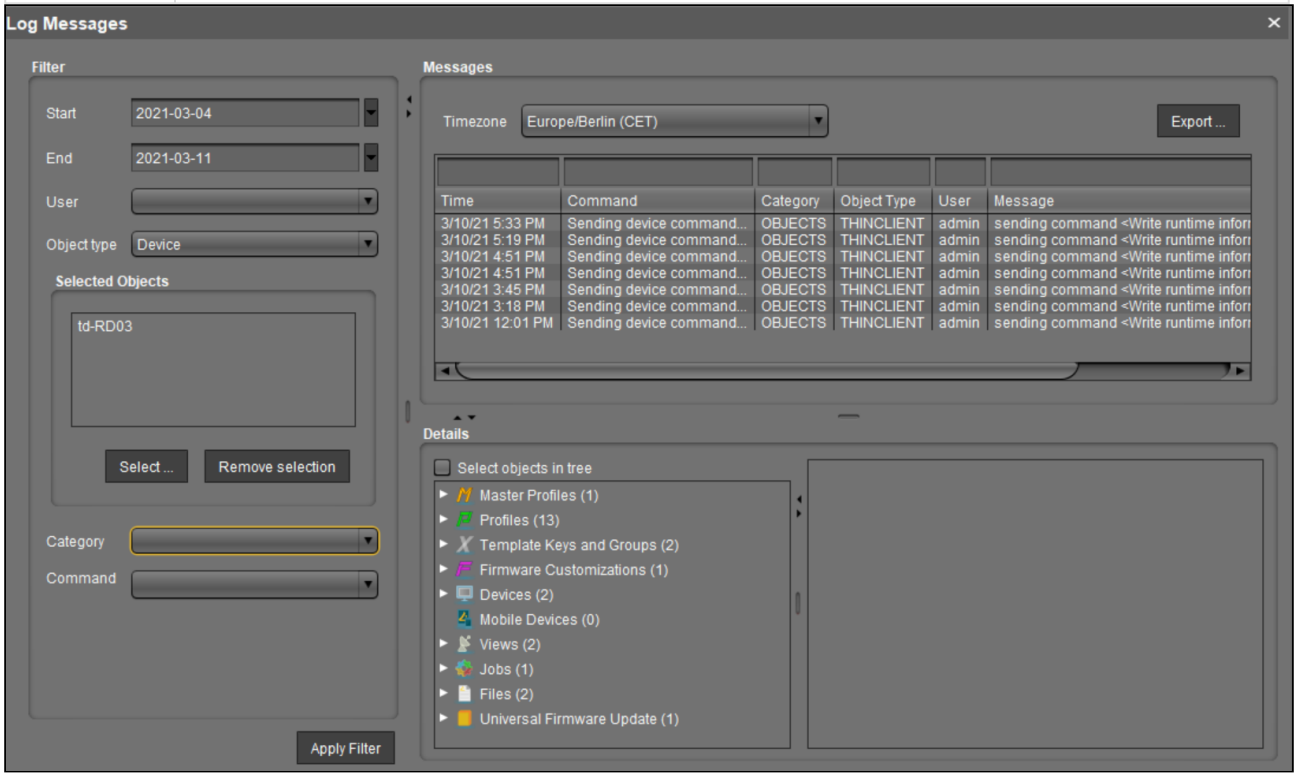
To set a filter for events, proceed as follows:

1. Specify the **Command** if you know which one you need.
2. Specify the **Unit ID** of the device for which you wish to display the events.



Filter for Messages

User	Select the name of the UMS administrator who is responsible for the message.
Object type	Specify an object for which you would like to display the messages.
Category	Each command belongs to a category, e.g. security, settings and objects.
Command	If a command is known, you can specify it yourself.
Time zone	You can specify the time zone with which the logging time for messages is shown.



Setting a Filter for Categories

→ To adjust the filter, select the option **Category** if you would like to select all messages for a specific category (e.g. those relating to firmware updates).
All commands within this category such as **Delete firmware update** or **Assign firmware update** will then be evaluated in order to identify the messages or events.

Notes

The quick filter does not apply to the export action.

One of the most important commands is the command `GET_SETTINGS_ON_REBOOT`. The time stamp for this command provides details of the time when the device last booted. This can be used to define a new **BOOT TIME** view criterion. With the help of this criterion, you can easily determine which devices have not been booted after a certain date.

> The administration settings for the number of messages and – more importantly – for the events should be handled with great care. The higher these values are, the more space will be required for the tablespace in the database. If you enable logging, you should monitor your database closely until you are sure that sufficient space is available for the messages and/or events.

Save Support Information / Send Log Files to Support

If you have problems with the UMS and contact your service provider, you can send various UMS log files to Support. The Support Wizard - How to Send Log Files in the IGEL UMS (see page 1032) will help you here to do this through the UMS Console. If you are using the UMS Web App, see How to Save Support Information and Log Files in the IGEL UMS Web App (see page 1382) .

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 https://support.igel.com/csm.

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[165] too.

165. https://www.igel.com/wp-content/uploads/2019/11/F-501-EN.pdf

Support Wizard - How to Send Log Files 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.

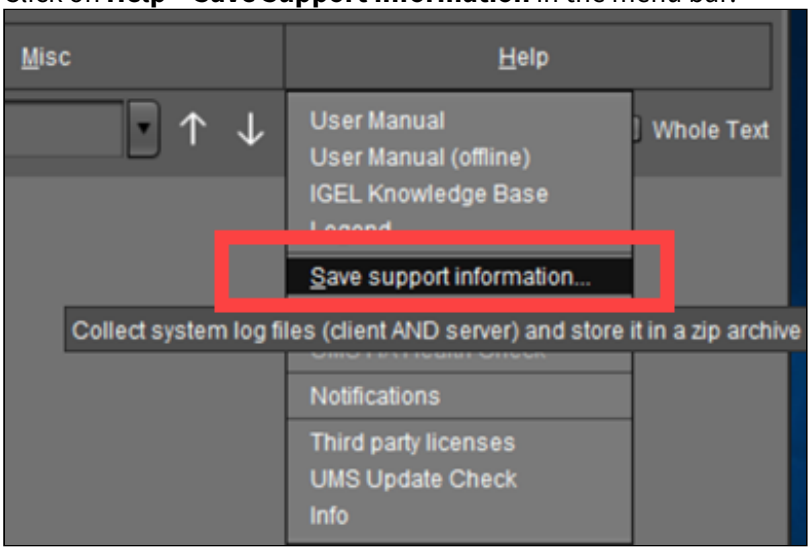
The Support Wizard saves log files from the UMS Server and UMS Console as well as profiles and associated firmware information for the selected devices in a ZIP file. If IGEL Cloud Gateway (ICG) is in use, log files from the connected ICGs and the basic information of the used ICG certificates will also 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 in the IGEL UMS (see page 987)), monitoring data for the UMS Server and UMS Load Balancer will be collected too.

> In order to send log files using the Support Wizard, the mail settings must be correct; further information can be found under Mail Settings (see page 993) . The support ID must also be valid.

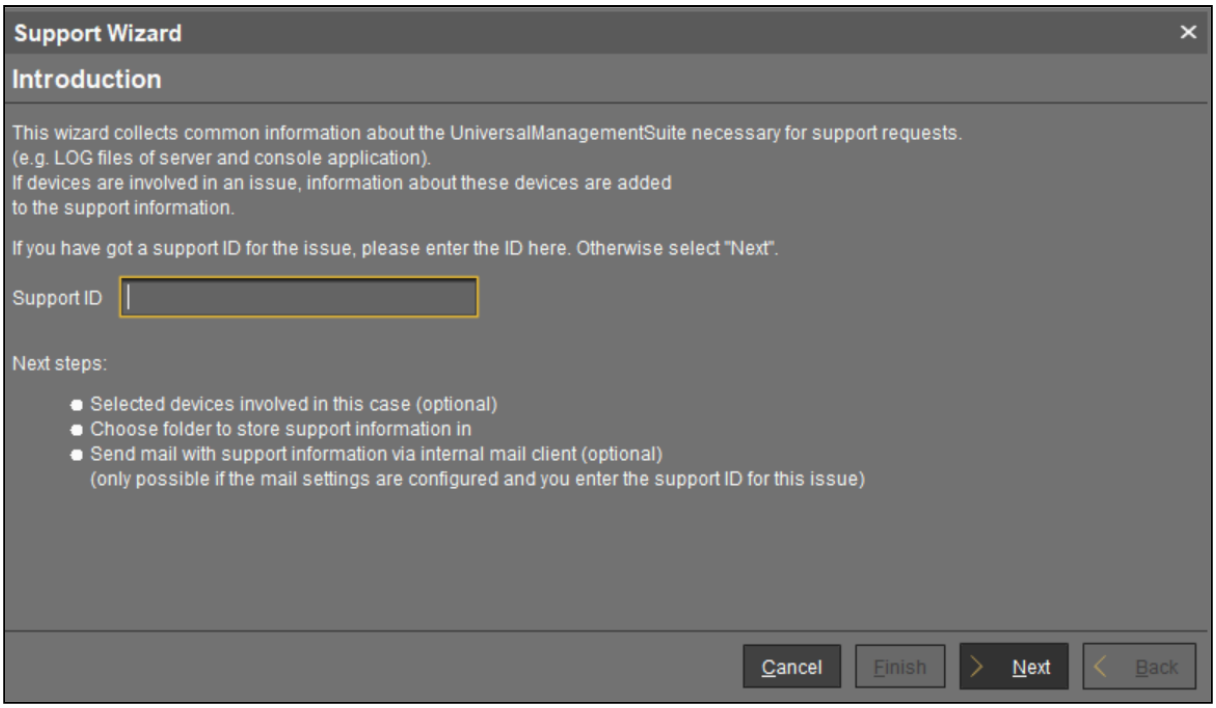
How to Send Log Files via Support Wizard in the IGEL UMS

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 **Next**.
4. If the support case concerns devices (otherwise, click **Next**): Highlight the devices where the problem has occurred.
5. If the support case concerns devices (otherwise click **Next**): Click on to select the highlighted devices.
6. Click **Next**.
7. Under **Number of days back**, specify the maximum age in days of the log entries to be sent.
8. Click **Next**.
9. Using **Look In**, select the directory in your file system in which the zipped log files are to be saved.
10. Click **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 **Send**.
13. Click **Finish**.

Related Topics

(en) Debugging / How to Collect and Send Device Log Files to IGEL Support

(11.10-en) Exporting the Local Configuration of the IGEL OS Device

Save Device Files for Support in the IGEL UMS

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 *How to Start with IGEL > 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 *IGEL OS > IGEL OS Reference Manual > Accessories > System Log Viewer*.

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 *IGEL OS > IGEL OS Reference Manual > Accessories > System Log Viewer*.

The IGEL UMS Administrator

The IGEL Universal Management Suite (UMS) Administrator is a standalone configuration tool to manage the UMS server-side settings, database connections, and system-level configurations. The UMS Administrator application is only available on a UMS Server as it enables you to change the communication between the services directly.

You can use it to 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.

⚠ The rights for changing the settings depend on whether the user is authorized to change IGEL UMS files on the server system.
To function properly, the UMS Administrator needs to be started with a user with database access, for example the UMS superuser.

Launching the UMS Administrator

ℹ 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`.

ℹ The default path to the UMS Administrator under Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

Changing the Language of the UMS Administrator

You can change the language of the Administrator tool under **File > Settings > Language**.

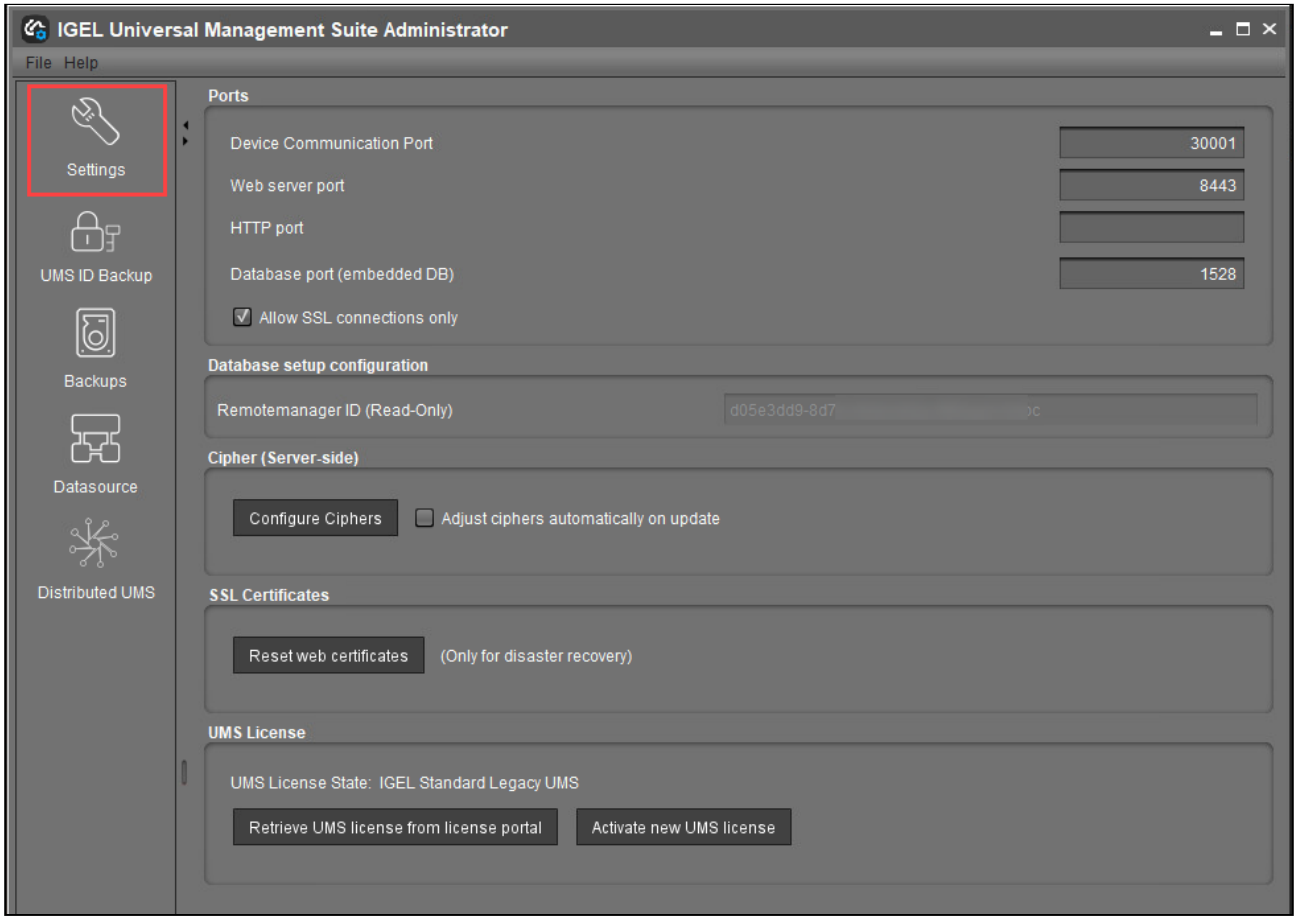
- Settings - Change Server Settings in the IGEL UMS Administrator (see page 1038)
- UMS ID Backup in the IGEL Administrator (see page 1043)
- Backups (see page 1050)
- Data Source (see page 1061)
- Distributed UMS - Perform Local UMS Actions in the IGEL UMS Administrator (see page 1077)
- IGEL UMS Administrator Command-Line Interface (see page 1079)

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.

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)

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 (see page 256).

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 (see page 1157). (Default: 8443)

If the port is changed, the service IGEL RMGUIServer/igelRMserver must be restarted.

If no Cluster Address (see page 909)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.

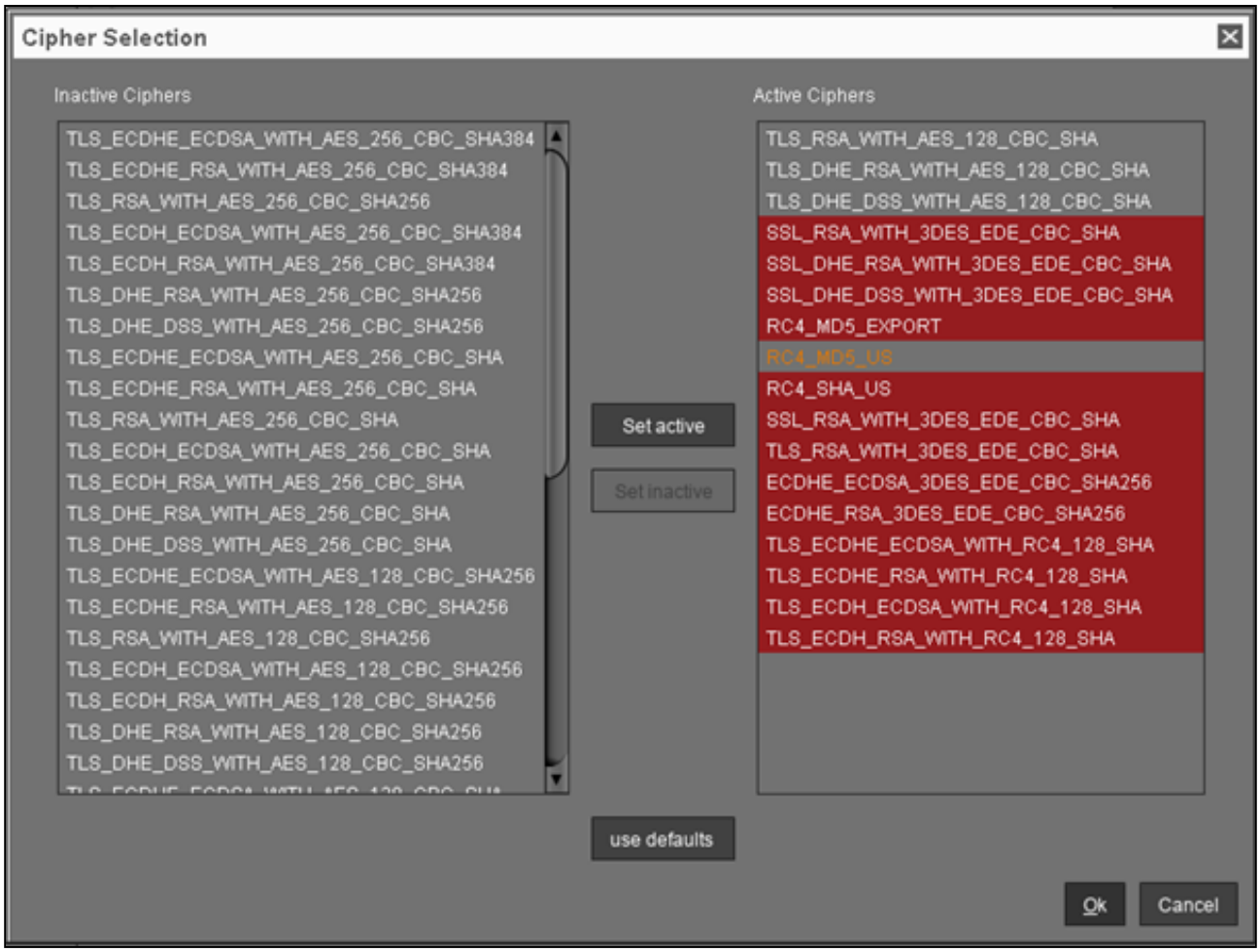
On new UMS installations, only the default ciphers (see page 1040) are activated. By updating the existing UMS installations, the already configured ciphers are kept.

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 (see page 256)). Also, it creates a new certificate chain which is then used for HTTPS.

If you want to use your own certificate or certificate chain after the reset, see How to Use Your Own Certificates for Communication over the Web Port (Default: 8443) in IGEL UMS[166].

UMS License

Shows the UMS License state, and you can perform license actions. The same actions are also available in the UMS Console, under UMS Licenses[167].

Retrieve UMS License from license portal

Use this button to automatically download the license file from the IGEL Licensing Portal (ILP). For this, the UMS needs to be connected to the ILP with the correct UMS ID.

You do not need Automatic License Deployment (ALD) to trigger the download through the **Retrieve UMS License from License Portal** button.

If Automatic License Deployment (ALD) is activated the license download is automatically done at server start.

Activate new UMS license

Use this button to manually select and upload a license file. This method can be used when the UMS is not connected to the ILP (for example, in air-gapped scenarios).

166. https://kb.igel.com/en/universal-management-suite/current/how-to-use-your-own-certificates-for-communication
167. https://kb.igel.com/en/universal-management-suite/current/ums-licenses

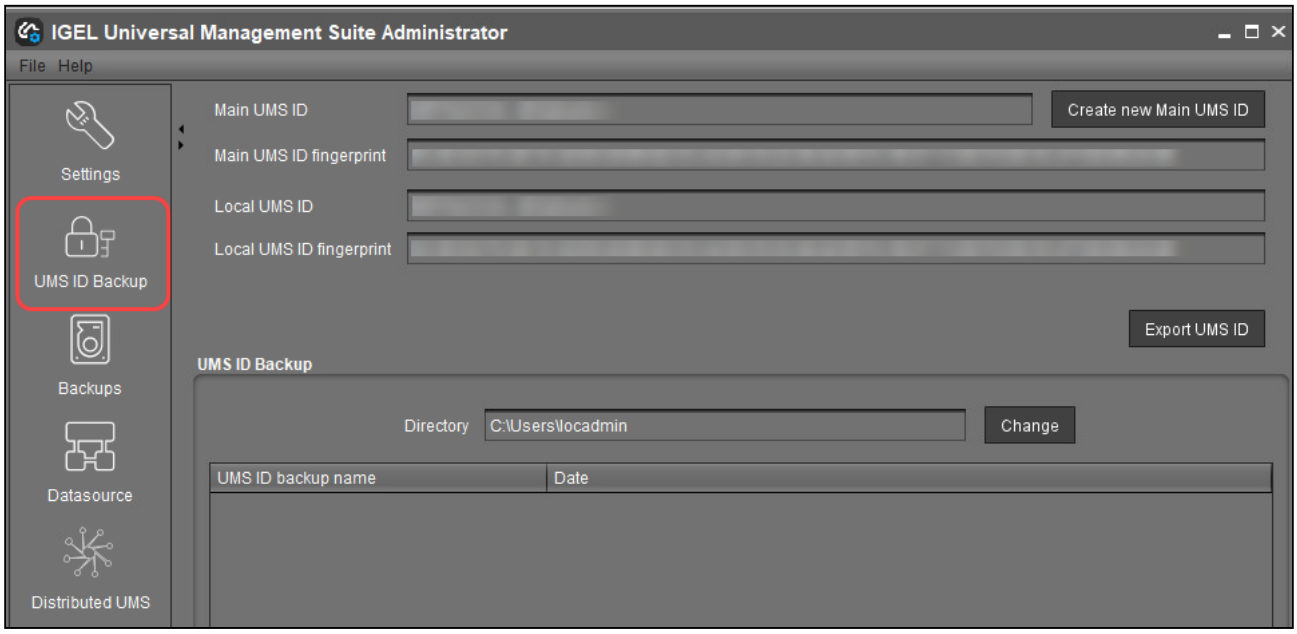
UMS ID Backup in the IGEL Administrator

In the IGEL Universal Management Suite (UMS) Administrator, you can create a backup of the UMS ID (called UMS Licensing ID before UMS 12) and export the UMS ID.

For information on the UMS ID, see UMS ID[168].

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**



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.

168. https://kb.igel.com/en/universal-management-suite/current/ums-id

Local UMS ID
The first and last 10 characters of the local UMS ID are displayed here.

> ⚠ In a Distributed UMS 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 How to Manually Synchronize the UMS ID (see page 521). 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.

Export UMS ID
Click to export the UMS ID to a selected folder.

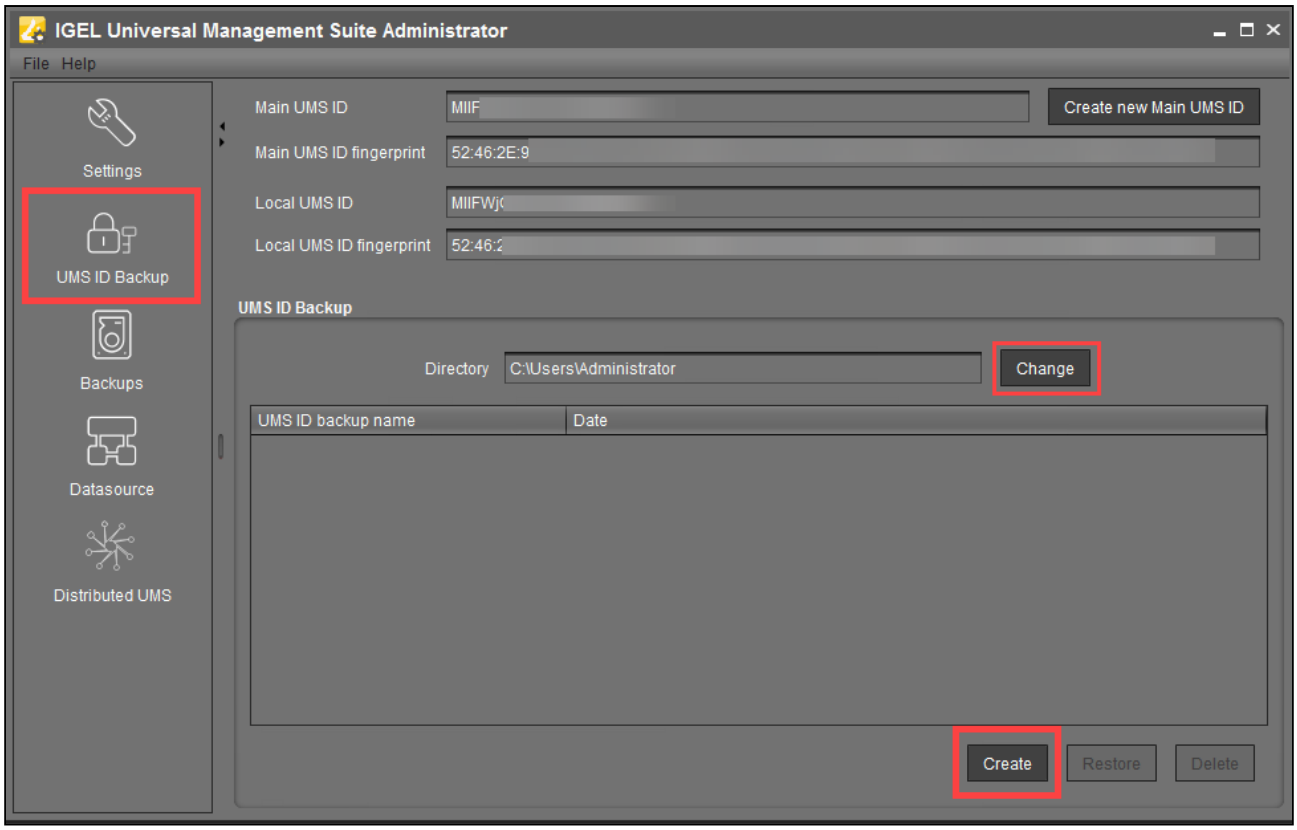
Directory
Path where to store the backup.

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**.

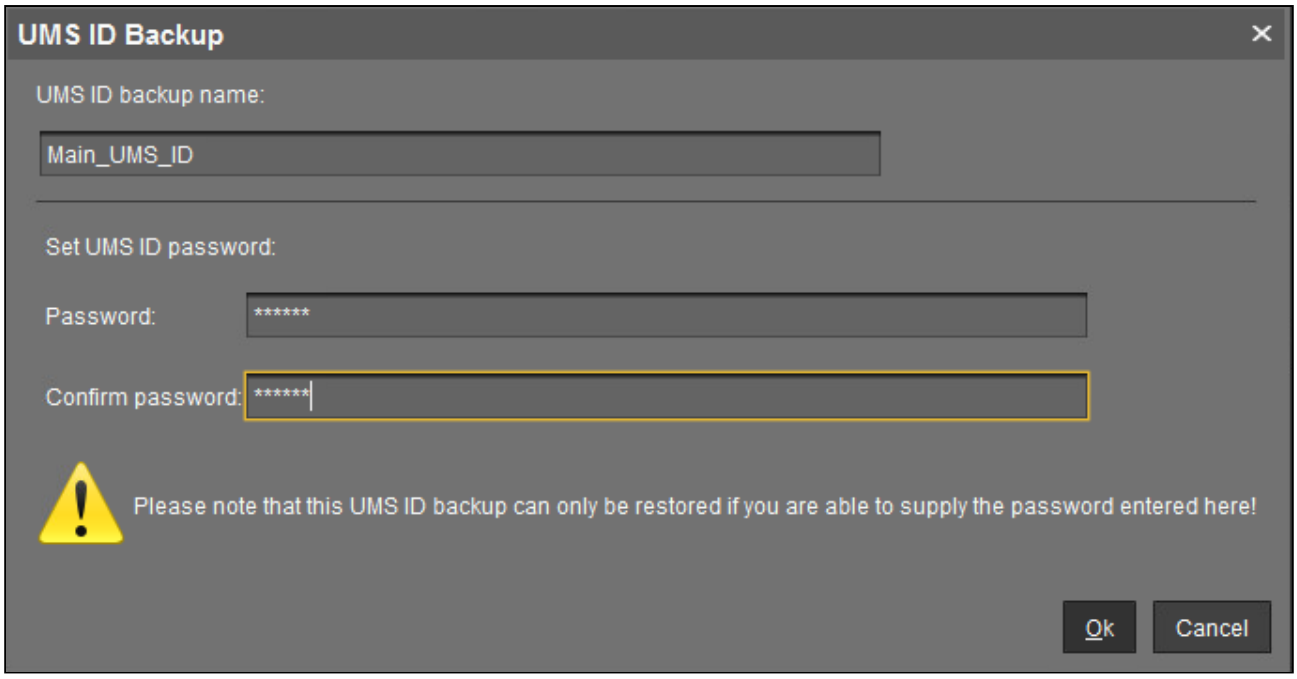


2. Click **Change** if you want to change the directory for storing the backup.

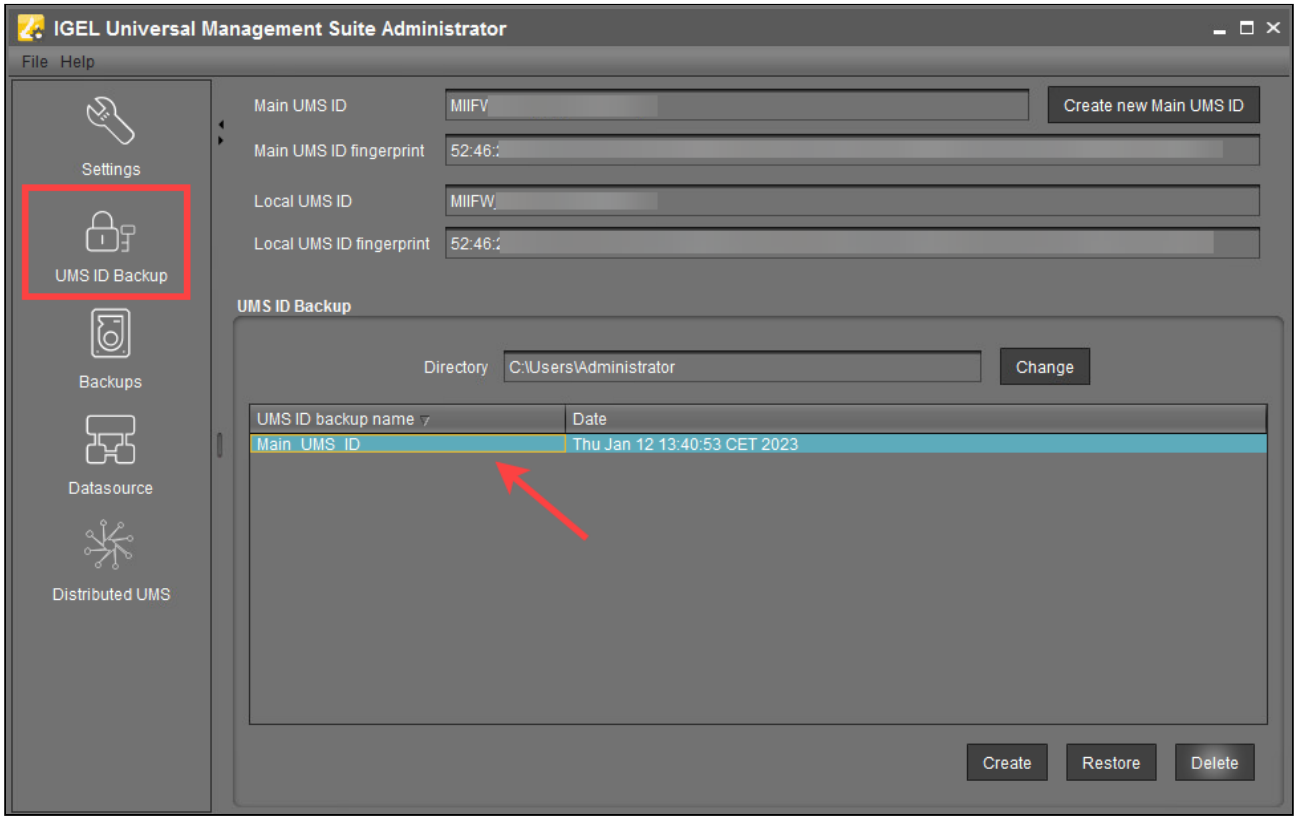
3. Click **Create**.
   The **UMS ID Backup** dialog opens.

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 How to Manually Synchronize the UMS ID (see page 521).

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.



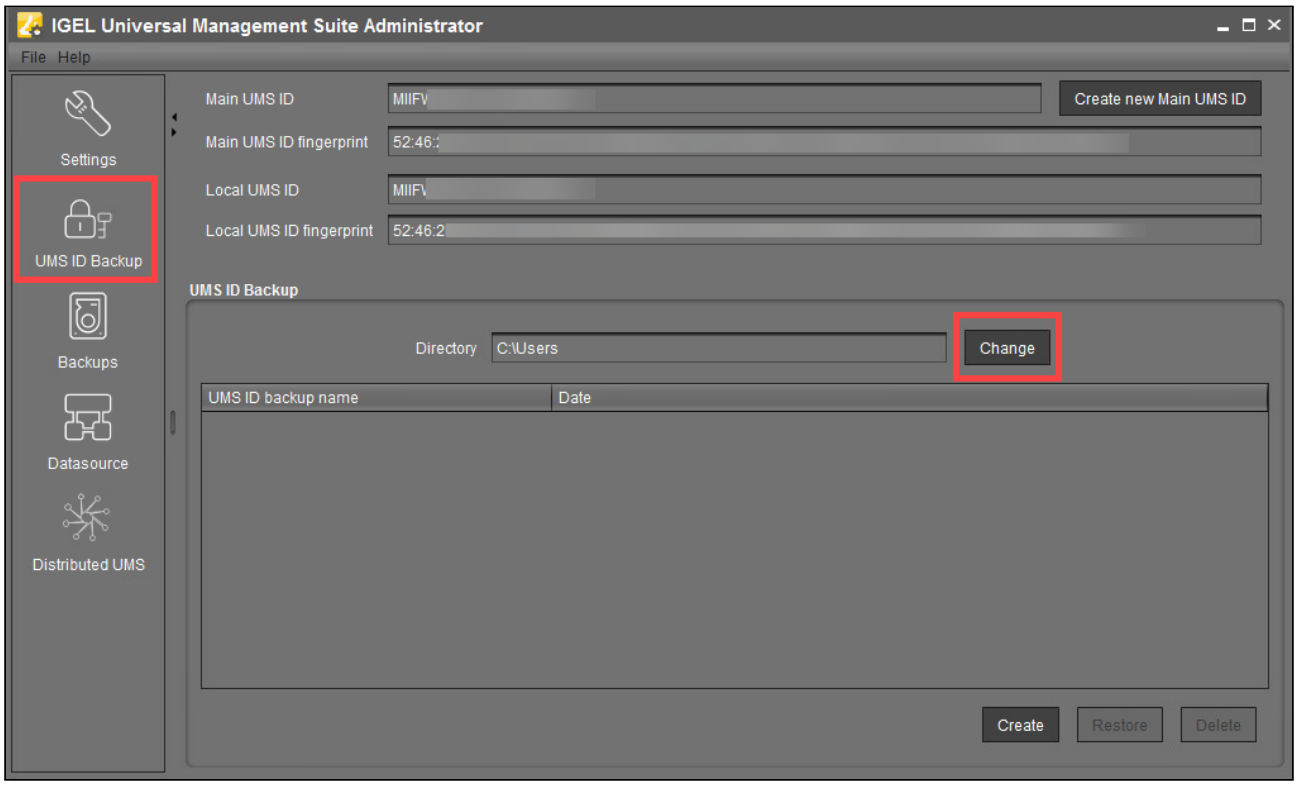
5. Click **OK**.
   The new backup file is listed under **UMS ID Backup**.



How to Restore a Backup of the UMS ID

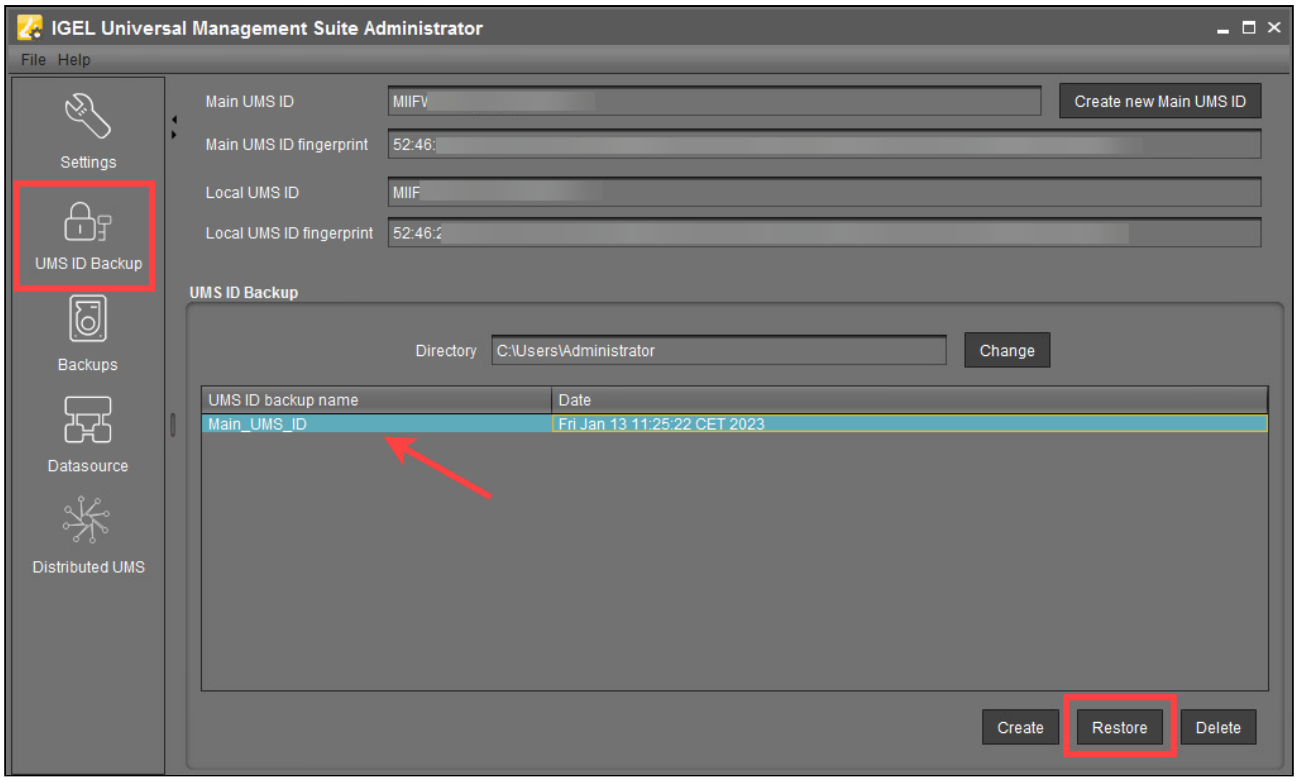
1. Open the UMS Administrator and go to **UMS ID Backup**.

2. Click **Change** and select the directory where the backup was saved.



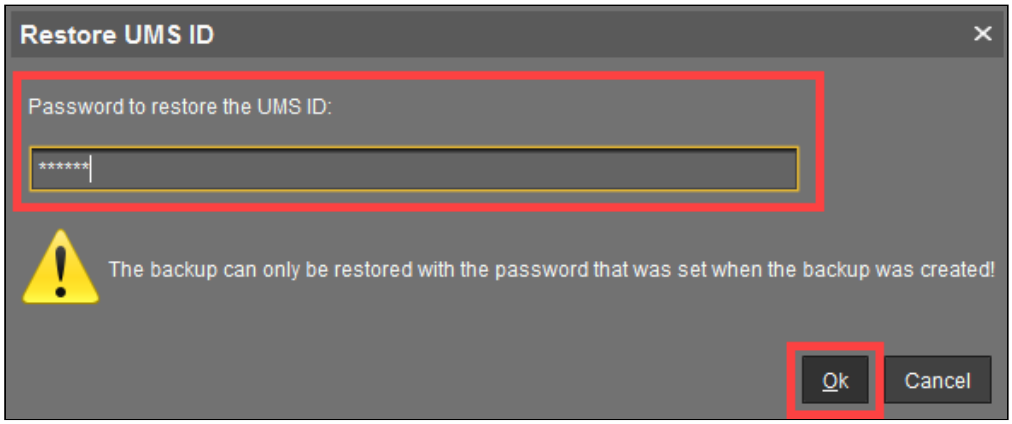
The backup appears in the list of the available UMS ID backups.

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

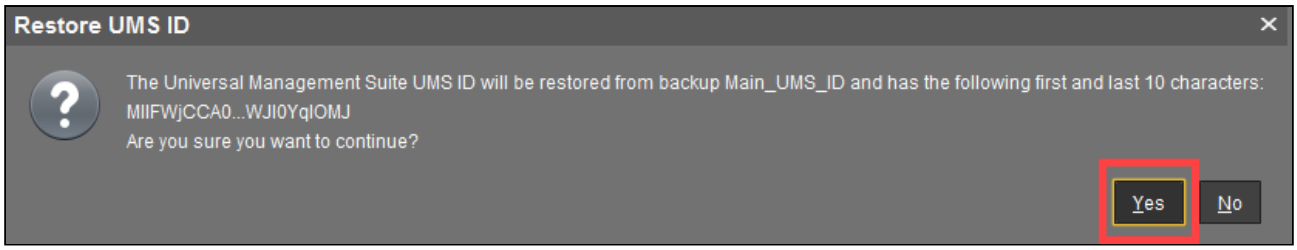


The **Restore UMS ID** dialog opens.

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



5. Confirm the restoring.


Restore UMS ID
The Universal Management Suite UMS ID will be restored from backup Main_UMS_ID and has the following first and last 10 characters:
MIIFWjCCA0...WJI0YqIOMJ
Are you sure you want to continue?
Yes
No

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 1051)
- Restoring a Backup (see page 1056)
- Deleting a Backup (see page 1059)
- Planned Backup (see page 1060)

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 1051).

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.

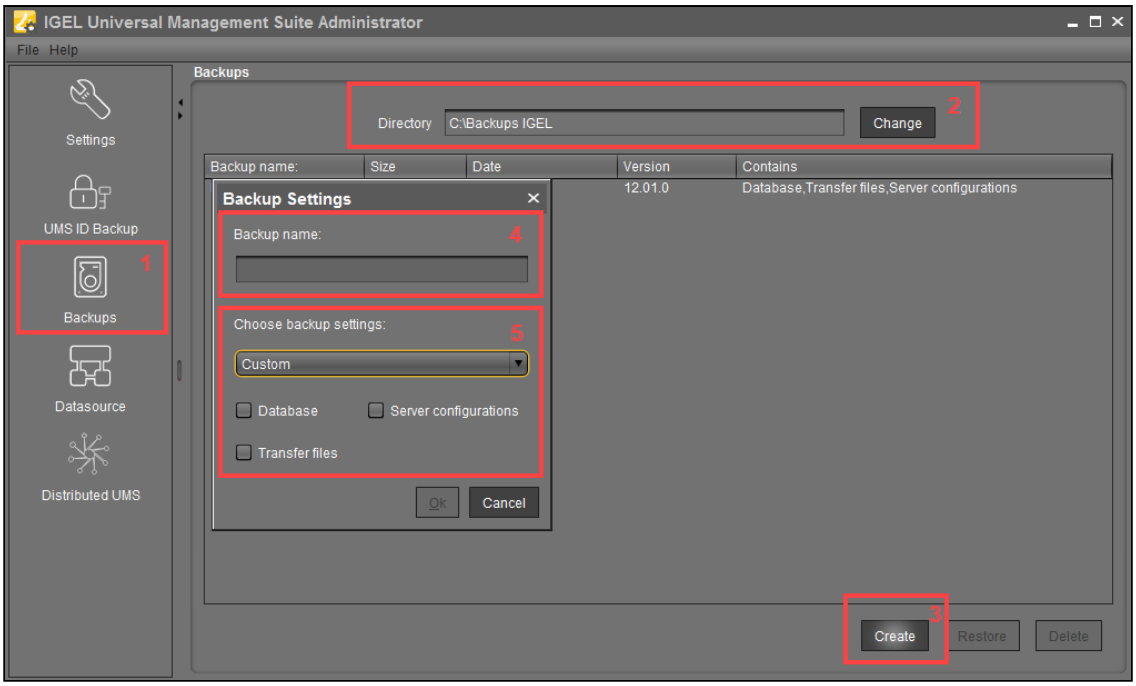
Menu path: **UMS Administrator > Backups**

> 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.
2. Go to **UMS ID Backup** and follow the instructions under UMS ID Backup in the IGEL Administrator (see page 1043) in order to create the backup of the UMS ID.
3. Select **Backups**.
4. Click **Change** to change the storage location for your backups.
5. Click **Create**.
6. Under **Backup name**, enter a name for the backup.
7. Select the backup settings under **Choose backup settings**:
   The following can be selected:
   - **Select all** (Default): Database, server configurations (see page 1053), 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 1056).
- As of UMS 12.07.100, the UMS license is included in the database backup. However, the UMS license will only be restored if it matches the UMS ID (i.e. the UMS ID of the installation must match the UMS ID which was registered at the IGEL License Portal). Therefore, if you restored the database backup, but the UMS license is not correct, restore the corresponding UMS ID backup (see UMS ID Backup in the IGEL Administrator[169]). Afterwards, restart the UMS Server service (see https://kb.igel.com/en/universal-management-suite/current/igel-ums-ha-services-and-processes) or click **UMS Administrator > Settings > UMS License > Retrieve UMS License from license portal** (see Settings - Change Server Settings in the IGEL UMS Administrator[170]).

169. https://kb.igel.com/en/universal-management-suite/current/ums-id-backup-in-the-igel-administrator
170. https://kb.igel.com/en/universal-management-suite/current/settings-change-server-settings-in-the-igel-ums-ad

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 1038) 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.

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 63), 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

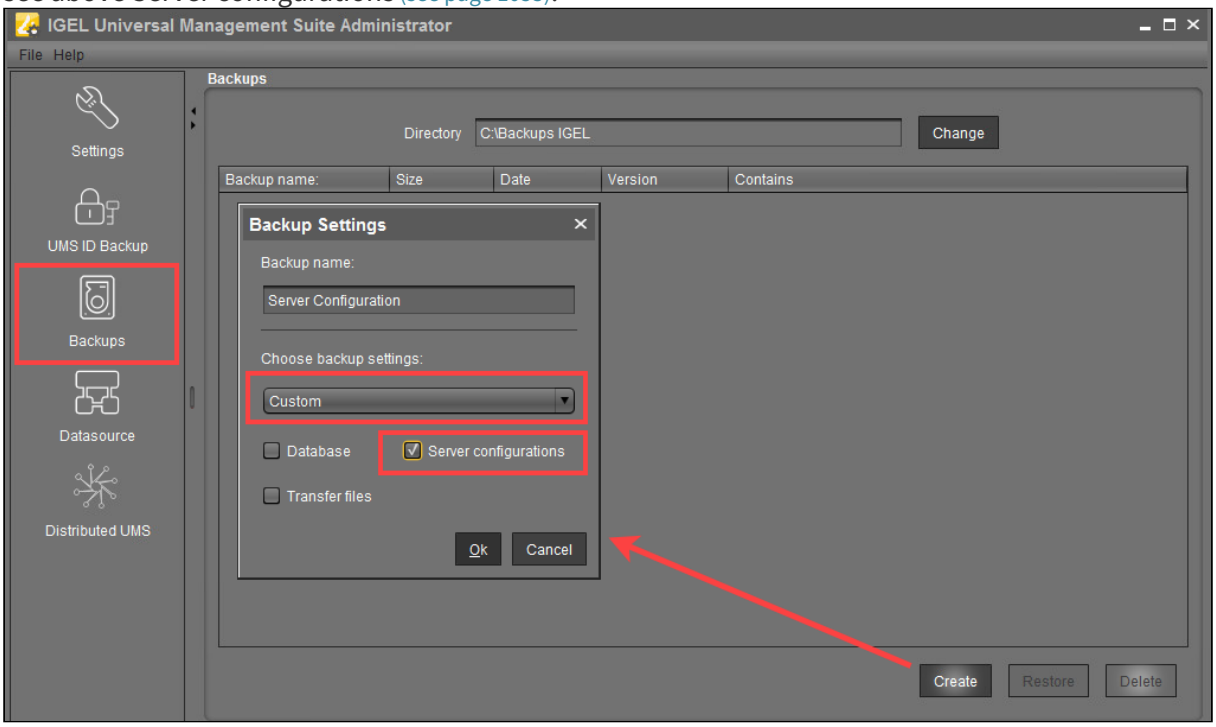
As of UMS version 5.09, all certificates are included in the database backup.
If you need to back up the certificates manually, you can find them here:

- `[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.
- As of UMS 12.07.100, the UMS license is included in the database backup. However, the UMS license will only be restored if it matches the UMS ID (i.e. the UMS ID of the installation must match the UMS ID which was registered at the IGEL License Portal). Therefore, if you restored the database backup, but the UMS license is not correct, restore the corresponding UMS ID backup (see UMS ID Backup in the IGEL Administrator[171]). Afterwards, restart the UMS Server service (see https://kb.igel.com/en/universal-management-suite/current/igel-ums-ha-services-and-processes) or click **UMS Administrator > Settings > UMS License > Retrieve UMS License from license portal** (see Settings - Change Server Settings in the IGEL UMS Administrator[172]).

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 1053):



171. https://kb.igel.com/en/universal-management-suite/current/ums-id-backup-in-the-igel-administrator
172. https://kb.igel.com/en/universal-management-suite/current/settings-change-server-settings-in-the-igel-ums-ad

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 1043).

> 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 How to Manually Synchronize the UMS ID (see page 521).

5. For HA installations (see page 1387) only: Save the current IGEL network token (allows the integration of new servers into the same HA network). This is usually a token created during the installation, see Installing the First Server in an HA Network (see page 1394). 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 Certificates in the IGEL UMS (see page 896)), this is the token to be backed up.

Restoring a Backup

Menu path: **UMS Administrator > Backups**

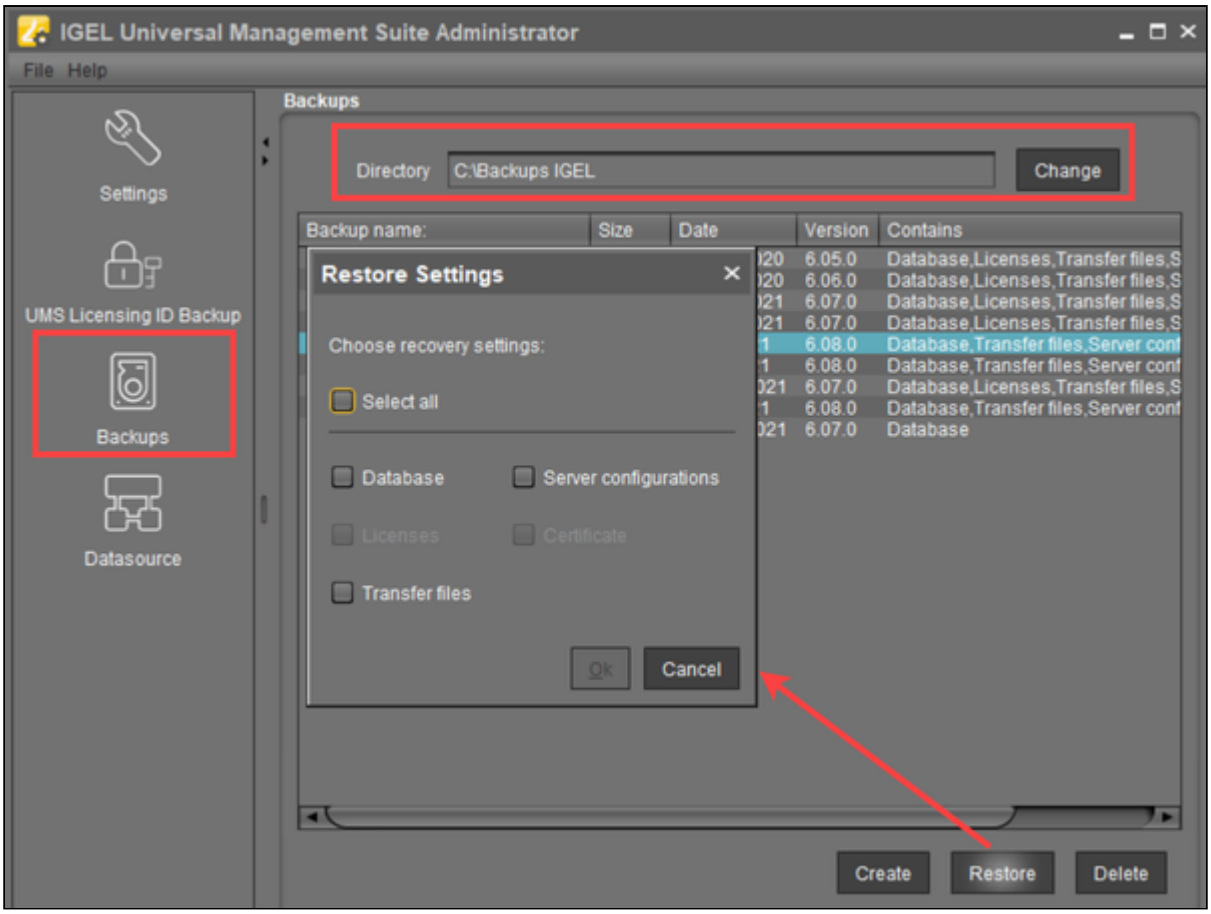
> Default path to the UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> The IGEL UMS Administrator application can only be started on the UMS Server.

> 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 1051).

> 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 **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.



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.

As of UMS 12.07.100, the UMS license is included in the database backup. However, the UMS license will only be restored if it matches the UMS ID (i.e. the UMS ID of the installation must match the UMS ID which was registered at the IGEL License Portal).
Therefore, if you restored the database backup, but the UMS license is not correct, restore the corresponding UMS ID backup (see UMS ID Backup in the IGEL Administrator[173]). Afterwards, restart the UMS Server service (see https://kb.igel.com/en/universal-management-suite/current/igel-ums-ha-services-and-processes) or click **UMS Administrator > Settings > UMS License > Retrieve UMS License from license portal** (see Settings - Change Server Settings in the IGEL UMS Administrator[174]).

173. https://kb.igel.com/en/universal-management-suite/current/ums-id-backup-in-the-igel-administrator
174. https://kb.igel.com/en/universal-management-suite/current/settings-change-server-settings-in-the-igel-ums-ad

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 920). See also Performance Optimizations in IGEL UMS (see page 225).

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 as Administrative Task in the IGEL UMS (see page 922).

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 63) .

- Activating a Data Source (see page 1062)
- Copying a Data Source (see page 1065)
- Optimizing the Active Embedded DB (see page 1068)
- Changing the UMS Superuser (see page 1070)
- How to Set Up a Data Source in the IGEL UMS Administrator (see page 1073)

Activating a Data Source

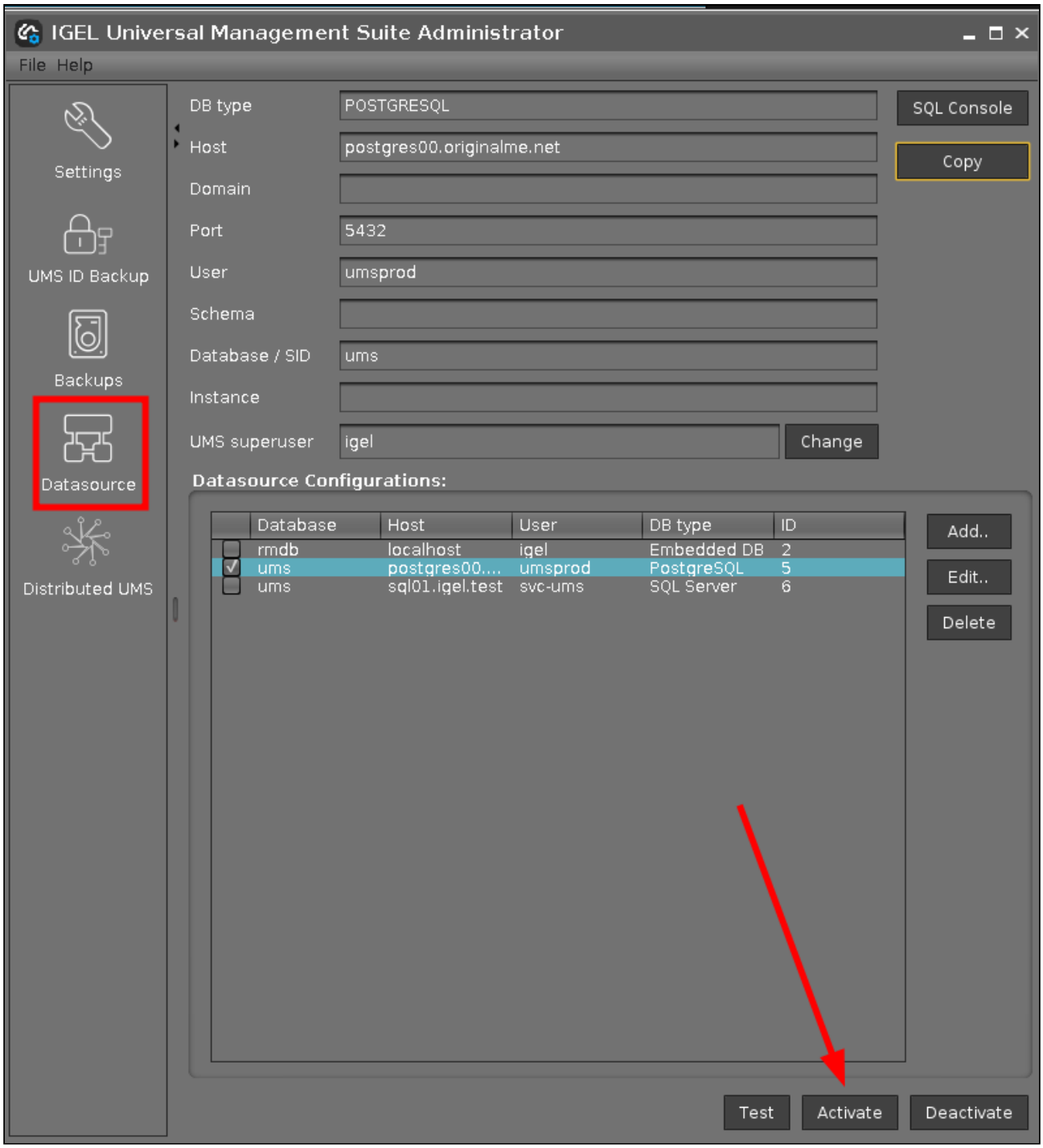
You can set up a number of data sources in the IGEL Universal Management Suite (UMS) Administrator. However, only one can be actively used by the UMS server.

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.

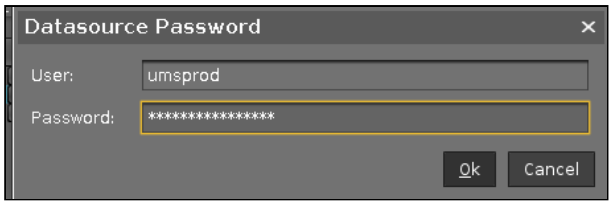
To activate a data source, proceed as follows:

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.

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.

4. Confirm each action.

Copying a Data Source

You can copy the data source of your IGEL Universal Management Suite (UMS) in the UMS Administrator as described in this article. This function is useful when migrating to a different database.

Example Configuration
To switch your UMS database from an Embedded DB to an external database system, see the detailed instructions in How to Migrate a UMS Database From Embedded DB to Microsoft SQL Server (see page 446) .

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.

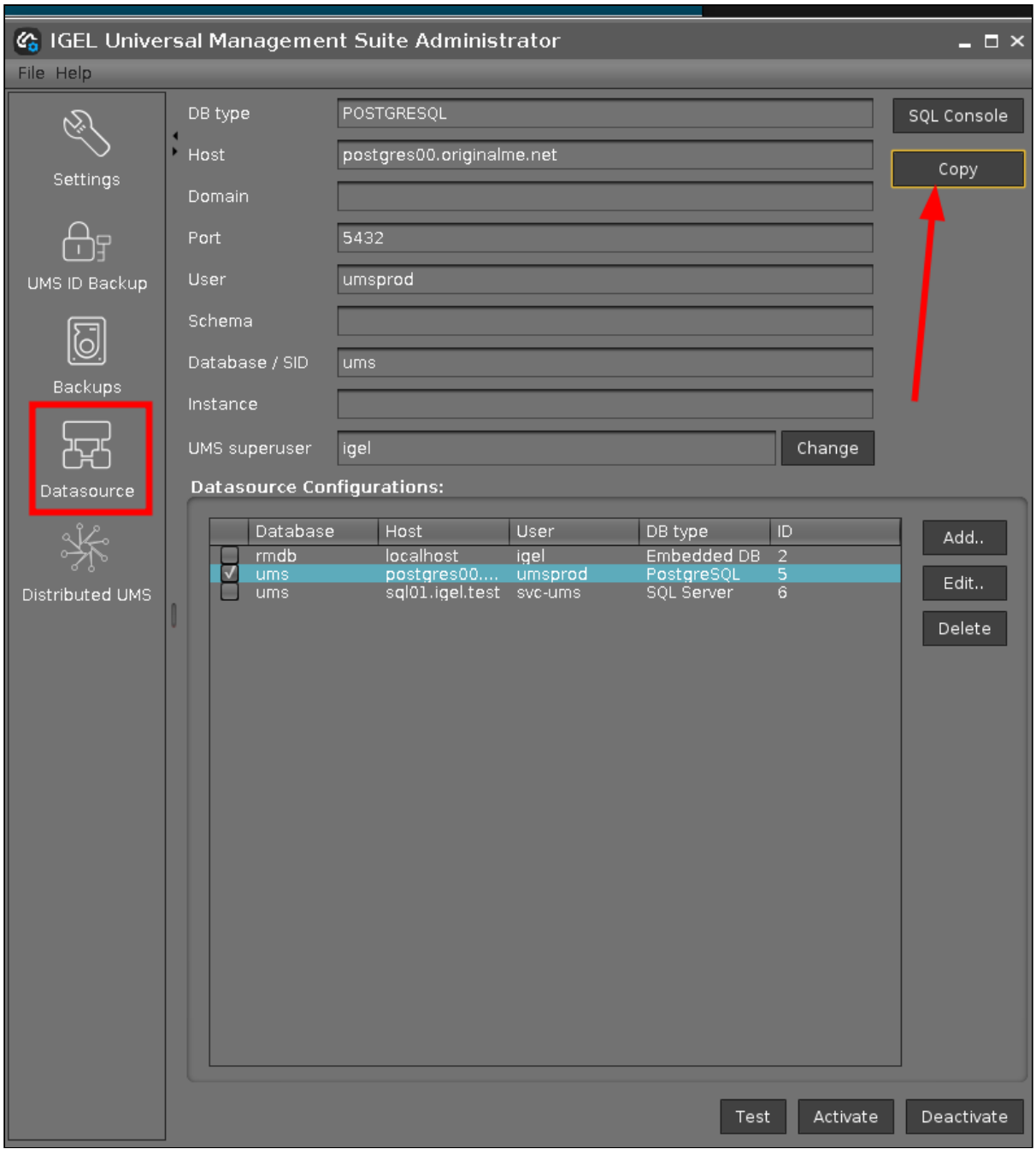
Known issue when migrating to an Oracle Database

It is not possible to migrate from a non-Oracle Database to an Oracle Database via RMAdmin. The initial use of an Oracle Database is possible and is supported. It is also possible to update an Oracle Database to a higher version.

General Instructions

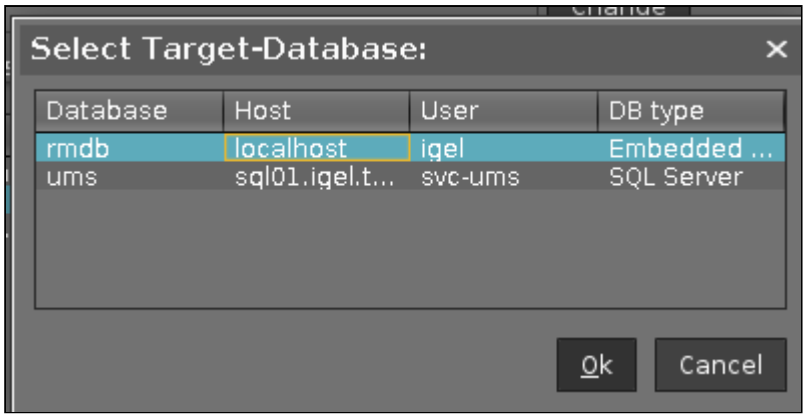
To copy one data source to another one:

1. Prepare the new database in accordance with the installation instructions for the UMS.
2. Set up a suitable new data source for this database system in the UMS Administrator.
3. Select the data source which is still active and in use.



4. Click **Copy** to copy the old data source to the new one.

5. Select the destination data source and click **OK**.



6. Start the process after entering the login data for the destination data source.

7. Activate the new data source.

8. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.

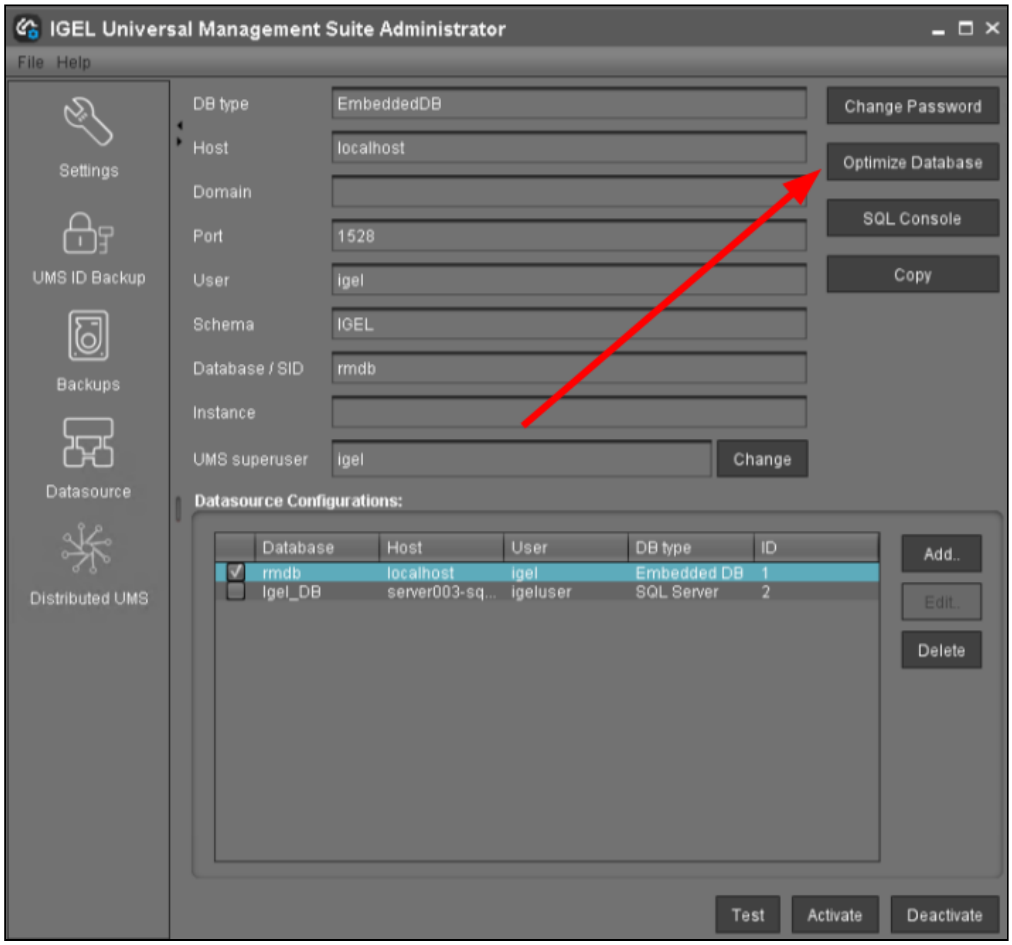
Optimizing the Active Embedded DB

You can optimize the embedded database of the IGEL Universal Management Suite (UMS) in the UMS Administrator to speed up database operations. When the database is optimized, the content of the database is restructured and the database index is renewed.

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.



A message window appears once the procedure has been successfully completed.

Changing the UMS Superuser

The UMS superuser is created initially during the installation of the IGEL Universal Management Suite (UMS). You can change the UMS superuser in the IGEL UMS Administrator.

You can also change the password of the UMS superuser in the IGEL UMS Web App, under **User Management**, see How to Change User Password in the IGEL UMS Web App (see page 1379) .

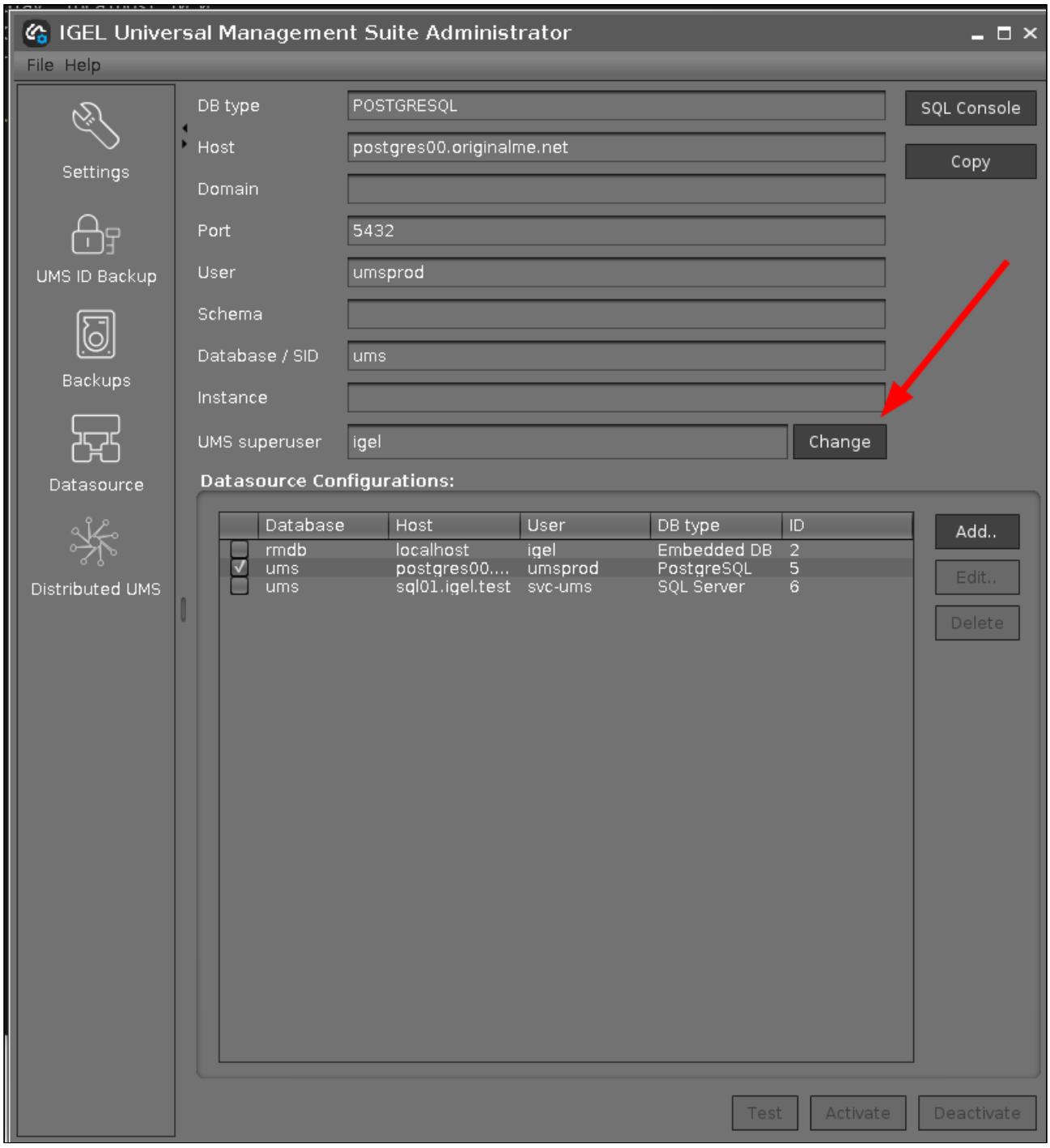
Menu path: **UMS Administrator > Datasource**

The UMS superuser 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 always has full access rights.

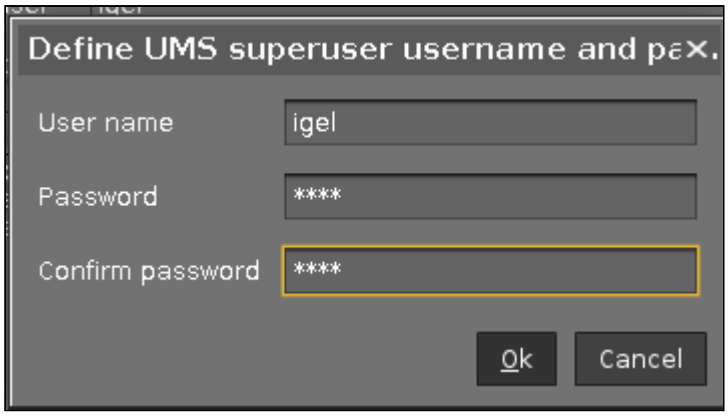
Changing the UMS superuser does not affect the user for database connections.

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.

1. Click **Change** next to the **UMS superuser** field.



2. Change the **User name** and **Password** for the UMS superuser and click **OK**.


Define UMS superuser username and pa×.
User name
igel
Password
****
Confirm password
****
Ok
Cancel

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

> For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 1440). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

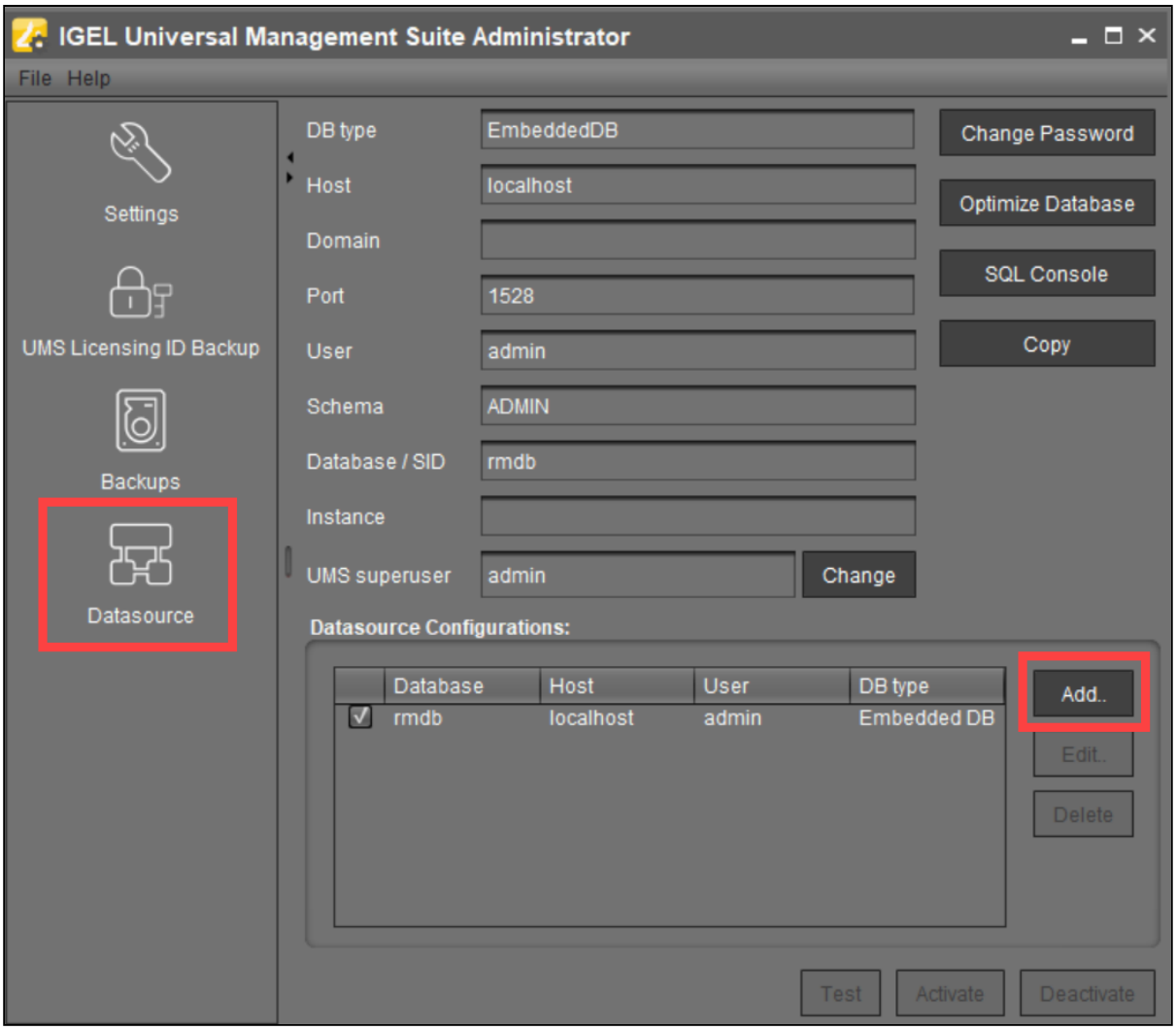
For information on the external database systems, see also Connecting External Database Systems (see page 63).

> 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.

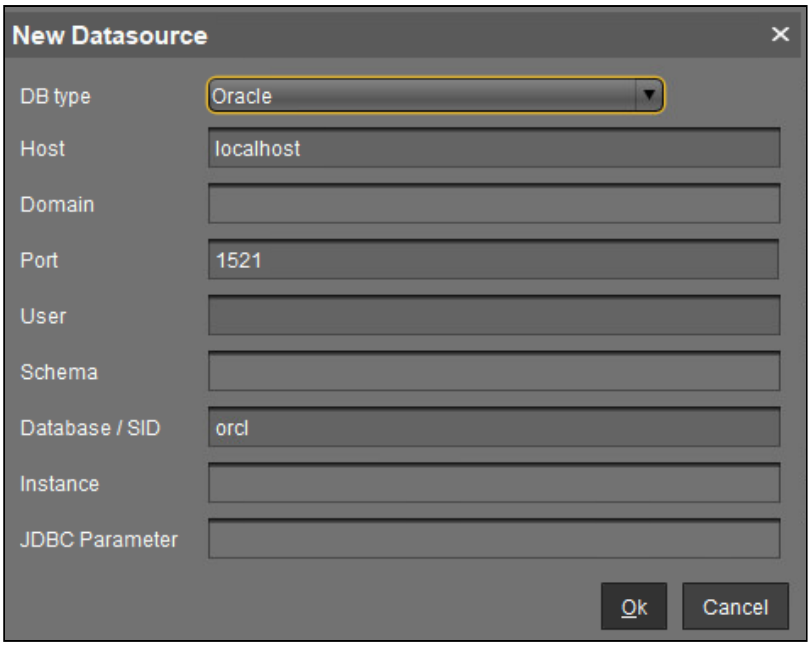
How to Add the Database Connection in the IGEL UMS Administrator

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**.

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.

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.

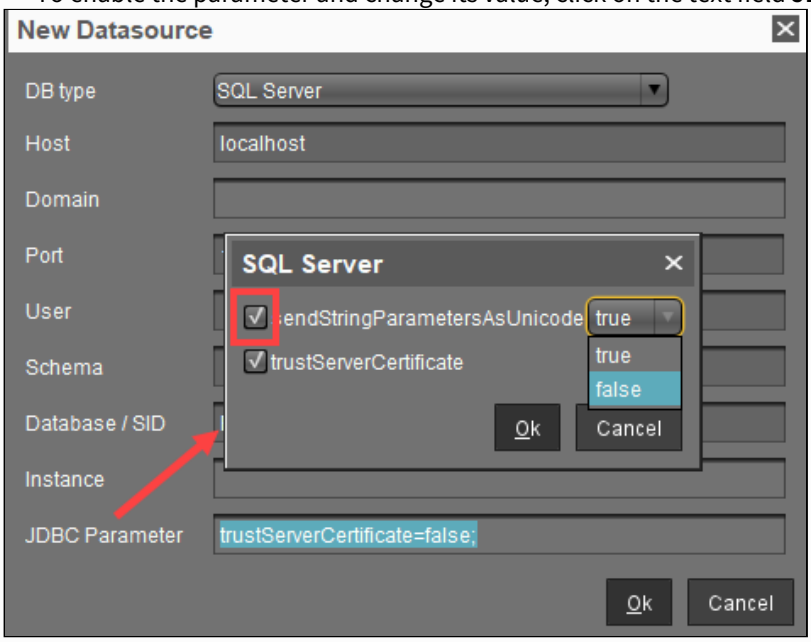
You can define additional parameters to be added to the JDBC URL via **JDBC Parameter**. Currently, the following parameters are supported:

- Microsoft SQL Server: `sendStringParametersAsUnicode` (Default value: `true`)
  This parameter can be modified to improve the query performance in some cases. See the Microsoft article setSendStringParametersAsUnicode Method (SQLServerDataSource)[175].
- 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[176].
  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`'.

175. https://docs.microsoft.com/en-us/sql/connect/jdbc/reference/setsendstringparametersasunicode-method-sqlserverdatasource?view=sql-server-ver16
176. https://learn.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver16

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**.



⚠ It is strongly recommended to set the option `sendStringParameterAsUnicode=false` when using MS SQL Server databases and UMS 12 to avoid performance problems.

3. Click on **Test** to test the connection to the database.
   This is also possible when a data source is inactive.
4. If required, **activate** the data source. See Activating a Data Source (see page 1062).

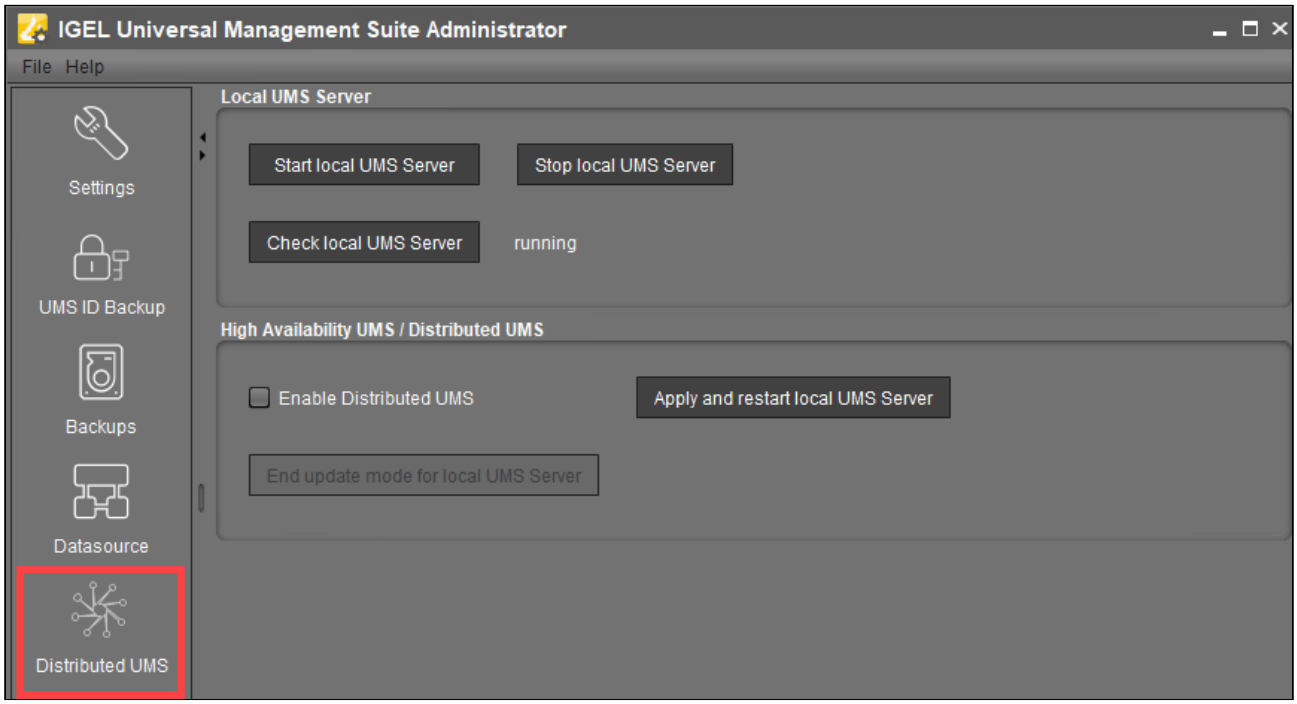
Distributed UMS - Perform Local UMS Actions in the IGEL UMS Administrator

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 1037).

> 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 (see page 1425).

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.

ℹ 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.

As of UMS 12.08.100, there is an additional `umsadmin-cli.sh` script that provides the same functionality as `umsadmin-cli.bin` on Linux machines, but without the QT dependency. It can be used whenever QT dependencies are not available or not wished, like on headless Linux machines or containers.
If the QT dependency is installed, you can freely decide between `.sh` or `.bin` scripts.

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@[redacted]:/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-[redacted]:/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 1084).

→ 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
```

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 1117).
2	Wrong usage of the CLI or invalid arguments

Command Reference

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.

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

Commands related to database ...

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
List all configured data sources	`db`	`list`					Shows the ID of the data source, which is required by other commands. The lowest ID is 1. IDs may change upon the creation and deletion of data sources. It is strongly recommended to always extract the ID before using it in other commands with --id The ID is calculated like this: highest existing ID + 1

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	Run `umsadmin-cli db list` to get a list of current data sources and select the ID of a data source. Run `umsadmin-cli db show --id <ID>` with that ID.

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 `umsadmin-cli db create`	Type, user, and port are required. Other options may or may not be required depending on the DB type `db create` will activate the database by default; this can be prevented by using `-A` or `--no-activate`. 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 `umsadmin-cli db create`	Embedded databases cannot be edited (as in the graphical UMS Administrator). All options are optional, except `--id`
			`-H`	`--host`	string	The database host	
			`-d`	`--domain`	string	The database domain	
			`-i`	`--id`	integer	The identifier of the database to be edited	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
			`-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.	For details on the JDBC parameters, see How to Set Up a Data Source in the IGEL UMS Administrator (see page 1073). Examples:

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value Type	Option Description	Remarks
							• `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
							• `rmadmin/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`	string	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

Commands related to 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 (see page 359).
			`-j`	`--java-webstart`	integer	Java Web Start port
			`-w`	`--web-server`	integer	UMS server port. For details, see UMS with Internal Database (see page 351) and UMS with External Database (see page 352).
			`-e`	`--embedded`	integer	Embedded database port
				`--ssl-only`	boolean	Allow SSL connections only

Cipher

Commands related to ciphers ...

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

Commands related to 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: • `ALL_SERVER` • `CURRENT_SERVER` (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 : • 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`	Named curve. Valid values: • `nist-p-384` (default) • `nist-p-256` • `nist-p-521`	
			`-o`	`--organization`	Organization (Mandatory option)	
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)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
				`--cn`	Common name	
			`-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.)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
				`--ca`	Certificate type: • `true` = CA certificate • `false` = End entity (default)	
			`-h`	`--hostname`	Hostname (hostname or one of these values: • 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	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
Export certificate	`web-certs`	`export-cert`	`-c`	`--cert-file`	Path to which the certificate should be exported (Name `cert.cert` is used when only a directory is specified.)	
			`-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	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			`-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	
Import certificate chain from keystore	`web-certs`	`import-cert-chain`	`-k`	`--keystore-file`	The keystore file	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
				`--password:file`	Path to a file containing the password	
				`--password:in`	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)	

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description	Remarks
			`-o`	`--organization`	Organization	
			`-l`	`--locality`	Locality	
			`-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: • `ALL_SERVER` • `CURRENT_SERVER`	

Accept Expired Client Certificates

Commands related to expired client certificates ...

Action	Primary Subcommand	Secondary Subcommand	Option Description
Enable the acceptance of expired client certificates	`accept-expired-client-certs`	`enable`	Enables the use of a custom `TrustManager` that accepts expired client certificates. As a result, the UMS can communicate with IGEL OS 12 devices that have expired client certificates.
Disables the acceptance of expired client certificates	`accept-expired-client-certs`	`disable`	Disables the use of a custom `TrustManager` that accepts expired client certificates. As a result, the UMS cannot communicate with IGEL OS 12 devices that have expired client certificates.
Show state of the option	`accept-expired-client-certs`	`state`	Shows if the custom `TrustManager` is enabled or disabled.

Superuser

Commands related to UMS 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
			`-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

Commands related to 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`)

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description
			`-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.
				`--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.

UMS License

Commands related to UMS License ...

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Value	Option Description	Remarks
Register a license to the UMS	`ums-license`	`register`	`-f`	`--filename`	`path to .lic file`	Path to the UMS license file.	During registration several errors could occur, e.g. the path doesn't exist, the file is invalid, the license already exists, the UMS ID doesn't match. When such an error occurs a corresponding error code is returned. See error codes under Error Numbers (see page 1117).
Returns current UMS License information	`ums-license`	`state`					
Delete all licenses previously imported with the command `register`	`ums-license`	`delete all`					

Network Token

Commands related to 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 `umstokeninstall-cli` in broker-only installations. It is equivalent to `umsadmin-cli token`.
			`--server`	boolean	Install token for UMS Server	
			`--broker`	boolean	Install token for broker	

UMS Cluster

Commands related to UMS cluster FQDN ...

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

Action	Primary Subcommand	Secondary Subcommand	Short Option	Long Option	Option Description
Delete the current UMS cluster FQDN	`ums-cluster`	`remove`			

Server

Commands related to UMS 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.
5003	Unable to set superuser credentials. There is no active data source.

Error number	Error description
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.
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!

Error number	Error description
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!
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!

Error number	Error description
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.
9800	Registration of UMS license failed! License file doesn't exist.
9801	Registration of UMS license failed! Invalid path specification.
9802	Registration of UMS license failed! License file is invalid.
9803	Registration of UMS license failed! License file already exists.
9804	Registration of UMS license failed! UMS ID doesn't match.
9805	Registration of UMS license failed! Invalid signature.
9806	Registration of UMS license failed! License expired.
9807	Registration of UMS license failed! Error during processing.

Error number	Error description
9808	Registration of UMS license failed! Further details are not available.
9809	Registration of UMS license failed! Error processing Commandline!.
9830	The license status could not be determined! Further details are not available.
9831	The license status could not be determined! There is no data available to determine the license status.
9832	The license status could not be retrieved in JSON Format! The data could not be processed.
9850	Deletion of registered licenses failed! Database Error.
9859	Deletion of registered licenses failed! Further details are not available.

Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices

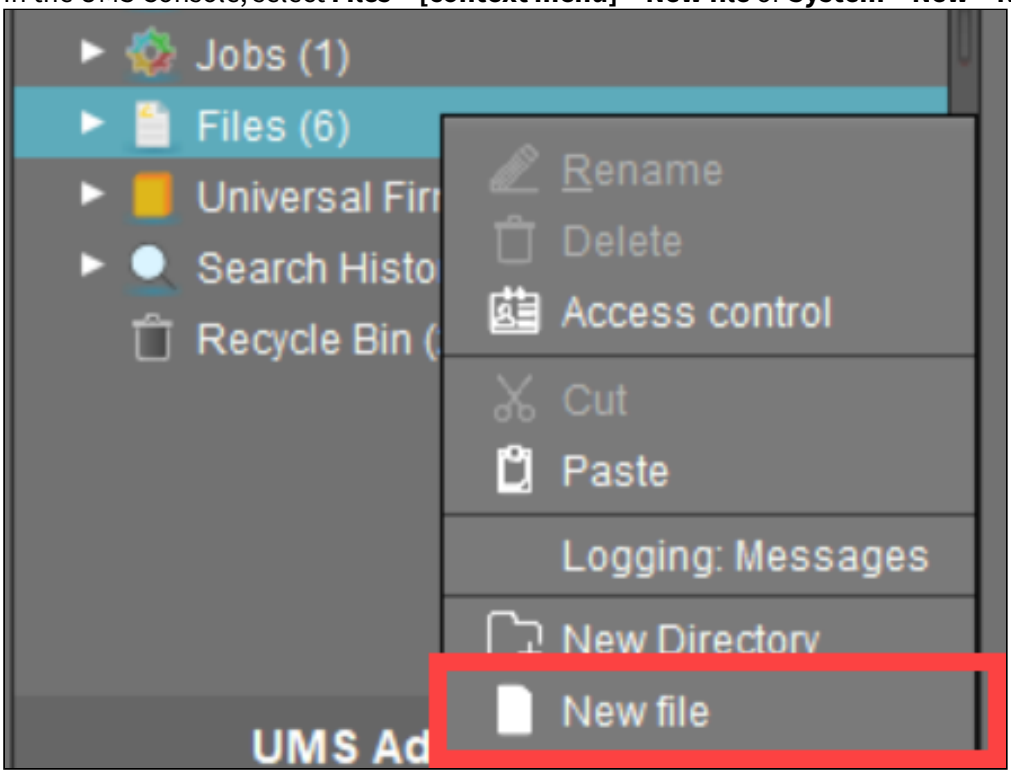
Through a **file transfer** functionality in the IGEL Universal Management Suite (UMS), you can save files in the device's local file system. A file must be registered on the UMS Server before it can be sent to the device. Examples include virus scanner signatures required locally on the device, browser 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 (see page 1290).

How to Register a File on the UMS Server

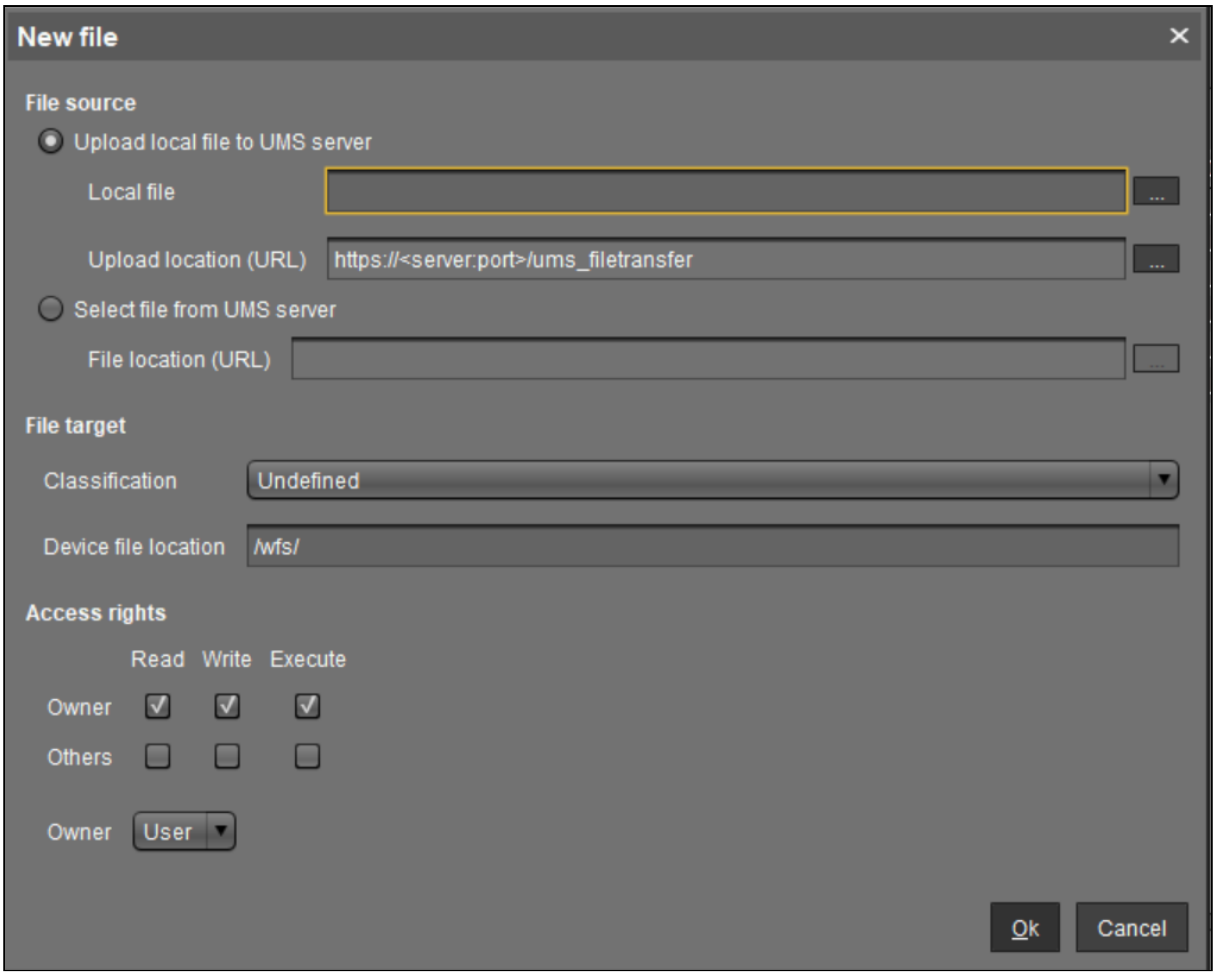
A file must be registered on the UMS Server before it can be loaded onto a device.

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**.



2. Under **File source**, select a local file or one already on the server.



3. Select the **upload location (URL)**. You can only use the directory `ums_filetransfer` or sub-directories created in it.
4. Under **Classification**, select the type of file. This serves to automatically establish suitable storage locations and file authorizations. Choose between:
    - **Undefined**
    - **Web browser certificate**
    - **SSL certificate**
    - **Java certificate**
    - **IBM iAccess certificate**
    - **App signing certificate**
    - **Common certificate**

      For information on certificate deployment, see *IGEL OS* > *IGEL OS Articles* > *Certificates* > *Deploying Trusted Root Certificates in IGEL OS*.

5. For the **Undefined** classification, specify the path in the devices'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? (see page 514)

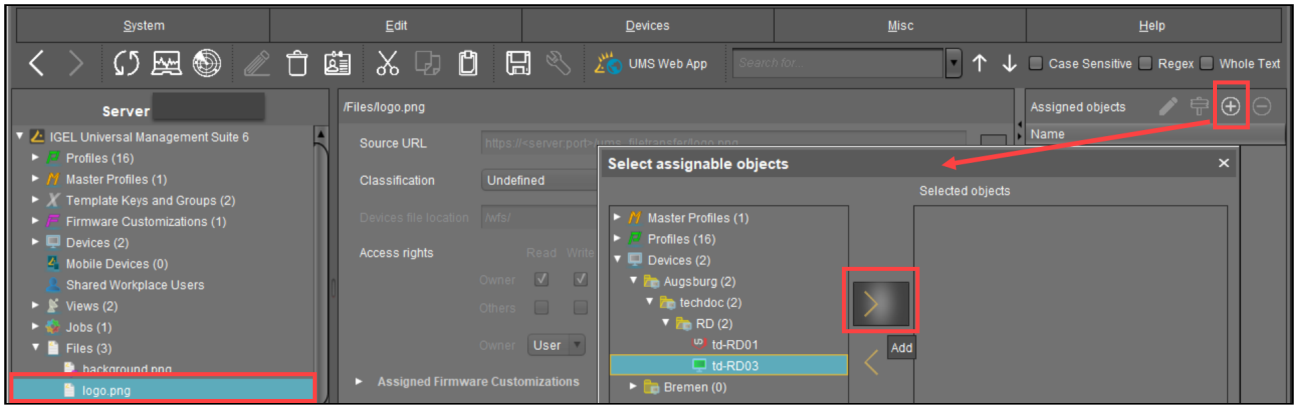
How to Transfer a File to a Device

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.

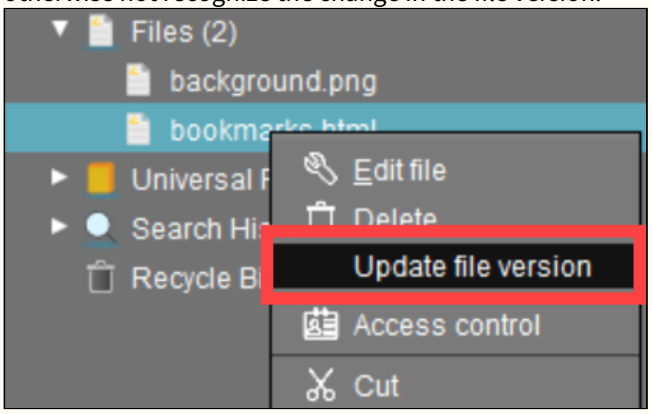
Example:



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.

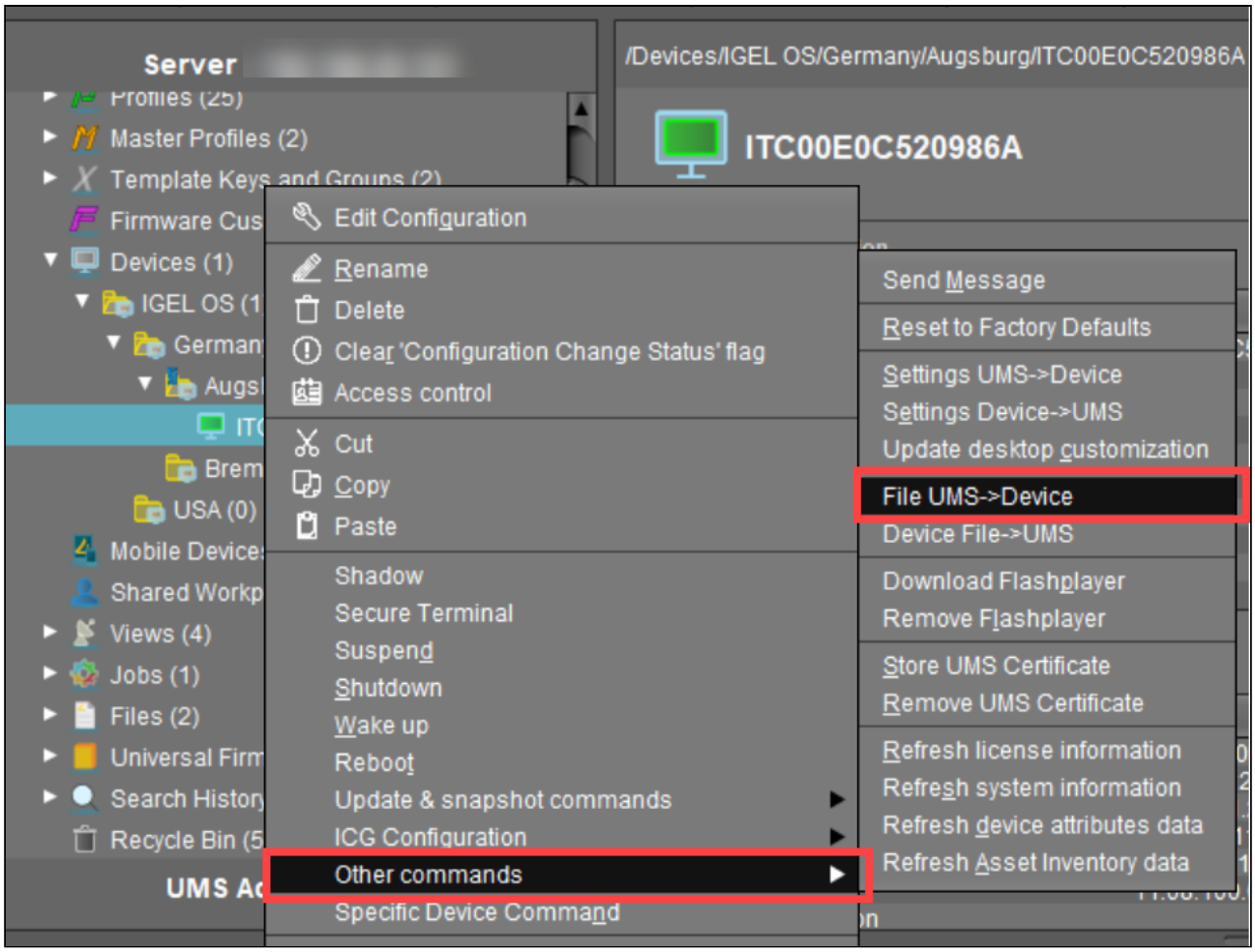
From UMS version 5.02.100, the IP address of the UMS is used when transferring the file. This ensures that the transfer works even in the event of DNS problems.

Transferring a File Without Assignment

A file registered on the UMS Server can also be transferred to the device without assignment:

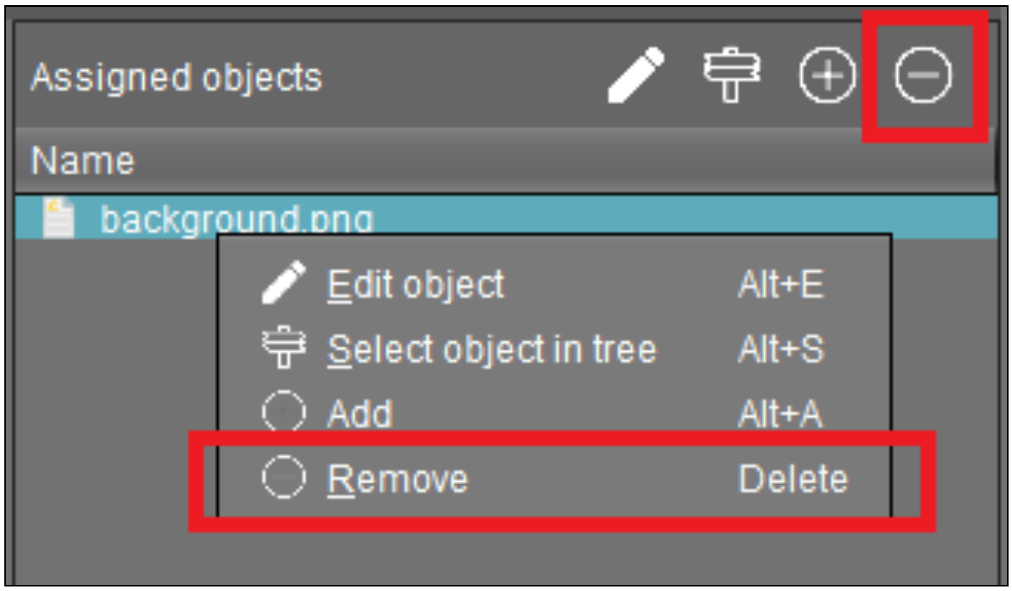
→ Select **Other commands > File UMS->Device** from the device's context menu or under **Devices** in the menu bar.

This is a straightforward file copying operation. The file is NOT updated if the file version on the UMS Server changes.

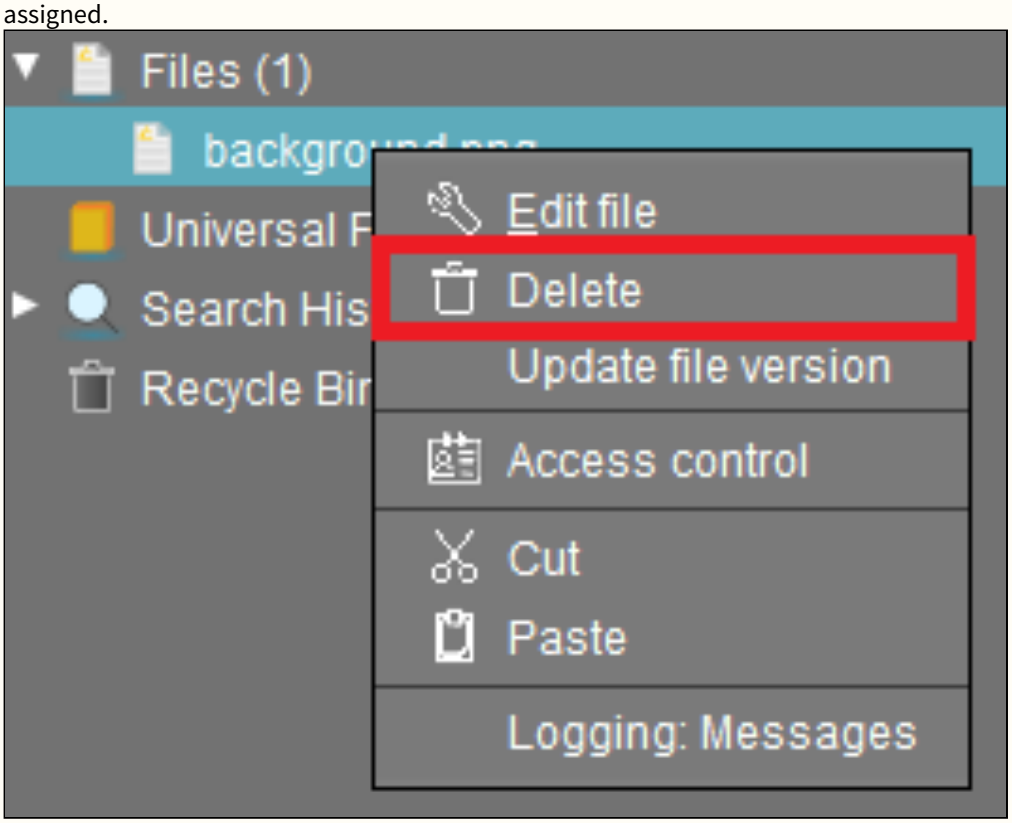


How to Remove a File from a Device

→ 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

How to Transfer a File to the IGEL UMS Server

The following article explains how you can transfer a file from your IGEL endpoint device to the IGEL Universal Management Suite (UMS). The process is different for IGEL OS 11 and IGEL OS 12 devices.

Transferring Files from OS 11 Devices

To download a file from an OS 11 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**.

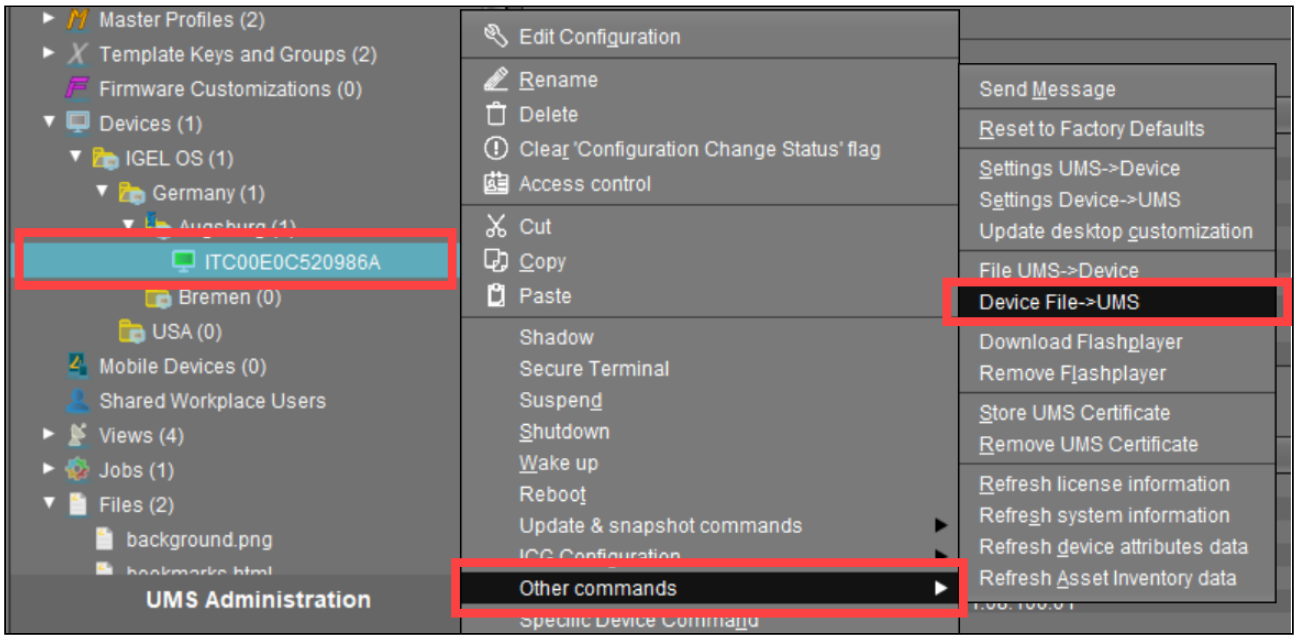
The UMS cannot search through the device's local file system. Therefore, you have to know the location and name of the file you would like to download to the web resource.

> 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 1123).

Example for How to Use the Command

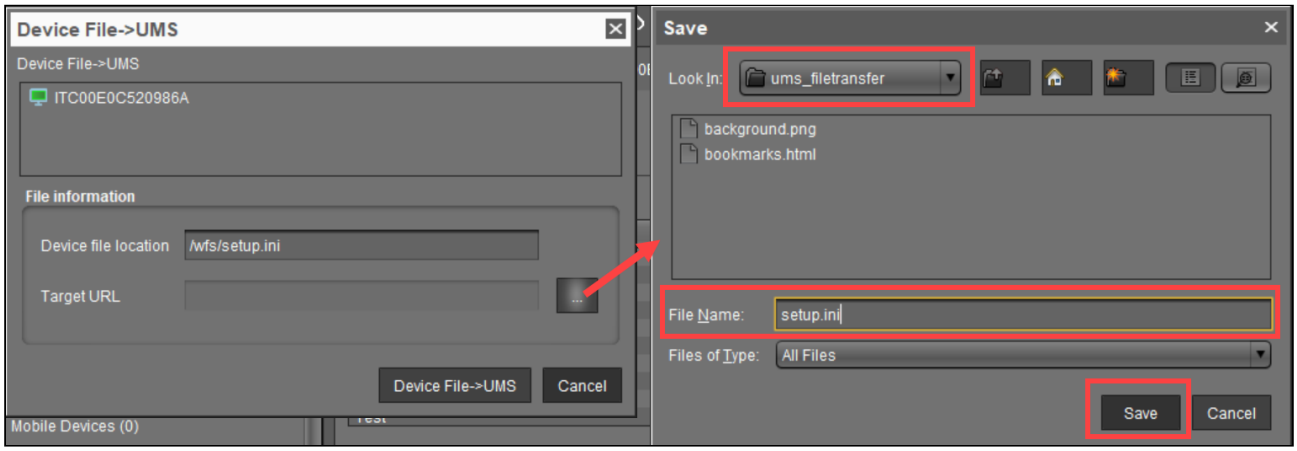
The **Device File->UMS** command can be used, for example, when you have to read out the current local configuration of the device and, thus, need to copy the two local files `setup.ini` and `group.ini` via the UMS.

1. Select **Other commands > Device File->UMS** from the device's context menu in the UMS Console.

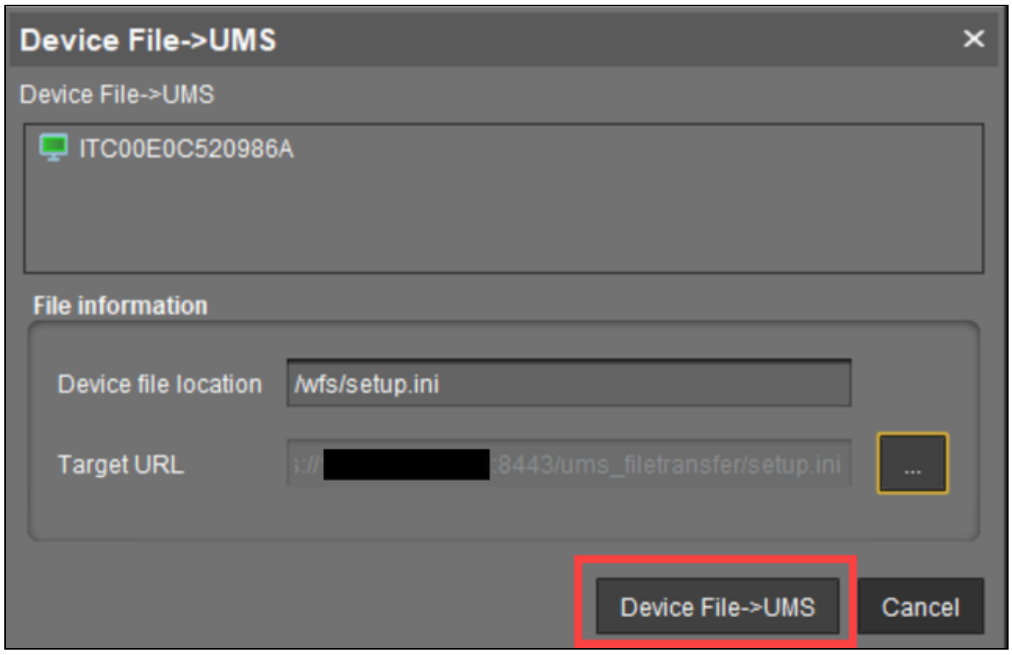


2. Under **Device file location**, specify `/wfs/` as the source.
   Example: `/wfs/setup.ini`

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[177].

177. https://kb.igel.com/en/igel-os/11.10.270/exporting-the-local-configuration-of-the-igel-os-d

Transferring Files from IGEL OS 12 Devices

To transfer files from IGEL OS 12 devices:

1. Enable SSH as described in SSH Access in IGEL OS 12[178] .

2. Use scp from a linux or windows terminal:

```
scp username@remote:/path /localpath
```

- Depending on the SSH access configuration, `username` could be `root` , `ruser` , or `user` .
- `remote` is the IP address of the OS 12 device.
- `/path` it the path to the `get_settings.json` on the OS 12 device
- `/localpath` is the path to where the file will be saved locally

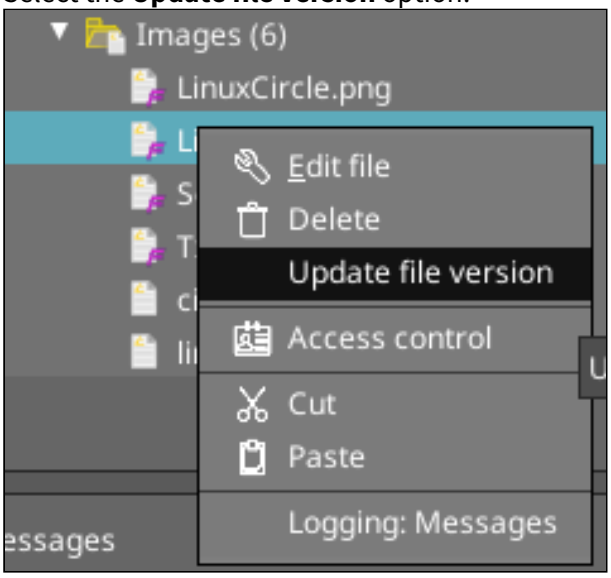
178. https://kb.igel.com/en/igel-os-base-system/12.6.1/ssh-access-in-igel-os-12

How to Update a File Version in the IGEL UMS

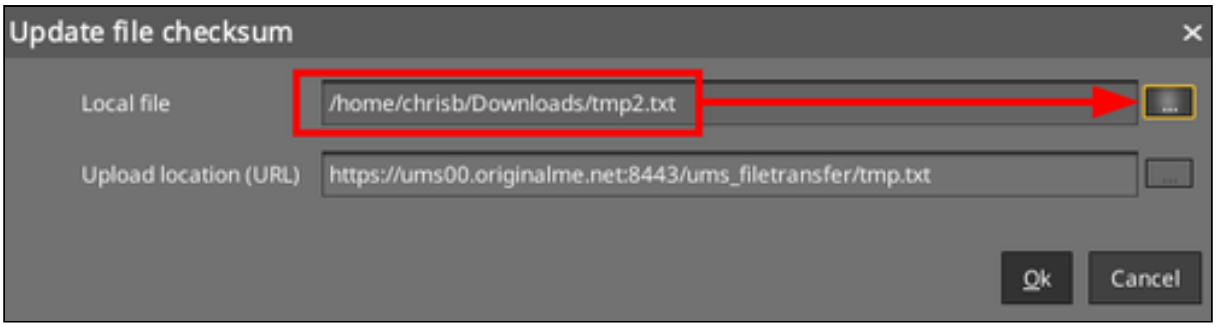
In order to update a file version once it is deployed to a device, you will want to utilize the **Update File Version** option in the IGEL Universal Management Suite (UMS).

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_filetransfter 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.

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

It is not always necessary to use these registration methods, since
- OS 12 devices get registered 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[179].
- OS 11 devices get registered when you set up the IGEL Cloud Gateway[180] on the device in the Setup Assistant for IGEL OS[181] or the ICG Agent Setup[182].

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

- Scanning the network for devices and registering the found devices
  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
  If you enable automatic registration and configure the DHCP tag and/or the DNS alias `igelrmserver` with the IP or FQDN of the UMS Server, all devices on the server's network will be automatically registered at startup.

IGEL recommends automatic registration when registering new 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 Onboarding IGEL OS 12 Devices[183].
Disable automatic registration as soon as all devices have been registered, so that no unknown devices can obtain sensitive settings.

- Importing devices
  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

179. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices
180. https://kb.igel.com/en/igel-cloud-gateway/current/icg-manual
181. https://kb.igel.com/en/igel-os/current/setup-assistant-for-igel-os
182. https://kb.igel.com/en/igel-os/current/using-icg-agent-setup
183. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices

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
  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.com/watch?v=1XMWDpv2wDI

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

https://www.youtube.com/watch?v=_evv-Vlixwg

How to Scan the Network for Devices and Register 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 and for the UMS Web App.

For an overview of device registration methods, see Registering IGEL OS Devices on the UMS Server (see page 1134).

> 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 Reverse Proxy in IGEL OS with SSL Offloading (see page 297) .

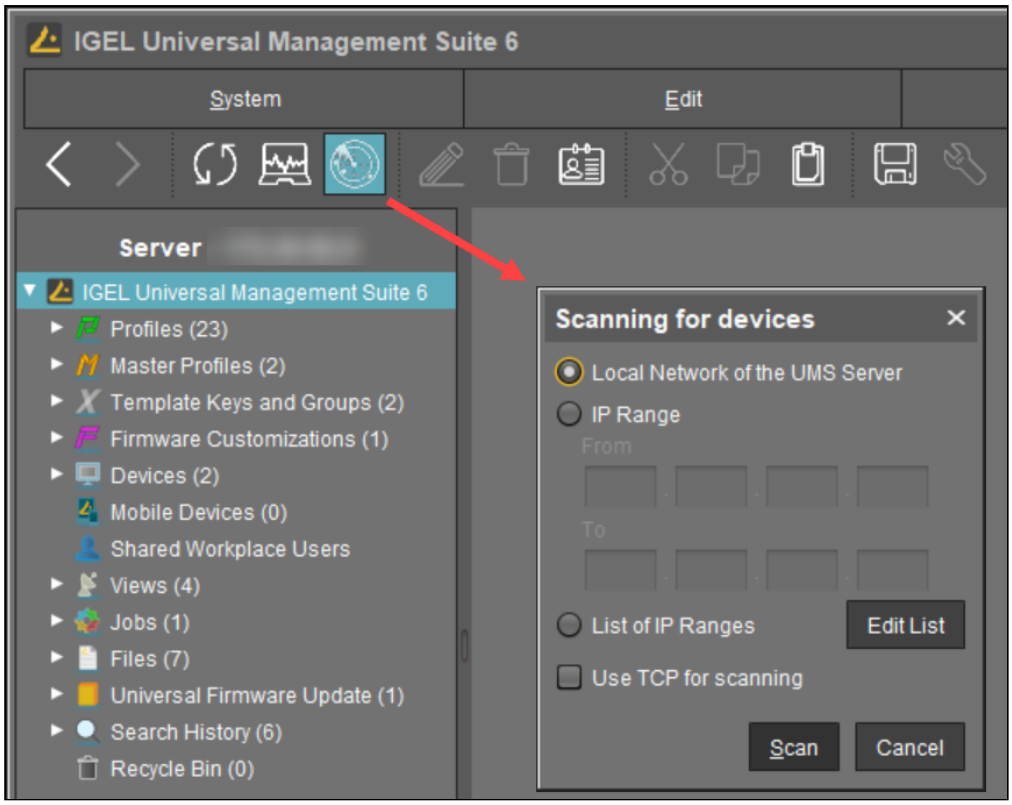
In order to find devices in the network, the following requirements must be met:

- 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.

     If there are a number of network interfaces, you should bear in mind that the broadcast message is only sent via the first network interface. If you use Windows, this is under the first item in the list of network connections.

   - **IP Range**: The UMS Server contacts each device in the given range.
   - **List of IP Ranges**: With **Edit list**, you can specify the IP ranges in which the UMS will search for devices.
   - **Use TCP for scanning**: If this option is enabled, communication with the devices will take place via TCP. If this option is disabled, UDP will be used.

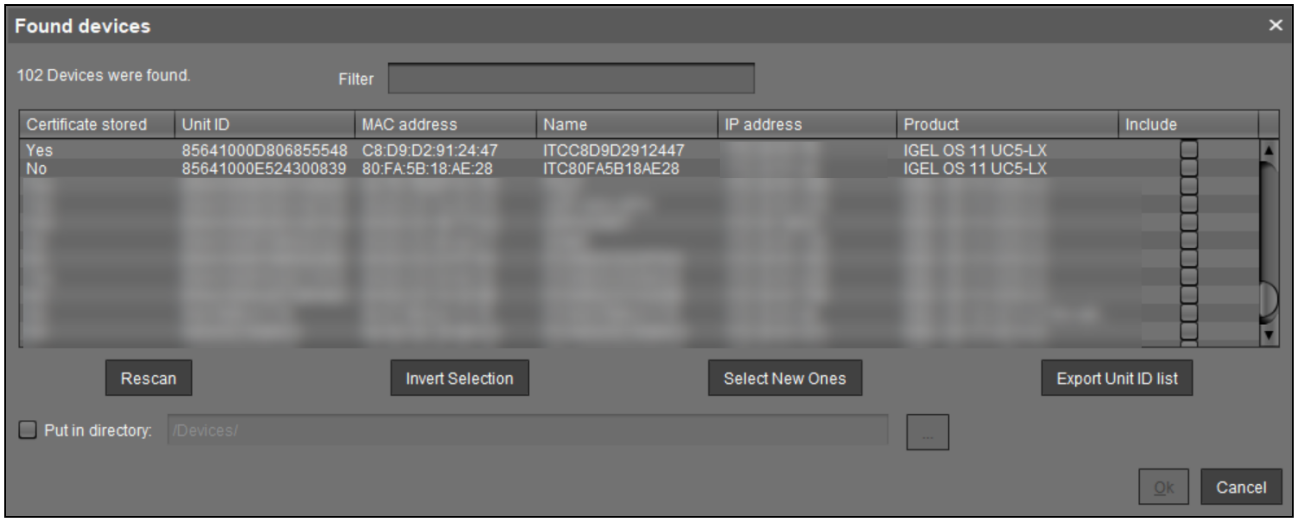
If TCP is used for searching, the search procedure will take longer; the scan results can be more reliable, however.

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

Devices with IGEL OS 12 that are already registered will not appear in the **Found devices** window. This is because IGEL OS 12 closes the scan port after registration with the UMS.

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** (only valid for IGEL OS 11 devices), **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.



Only valid for IGEL OS 11 devices: 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 already has 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 IGEL UMS Console (see page 693).
  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 (see page 533).

2. Select the devices that are to be registered. You have the following options:
   - Manual selection: In the **Include** column, highlight the devices that are to be registered.

- Selecting all devices that are not yet registered: Click on **Select New Ones**. This will highlight all devices that have not yet received a server certificate from the UMS.

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

> During registration, the UMS Server certificate is saved on the device. Further access to the device will now be validated on the basis of this certificate. Only the owner of the certificate can manage the device.

The result of the procedure and any error messages will be displayed in a new window. The devices will be placed in the **Devices** directory in the structure tree if no other directory was specified under **Put in directory**.

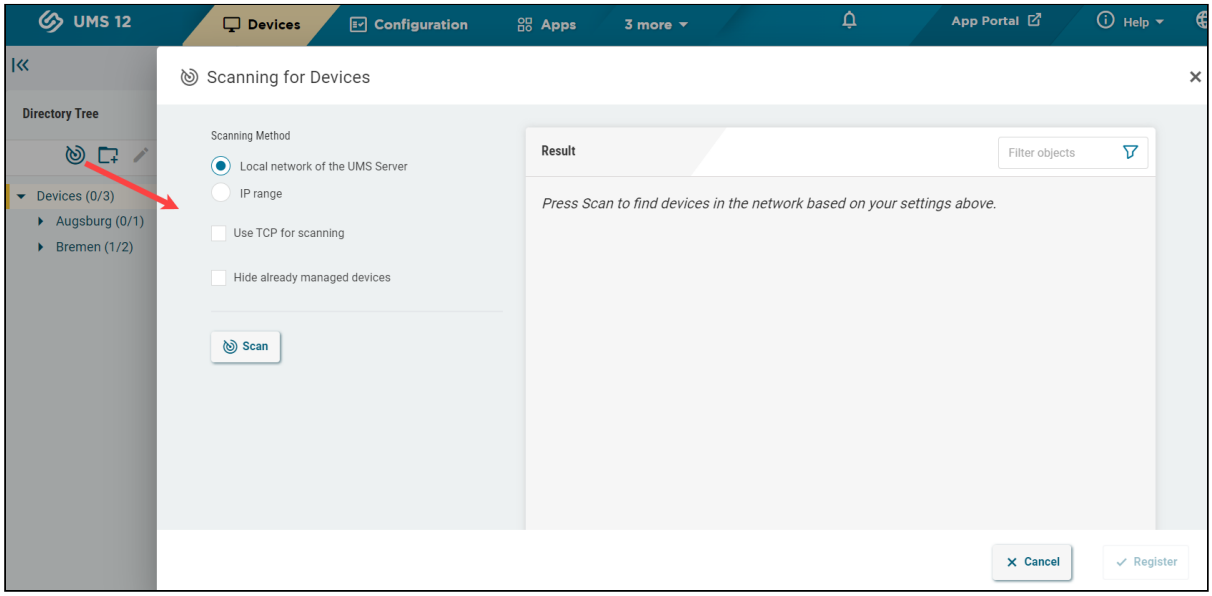
Scan and Register Function in the UMS Web App

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.

     > 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.

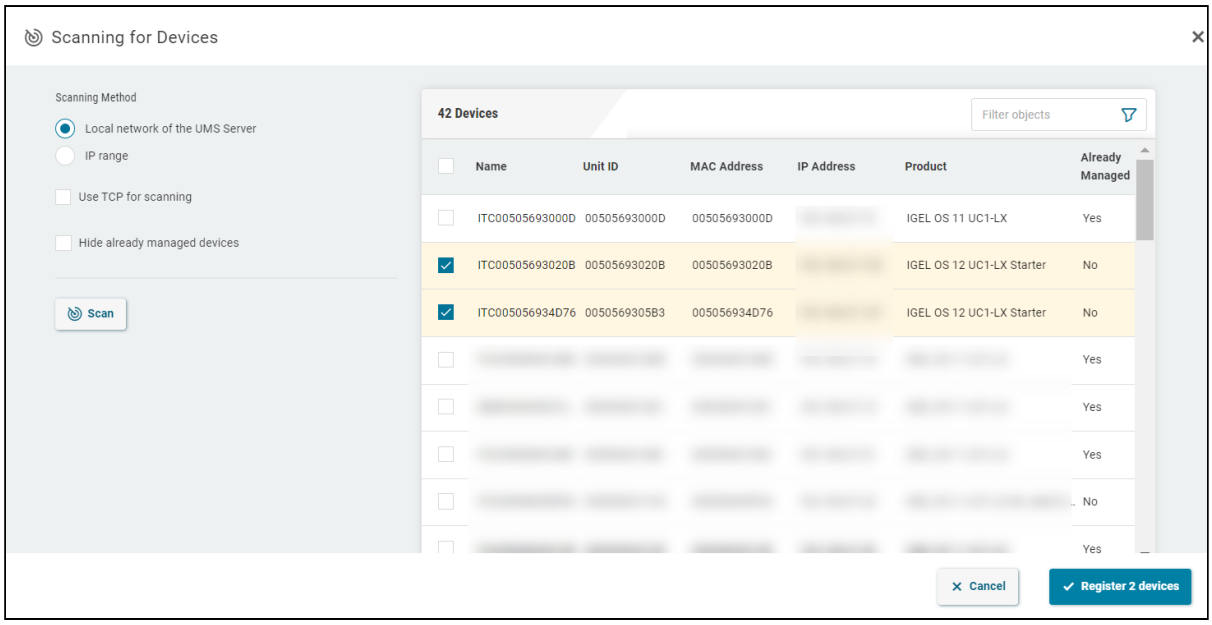
     > If TCP is used for searching, the search procedure will take longer; the scan results can be more reliable, however.

   - **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.

> Devices with IGEL OS 12 that are already registered will not appear in the **Found devices** window. This is because IGEL OS 12 closes the scan port after registration with the UMS.

As soon as you have obtained the search result, you can register new devices.

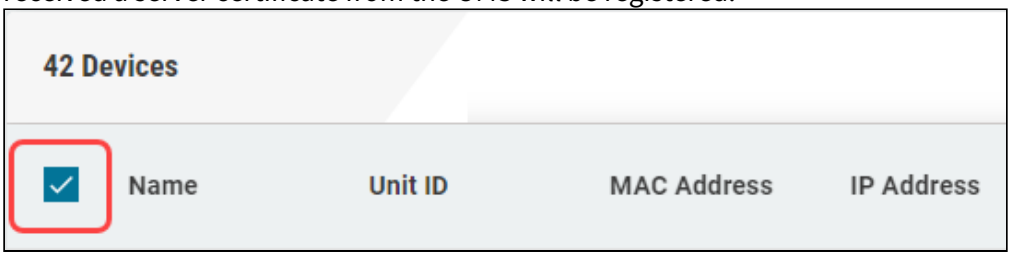
1. If you only want to see devices with a specific feature in the **Name**, **Unit ID**, **MAC Address**, **IP Address**, or **Product** column, enter the corresponding character string in the **Filter** field.
   Only valid for IGEL OS 11 devices: To filter the results in the **Already Managed** column, enable or disable **Hide already managed devices**.



Only valid for IGEL OS 11 devices: 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 864) 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 (see page 533).

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.



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.

> 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.

> In order for devices to be registered fully, the devices' firmware data must be available in the UMS. Further information can be found under How to Import Firmwares in the IGEL UMS (see page 800).

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 1151), 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 1144)
    - **Long Format**: See Import with Long Format (see page 1146)
    - **IGEL Serial Number Format**: See Import with IGEL Serial Number (see page 1149)
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 UMS (see page 903) .

- **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

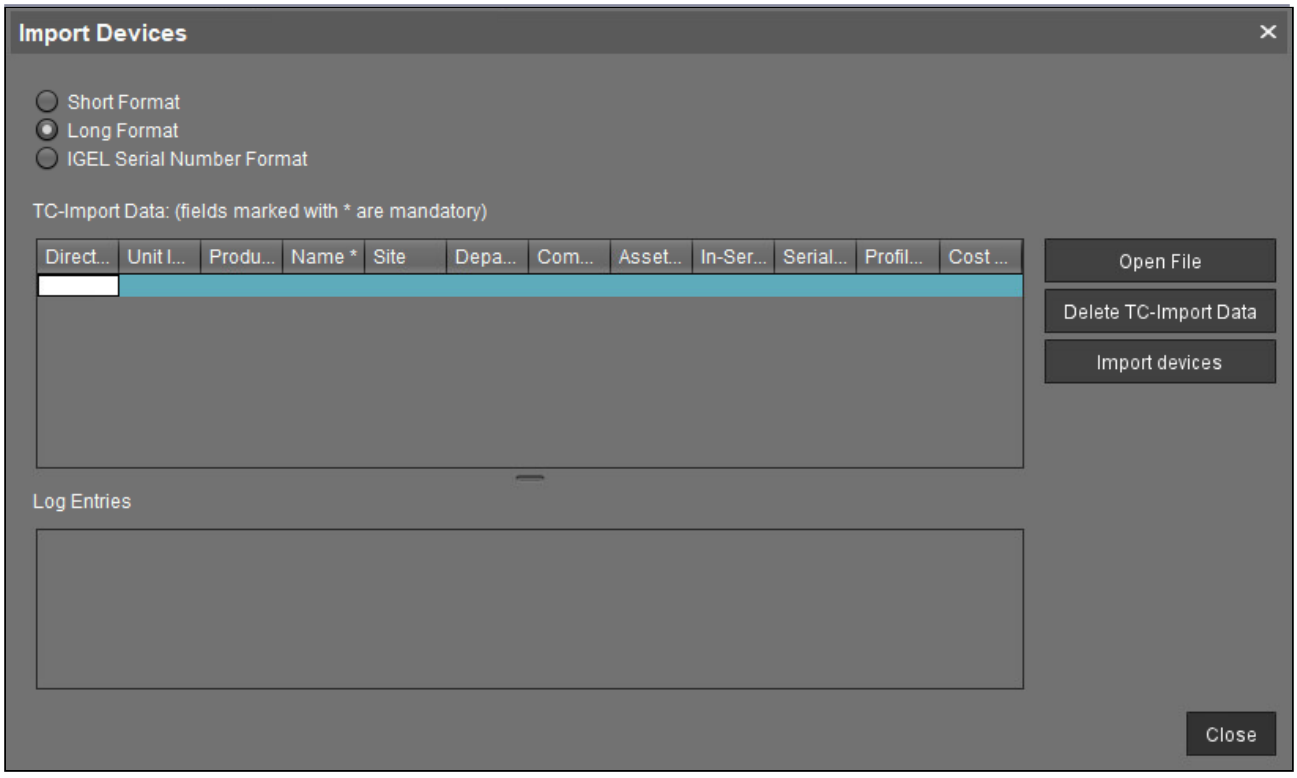
```
00E0C5540B8B;IGEL-Office15-2;111;26
```

```
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 this article. 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 UMS (see page 903).

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 Examples

For OS 11 Devices

For OS 11 devices use the following format in the uploaded CSV:

```
/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-3;Büro3;EDV;Schulz;42;01.06.2019;F46M;26;01
```

The 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).

For OS 12 Devices

For OS 12 devices use the following format in the uploaded CSV:

```
/Import;00E0C5540B9A;IGEL OS Base
System;12.4.2;IGEL-1;Büro1;EDV;Meier;0815;01.06.2019;F44M;26;01
```

The 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 UMS (see page 903).

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 How to Automate the Rollout Process in the IGEL UMS (see page 418).

For a general overview of device registration methods, see Registering IGEL OS Devices on the UMS Server (see page 1134).

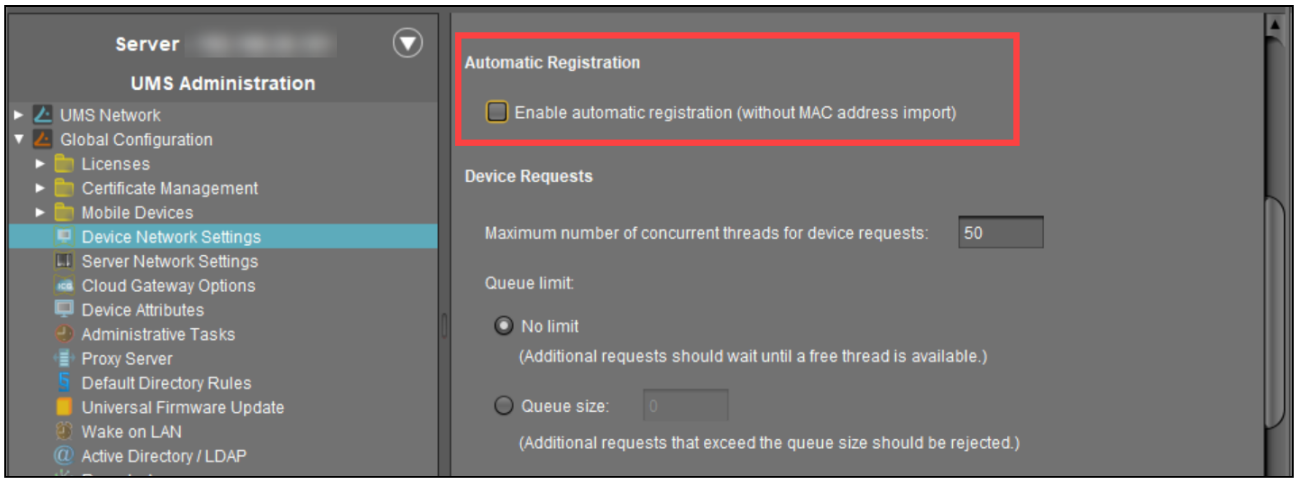
You can configure the UMS Server so that all IGEL OS devices on the server's network are automatically registered at startup. To do this, the devices must be given the address of the UMS Server via **DHCP or DNS**.

> 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 *How to Start with IGEL > 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.

> 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

IGEL UMS Web App

The IGEL Universal Management Suite (UMS) Web App is a web-based user interface to the UMS Server. The installation of the UMS Web App is handled via the UMS installer, see IGEL UMS Installation (see page 13).

> ⚠ The UMS Web App can currently be used only in addition to the Java-based UMS Console. Some features are currently available only in the UMS Web App, others only in the UMS Console; see the feature matrix under Overview of the IGEL UMS (see page 661).
> The range of functions available in the UMS Web App will constantly be expanded.
> All features that are already available in the UMS Web App are fully supported.

The main features of the UMS Web App include:

- managing device configuration and creating profiles
- shadowing of devices and various device commands (power control, update, sending/receiving settings, reset to factory defaults, etc.)
- assigning objects to devices and device directories
- importing and managing IGEL OS Apps and their versions
- monitoring the status of the UMS network
- configurable search functionality
- logging of actions

> ℹ If you would like to learn more about the role of the UMS Web App in your IGEL Environment, you can read our guide How to Start with IGEL[184], or take a look at the IGEL Academy[185] Courses.

184. https://kb.igel.com/en/how-to-start-with-igel/current/introduction
185. https://learn.igel.com/learn

Important Information for the IGEL UMS Web App

Take notice of the following information regarding the IGEL Universal Management Suite (UMS) Web App.

Supported Environment

- The minimal supported resolution is 768 px.
  If you want to use the UMS Web App on mobile devices, note that the min. supported width for the responsive design is 768 px.
- For RAM and disk space requirements, see Installation Requirements for the IGEL UMS (see page 10).
- For the supported browsers, see the “Supported Environment” section of the release notes[186] (as of UMS 12.08.100).

Installation

- In the case of a High Availability or Distributed UMS environment:
  - The UMS Web App does not necessarily have to be installed on every UMS Server. If you choose, however, to install the application on several UMS Servers, you can use it on all of them. The data will be synchronized.
  - The UMS Console and the UMS Web App can be installed on different servers.

Login

- The login data of the database user are not accepted for the UMS Web App. For how to log in to the UMS Web App, see How to Log In to the IGEL UMS Web App (see page 1157).

Permissions

- The UMS Web App and the UMS Console share the same permissions. For detailed information on access rights in the IGEL UMS, see General Administrator Rights in IGEL UMS[187].
- There are some permissions only applicable to the UMS Web App – **Delete Log Messages**, **Device Bulk Action**, and **App Management**. They can be set in the UMS Console under **System > Administrator accounts > New / Edit > General - WebApp** or in the UMS Web App in the **User Management** area. (see page 1362)
- Read permissions to a directory enable access to devices in this directory; permissions only to devices are not sufficient.
- For the assignment of apps (exception: IGEL OS Base System), you require the same permissions as for the assignment of profiles to devices, see Assignment of Objects (see page 1020). This is due to the fact that non-base-system apps are automatically assigned to devices via profiles that configure these apps (so-called implicit app assignment).

186. https://kb.igel.com/en/universal-management-suite/current/ums-release-notes
187. https://kb.igel.com/en/universal-management-suite/current/general-administrator-rights-in-igel-ums

- For the assignment of the IGEL OS Base System, the permission **Assign Base System / Firmware Update** is required (set under **UMS Console > Devices > [context menu of the device / device directory] > Access Control**).
- The following permissions are required:
  - Rights for the node **Server Network Settings** under **UMS Console > UMS Administration > Global Configuration** for the access to
    - **UMS Web App > Apps > Settings > App Portal**
    - **UMS Web App > Apps > Settings > Automatic Updates**
    - **UMS Web App > Network > Settings > Network > UMS Network Nickname**
    - **UMS Web App > Search > Settings**
  - Rights for the node **UMS Features** under **UMS Console > UMS Administration > Global Configuration** for the access to
    - **UMS Web App > Apps > Settings > UMS as an Update Proxy**
    - **UMS Web App > Network > Settings > UMS Features**
  - Rights for the node **First-authentication Keys** under **UMS Console > UMS Administration > Global Configuration** for the access to
    - **UMS Web App > Devices > Settings > First Authentication Keys**

Synchronization between the UMS Console and the UMS Web App

- The UMS Web App and the UMS Console share the same database, user rights, and certificates.
- Changes made in the UMS Console are immediately available in the UMS Web App, and vice versa.
- Device changes and permission changes because of moving a device to another directory are reported almost instantly to the indexer, so that all changes are immediately searchable. However, the change of permissions for a user or a group is currently not recognized “on the fly”. A user needs to log out and log in again for these changes to take effect.

Logging

- Not all actions performed in the UMS Console are displayed in the UMS Web App. Logs of the UMS Web App are not displayed in the UMS Console.
- Log files for the UMS Web App can also be found in `/rmguiserver/logs/wums*`

Certificate

- By default, browsers do not accept the self-signed certificate used by the UMS Server and display a security warning. For how to solve the problem, see Troubleshooting: Browser Displays a Security Warning (Certificate Error) when Opening the UMS Web App (see page 564).

Bulk Actions

- The simultaneous selection of several devices or directories is currently not possible. If you want to execute bulk commands, you can do it now only by selecting an individual directory.

How to Log In to the IGEL UMS Web App

The following article describes how you can open the IGEL Universal Management Suite (UMS) Web App and which credentials you can use to log in. For a short overview of the UMS Web App, see IGEL UMS Web App (see page 1154).

Centralized Login Process

→ If you are using IGEL UMS version 12.08.100 or higher, you can log in to the UMS Web App together with the UMS Console with the centralized login process. For instructions, see Connecting the UMS Console to the IGEL UMS Server[188] .

> To ensure that all UMS users can log in to the UMS without any issues, please check the UMS Login Requirements[189].

Troubleshooting

If you experience any issue during the login, see the related troubleshooting articles under Start of the UMS Console / Web App[190] .

How to Access the IGEL UMS Web App

To open the IGEL UMS Web App:

→ In the web browser, open the URL `https://<server>:8443/webapp` .

> "8443" is the default GUI server port, see "GUI server port" under Settings - Change Server Settings in the IGEL UMS Administrator (see page 1038). For detailed information on the UMS ports, see IGEL UMS Communication Ports (see page 256).
> If you have changed the GUI server port, adjust the URL accordingly.

OR

→ If you are logged in to the UMS Console, click the icon in the symbole bar:

Login Data for the IGEL UMS Web App

To log in to the IGEL UMS Web App, you can use:

188. https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server
189. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements
190. https://kb.igel.com/en/universal-management-suite/current/start-of-the-ums-console-web-app

- The credentials of the UMS superuser, which can be changed in the UMS Administrator, see Changing the UMS Superuser (see page 1070), or in the UMS Web App, see How to Change User Password in the IGEL UMS Web App[191] .
- The additionally created administrator accounts, which can be added in the **UMS Console > System > Administrator accounts**, see How to Create Administrator Accounts in the IGEL UMS[192], or in the UMS Web App, see User Management and IdP Management in the IGEL UMS Web App[193] .

⚠ The login data of the database user are not accepted for the UMS Web App.
For users imported via LDAP enter the **Username** in the <username>@<domain> format. For example:
`username@domainname.com`

ℹ The UMS implements login brute-force protection:
- After several failed login attempts, the user account will be temporarily blocked. This includes also accounts that do not exist.
- To prevent probing, dynamic login delay (milliseconds) is implemented. This is required since the response time could be an indicator of the (non-)existence of an account.

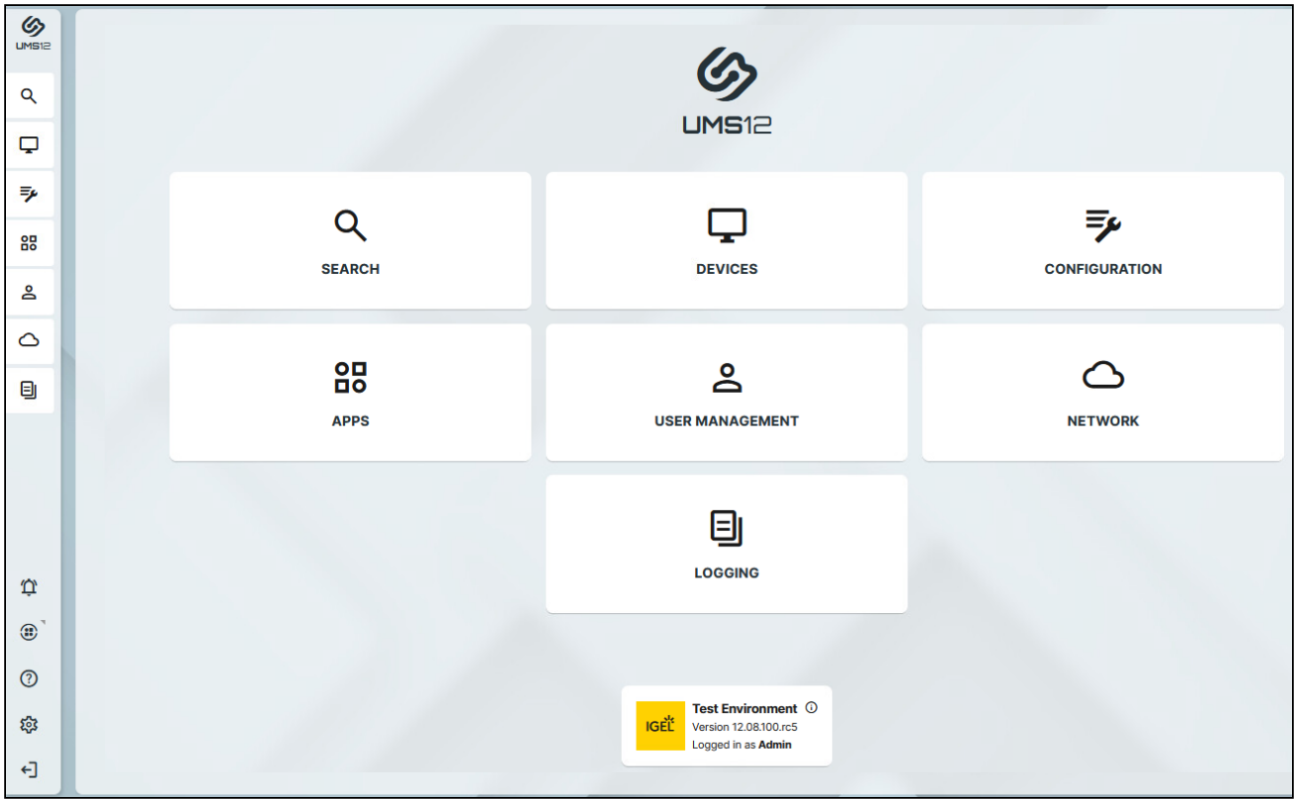
191. https://kb.igel.com/new-features/current/how-to-change-user-password-in-the-igel-ums-web-ap
192. https://kb.igel.com/en/universal-management-suite/current/how-to-create-administrator-accounts-in-the-igel-u
193. https://kb.igel.com/en/universal-management-suite/current/user-management-and-idp-management-in-the-igel-ums

IGEL UMS Web App User Interface

The following article describes the user interface of the IGEL Universal Management Suite (UMS) Web App that is introduced with the IGEL UMS version 12.03.100.

You can also find information about the new user interface in this IGEL Community video (see page 1163).

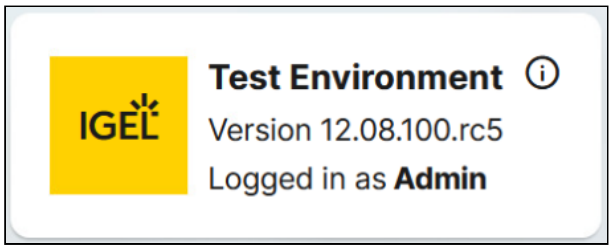
Home Page



→ Click the tiles or the corresponding sidebar buttons to go to an area. For more Information on each area, see:

- Search for Devices in the IGEL UMS Web App (see page 1164)
- Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App (see page 1176)
- Configuration - Centralized Management of Device Settings in the IGEL UMS Web App (see page 1239)
- Apps - Import and Configure Apps for IGEL OS 12 Devices via the UMS Web App (see page 1294)
- User and Role Management in the IGEL UMS Web App (see page 1362)
- Network Settings in the IGEL UMS Web App (see page 1347)
- Logging in the IGEL UMS Web App (see page 1353)

System Info Box



The info box at the bottom of the home page shows version information on your IGEL UMS and the username of the currently logged-in user. If specified, the nickname of your UMS is also displayed here; see Network Settings in the IGEL UMS Web App (see page 1347).
The same info box is also displayed on most of the areas.

→ Click to view further details.

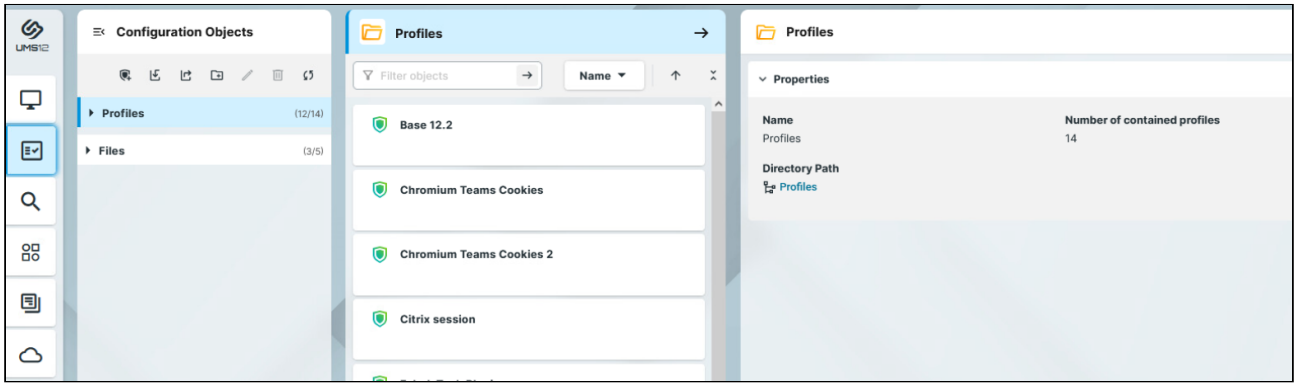
Sidebar Buttons

	Takes you back to the home page.
	Under **Messages**, you can view the current state and the results of the device commands and of other actions such as the import of IGEL OS Apps, etc. The messages are automatically deleted at the reloading of the UMS Web App page in the browser. → Click a message to view details. • A successfully executed command is marked with • A failed command is marked with a warning symbol • A partially failed command is marked with a warning symbol
	Direct link to the IGEL App Portal. The link opens in a new browser tab.

	Under **Help**, you can: • find a link to the UMS Web App documentation on kb.igel.com[194]. The link opens in a new browser tab when clicking **Open Knowledge Base**. • **Save Support Information** for the IGEL UMS, see How to Save Support Information and Log Files in the IGEL UMS Web App (see page 1382). • find a link to Quick Start Configuration Profiles for Setting up Your IGEL Environment[195] to **Download Quick Start Configurations**.
	Under **Preferences**, you can: • set the language of the IGEL UMS Web App • change the appearance to **Dark Mode** or **Light Mode** • change the password of the currently logged-in local user, including the UMS superuser. For more information, see How to Change User Password in the IGEL UMS Web App (see page 1379).
	Logout from the UMS Web App

Layout

In the **Search**, **Devices**, **Configuration**, **Apps** and **Network** areas, the interface is organized into a horizontal layout where the window is divided into several panels.



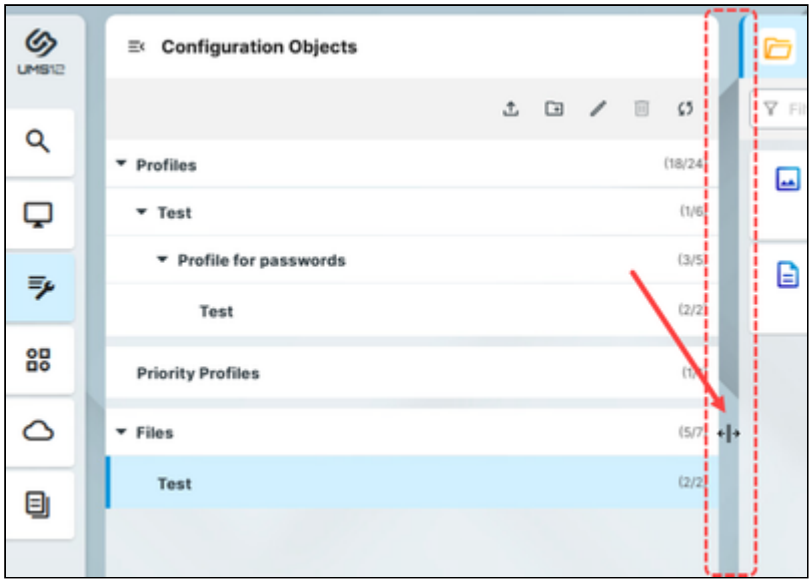
Generally, the information displayed on the panels and the functions follow a left to right logic. That means, you will find:

- structuring on the left,
- list of items to be managed in the middle,
- detailed information and item management on the right.

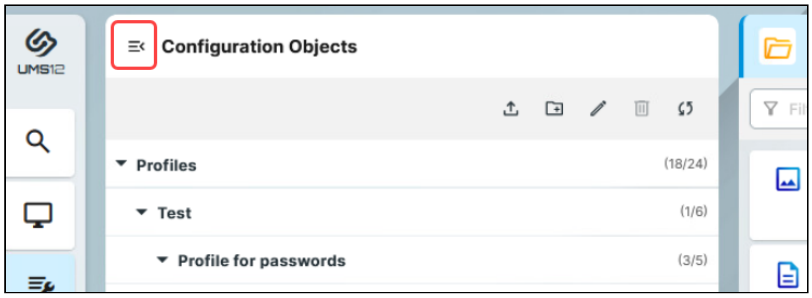
194. http://kb.igel.com/
195. https://kb.igel.com/en/how-to-start-with-igel/current/quick-start-configuration-profiles-for-setting-up-

Changing the Layout

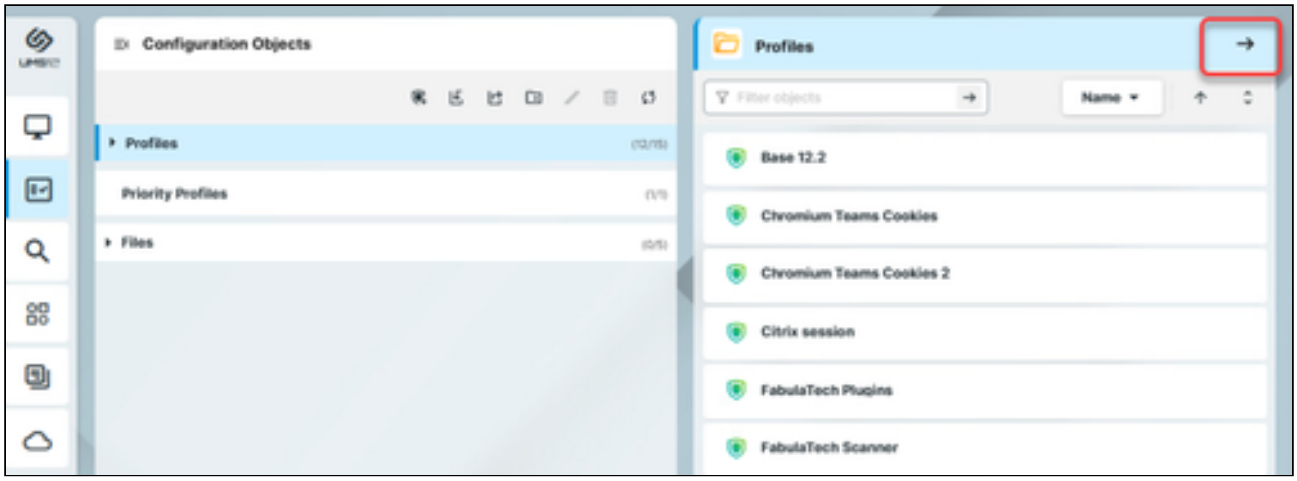
You can change the width of the panels by clicking and holding in between the panels as you resize the panel:

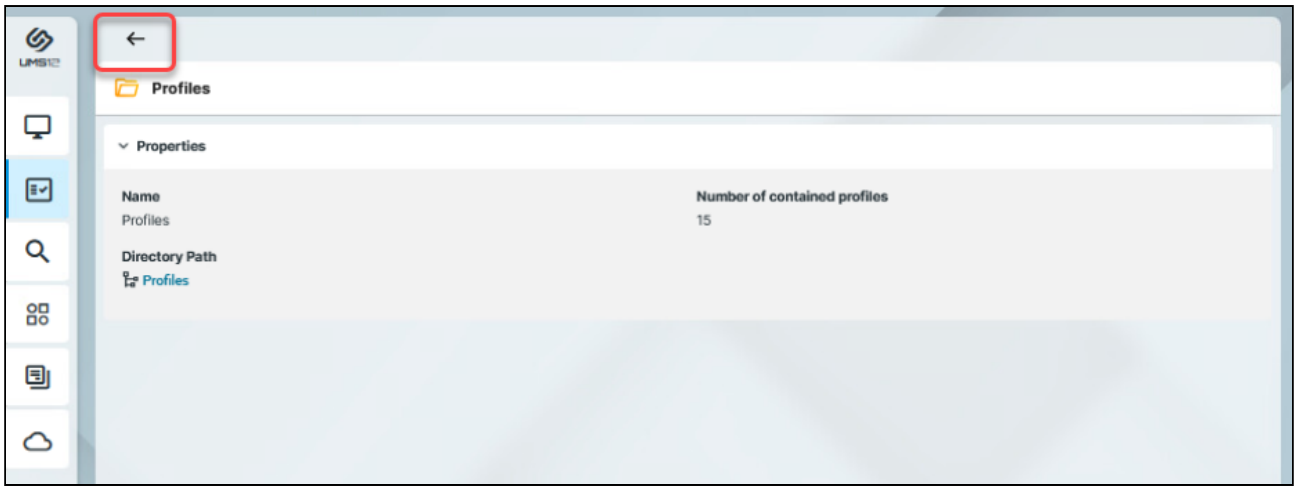


You can collapse and expand the left panel by clicking the icon in the top corner:



When the browser window gets resized, and there is not enough space to display all the panels next to each other, you can use arrows to switch between the panel





IGEL Community Video - New User Interface

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

https://www.youtube.com/watch?v=rhx98Af6Bxs

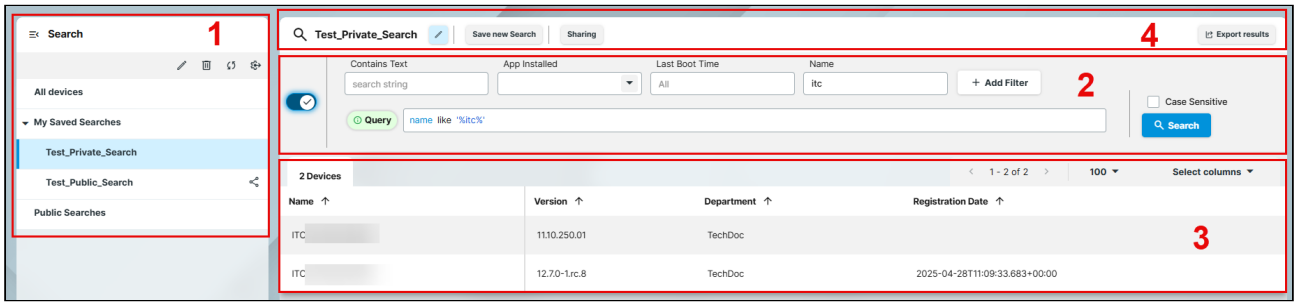
Search for Devices in the IGEL UMS Web App

In the **Search** area of the IGEL Universal Management Suite (UMS) Web App, you can search for devices according to the configured criteria and save your search for later.

You can also create Advanced Searches, that you can use in Jobs and Administrative Tasks in the UMS Console, see How to Use Advanced Search in the IGEL UMS Web App[196].

> The **Search** feature of the UMS Web App is a successor to views in the UMS Console (see page 818). It does not currently include all the criteria that are available for views but the range of the criteria will constantly be expanded.

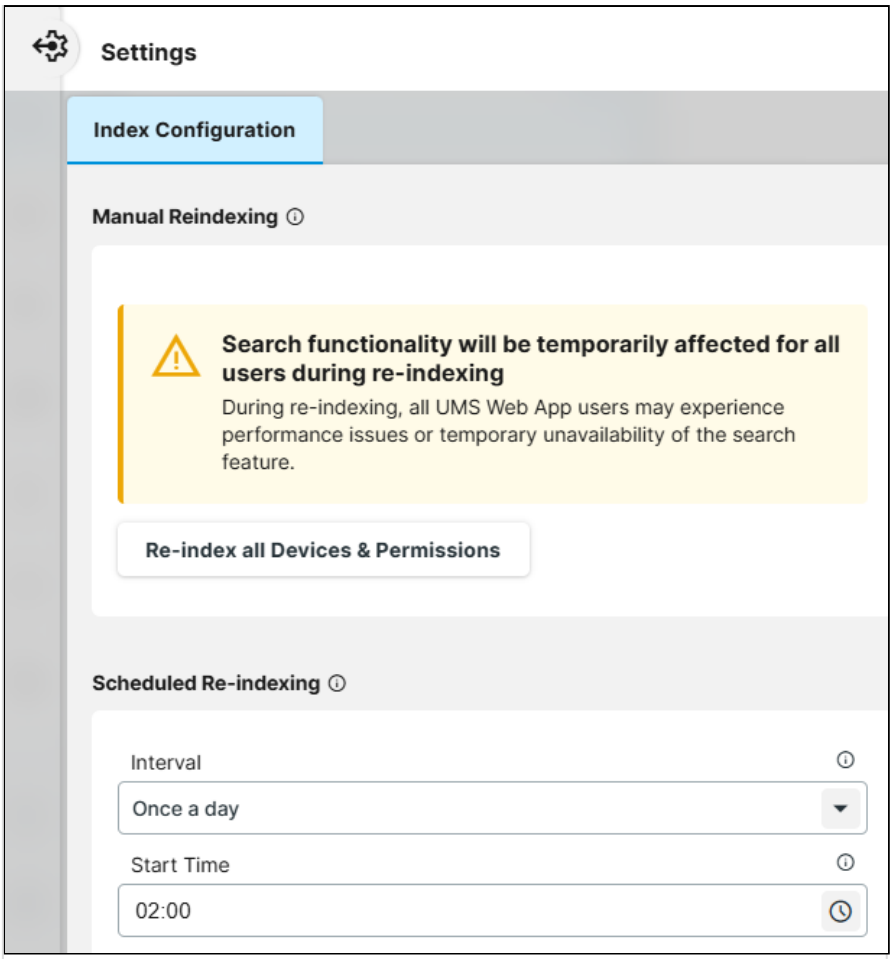
Menu path: **UMS Web App > Search**



196. https://kb.igel.com/en/universal-management-suite/current/how-to-use-advanced-search-in-the-igel-ums-web-app

1	List of searches	You can find here the list of all searches that you saved. → To collapse the list to the left, click  at the top. Selecting **All devices** shows a result list of all the devices registered in the UMS with no values specified for the filters. Under **My Saved Searches**, you can find the searches that you created and saved. If you see the  icon next to the search, the search is shared with other users of the UMS. → To rename a search, select the search and click  . Enter a new name and press `[Enter]` or click the tick. → To delete a search, select the search and click  . ⚠ Searches are removed permanently, i.e. without being placed into the recycle bin (see page 864). Under **Public Searches**, you can find searches shared by other users of your UMS. For details, see How to Share Searches in the IGEL UMS Web App (see page 1171) . ℹ You cannot rename or edit searches under **Public Searches**. Those searches can only be edited by the users who created and shared them. → Click  to open the **Settings** area. For the access, you require rights for the node **Server Network Settings** under **UMS Console > UMS Administration > Global Configuration**. For more information on rights, see Object-Related Access Rights[197].

197. https://kb.igel.com/en/universal-management-suite/current/object-related-access-rights



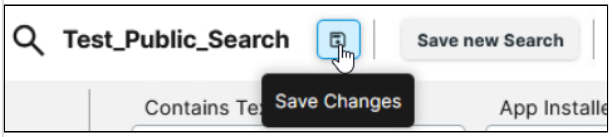
Reindex all devices and permissions: Triggers the immediate reindexing of the database. Note that all UMS Web App users may experience performance issues or temporary unavailability of the search feature during the reindexing.

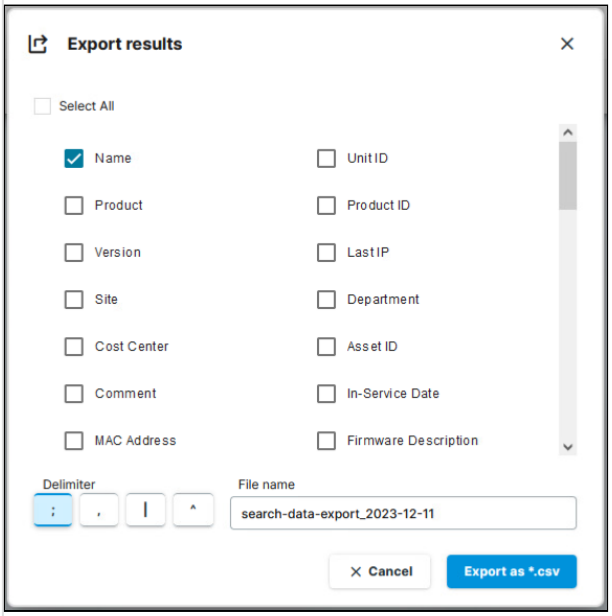
Scheduled reindexing: Defines when and how often the index should be fully re-created. This ensures that no devices changes are missed from the search.

Interval: Specifies how frequently the index should be fully rebuilt. (Default: Once a day)

Start time: Start point from which the next index rebuild will be calculated based on the defined interval. (Default: 02:00)

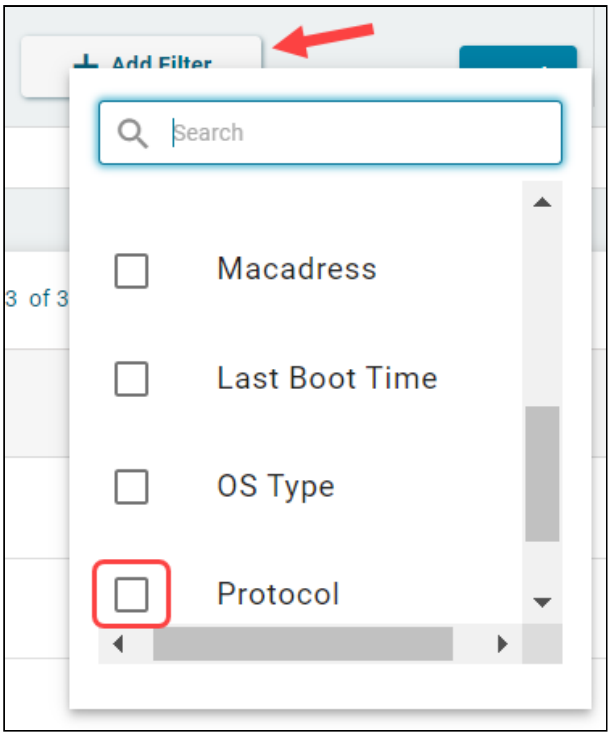
		⚠ Note that the **Search** functionality will be unavailable for all users during the reindexing! Performance issues are possible. Therefore, plan the reindexing time accordingly.
2	Filters	→ To add a filter field, click **Add Filter**. For more details, see How to Add a Search Criterion (see page 1169). ℹ Currently, the number of criteria that you can add via the **Add Filter** button is limited. You can use more search criteria in the **Query** field. → To remove a filter field, click 
	Advanced search	The **Advanced search** toggle button activates the **Query** field that you can use for complex searches. The main features of the query: • SQL-like query language • Autocompletion • Can be copied and pasted For details, see How to Use Advanced Search in the IGEL UMS Web App (see page 1174)
	Case sensitive search	When the **Case Sensitive** checkbox is enabled, all the input in all the text fields is taken case sensitive. When disabled, the search disregards the cases used in the input. To set case sensitive search for selected fields only, you add the **cs.** prefix to the values in the WQL query. For example: 

3	Search results	Lists the devices that fulfill the specified search criteria. Clicking a device name opens a new browser tab showing the information on this device, see Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App (see page 1176). To manage the list, you have the following options: • Add/remove columns through **Select columns** • Set paging for the navigation • Define the number of devices to be displayed on one page
4	Save search	Click the **Save new Search** button to save your current search as a new search under **My Saved Searches**. Clicking the **Save Changes** icon saves the changes you made in the already saved search. 
	Share Option	You can share your saved searches with others through **Share Option**. For details, see How to Share Searches in the IGEL UMS Web App (see page 1171) .

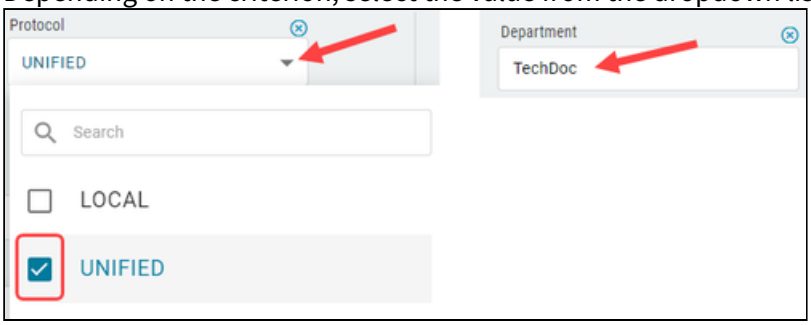
Export search results	Clicking the **Export results** button opens an **Export results** dialog, where the parameters and delimiters for the CSV export file can be configured. Columns that are selected under **Select columns** in the search results area are automatically included in the export file if not disabled manually in this dialog. 

How to Add a Search Criterion

1. Click **Add Filter** and select the required search criterion. To narrow down the list of criteria, start typing the name of the criterion in the **Search** field:



2. Depending on the criterion, select the value from the dropdown list or type it in the field.



The list of search results automatically updates based on your selection or the value you type.

How to Share Searches in the IGEL UMS Web App

With IGEL UMS version 12.05.100 or higher, you can make your saved searches publicly available to cooperate with colleagues.

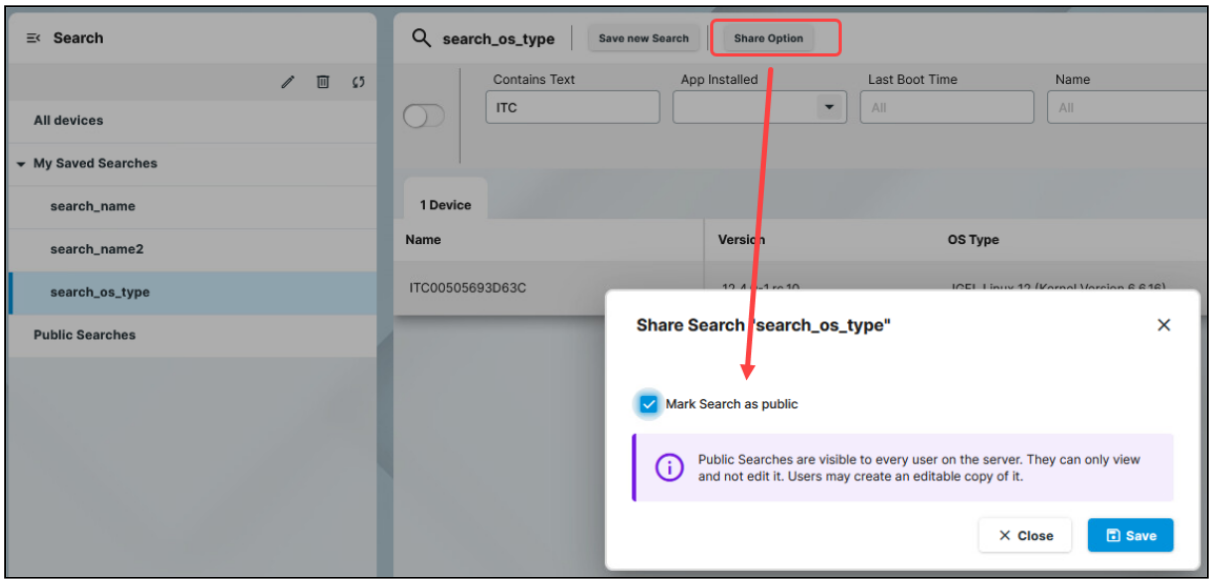
> Public Searches can only be edited or deleted by the original owner but they can be copied and saved as a new private search by anyone.

You might want to use the shared searches in jobs or administrative task. For details, see How to Use Advanced Search in the IGEL UMS Web App (see page 1174) .

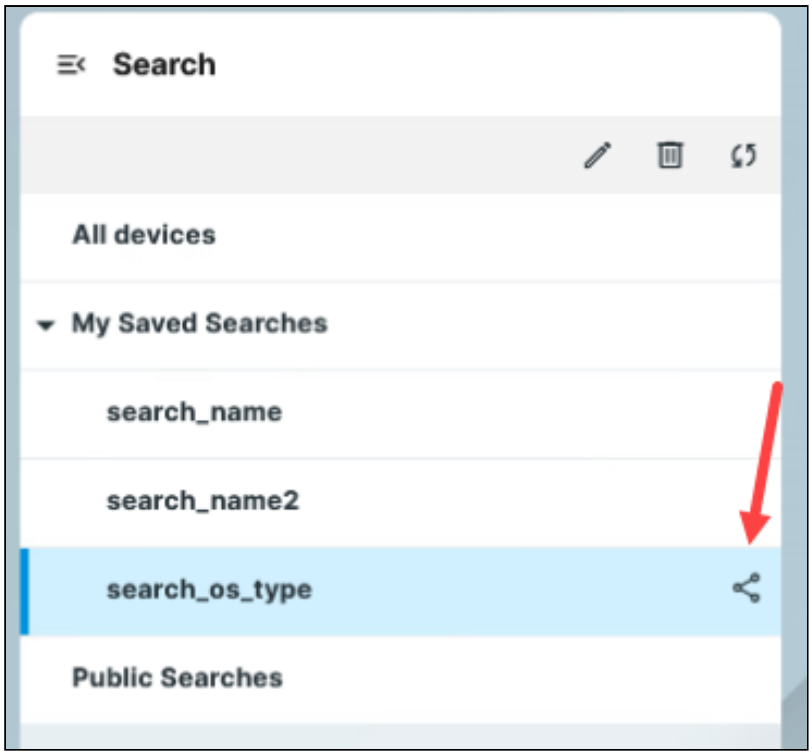
Make the Search Public

To share a Search with others:

1. Create a search using filters and queries.
2. Save the Search with **Save new Search**.
   It is now saved under **My Saved Searches**.
3. Select the saved search and click **Share Option**.



4. Activate the **Mark Search as public** option and save.
   The shared search gets marked with the **Shared** icon.



Other users of the UMS will see the shared search listed under **Public Searches**, but only you can edit, rename and delete the Search.

Remove the Search from Public Searches

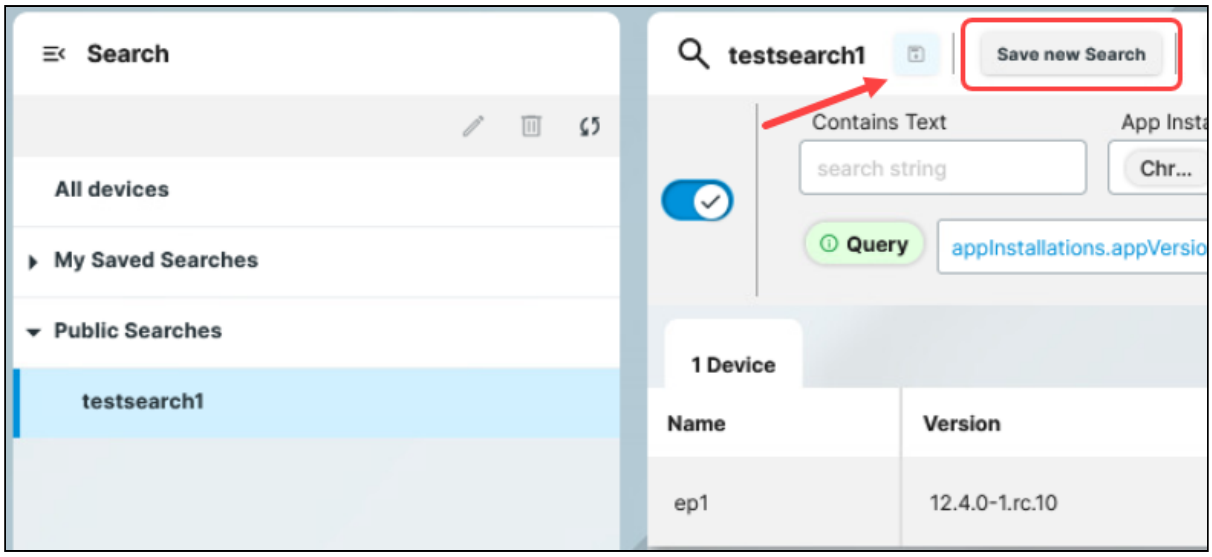
To remove the Search from shared searches:

1. Select the Search.
2. Click **Share Option**.
3. Deactivate the **Mark Search as public** option and save.

Modify Public Searches

Under **Public Searches**, you can see the Searches shared by other users of your UMS.

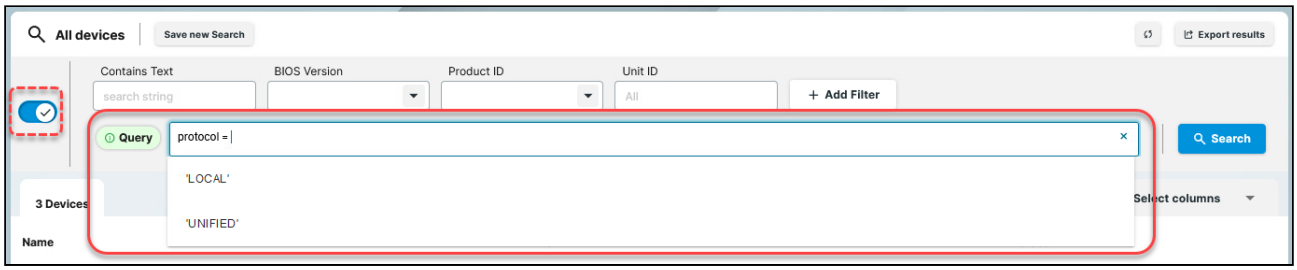
When you select a public search you can modify the filters and query, and thus change the result list momentarily. However, you cannot save the modifications for later, as you would do with your private searches. If you want to use the modified search later, click **Save new Search** to save a copy of the search as a private search.


Search
All devices
My Saved Searches
Public Searches
testsearch1
testsearch1
Save new Search
Contains Text
search string
Chr...
Query
appInstallations.appVersio
1 Device
Name
Version
ep1
12.4.0-1.rc.10

How to Use Advanced Search in the IGEL UMS Web App

You can create complex searches using the query in the Universal Management Suite (UMS) Web App. You can use the saved advanced searches in Jobs and Administrative tasks in the UMS Console.

Create Advanced Search



1. Activate the **Query** using the **Advanced search** toggle button.
2. Click in the query field.
   The list of available criterion is displayed.

> Advanced search uses autocompletion that also works when a criterion / operator / value is entered only partially. It will then only show items matching the already entered fragment.

3. Select the required criterion from the list.
   Based on the selected criterion, the list of available operators is displayed.
4. Select the required operator.
   Based on the selected operator, the list of available values is displayed.
5. Select the value.
6. To define further criteria, select the logical operator AND or OR.
7. After the query is complete, press [Enter] or click **Search**.
   The list of search results updates.
   If there is an error in the query, an error message is displayed explaining the problem.
8. You can save the search by clicking **Save new Search**.

Using Advance Searches in Jobs and Administrative Tasks in the UMS Console

In jobs you can use the saved advance searches as assignment objects. For details, see How to Set Up a New Job in the IGEL UMS (see page 848) and Assigning Objects to a Job in the IGEL UMS (see page 855).

You can also use the saved advance searches in Administrative tasks, for example:

- Delete Devices as an Administrative Task in the IGEL UMS (see page 941)
- Export View or Advanced Search Result via Mail as an Administrative Task in the IGEL UMS (see page 944)
- Save View or Advanced Search Results in the File System in the IGEL UMS (see page 947)
- Assign Objects to the Devices of Views or Device Searches in the IGEL UMS (see page 950)

The newly saved searches are shown after the refresh of the UMS Console.
Updating the advanced search will automatically update the Jobs / Administrative tasks where it is used.

Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App

In the **Devices** area of the IGEL Universal Management Suite (UMS) Web App, you can manage devices registered on the UMS Server. All devices registered on the UMS Server are shown.

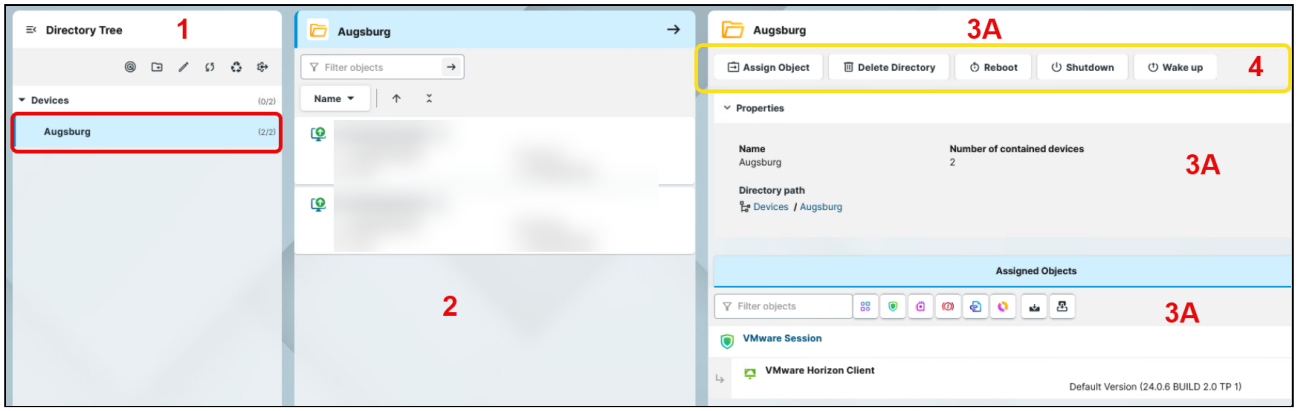
Device changes made in the UMS Console are immediately available in the UMS Web App, and vice versa.

Menu path: **UMS Web App > Devices**

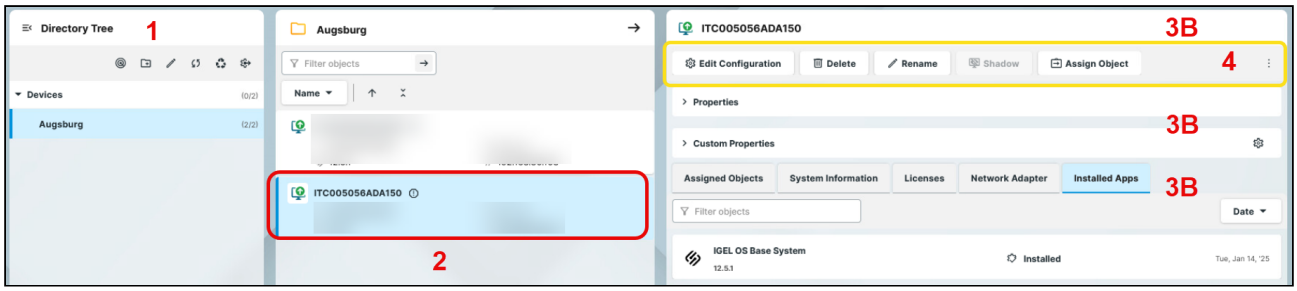
You can structure the **Devices** area by creating directories and subdirectories. When doing so, you should bear in mind that each device can only be stored in a single directory.

Avoid placing too many devices in one folder. If the user interface feels sluggish, refer to the tips regarding the folder structure under Performance Optimizations in IGEL UMS (see page 225).

Directory level:



Device level:



1	Directory Tree	Shows all created directories and subdirectories. The format (x/y) specifies 1) the number of devices contained directly in the directory and 2) the total number of devices in the directory & all subdirectories of this directory. • Creating a Directory Structure in the IGEL UMS Web App (see page 1234) • Renaming a Directory in the IGEL UMS Web App (see page 1238) • Moving a Device Directory (see page 1237) • Copying a Device Directory in the IGEL UMS Web App (see page 1236) • Moving Devices in the IGEL UMS Web App (see page 1235) • Scanning the Network for Devices and Registering Devices on the IGEL UMS (see page 1136) → To delete a device directory, click the **Delete Directory** button in the device command area (4). For more information, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356). → To open the **Settings** area, click  . Here, you can • manage custom device attributes[198] • configure first-authentication keys (see page 1228)
2	Device list	Shows all devices directly contained in the directory selected in the **Directory Tree**. → Right-click on the device opens a context menu with device commands. For details on the device commands, see Device Commands (see page 1184) below. • Paging for the navigation in the device list • Defining the number of devices to be displayed on one page • Filtering devices by **Name**, **Product ID**, **Unit ID**, **Version**, and **IP Address** • Sorting devices by **Name**, **Product ID**, **Unit ID**, **Version**, and **IP Address**

198. https://kb.igel.com/en/universal-management-suite/current/how-to-manage-custom-device-attributes-in-the-igel

3A	Directory information	Details for the directory selected in the **Directory Tree** **[Directory Name]**: The name of the selected directory **Properties**: Properties of the selected directory, e.g. the full **Directory Path**, **Number of contained devices** **Assigned Objects**: Directly and indirectly assigned objects, e.g. profiles, files, firmware updates, etc. For details, see Assigning Objects in the IGEL UMS Web App (see page 1187).

3B	Device information	Details for the device selected in the device list **Status display** The status of the selected device. For icons showing the device's status, see Status Displays (see page 1176) below. **[Device Name]** The name of the selected device. **Properties** Properties of the selected device, e.g. **Last IP**, **MAC Address**, **Unit ID**, **Directory path**, **Last Contact** (see page 543), etc. The unit ID serves as a unique identifier of an endpoint device in the UMS. 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. If the device is a UD Pocket, the unit ID is set to the serial number (without spaces and special characters), preceded by the prefix consisting of the USB vendor and product ID. **Custom Properties** Allows changing such customizable properties as **Site**, **Department**, device attributes. To edit the properties, click  . Here you can find the custom device attributes you configured through the UMS Console or the UMS Web App. For details, see How to Manage Custom Device Attributes in the IGEL UMS Web App (see page 1219) and Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879) . Whether you can change the values for the device attributes depends on your configuration of the **Global Overwrite Rule** and/or **Overwrite Rule** for a specific device attribute, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879). ## Tabs The following tabs are displayed only if data is available: • **Licenses** • **Network Adapter**

- **Installed Apps**
- **User Login History**
- **Monitor Information**
- **Peripherals** (license required)

Assigned Objects

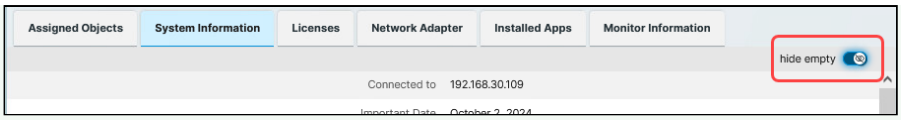
Shows the directly and indirectly assigned objects, e.g. profiles, apps, files, etc. For details, see How to Assign Objects in the IGEL UMS Web App (see page 1187).

System Information

Shows such properties as **CPU Type**, **Memory Size**, **Device Type**, and the custom device attributes.

→ To copy a property's value, click  .

Use the **hide empty** toggle to hide empty system information entries.



Licenses

Details on the licenses for the selected device. To copy a value, click .

Network Adapter

Displays information about all available network adapters of a device. The section is available for devices with IGEL OS 11.07.100 or higher. For details, see the section "Network Adapters" under View Device Information in the IGEL UMS (see page 778).

Installed Apps

Shows all apps present on the IGEL OS 12 device, their status and time when the device delivers the message about the app status. For details, see Checking Installed Apps via the IGEL UMS Web App (see page 1317).

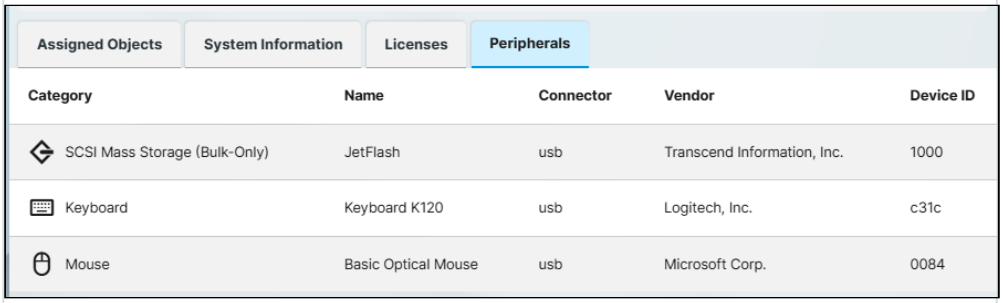
Monitor Information

Shows details for the connected monitors. Note that the **Date of Manufacture** is combined from the values of week/year of manufacture.

Peripherals

Shows information about peripherals connected to an endpoint device. This tab is only shown if the required license is available and the Asset Inventory Tracker is activated under **UMS Console > UMS Administration > Global Configuration > UMS Features > Enable inventory tracking**. For more information, see "Asset Inventory" under View Device Information in the IGEL UMS (see page 781).

To refresh the information about the connected peripherals, you can click **Reload tree** button or reselect an endpoint device.



User Login History

Shows up to 10 last user logins if the logging is enabled. For details on the logging activation, and the logged information, see the section "User Login History" under View Device Information in the IGEL UMS (see page 778).

Hypervisor

The virtual machines running on the IGEL OS 12 devices can be managed here. For details, see How to Manage Virtual Machines Running on IGEL OS 12 from the IGEL UMS Web App (see page 1232) .

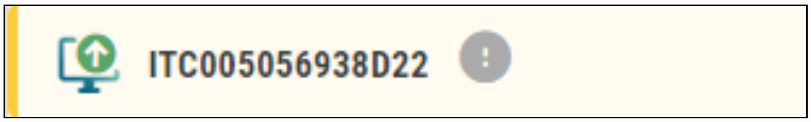
4	Device commands	Device commands, e.g. power control commands, firmware updates, etc., are executed for an individual directory or an individual device. The status of the command execution is shown under **Messages** (see page 1159)  → Click  to view all available device commands. For details on the device commands, see Device Commands (see page 1184) below.

Status Displays

The UMS monitors the status of the devices by regularly sending UDP packets. In accordance with the preset, this occurs every 3 seconds. For information on how to change the interval for the online check, see Devices - Managing Devices in the IGEL UMS (see page 776).

When the device is connected via IGEL Cloud Gateway (ICG), a cloud symbol icon  is added to the device.

The exclamation mark indicates that changes, i.e. new configurations, files, profiles, etc., have not yet been transferred to the device.



Icons for an IGEL OS Device

The following icons show the status of an IGEL OS device:

	The device is online.
	The device is offline.
	The device is being updated.
	The status of the device is unknown or has not yet been processed.

Device Commands

The following commands can be executed for an individual device as well as for an individual directory (with the exception of shadowing and configuration editing). The commands are grouped in categories.

> If a user does not have sufficient rights, the command icons are grayed out. For information on permissions in the UMS, see Access Rights (see page 1010).

Edit configuration	Allows you to edit configuration parameters for the selected device. Here, you edit the device setup as you would if you were working at the endpoint device itself.
Rename	Allows you to rename the selected device. The name of a device does not need to be identical to the name of the device in the network. The name of a device does not need to be unique and can be used a number of times. For other renaming options, see How to Rename IGEL OS Devices (see page 538).
Delete / Delete Directory	Allows you to delete the highlighted device / device directory. If recycle bin is enabled, this will send the device to the recycle bin, where you can restore / permanently delete it. For details, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).
Shadow	Shadowing: Launches a VNC session for the highlighted device if shadowing is enabled for this device, see (12.4-en) Shadow Settings in IGEL OS 12 . For details on shadowing in the UMS, see Shadowing - Observe IGEL OS Desktop via VNC (see page 810) and IGEL UMS and Devices Secure Shadowing Communication Flow (see page 366) .
Assign object	Assigns / detaches an object, e.g. a profile, a file, etc. For details, see How to Assign Objects in the IGEL UMS Web App (see page 1187) .
Reboot	Restarts the highlighted device.
Shutdown	Shuts down the highlighted device.

Wake up	Starts the highlighted device via the network (Wake-on-LAN). For details on configuring Wake-on-LAN in the UMS, see Wake on LAN (see page 981).
Suspend	Puts the highlighted device into suspend mode.
Send settings	Reads out the complete last device configuration from the UMS database and sends it to the highlighted device.
Receive settings	Reads the local configuration of the highlighted device, sends it to the UMS, and writes it to the database.
Reset to factory defaults	Resets the highlighted device to the factory defaults; see Resetting a Device to Factory Defaults via the IGEL UMS Web App (see page 1223). For other methods of resetting a device to factory defaults, see (11.10-en) Reset to Factory Defaults and (11.10-en) How to Reset a Device with Unknown Administrator Password .
Update	OS 11: Carries out a firmware update on the highlighted IGEL OS 11 device. OS 12: Triggers the activation of the assigned app version for the selected IGEL OS 12 devices. For details when the **Update** command is required, see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334).
Update on shutdown	Only for OS 11: Updates the firmware when the highlighted IGEL OS 11 device is shut down.
Refresh system information	Refreshes the system information for the highlighted device.
Refresh license information	Refreshes the license information for the highlighted device.
Export as Profile	Exports device settings, see Exporting Device Settings as a Profile in the IGEL UMS Web App (see page 1226).
Send message	Sends a message to the highlighted device; see Sending a Message to Devices via the IGEL UMS Web App (see page 1192).

Specific Device Commands	Opens a menu of the specific device commands that are available for the folder or device. Which commands are available depends on the following criteria: • The device has IGEL OS 12.3 or higher • An app that supports specific device commands is installed on the device.

How to Assign Objects in the IGEL UMS Web App

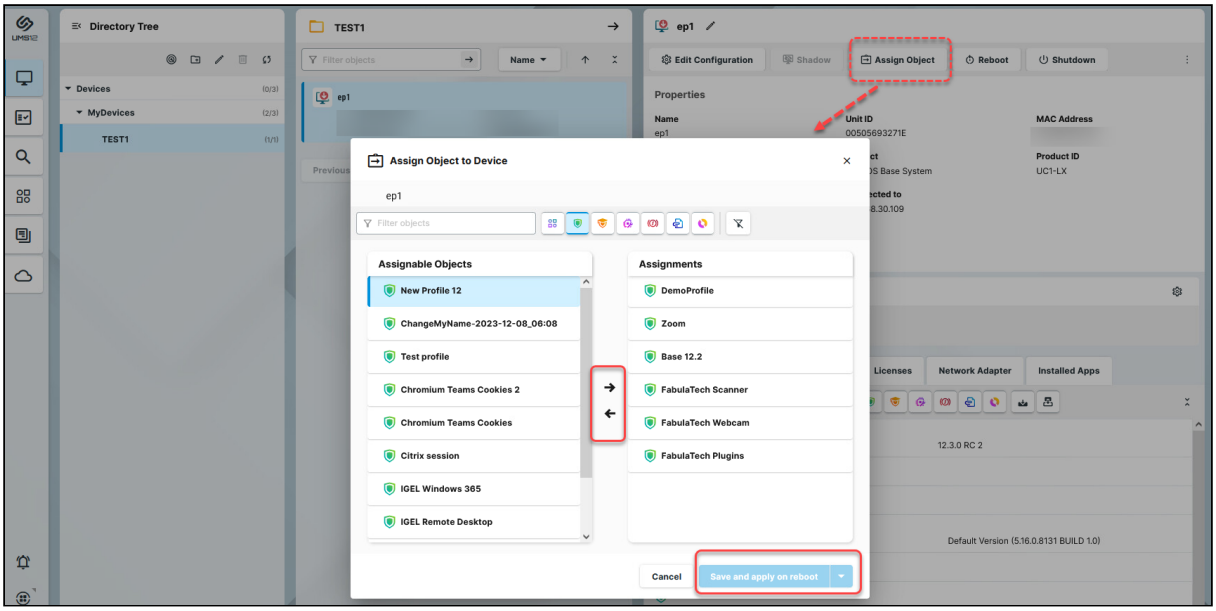
In the IGEL Universal Management Suite (UMS) Web App, you can assign an object (e.g. file, profile, app, etc.) to a device or device directory.

Menu path: **UMS Web App > Devices**

To assign (or to detach) an object, proceed as follows:

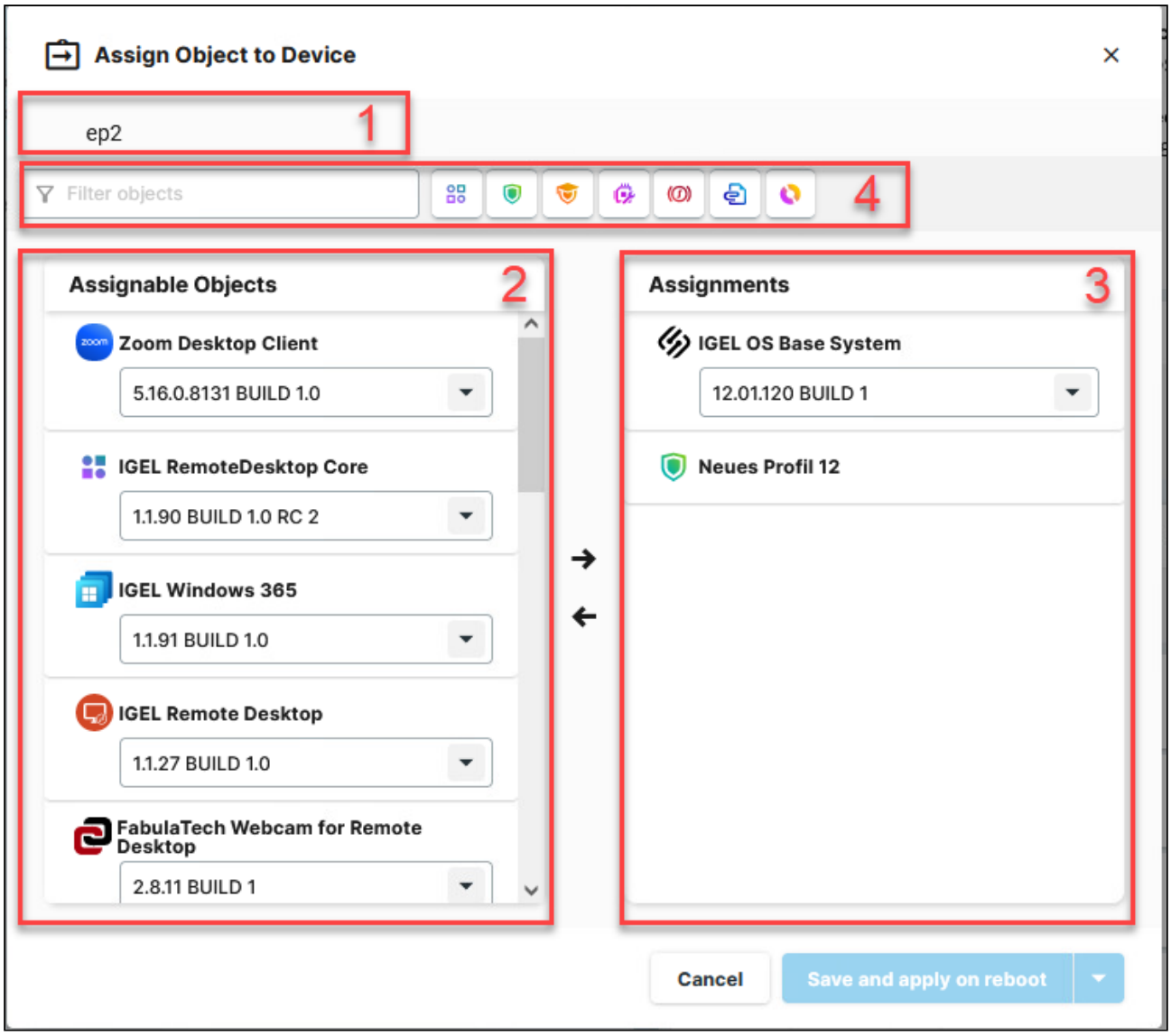
1. In the **UMS Web App > Devices**, select the desired directory / device and click **Assign object**.

   It is not possible to assign an object to the root directory "Devices".

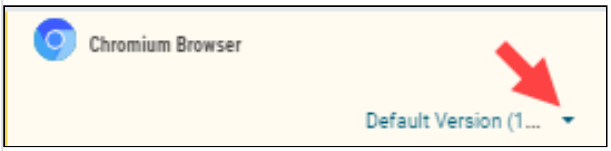


2. Select the required object and use the arrow buttons or drag & drop.
3. Decide whether the new settings are to take effect immediately or at the next reboot of the device.

Assign Object to Device Dialog



1	Name of the directory / device	Name of the directory / device to which the object is assigned
2	Assignable objects	Shows all objects that can be assigned to the directory / device. The following objects can be assigned:

		: Apps (for IGEL OS 12 devices). An app version to be assigned is chosen in the selection list that shows all versions of the selected app available under Apps - Import and Configure Apps for IGEL OS 12 Devices via the IGEL UMS Web App (see page 1294).  **Implicit App Assignment via a Profile** An app is automatically assigned via a profile configuring this app. Exception: IGEL OS Base System app An implicit app assignment is overwritten if you assign an app explicitly, i.e. if you select an app as an object in the **Assign object** dialog. For more information, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252). : Profiles. For general information on profiles, see Profiles in the IGEL UMS (see page 695). See also Configuration - Centralized Management of Device Settings in the IGEL UMS Web App (see page 1239). : Priority profiles. For details, see Priority Profiles in the IGEL UMS (see page 744). : Corporate identity customizations. For details, see Corporate Identity Customizations in the IGEL UMS (see page 764). : Template keys and value groups. For details, see Template Profiles in the IGEL UMS (see page 746). : Files. For details, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices (see page 1123). : Firmware updates (for IGEL OS 11 devices). For details, see Universal Firmware Update in the IGEL UMS (see page 856).
3	Assignments	Shows all objects directly assigned to the directory / device.

4	Filter	Filters the objects under **Assignable objects** and **Assignments** according to • the selected object type • the entry in the text field The above filter criteria are linked with the operator *AND*. → Click to remove all filters.

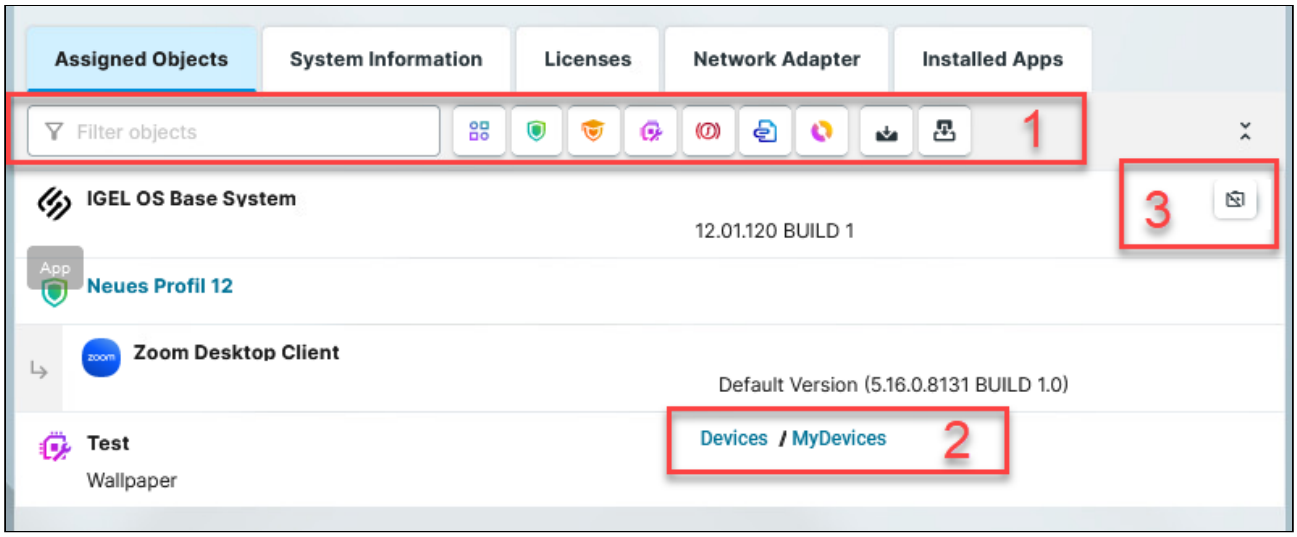
Assigned Objects

Objects 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.

→ To view all assigned objects, i.e. directly and indirectly assigned objects, select the desired directory / device and go to **Assigned Objects**.

> All implicitly assigned apps, i.e. apps assigned to devices via a profile, are displayed directly under this profile.



1	Filters the assigned objects according to • the selected object type • the entry in the text field • direct or indirect assignment type The above filter criteria are linked with the operator *AND*. → Click to remove all filters.

2	For indirectly assigned objects only: Specifies the path to the directory the object assignment is inherited from.
3	For directly assigned objects only: Detaches the object from the directory / device.

How to Send a Message to Devices via the IGEL UMS Web App

In the IGEL Universal Management Suite (UMS) Web App, you can send a message to IGEL OS 12 devices. Currently, only plain text messages are supported, i.e. simple string messages without formatting and HTML codes.

Sending a message to IGEL OS 11 devices via the UMS Web App is currently not possible. Use the UMS Console, instead; see Sending Messages to Devices in the IGEL UMS (see page 804).

Menu path: **UMS Web App > Devices > Send message**

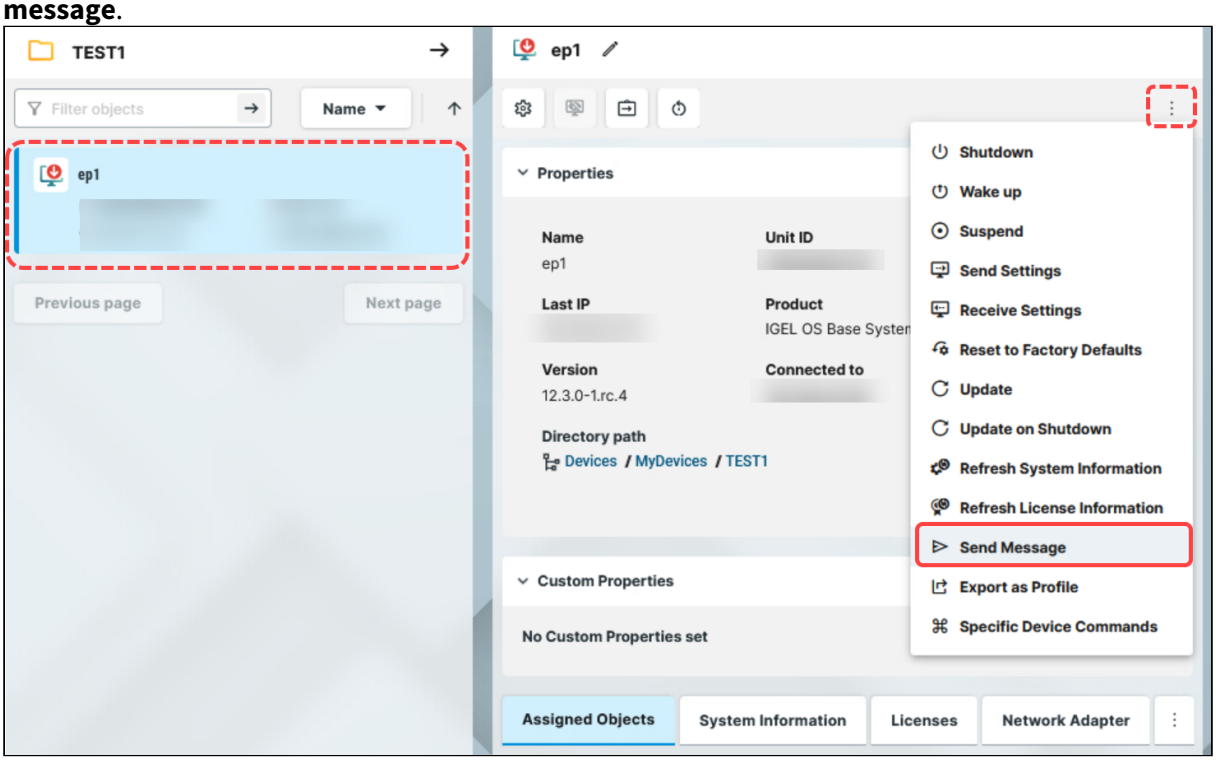
To send a message to IGEL OS 12 devices, the following permissions are required:

- **Read** and **Send Message** (set in the UMS Console via **[context menu of a device / device directory] > Access Control**)
- **Device Bulk Action** if a message should be sent to multiple devices (set in the UMS Console under **System > Administrator accounts**)

For general information on rights and permissions, see Create Administrator Accounts.

To send a message:

1. In the **UMS Web App > Devices**, select the required device / device directory and click **Send message**.

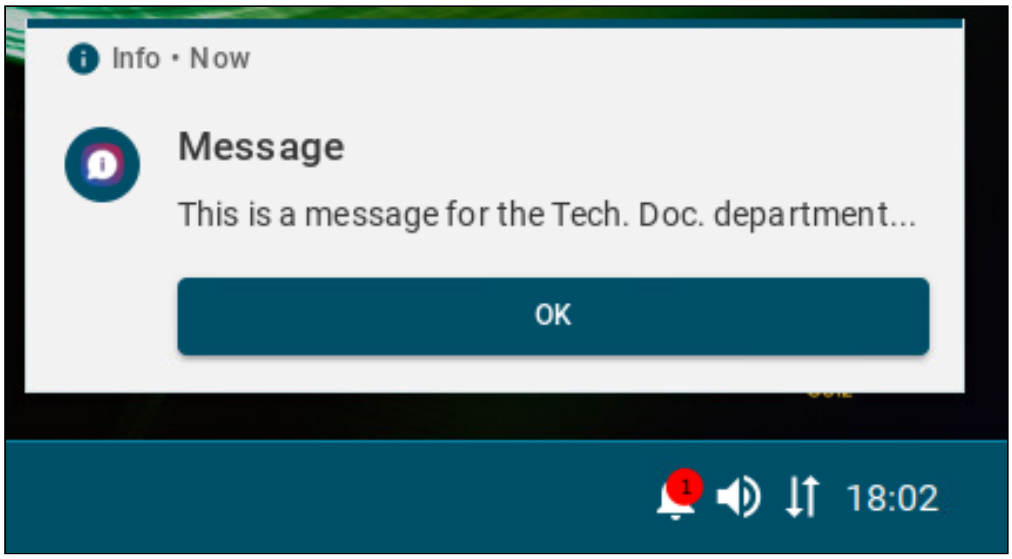


2. Type your message. Do not use HTML or other codes.

3. Click **Send message**.

Your message will be sent to the devices shown in the list. This device list is read-only, i.e. you cannot select the devices here.
If you have selected the device directory for sending a message, the number of affected devices is shown.

On the device, the message is displayed in a **Message** window, and, if not closed, also in the Notification Center. For details, see *How to Start with IGEL > IGEL OS Notification Center*.



UMS as a Certificate Authority (CA) Proxy

With the CA Proxy feature, you can use the IGEL Universal Management Suite (UMS) to enroll endpoint devices known to the UMS into an external PKI via the EST protocol.

Briefly, the process is as follows:

As a precondition, a certificate profile has been defined in your PKI. The trust material for establishing an mTLS connection to the PKI has been configured in the UMS. When the endpoint device is configured to use the UMS as a Registration Authority / CA proxy, it sends a Certificate Signing Request (CSR) to the UMS. The UMS forwards this CSR to the PKI using the EST protocol. The PKI returns the signed certificate to the UMS. The UMS sends the issued certificate with the complete CA certificate chain of the issuer to the device.

This feature has been tested with EJBCA Enterprise with the EST alias set to “RA mode”.

Supported Encryption Algorithms for the Device Certificates

For the device certificates, the following encryption algorithms are supported:

- RSA 2048
- RSA 3072
- RSA 4096
- RSA 8192
- ECDSA ed25519
- EC brainpoolP256r1
- EC brainpoolP384r1
- EC brainpoolP512r1
- EC prime256v1
- EC secp256k1
- EC secp384r1
- EC secp521r1

Requirements

IGEL OS Endpoint Devices

- Endpoint devices with IGEL OS 12.7.2 or higher

IGEL Universal Management Suite (UMS)

- IGEL UMS 12.09.110 or higher
- IGEL UMS Enterprise License

PKI / EST Server

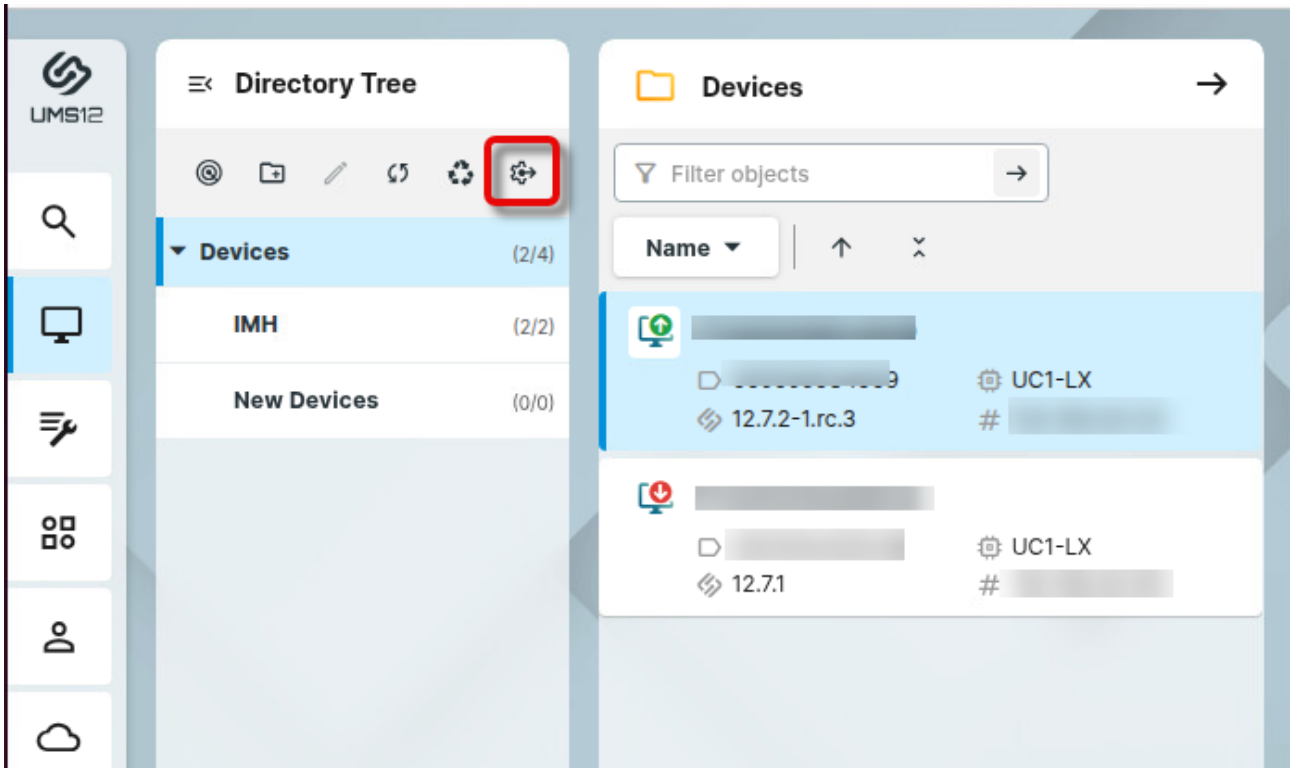
- Your PKI uses Enrollment over Secure Transport (EST) as the protocol
- Your EST configuration supports the default endpoint for EST as defined in RFC 7030

    - Without an optional CA label: `/.well-known/est/<operation>`
    - If an optional CA label is defined: `/.well-known/est/<CA label>/<operation>`
- For the mTLS connection between the UMS and the PKI, the following encryption algorithms are supported:
    - RSA
    - ECDSA-p-256/384/512
    - ED-25519/448
- To build the mTLS connection between the UMS and the PKI, the following data and trust material must be available:
    - Hostname of the EST server
    - Port of the EST server
    - A Java Keystore file (`.jks`) that contains the following:
        - The web certificates for the EST server
        - The key pair for the client certificate and private key that the UMS will use to communicate with the PKI
    - The private key and keystore must have the same password

Configuring the UMS to Act as a CA Proxy

> The certificate profile on the PKI and the endpoint device must match.

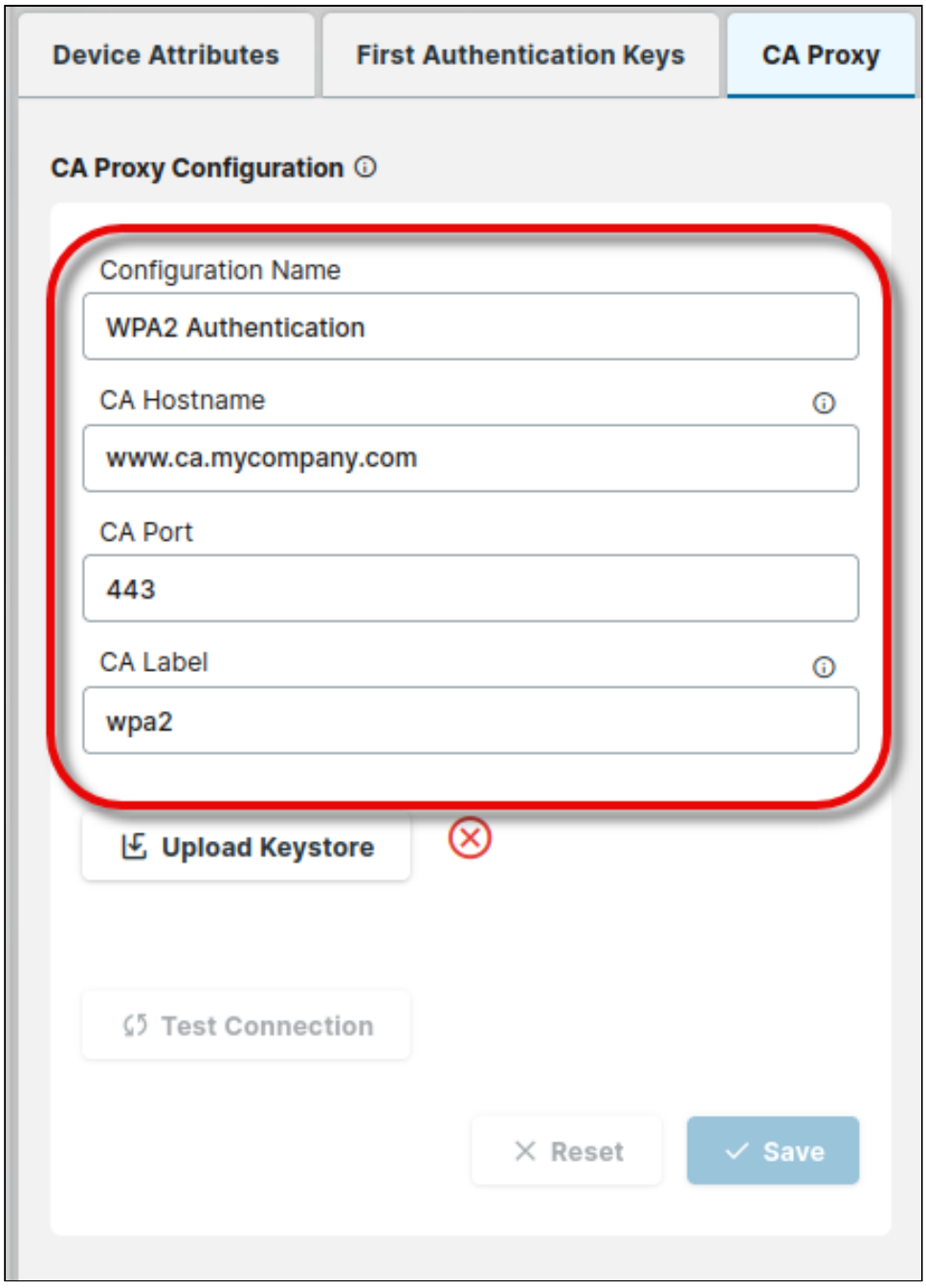
1. In the UMS Web App, go to the **Devices** area and click .



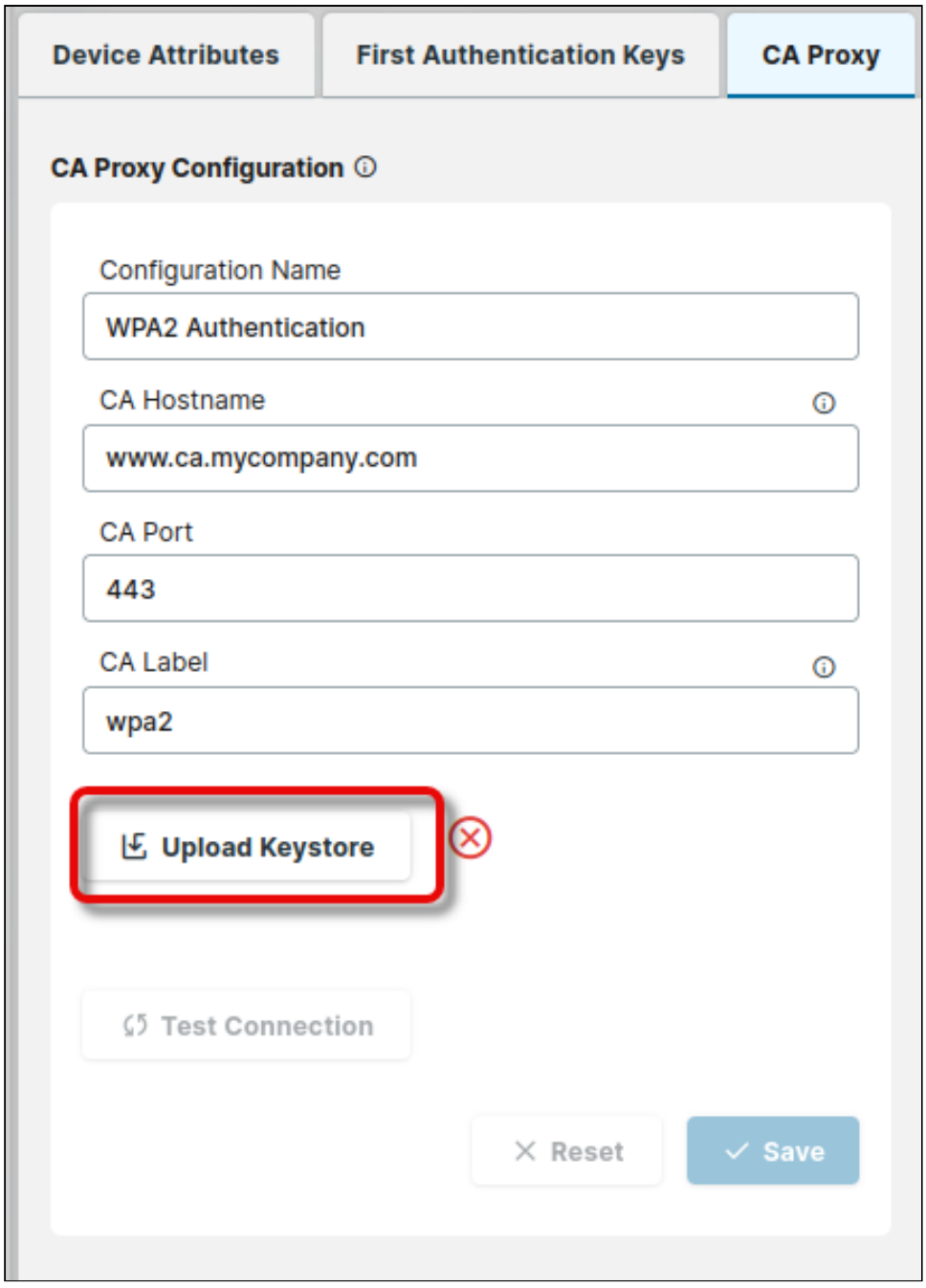
2. Select the **CA Proxy** tab and enter the following data:
   - **Configuration Name**: Display name for your EST configuration
   - **CA Hostname**: The URL of your EST server
   - **CA Port**: The port required to connect to the EST server. Default: 443
   - **CA Label**: The optional EST CA label as outlined in RFC 7030 Section 3.2.2. Allowed characters: Letters, numbers, underscores (“_“), minus signs (“-”).

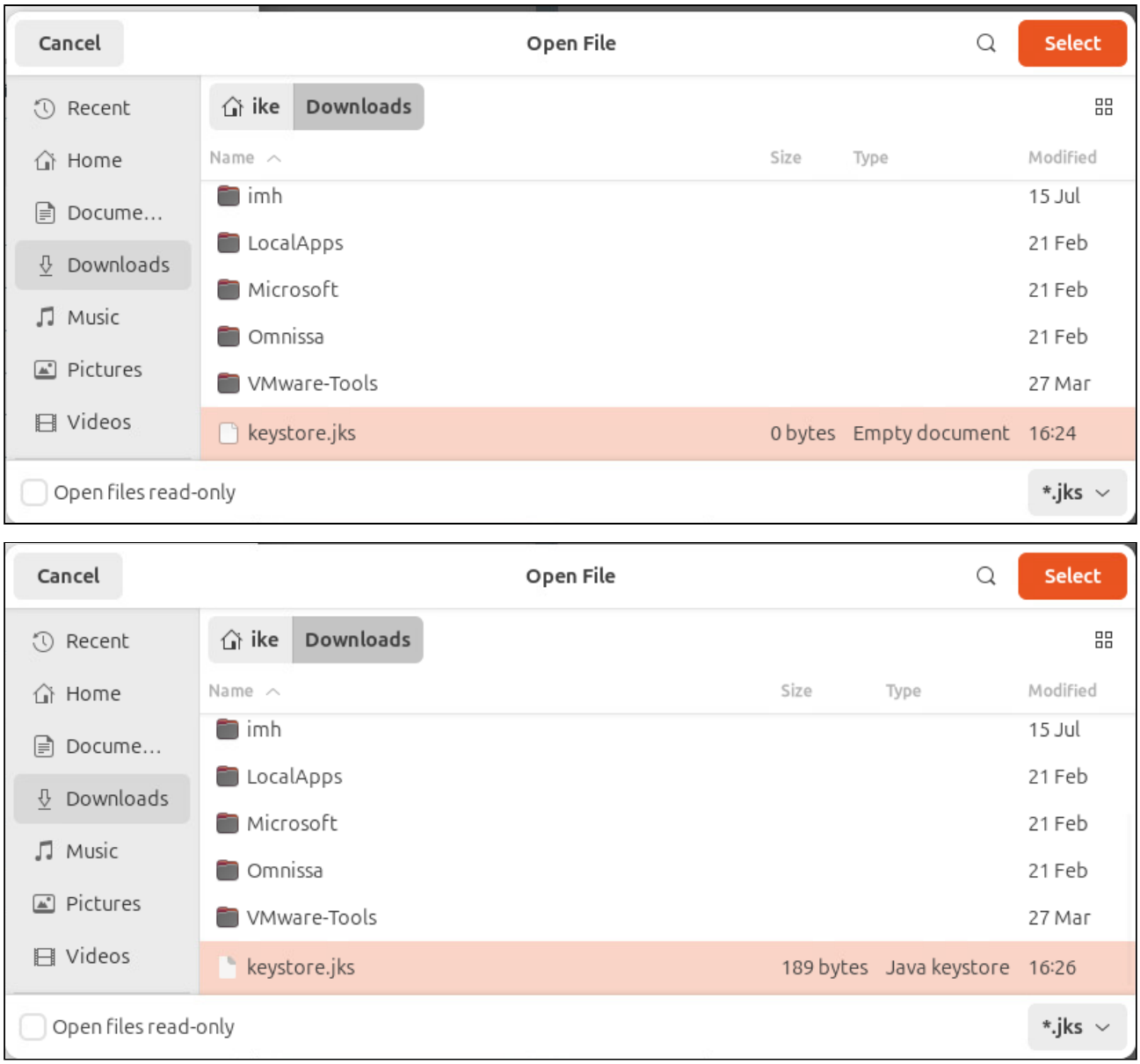
The EST CA label may be required to match the case of the CA label in your PKI. In the case of EJBCA, this setting is referred to as the alias, which is case-sensitive.

Example: If you have an alias called “VPN” in EJBCA Enterprise, then you must set the CA label to “VPN”; adding “vpn” or “Vpn” will not work.

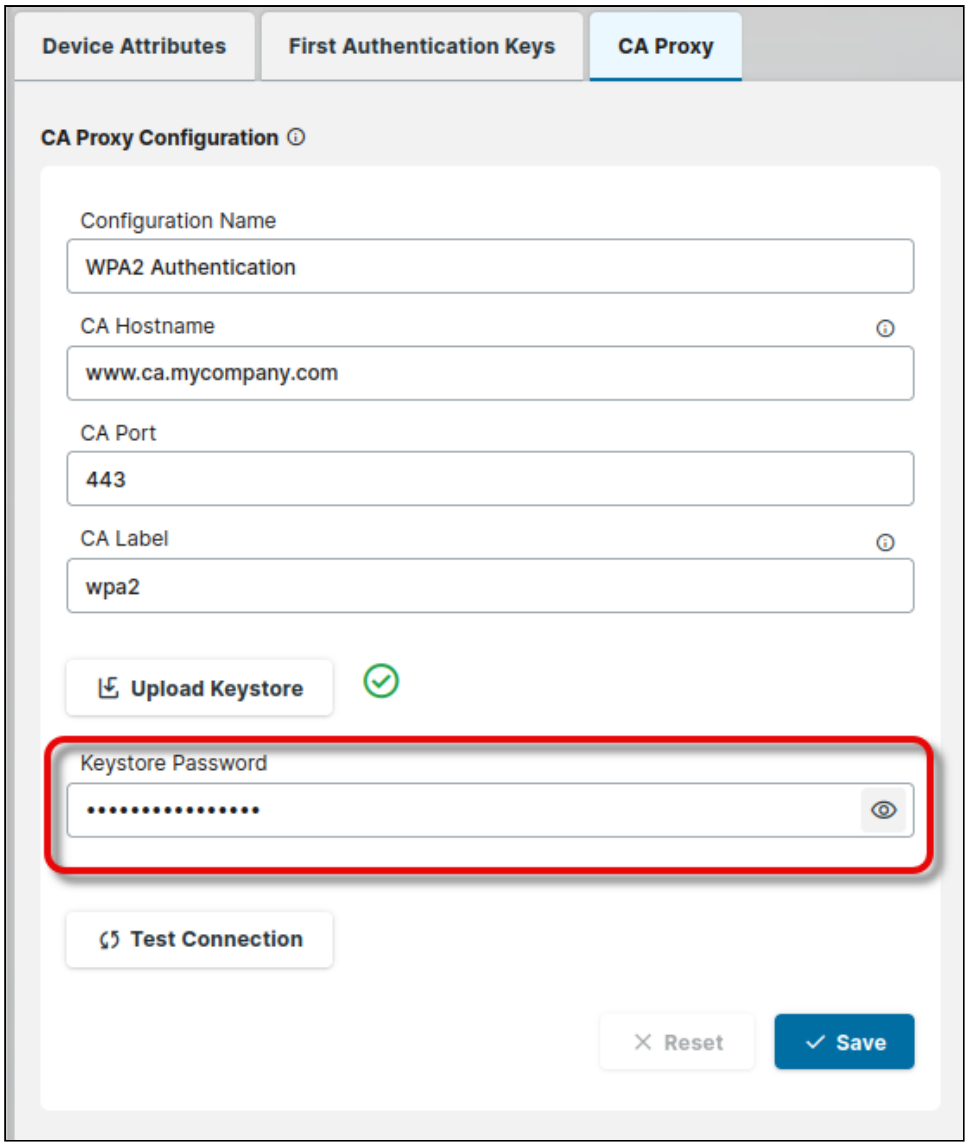


3. To upload the keystore you have obtained from your PKI, click **Upload Keystore** and select the keystore file.

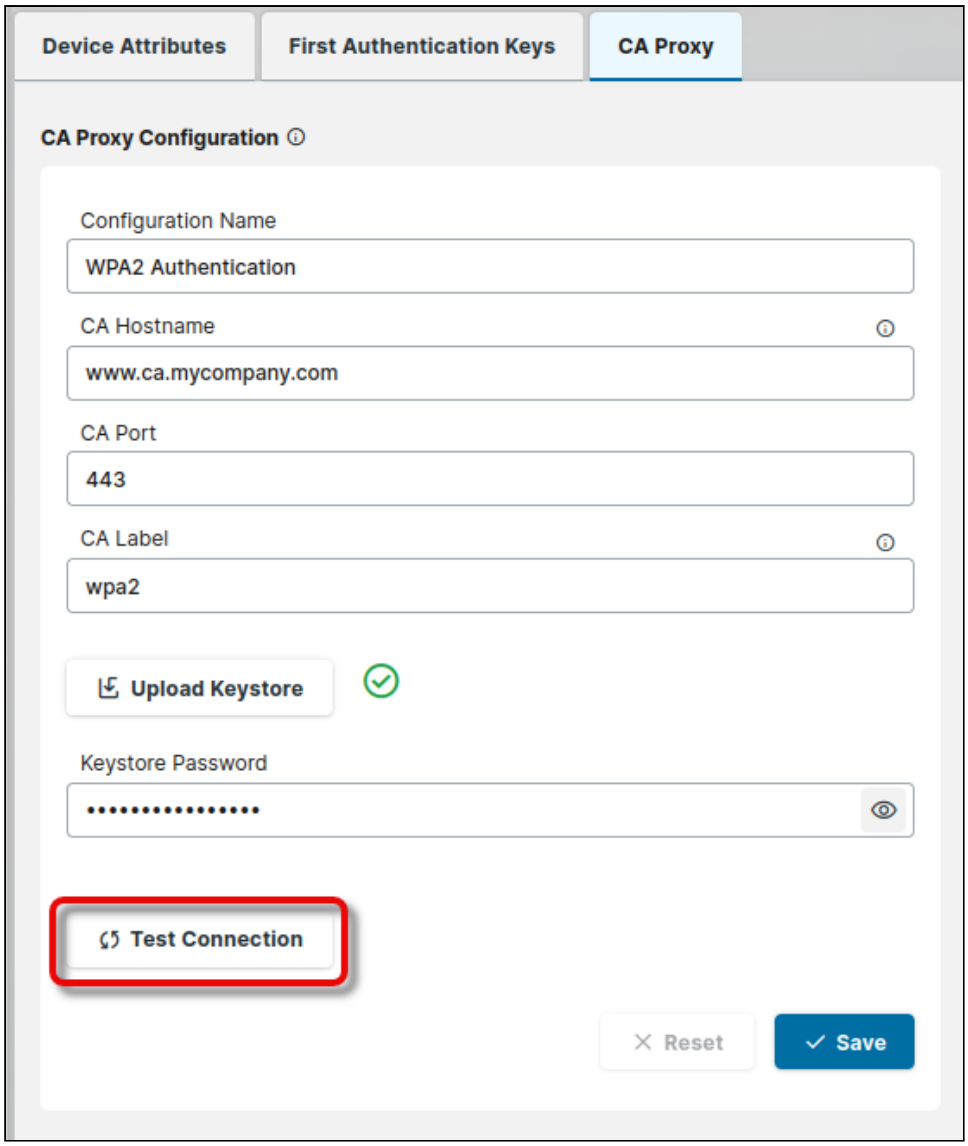

Device Attributes
First Authentication Keys
CA Proxy
CA Proxy Configuration
Configuration Name
WPA2 Authentication
CA Hostname
www.ca.mycompany.com
CA Port
443
CA Label
wpa2
Upload Keystore
Test Connection
Reset
Save



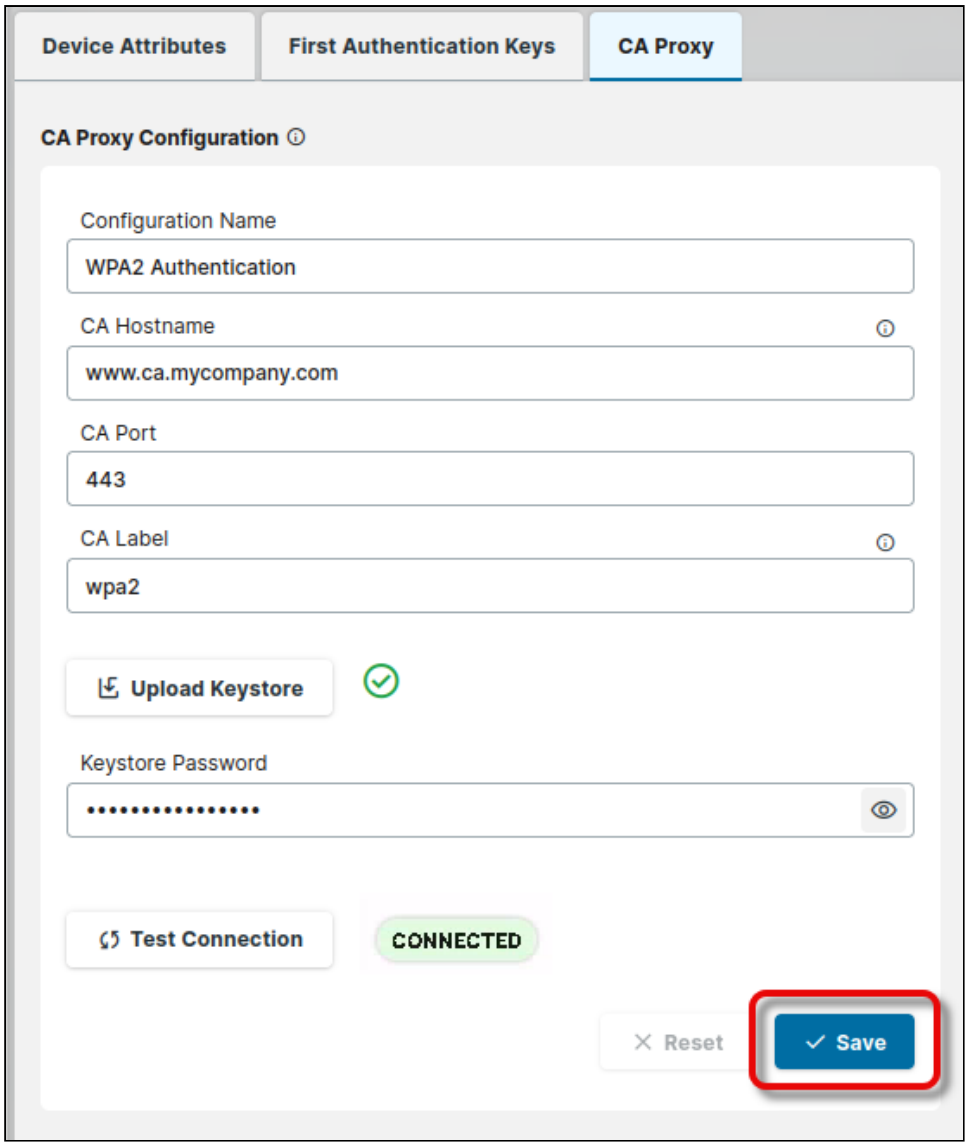
4. Enter the **Keystore Password**. Note that the keystore and the keys therein must have the same password.



5. To test your connection, click **Test Connection**.



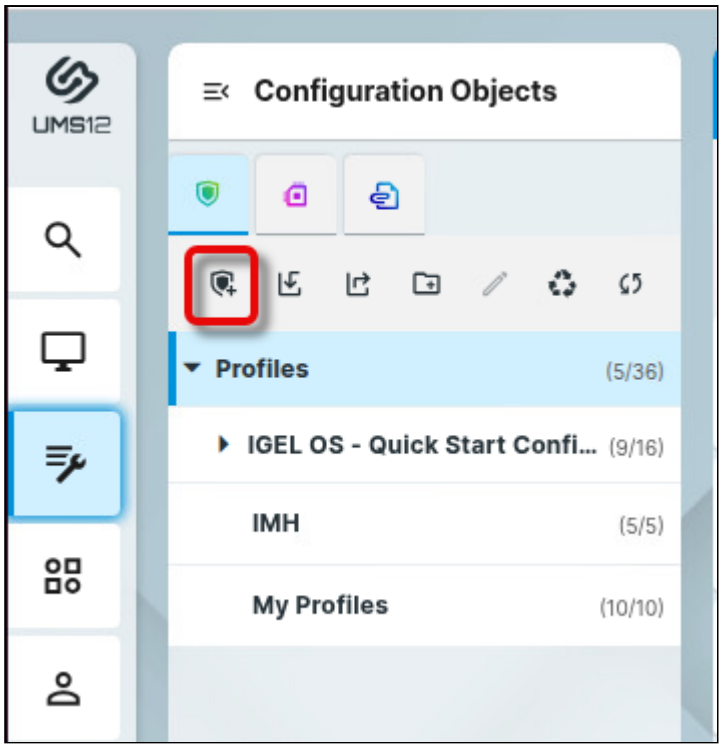
6. Review your configuration and click **Save**.



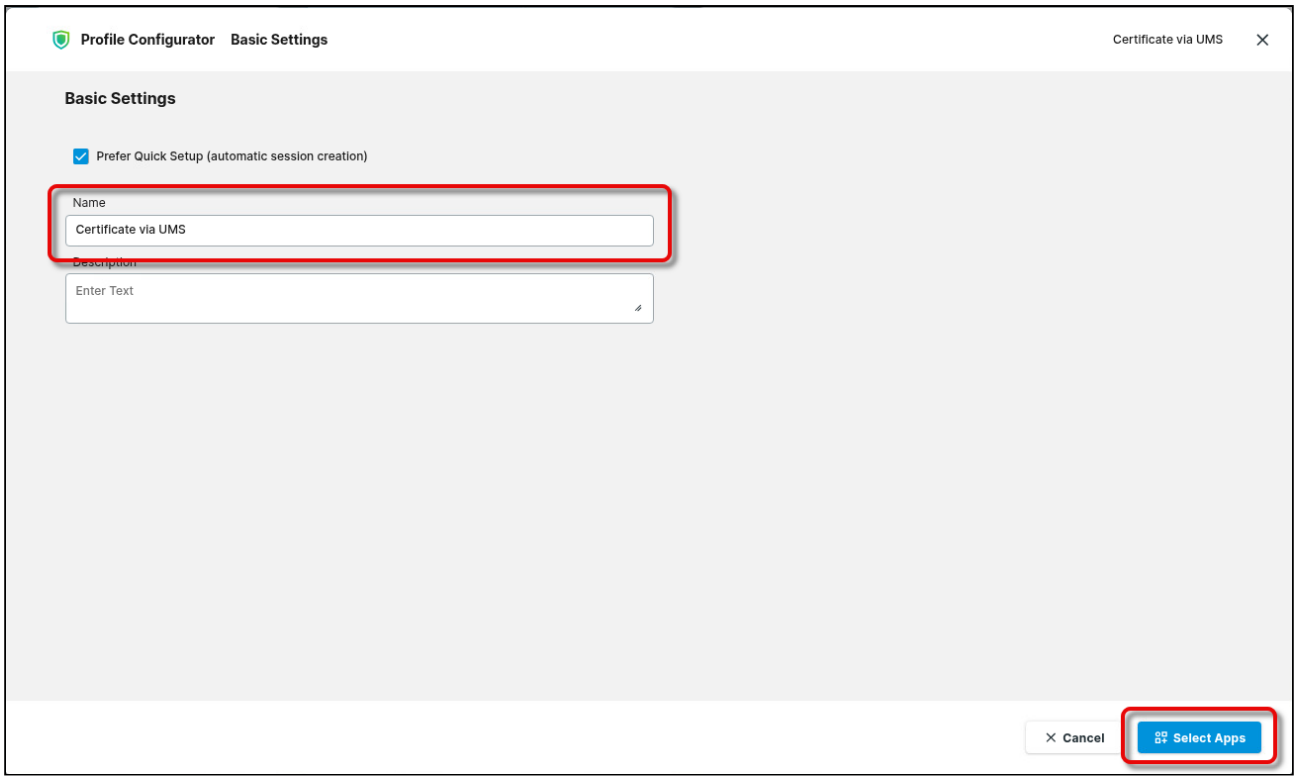
Configuring the Endpoint Device to Use the UMS as CA Proxy

Creating a UMS Profile

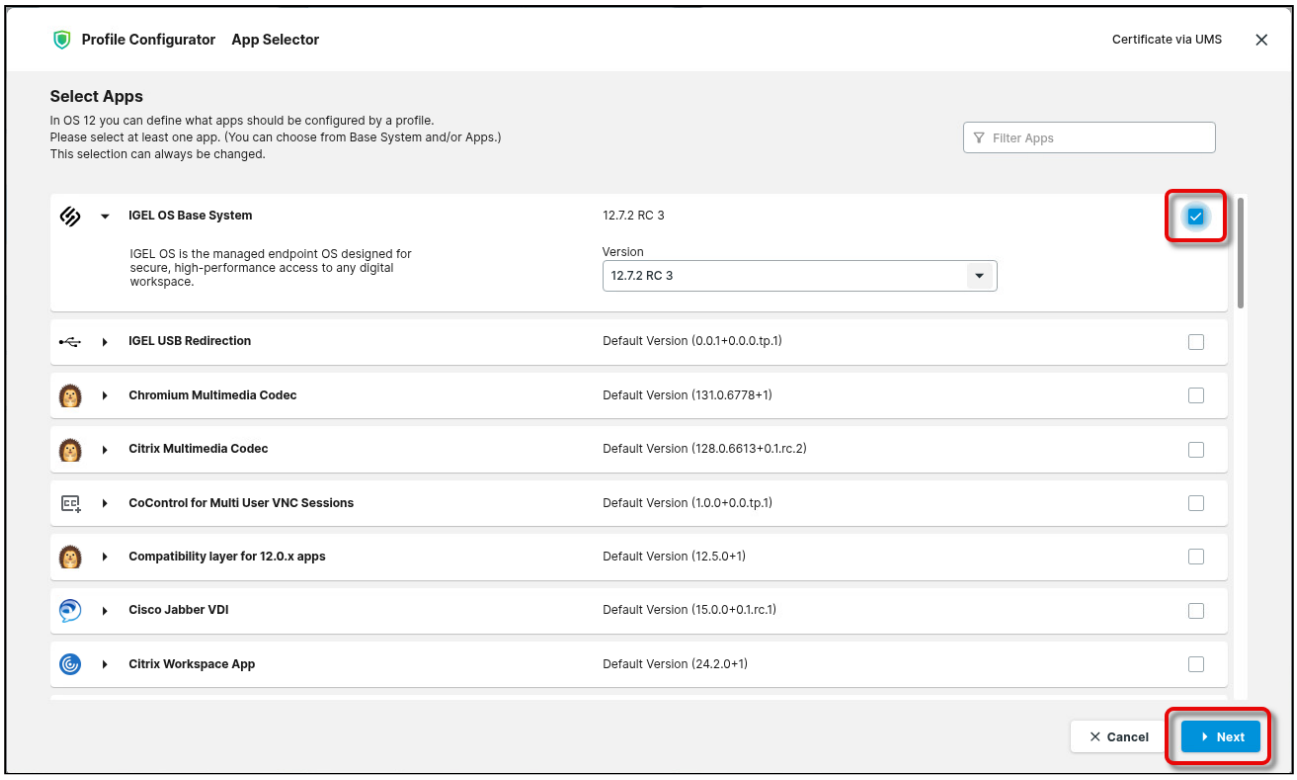
1. In the UMS Web App, go to the **Configuration** section and click to create a new UMS profile.



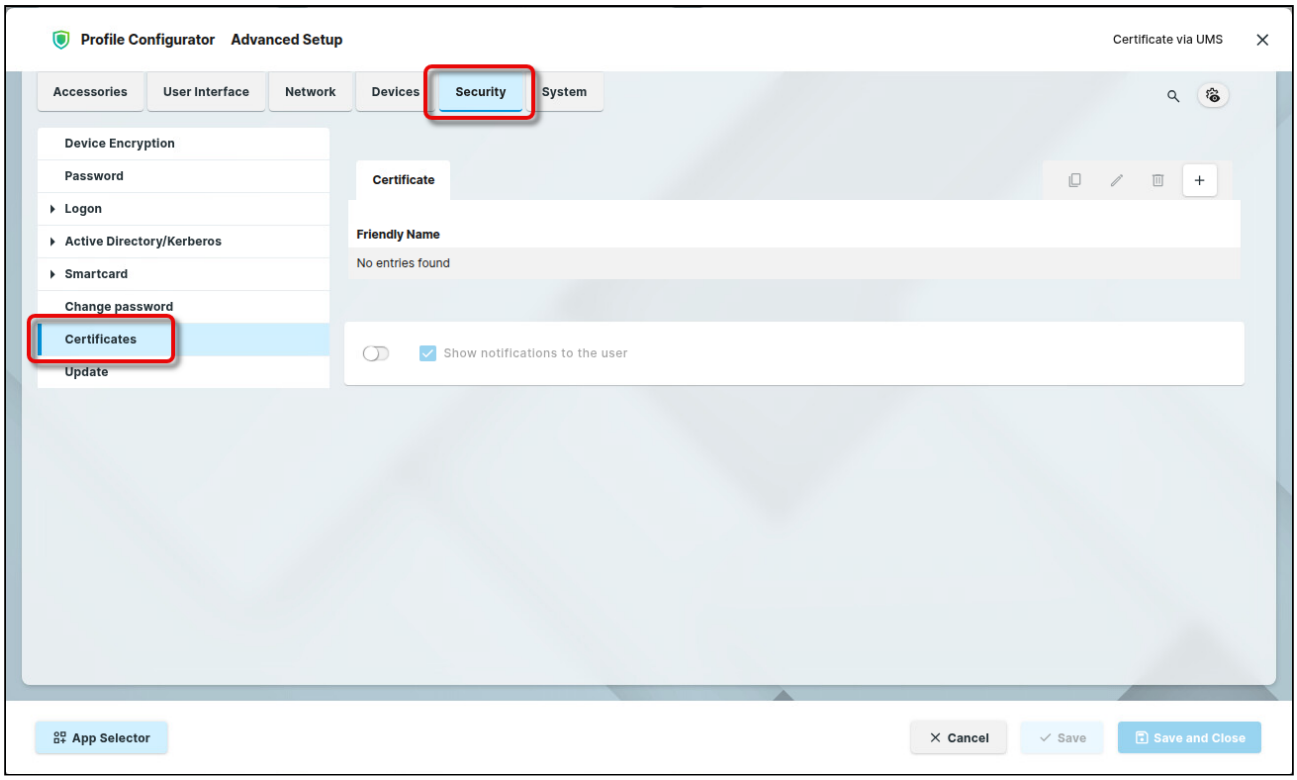
2. Enter an appropriate name for the profile and click **Select Apps**.



3. Select **IGEL OS Base System** and click **Next**.

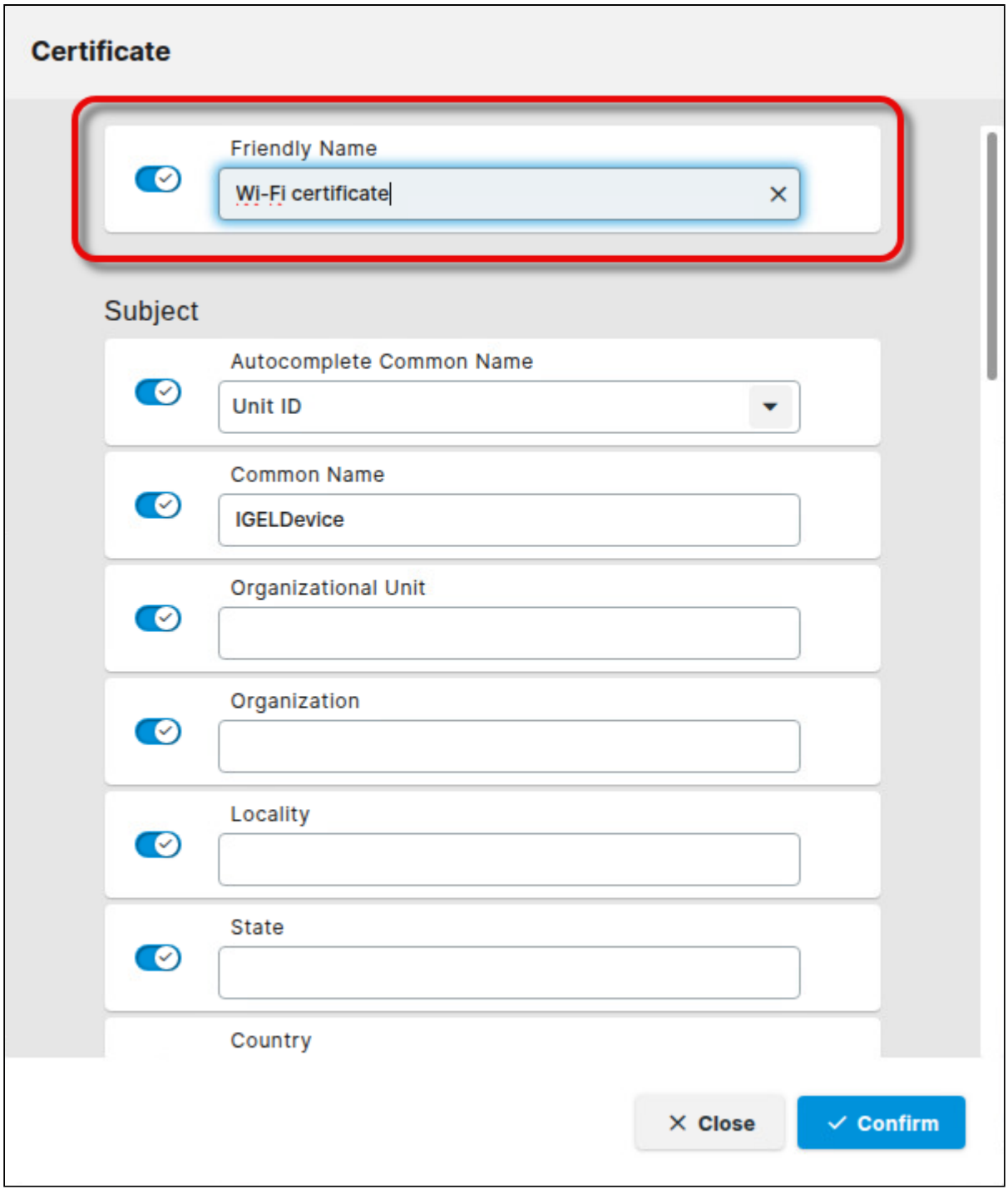


4. Go to **Security > Certificates** and click + to add a new certificate.



5. Under **Friendly Name**, enter a name for the certificate.

⚠ This name must be unique among all configured certificates on the device. It will be used as a directory name for storing the certificate files on the device. If the name has already been taken, a warning will be displayed, and an entry will be written to the system log.


Certificate
Friendly Name
Wi-Fi certificate
Subject
Autocomplete Common Name
Unit ID
Common Name
IGELDevice
Organizational Unit
Organization
Locality
State
Country
Close
Confirm

6. Enter the data for the endpoint device's certificate profile according to the certificate profile you have configured in the PKI.

The certificate profile on the endpoint device and the certificate profile defined in the PKI must match. If the certificate enrollment fails, it is recommended to check the logs of the PKI.

Some certificate parameters can be derived automatically from the device; this is done with the following parameters:

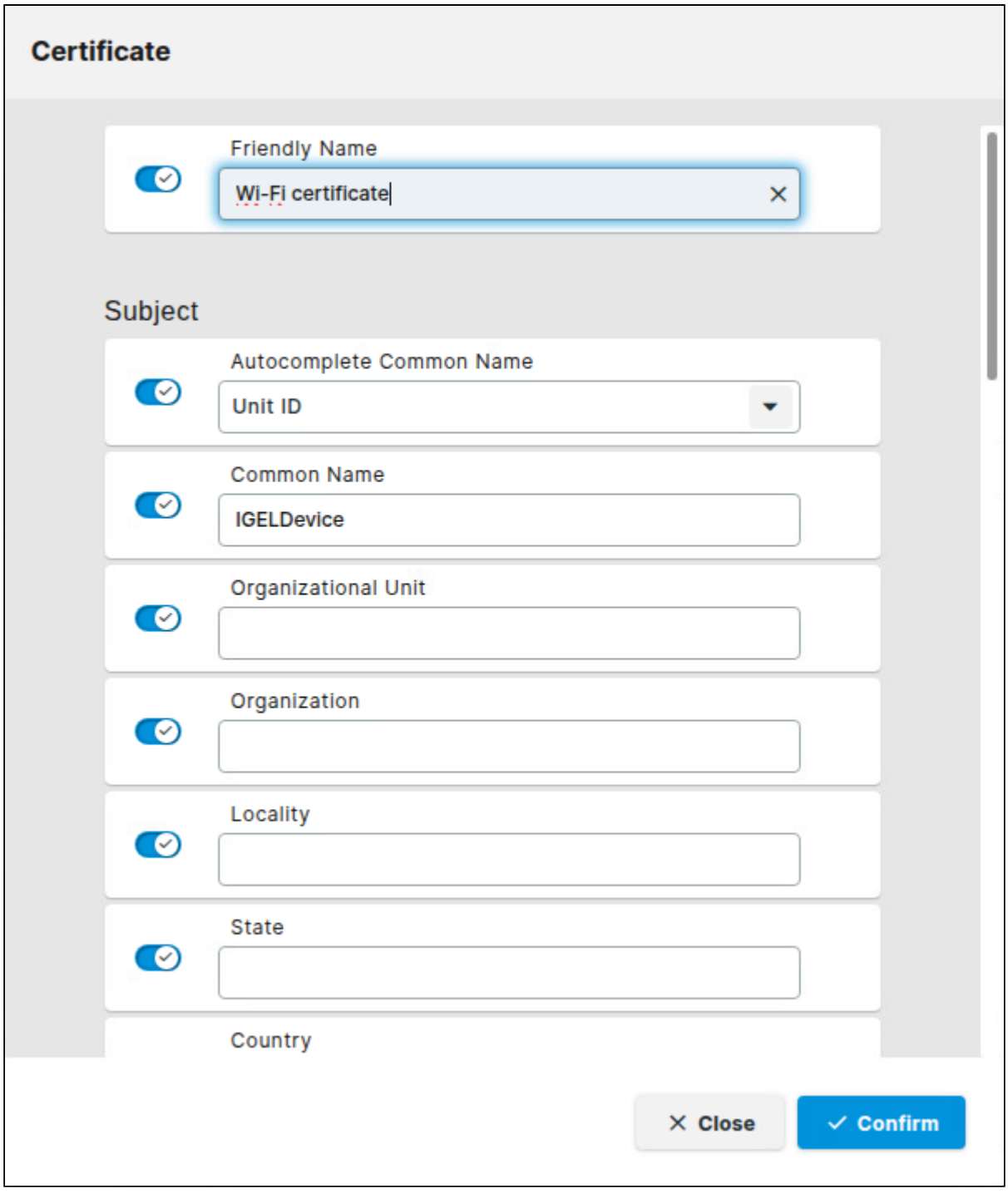
Subject

- **Autocomplete Common Name**
  The parameter replaces the occasionally configured **Common Name**.
  - **Hostname**: The device's hostname is used as the common name
  - **Unit ID**: The device's unit ID is used as the common name

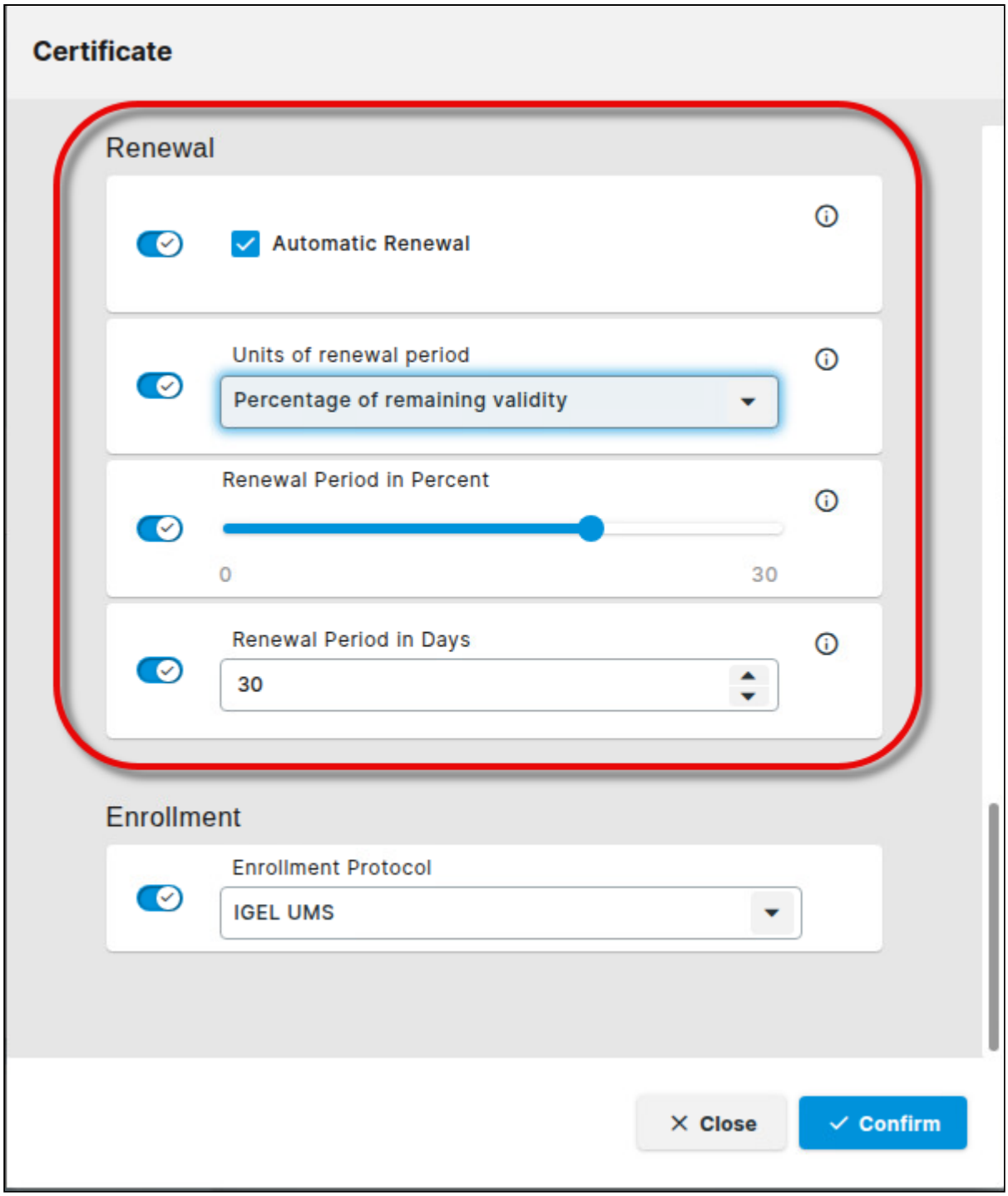
Subject Alternative Name

These auto-completed names are always added to the configured Subject Alternative Name:

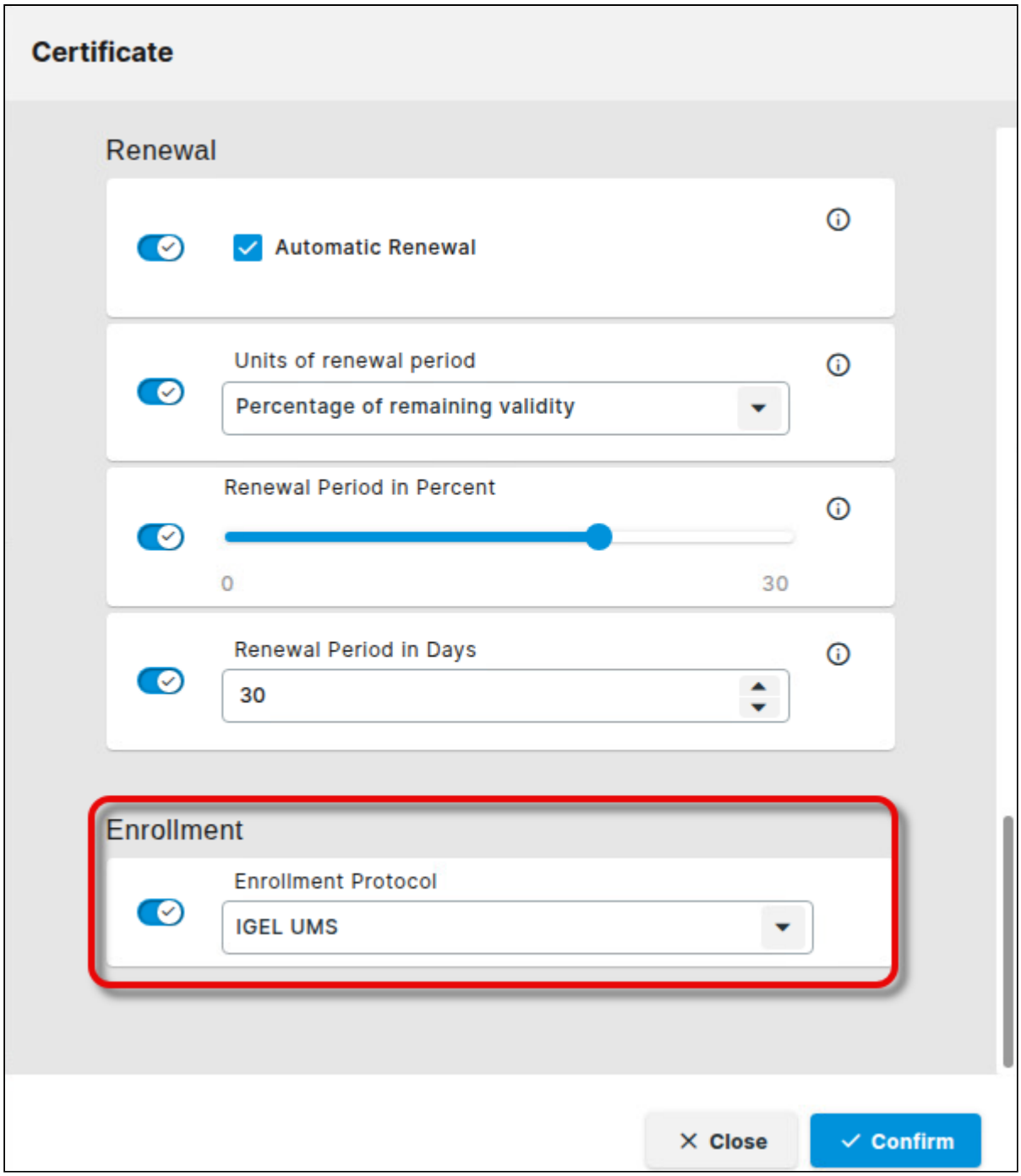
- **Autocomplete Hostname**: If enabled, the device's hostname is used in the subject alternative name
- **Autocomplete IP Address**: If enabled, the device's IP address is used in the subject alternative name


Certificate
Friendly Name
Wi-Fi certificate
Subject
Autocomplete Common Name
Unit ID
Common Name
IGELDevice
Organizational Unit
Organization
Locality
State
Country
Close
Confirm

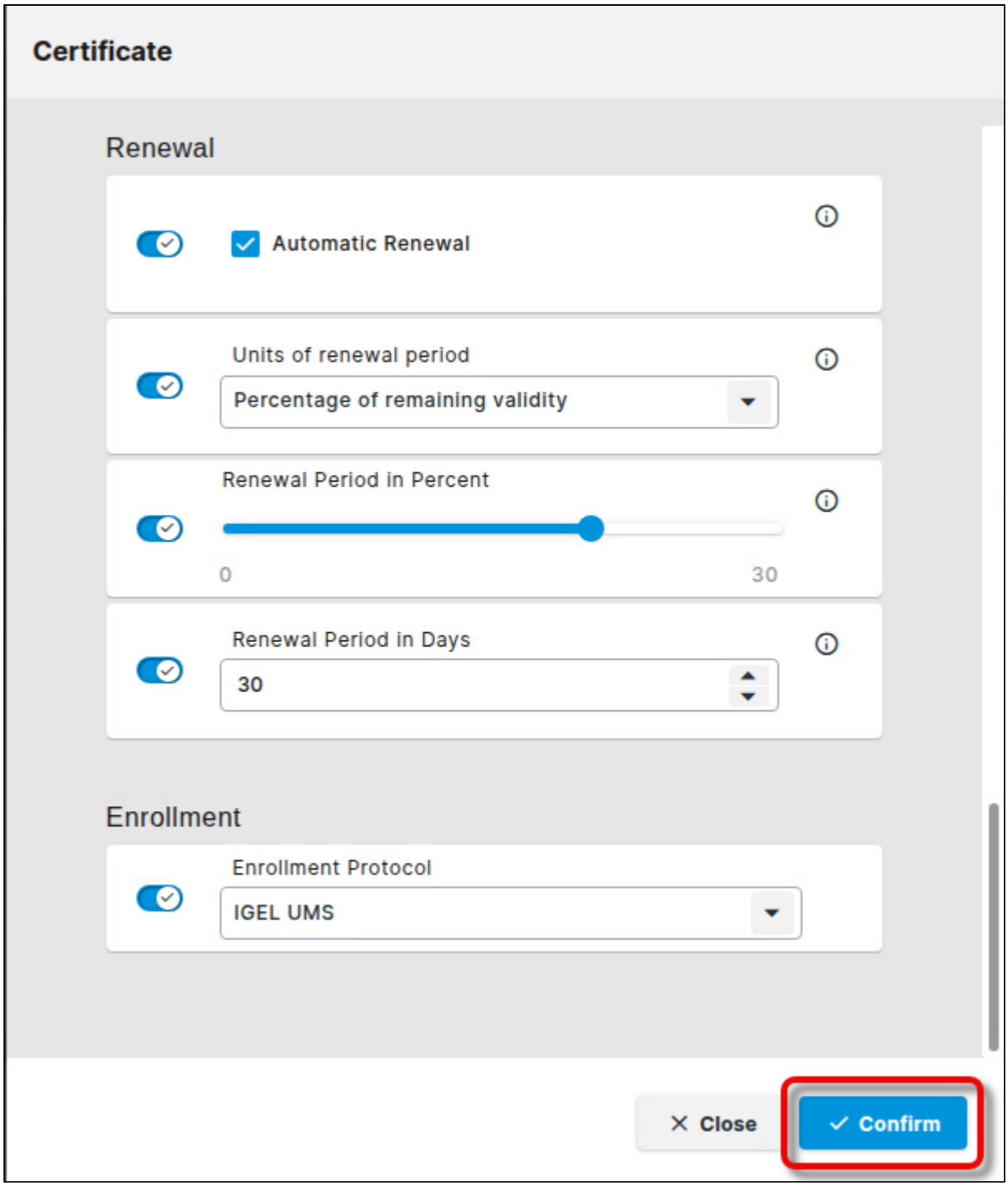
7. Edit the settings for certificate renewal according to your needs.
    - **Automatic Renewal**: When enabled, the certificate renewal will be triggered automatically, according to the settings below.
    - **Units of renewal period**: Choose whether the automatic certificate renewal will be triggered after a specified percentage of the validity period has passed or after a specified number of remaining days has been reached.
    - **Percentage of remaining validity**
    - **Days of remaining validity**
    - **Renewal Period in Percent**: Specifies the percentage of the validity period after which the renewal will be triggered. Only effective if **Units or renewal period** is set to **Percentage of remaining validity**.
    - **Renewal Period in Days**: Specifies the number of days remaining before the renewal is triggered. Only effective if **Units or renewal period** is set to **Days of remaining validity**.



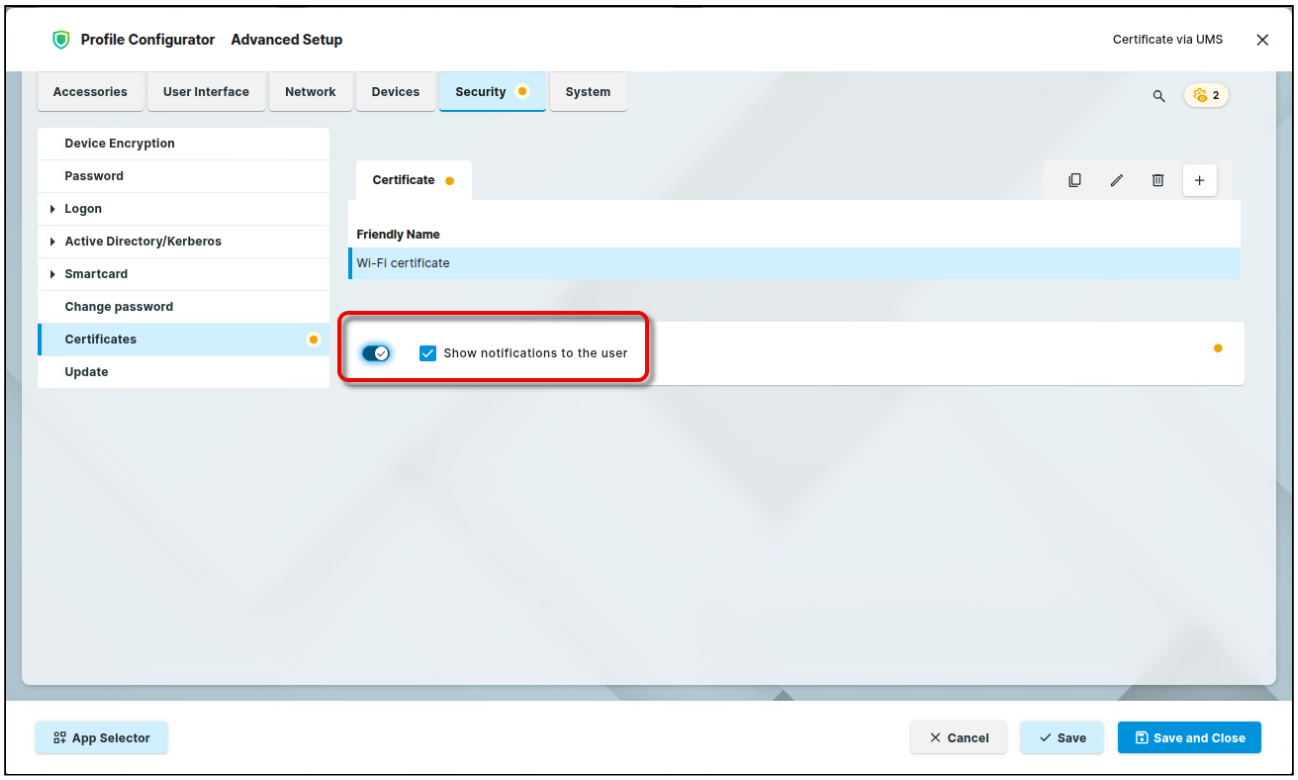
8. Set **Enrollment Protocol** to **IGEL UMS**.



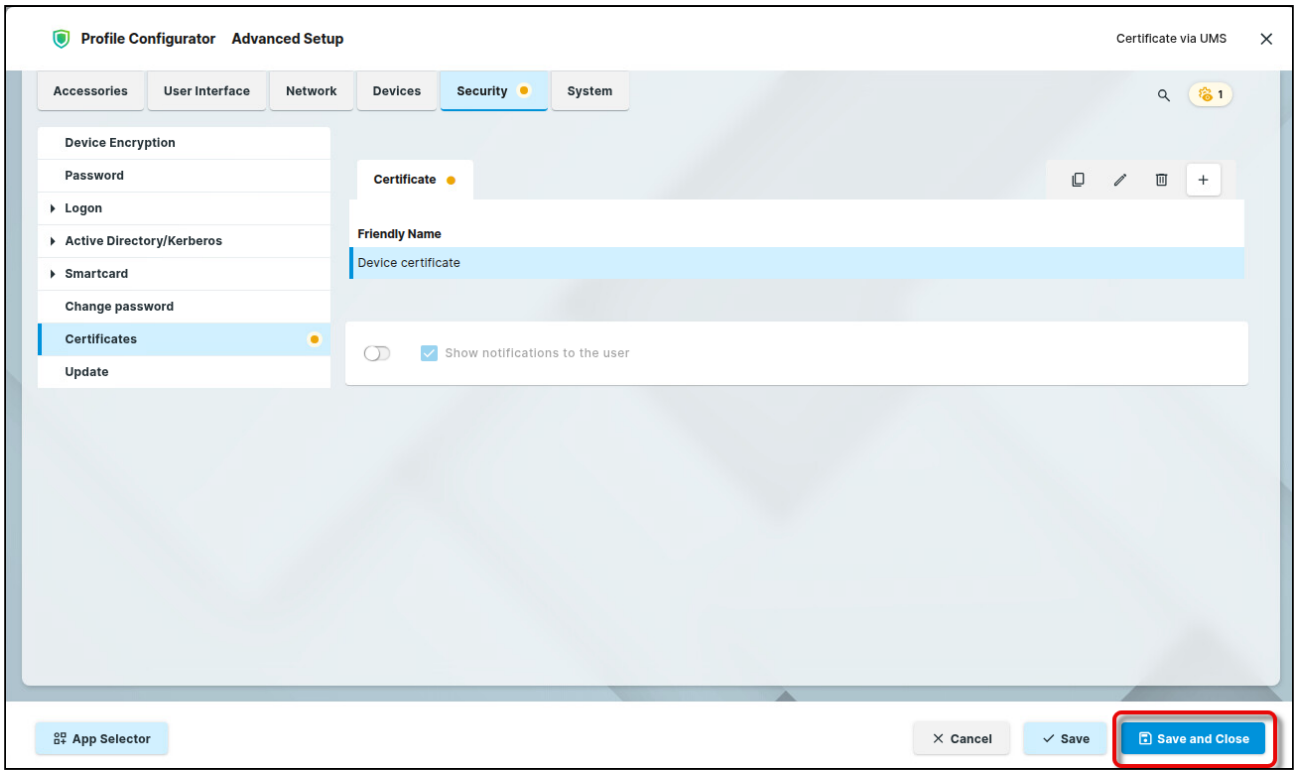
9. When you are done, click **Confirm**.



10. Review the setting **Show notifications to the user**. If enabled (default), the user is notified about the certificates on the device.

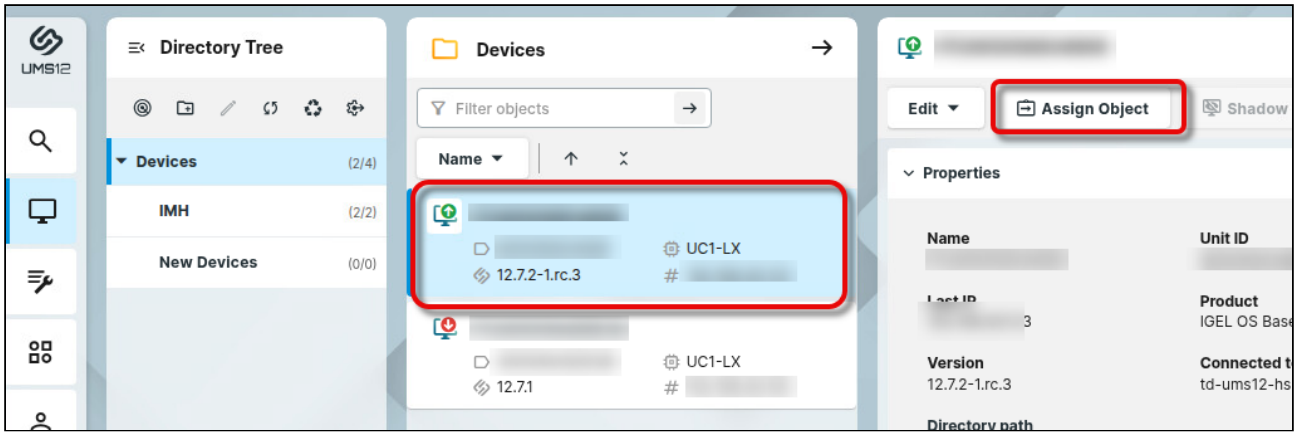


11. Click **Save and Close** to finalize your profile.

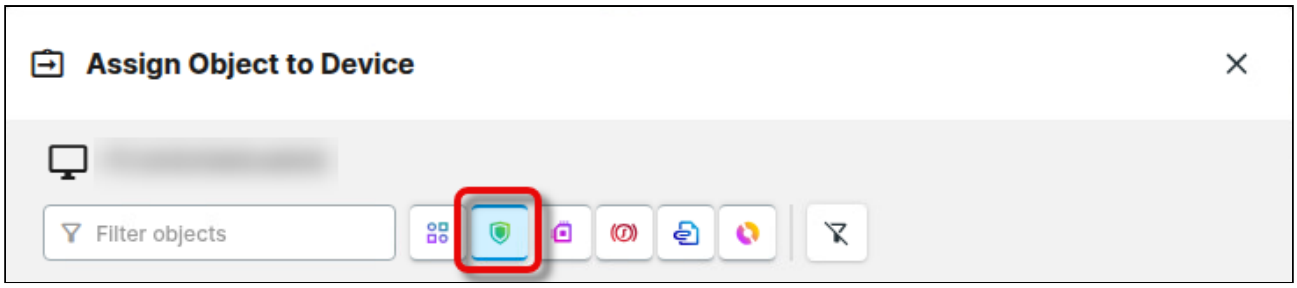


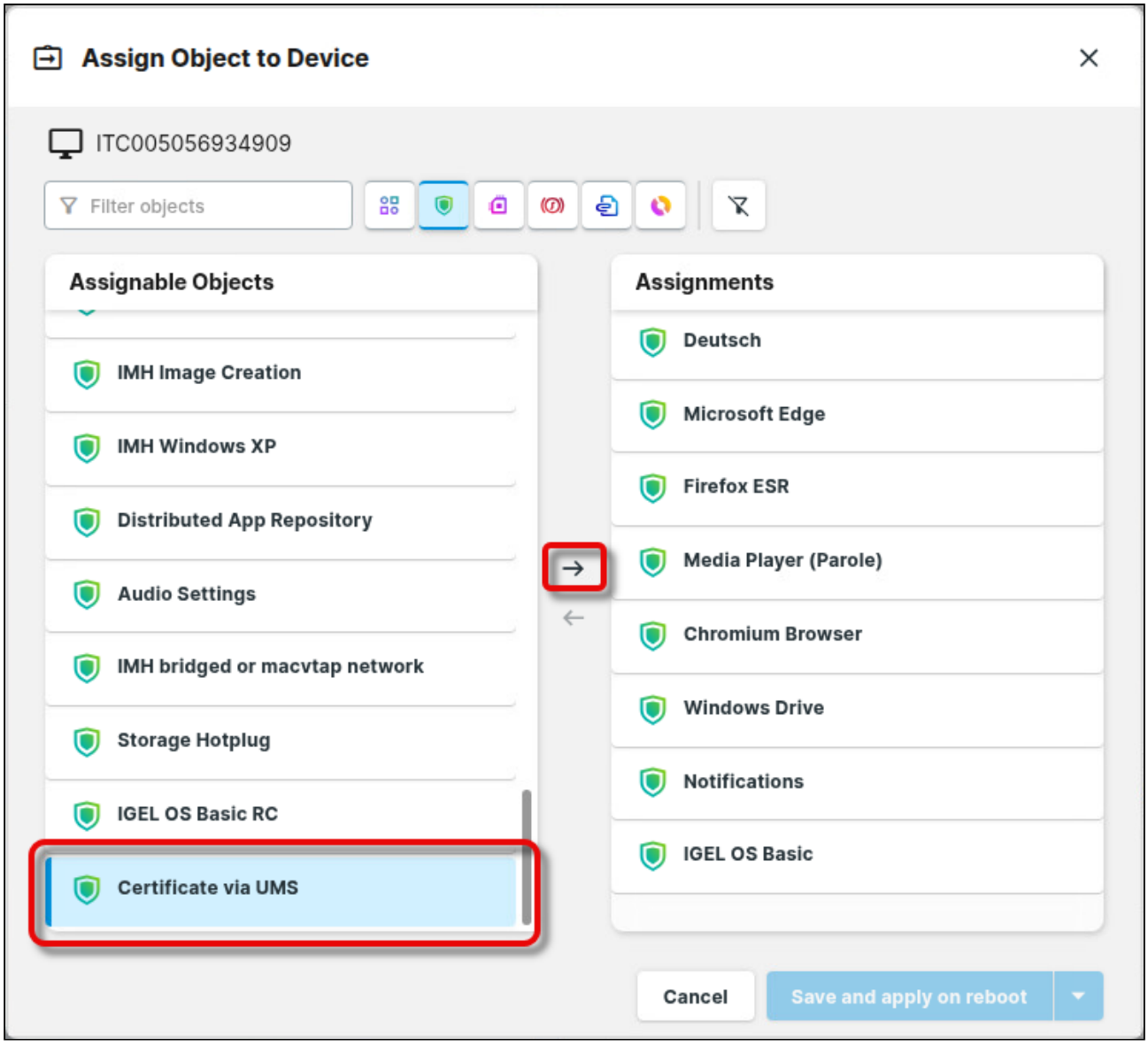
Assigning the Profile to the Devices

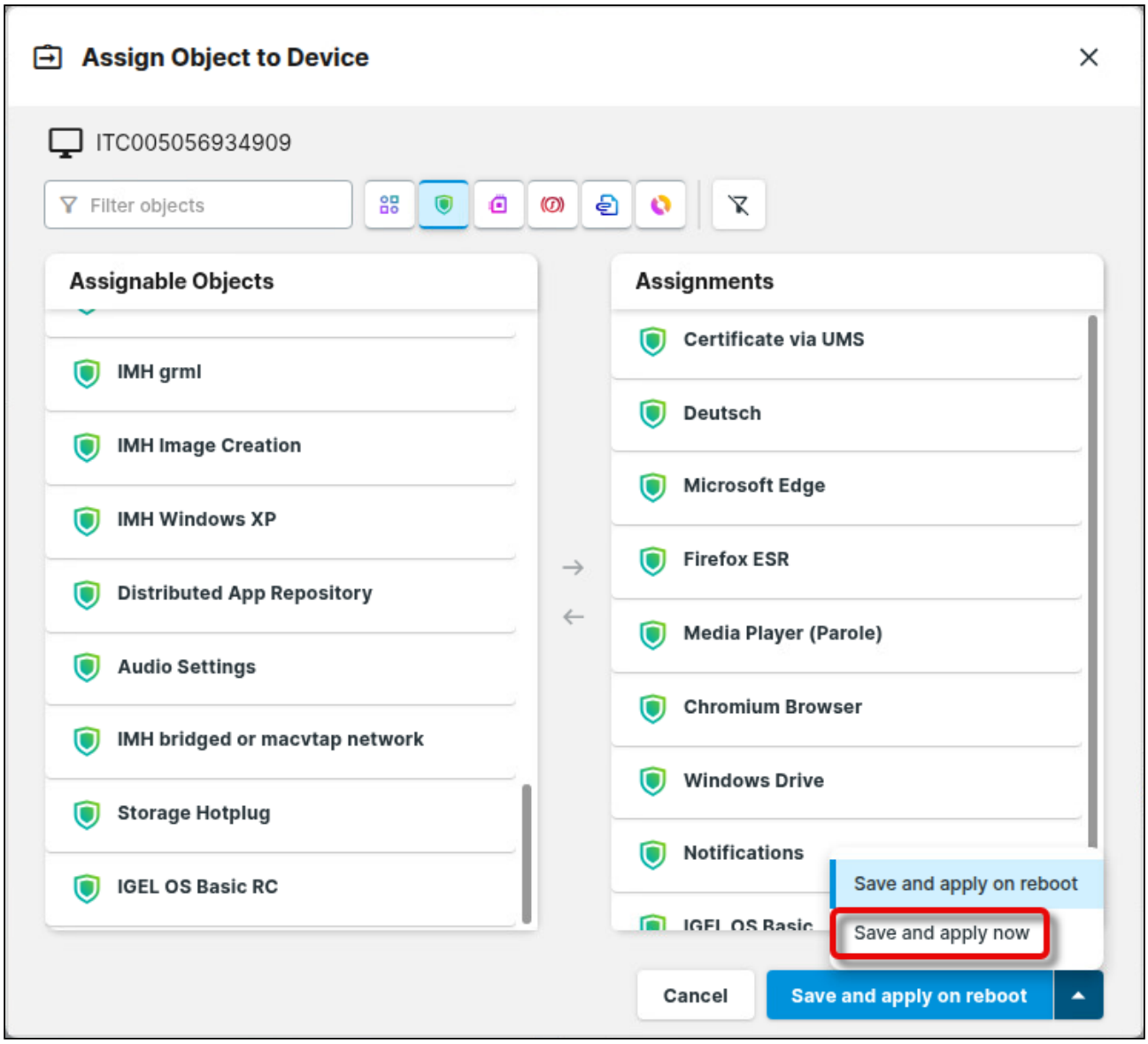
1. Go to the **Devices** area and select the relevant device or the relevant directory of devices.



2. Set the filter to show only profiles and select the profile you previously created.


Assign Object to Device
Filter objects


Assign Object to Device
ITC005056934909
Filter objects
Assignable Objects
IMH Image Creation
IMH Windows XP
Distributed App Repository
Audio Settings
IMH bridged or macvtap network
Storage Hotplug
IGEL OS Basic RC
Certificate via UMS
Assignments
Deutsch
Microsoft Edge
Firefox ESR
Media Player (Parole)
Chromium Browser
Windows Drive
Notifications
IGEL OS Basic
Cancel
Save and apply on reboot



The devices will try to obtain their certificates via the UMS immediately.

When **Show notifications to the user** is enabled (see Creating a UMS Profile, step 10 (see page 1213)), a notification about the successful certificate enrollment is shown on the device.

How Can I Verify if the Certificate Has Been Deployed on the Device?

Using the Friendly Name as the path to the enrolled certificate easily allows to configure it in use cases like 802.1x authentication or VPN.

→ Open a Local Terminal on the device and check for the following files:

- `/wfs/igel-certs/<FRIENDLY NAME>/cert.pem` - The enrolled certificate in PEM format

- `/wfs/igel-certs/<FRIENDLY NAME>/cert.pfx` - This is a PKCS12 container including the private key, certificate and CA certificates. The container is protected by the configured key's password.
- `/wfs/igel-certs/<FRIENDLY NAME>/pkey.pem` - The private key in PEM format protected by the configured password
- `/wfs/igel-certs/<FRIENDLY NAME>/cacerts.pem` - The CA certificate(s). Additionally, all the CA certificates are automatically installed to the system-wide OpenSSL repository of CAs in `/etc/ssl/cert/ directory`.
- `/wfs/igel-certs/<FRIENDLY NAME>/cacerts/<CN>.pem` - The CA certificate from the bundle `cacerts.pem`. Additionally, all the CA certificates are automatically installed to the system-wide OpenSSL repository of CAs in `/etc/ssl/cert/ directory`.

→ To review the relevant log entries, enter `journalctl | egrep 'rmagent|igel-certs'`

How to Manage Custom Device Attributes in the IGEL UMS Web App

In the IGEL Universal Management Suite (UMS) Web App, you can manage custom device attributes in the **Devices** area. You can define values for these attributes per device and use the custom device attributes in:

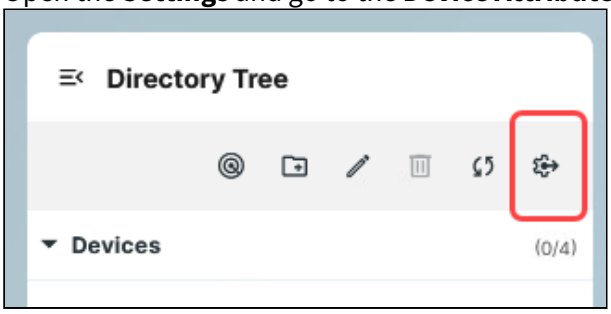
- Searches in the Search for Objects in the IGEL UMS Console (see page 693) and the Search for Devices in the IGEL UMS Web App (see page 1164)
- Views - Filtering for Devices in the IGEL UMS (see page 818)
- Default Directory Rules (see page 969)

You can also manage custom device attributes in the UMS Console. For details, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879) .

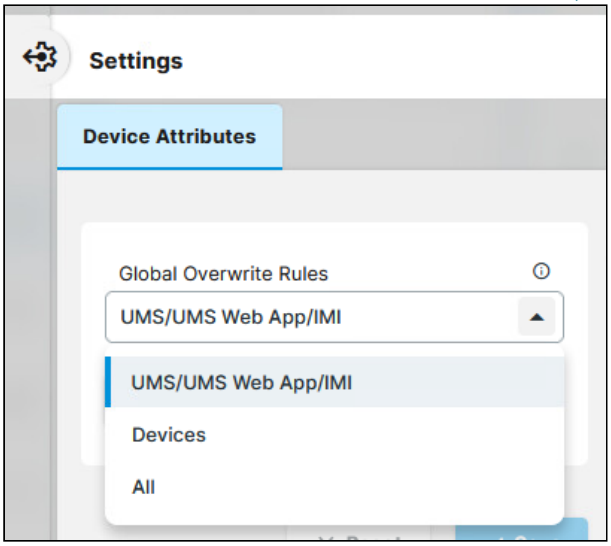
Set Global Overwrite Rule

The overwrite rule defines how the values of device attributes can be set and changed. To define the default overwrite rule for those device attributes whose overwrite rule is set to **Global setting**:

1. Open the **Settings** and go to the **Device Attributes** tab.



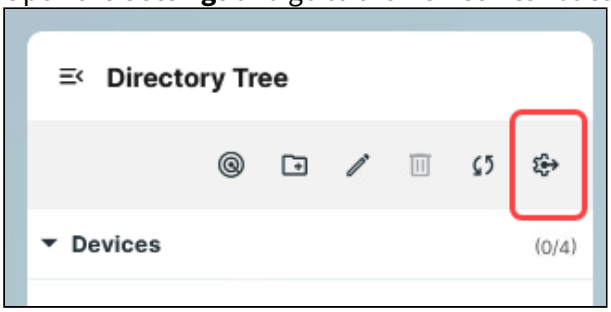
2. Select the **Global Overwrite Rule** from the drop-down menu. For details, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879) .



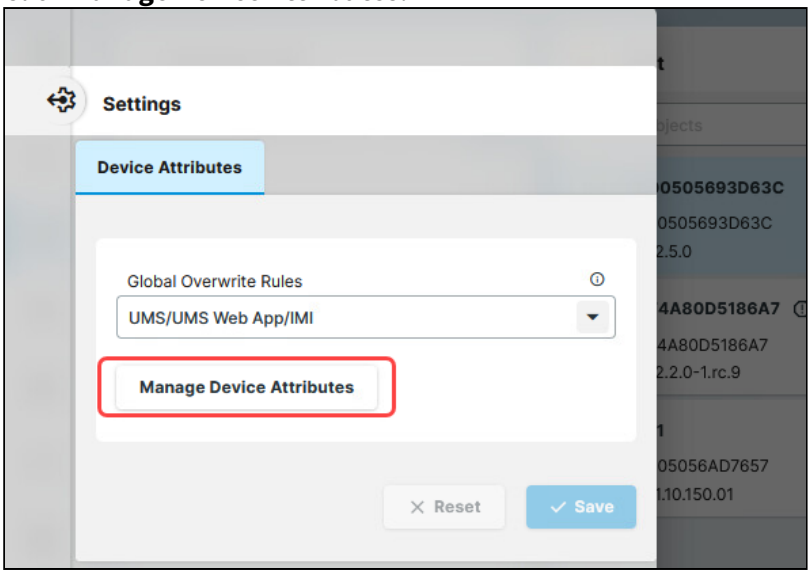
Add and Edit Device Attributes

To add a new attribute or edit an existing one:

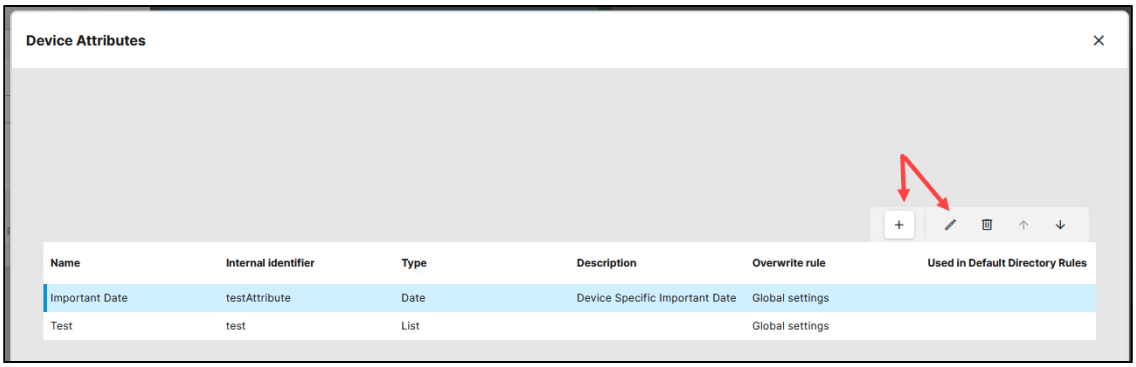
1. Open the **Settings** and go to the **Device Attributes** tab.



2. Click **Manage Device Attributes.**



3. Here you can:
   - add a new attribute by clicking **+**.
   - edit a selected attribute by clicking the pencil icon.
   - delete an attribute by clicking the bin icon.
   - use the up and down arrows to change the order of the additional attributes.

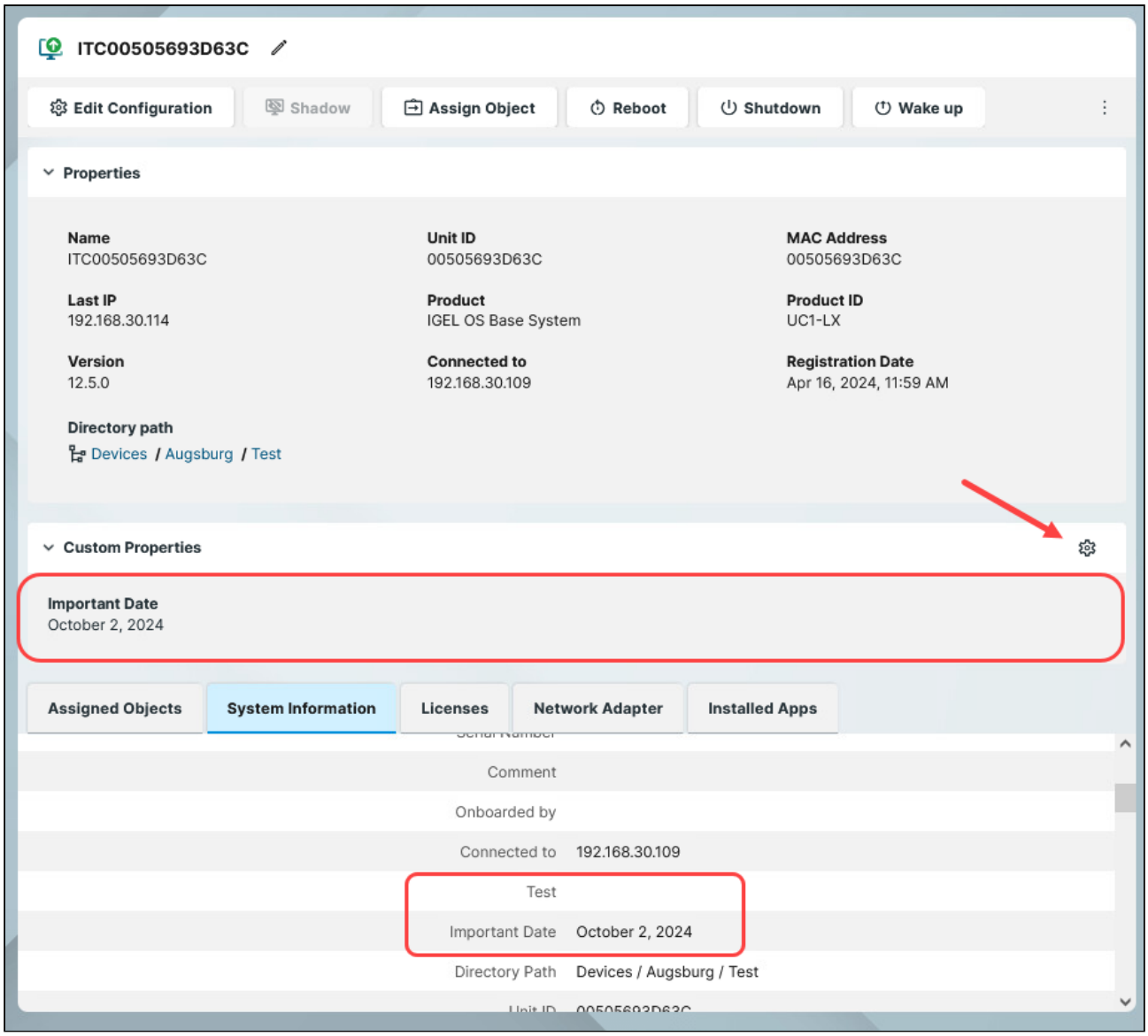


4. You can configure the parameters of the attribute, like **Name**, **Type**, **Description**. For details on the parameters, see Managing Device Attributes for IGEL OS Devices in the IGEL UMS (see page 879) .
5. Save the attribute and close the dialog.

Set the Attribute Value for the Device

You can find the configured custom device attributes and their values defined for the selected device under **Custom Properties** and also under the **System Information** tab.

→ You can set the attribute value for the device by clicking the settings icon under **Custom Properties**.


ITC00505693D63C
Edit Configuration
Shadow
Assign Object
Reboot
Shutdown
Wake up
Properties
Name
ITC00505693D63C
Unit ID
00505693D63C
MAC Address
00505693D63C
Last IP
192.168.30.114
Product
IGEL OS Base System
Product ID
UC1-LX
Version
12.5.0
Connected to
192.168.30.109
Registration Date
Apr 16, 2024, 11:59 AM
Directory path
Devices / Augsburg / Test
Custom Properties
Important Date
October 2, 2024
Assigned Objects
System Information
Licenses
Network Adapter
Installed Apps
Comment
Onboarded by
Connected to
192.168.30.109
Test
Important Date
October 2, 2024
Directory Path
Devices / Augsburg / Test

How to Reset a Device to Factory Defaults via the IGEL UMS Web App

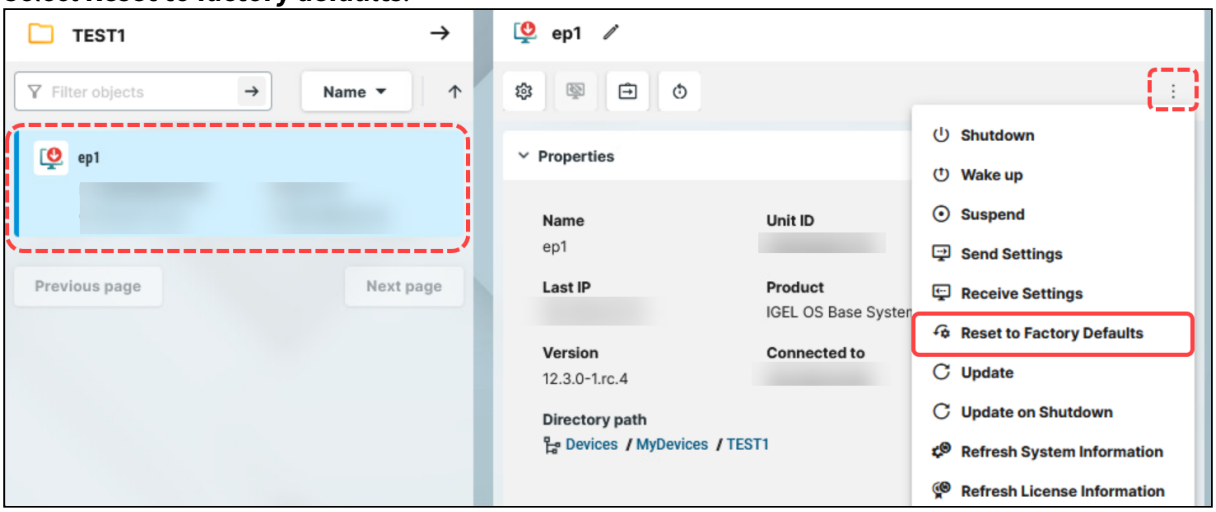
In the IGEL Universal Management Suite (UMS) Web App, you can reset a device to factory defaults. This may be necessary, for example, because of misconfiguration or if the administrator password for IGEL OS has been lost and the local setup is therefore no longer accessible.

> ⚠ If you select **Reset to factory defaults**, all personal settings on the device (including your password and the sessions you have configured) will be lost and the device will be removed from the UMS. You will have to register your device with the UMS again.

Menu path: **UMS Web App > Devices > Reset to factory defaults**

To reset a device to factory defaults, proceed as follows:

1. In the **UMS Web App > Devices**, select the required device and click ⋮.
2. Select **Reset to factory defaults**.



3. Confirm the dialog.
4. Confirm on the device that it can be restarted or wait till the device restarts automatically.

   After the reboot, you will see the Setup Assistant and can register your device with the UMS Server anew.

Remote Access to Devices via Shadowing in the IGEL UMS Web App

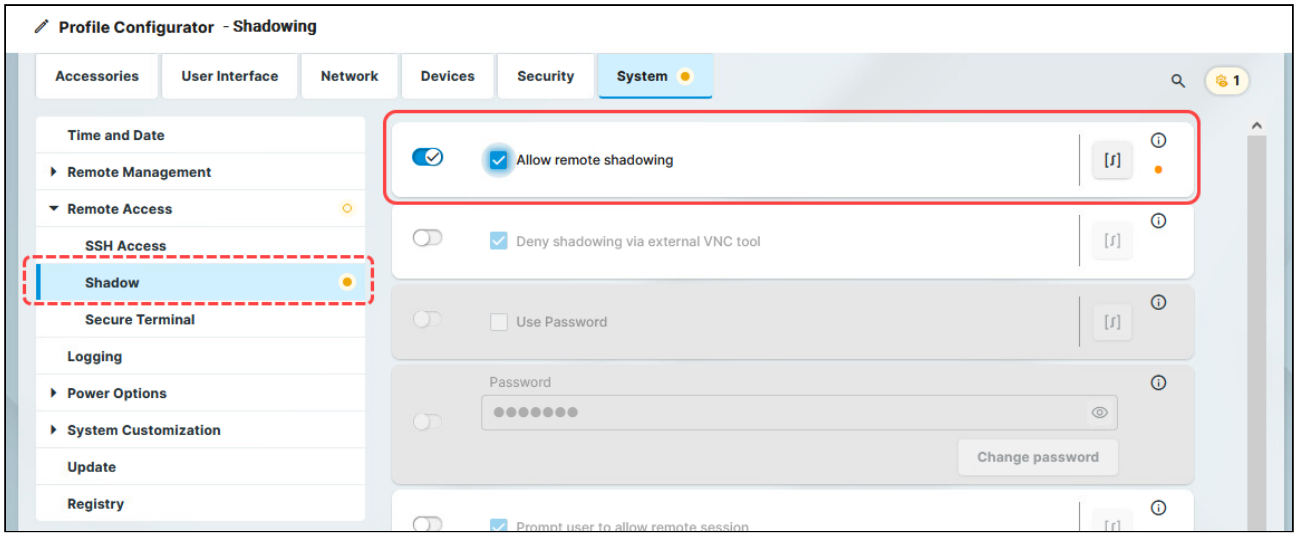
You can observe the desktop of an device on your local PC via shadowing with VNC. Shadowing via the UMS Web App and the UMS Console is supported for IGEL OS 12 and OS 11 devices. For more information on shadowing via the UMS Console, see Shadowing - Observe IGEL OS Desktop via VNC (see page 810).

> To shadow the device, you will require **Remote access** permission, which can be set in the UMS Console via **[context menu of the device / device directory] > Access control**. See Object-Related Access Rights (see page 1016).

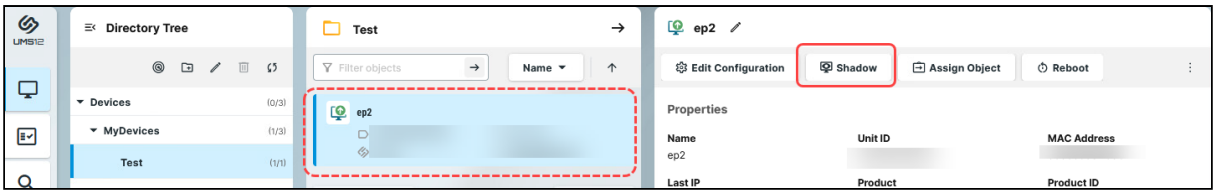
To shadow the IGEL OS 12 device:

1. Create a profile for IGEL OS base system and go to **System > Remote Access > Shadow**. For how to create profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).
2. Enable **Allow remote shadowing** and configure other settings according to your needs.

> **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 814) via plain VNC protocol.



3. Save the settings and assign the profile to the required devices.
4. Under **Devices**, select the device and click **Shadow**.



The shadowing request will be sent to the device. If you decided to enable **Prompt user to allow remote session**, the user must accept the shadowing request.

How to Export Device Settings as a Profile in the IGEL UMS Web App

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 or if you want to import them later as a profile, for example, to another UMS installation.

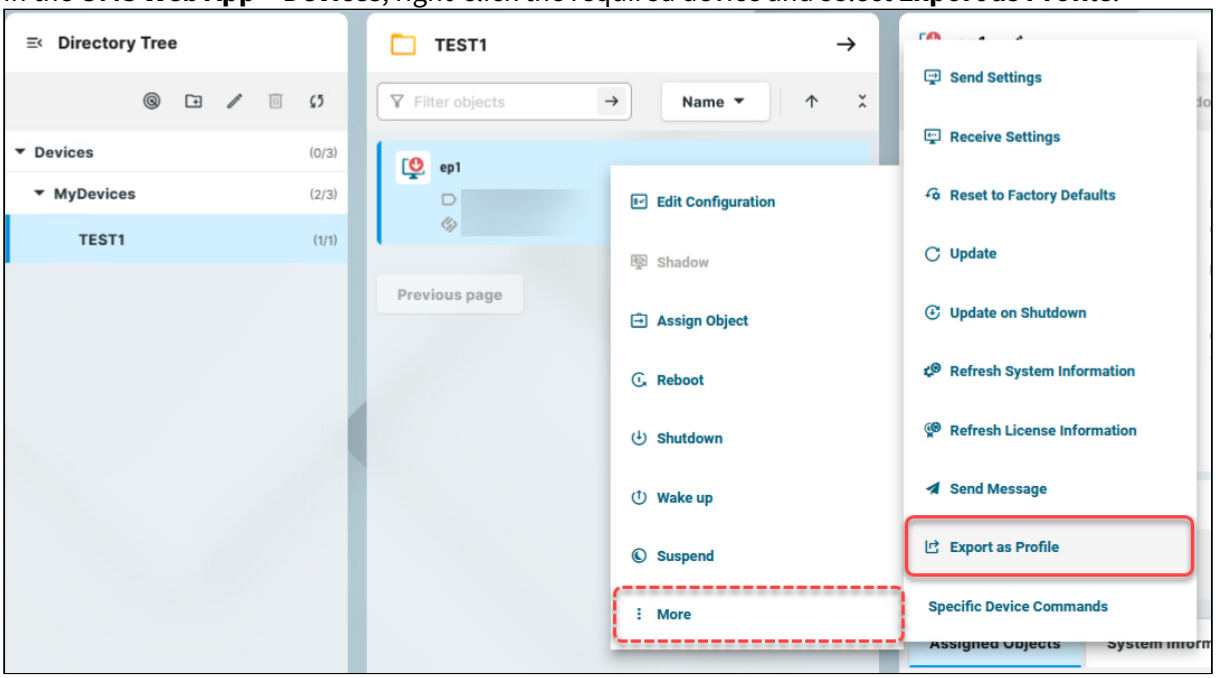
> In the UMS Web App, you can export device settings for IGEL OS 12 devices only. If you need to export the settings of IGEL OS 11 devices, see How to Export Device Settings in the IGEL UMS (see page 801).

If you want to export purely profiles, see Exporting and Importing Profiles in the IGEL UMS Web App (see page 1269).

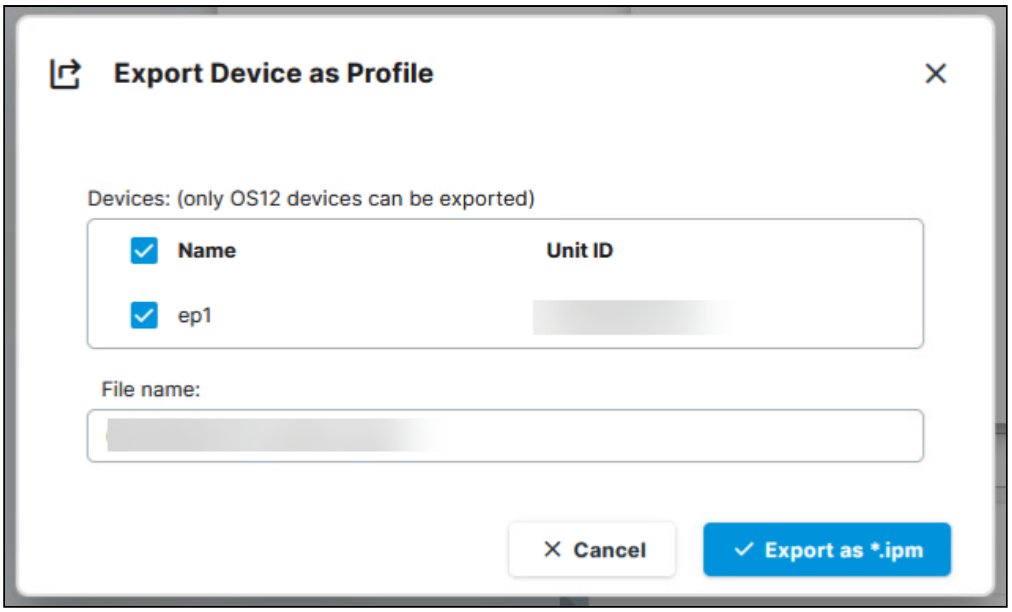
Menu path: **UMS Web App > Devices > [name of the device] > Export as Profile**

To export device settings, proceed as follows:

1. In the **UMS Web App > Devices**, right-click the required device and select **Export as Profile**.



2. Specify the desired **file name**.
3. Confirm the export.



The device settings are saved as an `.ipm` file, which also includes the metadata of IGEL OS Apps these device settings are based on. Therefore, it is not necessary to additionally import the required apps / app versions from the IGEL App Portal (or from the UMS).

> If the UMS to which you import the exported file has UMS as an Update Proxy feature activated but the fallback to the App Portal is disabled, you may nevertheless require the app binaries, see Configuring Global Settings for the Update of IGEL OS Apps (see page 1342).

You can now import the exported file as a profile as described under Exporting and Importing Profiles in the IGEL UMS Web App (see page 1269).

> All passwords are excluded, i.e. replaced with a placeholder in the exported file. If you import the exported device settings later as a profile, no passwords will be included. You will have to set the passwords anew.

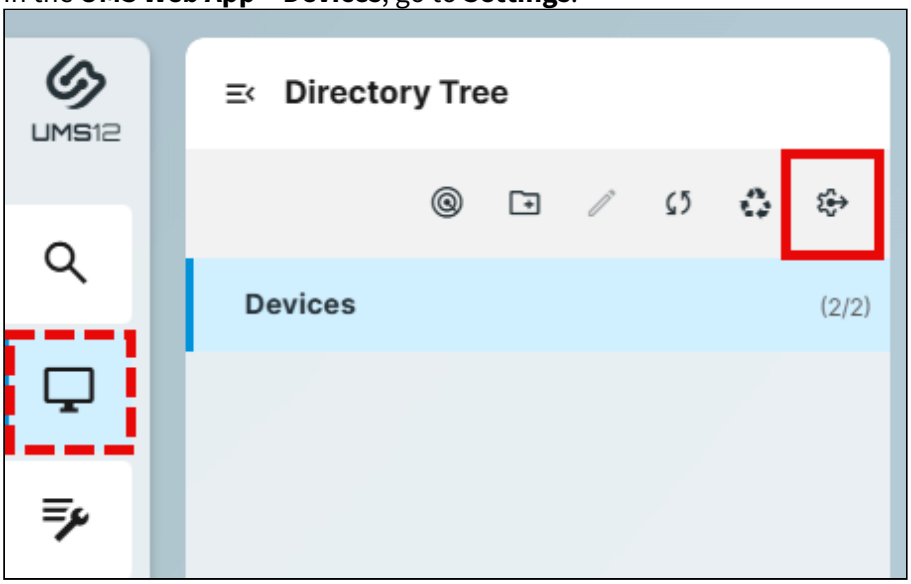
How to Manage First-Authentication Keys in the IGEL UMS Web App

In the IGEL Universal Management Suite (UMS) Web App, you can create and edit first-authentication keys in the area **Devices > Settings**. First-authentication keys can be used for onboarding IGEL OS 12 and IGEL OS 11 devices. For more information, see Onboarding IGEL OS 12 Devices[199].

To access **UMS Web App > Devices > Settings > First Authentication Keys**, you need the rights for the node **First-authentication Keys** under **UMS Console > UMS Administration > Global Configuration**, see First-authentication Keys in the IGEL UMS[200].
For more information on rights, see Object-Related Access Rights[201].

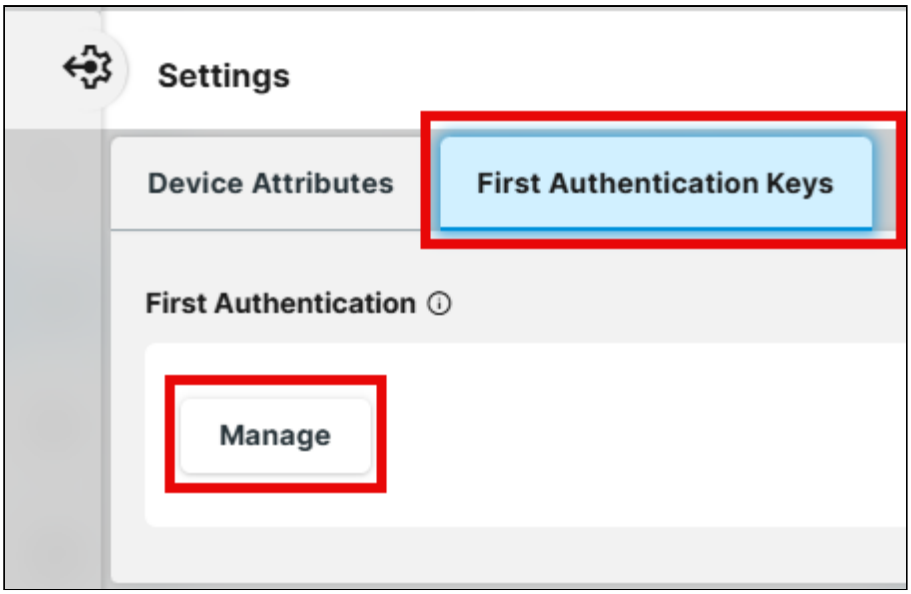
Create First-Authentication Keys

1. In the **UMS Web App > Devices**, go to **Settings**.

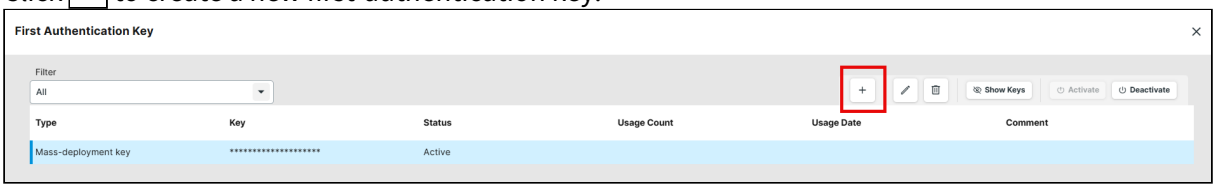


2. Under **First Authentication Keys**, click **Manage**.

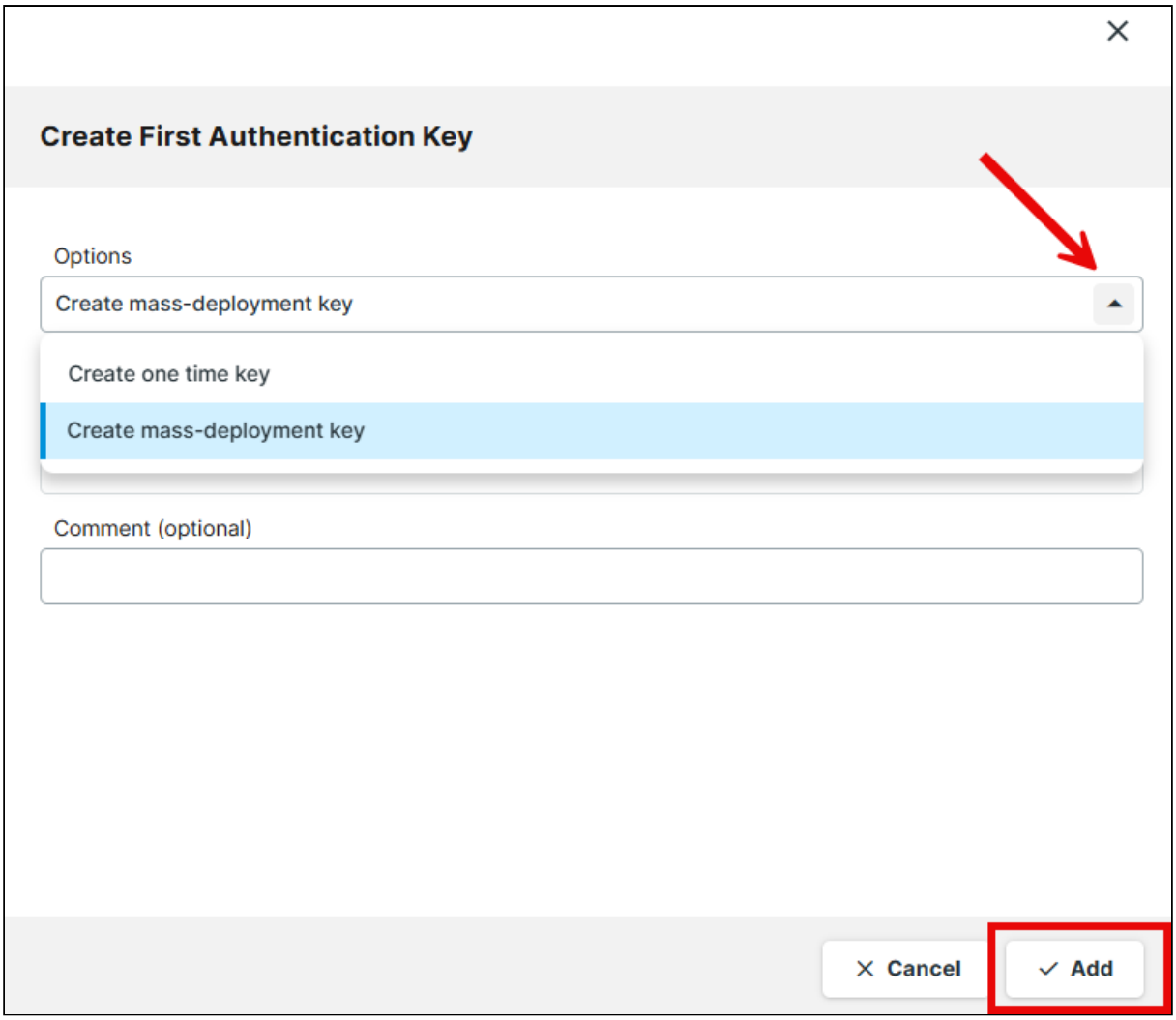
199. https://kb.igel.com/en/how-to-start-with-igel/current/onboarding-igel-os-12-devices
200. https://kb.igel.com/en/universal-management-suite/current/first-authentication-keys-in-the-igel-ums
201. https://kb.igel.com/en/universal-management-suite/current/object-related-access-rights



3. Click + to create a new first-authentication key.



4. Under **Options**, select the type of the key you require.



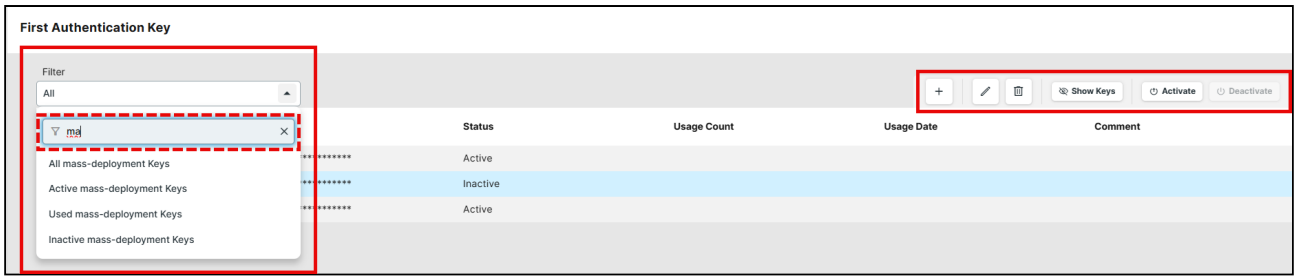
You have the following options:

- **Create one time key**
  One-time keys can be used by any random device for the onboarding, but cannot be re-used by any other device. Hence, the number of keys must match the number of devices.
  - **Quantity**: Desired number of passwords to be created.

- **Create mass-deployment key**
  Multiple-time keys that can be used by any device for the onboarding and will remain valid after the use.
  - **Generate random mass key**
    - ☑ A random multiple-time password will be generated. (Default)
    - ☐ You can enter the desired password yourself. Note that it is not possible to create more than one first-authentication key with the same password.

5. Click **Add** to save the key.

Actions for the First-Authentication Keys



	Create new first-authentication keys.
	Edit the selected key.
	Delete the selected key.
Show keys	Displays all passwords.
Hide keys	Hides all passwords.
Activate	Enables the selected key. The key can be used for onboarding.
Deactivate	Disables the selected key. The key cannot be used for onboarding. Key deactivation does not affect devices that have already been onboarded with this key.
Filter	Displays the keys according to the selected filter criterion.

How to Manage Virtual Machines Running on IGEL OS 12 from the IGEL UMS Web App

The IGEL Managed Hypervisor (IMH) provides centralized management capabilities and with the IGEL Ready partner integrations it ensures high availability and operational continuity for critical environments. Using the IMH app, it is possible to run virtual machines on IGEL OS 12 devices and provide a secure and manageable solution to run old workloads in a modern infrastructure.

The virtual machines running on the IGEL OS 12 devices can be centrally managed through the IGEL Universal Management Suite (UMS) Web App.

Use Cases

You can find more information on the use cases of the IGEL Managed Hypervisor and request a demo on the IGEL webpage Secure, Managed IT and OT Systems | IGEL Technology[202] .

Requirements

Licensing

- You need a UMS License that includes the management feature.
- You need the IGEL MANAGED HYPERVISOR add-on license to use the IMH app.

For details, see IGEL MANAGED HYPERVISOR Add-On License[203].

If your UMS license expires, you will no longer be able to perform actions, but you will still see a list of VMs.

Permissions

- As an administrator, you need to have the **Managed Hypervisor** global permission enabled.

For details on permissions, see How to Create Administrator Accounts in the IGEL UMS[204].

Software

- You need IGEL UMS 12.09.100 or higher and IGEL OS 12.7.0 or higher
- You need the IGEL Managed Hypervisor app[205] installed on the IGEL OS 12 device. Otherwise, the tab in the UMS Web App is not visible.

202. https://www.igel.com/secure-managed-hypervisor/
203. https://kb.igel.com/en/igel-subscription-and-more/current/igel-managed-hypervisor-add-on-license
204. https://kb.igel.com/en/universal-management-suite/current/how-to-create-administrator-accounts-in-the-igel-u
205. https://kb.igel.com/en/igel-apps/current/igel-managed-hypervisor

Managing Virtual Machines in the UMS Web App

You can find a demo video on managing virtual machines through the UMS Web App below.

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

https://www.youtube.com/watch?v=d6xwL13PQ7g

To manage the virtual machines deployed on the IGEL OS 12 devices:

1. In the UMS Web App go to the **Devices** area.

2. Select the device and go to the **Hypervisor** tab.

4. Select a virtual machine from the list of the deployed virtual machines to display machine information. You will find status information displayed, for example:
   - State of the machine (for example, Running)
   - Number of CPUs
   - RAM
   - Description

If you click refresh at the top of the list, you update the list to reflect the current state of the virtual machines. The refresh process reloads the VM list and any changes made to the VM configurations.

5. Use the action buttons on the right to manage the selected VM. You can:
   - Start the virtual machine: ▶
   - Stop the virtual machine: ■

You can perform the actions as bulk actions for all the machines at once.

You need to confirm all actions in a confirmation dialog before the action is performed.

Creating a Directory Structure in the IGEL UMS Web App

In the IGEL Universal Management Suite (UMS) Web App, you can create device directories. You can create as many directories and subdirectories as you want in order to group the devices together.

Menu path: **UMS Web App > Devices**

General Information

You may freely organize your device structure in the IGEL UMS. Take advantage of this freedom and build well-thought-out, intelligent directory structures. You will need a smart structure, for example, for the automatic rollout when devices will be stored directly in the correct directory and the right configurations (profiles, apps) will be automatically assigned to them.

How deeply you want to structure your tree is up to you. The system allows you to nest directories as deeply as you want.

It would be advisable to arrange the directories referring to your company's structure. You could classify the devices, for example, according to branch offices, departments, or tasks.

When you create sub-directories, the devices organized in it form subgroups of a group.

A device that is unequivocally identified by its MAC address can only be stored in a single directory, i.e. only as a member of a single group.

Actions performed at the directory level apply to all subdirectories and devices contained in this directory. Performing actions at the directory level requires certain permissions, see the "Permissions" section under Important Information for the IGEL UMS Web App (see page 1155).

Creating a Device Directory

To create a directory or subdirectory, proceed as follows:

1. In the **Directory Tree**, select a directory, e.g. "Devices".
2. Click .
3. Enter a name for the new directory.
4. Press [Enter].
   The new directory will be displayed below the selected directory in the **Directory Tree**.

You can now move devices to this new directory.

How to Move Devices in the IGEL UMS Web App

Since a device can only be stored in a single directory in the IGEL Universal Management Suite (UMS), you cannot copy devices, but only move them.

> ⚠ If profiles and apps are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, the configuration of the device will change too. Moving an IGEL OS 12 device to another directory can lead to the uninstallation of apps.
> The new configuration can take effect either immediately or when the device is next rebooted.

Menu path: **UMS Web App > Devices**

Devices are moved via drag & drop:

1. In the **Directory Tree**, select a directory that contains the device to be moved.
2. Select the relevant device.
3. Drag the device to the directory required and drop it.
   The **Move device** dialog opens.
4. Select when you want the changes to take effect.
5. Confirm that you wish to move the device by clicking on **Move**.

How to Copy a Device Directory in the IGEL UMS Web App

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. In the **Directory Tree**, click on the directory that you want to copy.
2. Press [Ctrl + C].
3. Click on the directory in which you would like to paste the copy of the directory.
4. Press [Ctrl + V].
5. Confirm the **Copy directory** dialog.
   A new device directory that 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.

> You can copy a device directory also via drag & drop while holding down the [Ctrl] key.

Moving a Device Directory

When moving a device directory to another directory, the directory itself, its subdirectories, and devices contained in them will be moved.

Menu path: **UMS Web App > Devices**

To move a device directory, proceed as follows:

1. In the **Directory Tree**, click on the directory that you want to move.
2. Click [Ctrl + X].
3. Click on the directory in which you would like to move the directory.
4. Click [Ctrl + V].
   The **Move directory** dialog opens.

> If profiles and apps are indirectly assigned to a device or revoked as a result of the device being moved to a different directory, the configuration of the device will change too. Moving an IGEL OS 12 device to another directory can lead to the uninstallation of apps.
> The new configuration can take effect either immediately or when the device is next rebooted.

5. Select when you want the changes to take effect and confirm this by clicking on **Move**.

> You can move a directory also by dragging and dropping it to another directory.

How to Rename a Directory in the IGEL UMS Web App

To rename a directory or subdirectory in the IGEL Universal Management Suite (UMS) Web App:

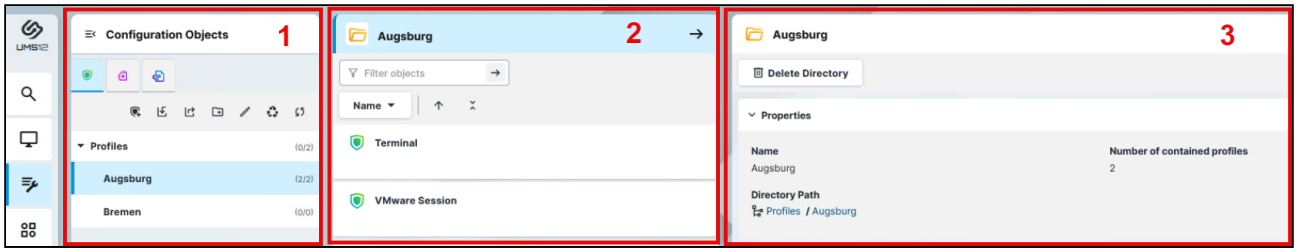
1. Go to the **Directory Tree**.
2. Select a directory you want to rename.
3. Click .
4. Enter a new name for the directory.
5. Press [Enter].

Configuration - Centralized Management of Device Settings in the IGEL UMS Web App

In the **Configuration** area of the IGEL Universal Management Suite (UMS) Web App, you can create and manage configuration objects, such as profiles and files, to support the centralized management of device settings. In this article we introduce the area and the general use. You can find more detailed or specific information in the following articles:

- How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252)
- How to Check which Profiles Define Parameters in the IGEL UMS Web App (see page 1268)
- Exporting and Importing Profiles in the IGEL UMS Web App (see page 1269)
- How to Use Template Profiles in IGEL UMS Web App (see page 1272)
- How to Use Corporate Identity Customizations in IGEL UMS Web App (see page 1279)
- Upload and Assign Files in the IGEL UMS Web App (see page 1290)

Menu path: **UMS Web App > Configuration**



1	Configuration Objects	The objects are grouped according to their types into the following tabs: •  **Profiles** •  **Priority Profiles** •  **Corporare Identity Customizations** (CICs) •  **Files**

> To use priority profiles, they have to be enabled under **Network > Settings > UMS Features**, see Network Settings in the IGEL UMS Web App (see page 1347). Once enabled, you can create priority profiles in the same way as the standard profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).

Depending on the selected tab, you have different action buttons at the top of the list, but you can always structure the objects into a directory structure. The structure tree shows all created directories and subdirectories with information on the contained objects. The format (x/y) specifies:

x - the number of objects contained directly in the directory and

y - the total number of objects in the directory & all subdirectories of this directory.

Click for more on how to structure your objects in all the tabs...

→ To create a directory, click  .

→ To rename a directory, click  .

→ To delete a directory, click **Delete Directory**  in the management panel.

→ To open the **Recycle Bin**, click  . For more information, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).

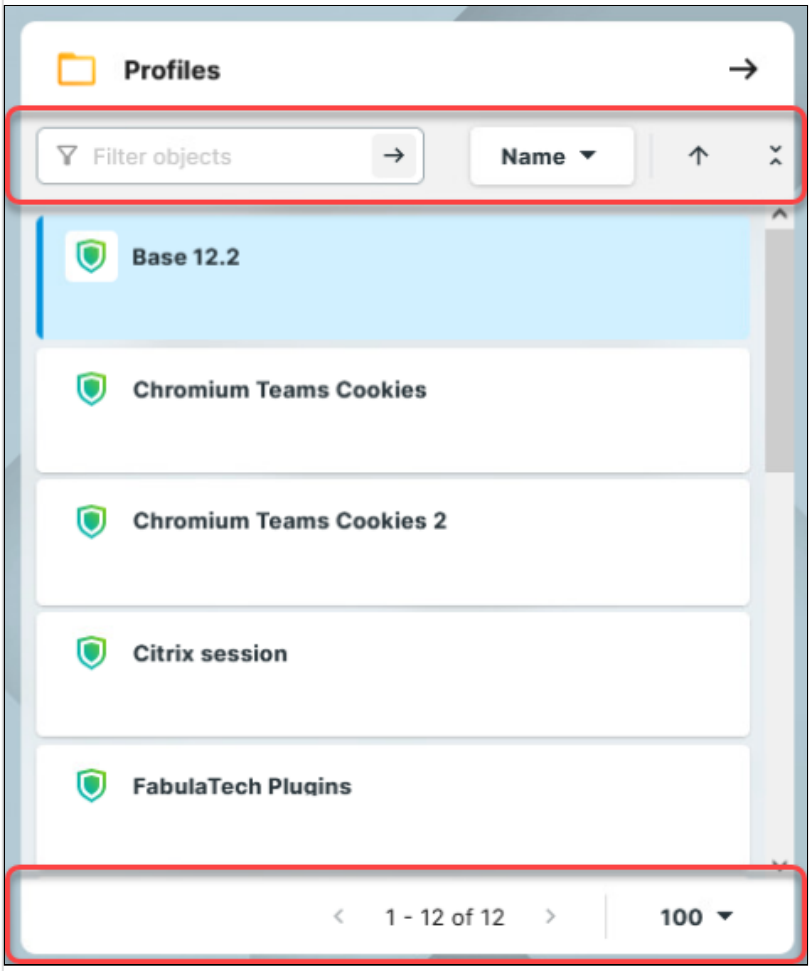
→ To refresh the **Configuration Objects** tree, click  .

→ To expand/minimize the list of subdirectories of a directory, click the arrow icon next to the directory name, or double click the directory element.

→ To move a configuration object to another directory, select the object and move it per drag & drop to the desired directory.

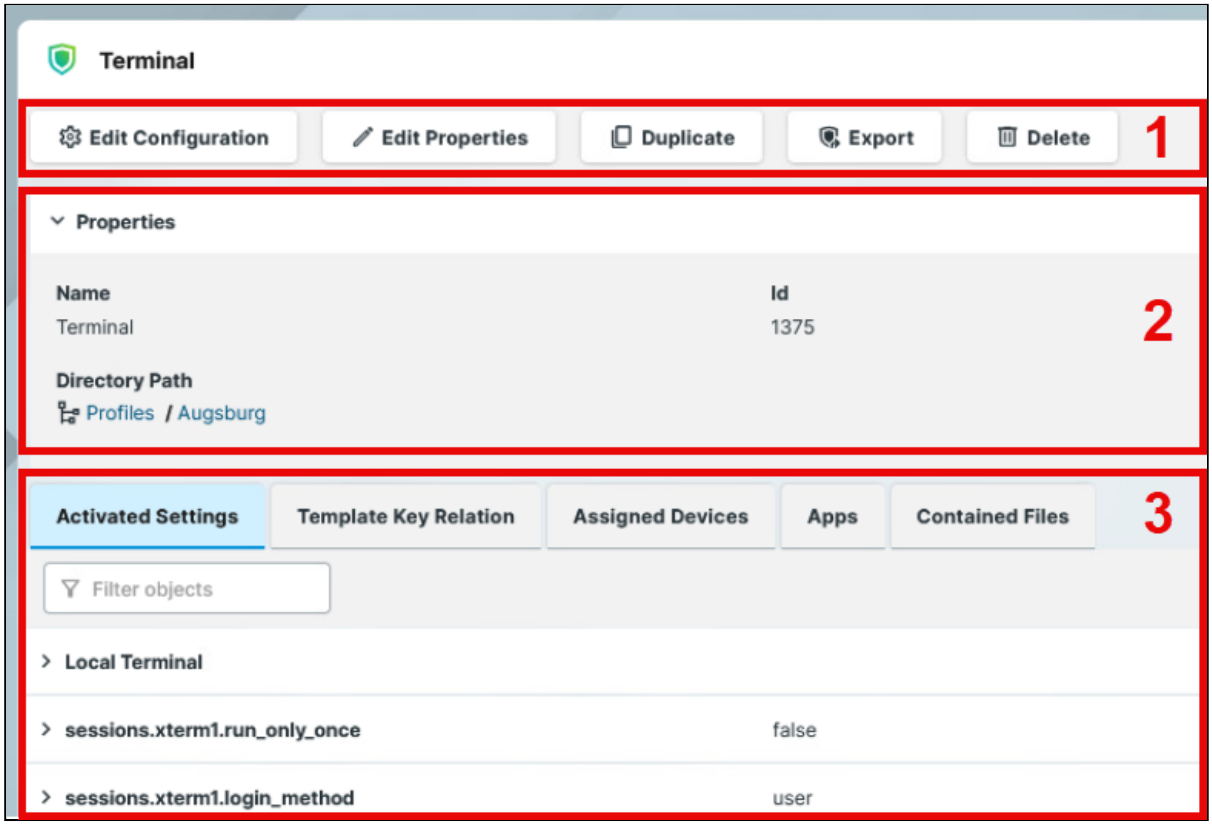
→ To move a directory to another directory, select the directory and move it per drag & drop to the desired directory or use [Ctrl + X], [Ctrl + V].

		It is currently not possible to copy objects in the UMS Web App. For profiles, you can use the **Duplicate** function or, alternatively, export and import function, see Exporting and Importing Profiles in the IGEL UMS Web App (see page 1269). For CICs, you can also use export and import function, see How to Use Corporate Identity Customizations in IGEL UMS Web App (see page 1279).

2	Object List	When you select a directory in the tree, the object list shows all the objects contained in that directory. → Right-click on the object opens a context menu with the actions available for the selected object. These are the same actions that are also available in the management panel. For details, see the sections Profile Management (see page 1239), File Management (see page 1239) and Corporate Identity Customizations (see page 1239).  Click for a list of actions you can use on the listed objects... • Use the free text filter to filter for objects that contain the text in their name • Sort profiles by **Name** and **Version** • Sort files by **Name** and **Size** • Sort CICs by **Name** and **Use Case** • Collapse and expand the object details • Use the paging for the navigation in the object list • Set the number of objects to be displayed on one page

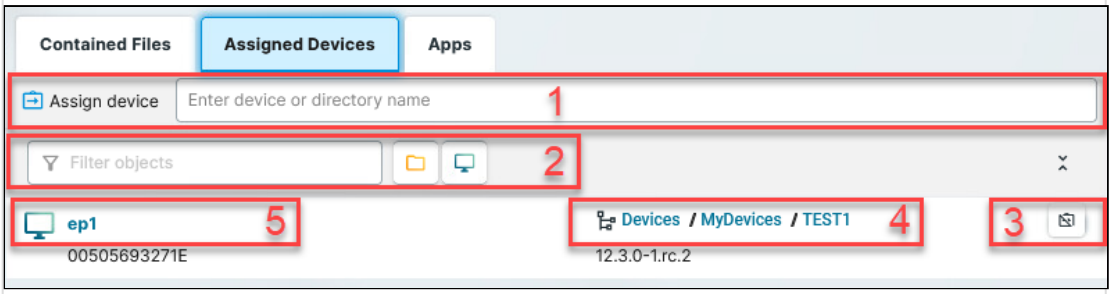
3	Management Panel	The content of the panel changes based on the selected item. 1. When you select a directory in the tree, the panel shows directory information. • You can find here the **Properties** of the selected directory, e.g. the **Name** and **Directory Path**. • You can click the **Delete Directory** button to delete a directory. If recycle bin is enabled, this will send the object to the recycle bin, where you can restore / permanently delete it. For details, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356). 2. When you select an object from the object list, the panel shows the details of the selected object and all the functions for the management of the object. For details, see the sections Profile Management (see page 1244), File Management (see page 1248) and Corporate Identity Customizations (see page 1250).

Profile Management Panel

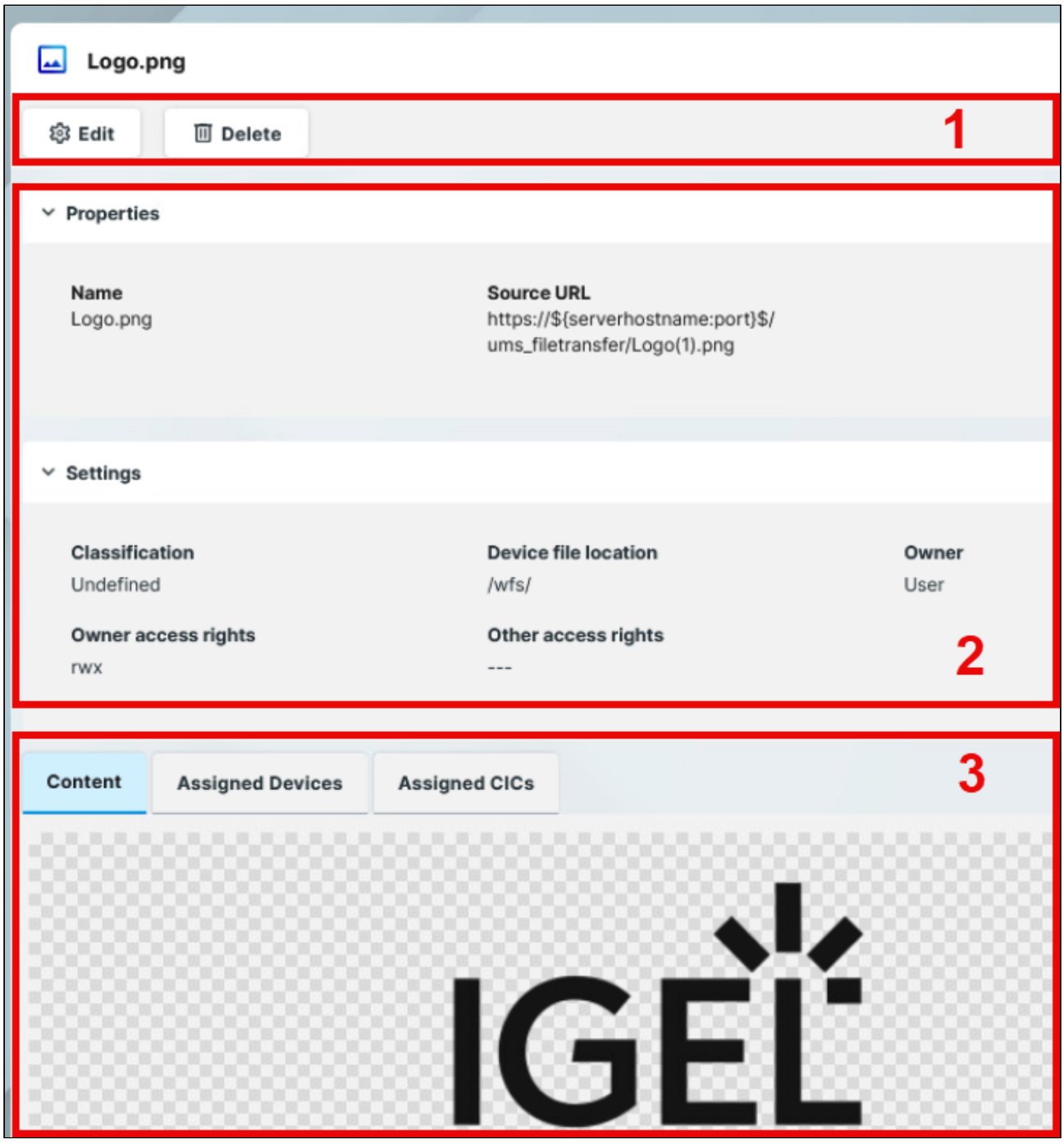


1	Action Buttons	→ To edit the configuration parameters of a profile, double click the profile in the object list, or select the profile and click **Edit Configuration** button or context menu item. → To rename the profile or to edit other properties like **(Do NOT) overwrite sessions** setting, click **Edit Properties**. **Overwrite sessions** option should be activated only in exceptional cases. With this option, you can override free instances (see page 699) of all other profiles. Detailed information on this option can be found under Creating Profiles in the IGEL UMS (see page 701). → To copy a profile, click **Duplicate**. A new profile with the same settings and properties as in the original profile will be created. To use the **Duplicate** function, you need read and write rights for the object and the parent folder. For more information on rights, see Object-Related Access Rights (see page 1016) and How to Create Administrator Accounts in the IGEL UMS. → To export the profile, click **Export**. For more information, see Exporting and Importing Profiles in the IGEL UMS Web App (see page 1269) . → To delete a profile, click **Delete**. If recycle bin is enabled, this will send the profile to the recycle bin, where you can restore / permanently delete. For details, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).
2	Profile information	For profiles, the information panel shows the **Properties** of the selected profile, e.g. its **Name**, **Version** it is based on (for IGEL OS 11 profiles only), etc. **Id** Profile ID. If several profiles are assigned to a device on an equal basis, the newer profile with the higher profile ID has priority. For more information on prioritization of profiles, see Order of Effectiveness of Profiles (see page 729) and Prioritization of Profiles in the IGEL UMS (see page 728). **Directory Path** Full directory path for the selected profile

3	Activated Settings	Shows all configuration settings activated in the selected profile. **Key** Key of the configuration parameter → Click the i-icon to open the tooltip. **Display name** Name of the configuration parameter as displayed in the IGEL Setup and the configuration dialog in the UMS Console. **Value** A value set for the parameter. All password values are anonymized. → If a parameter receives a value from a template key (see Template Profiles in the IGEL UMS (see page 746)), click  to jump to the corresponding template key. ⚠ Settings activated for the newly created profiles as well as setting changes are displayed in the UMS Web App under **Activated Settings** not immediately, but after the next reindexing, which is executed, in this case, with a one-day interval.
	Template Key Relation	Shows template keys used in the profile, see Template Profiles in the IGEL UMS (see page 746) and How to Use Template Keys in Profiles (see page 756). **Template Key** Name of the template key **Parameter** Key of the configuration parameter for which a template key is configured **Template Expression** A template key configured Example of template expressions: `SSH on §{MAC}` – static template key configuring the name for the SSH session, which will be composed of "SSH on" and the MAC address of the endpoint device

Contained Files	Shows all files assigned to the selected profile. For details on the file upload, see Upload and Assign Files in the IGEL UMS Web App (see page 1290).  1: Here you can quickly add a file to the profile. → Enter the name of the file and select in the list. 2: Filters the files added to the profile according to the entered string. 3: Detaches the selected file from the profile.
Assigned Devices	Shows all devices the selected profile is assigned to.  1: Here you can quickly assign the profile to a device or a device directory. → Enter the name of the device or device directory and click the name in the list. 2: Filters the devices / device directories assigned to the selected profile. The filter criteria are linked with the operator *AND*. → Click  to remove all filters. 3: Detaches the selected device / device directory from the profile. 4: Jumps to the corresponding device directory and shows all **Assigned Objects** for it. 5: Jumps to the corresponding device and shows all **Assigned Objects** for it.
Apps	Shows which apps / app versions are configured by the selected OS 12 profile.

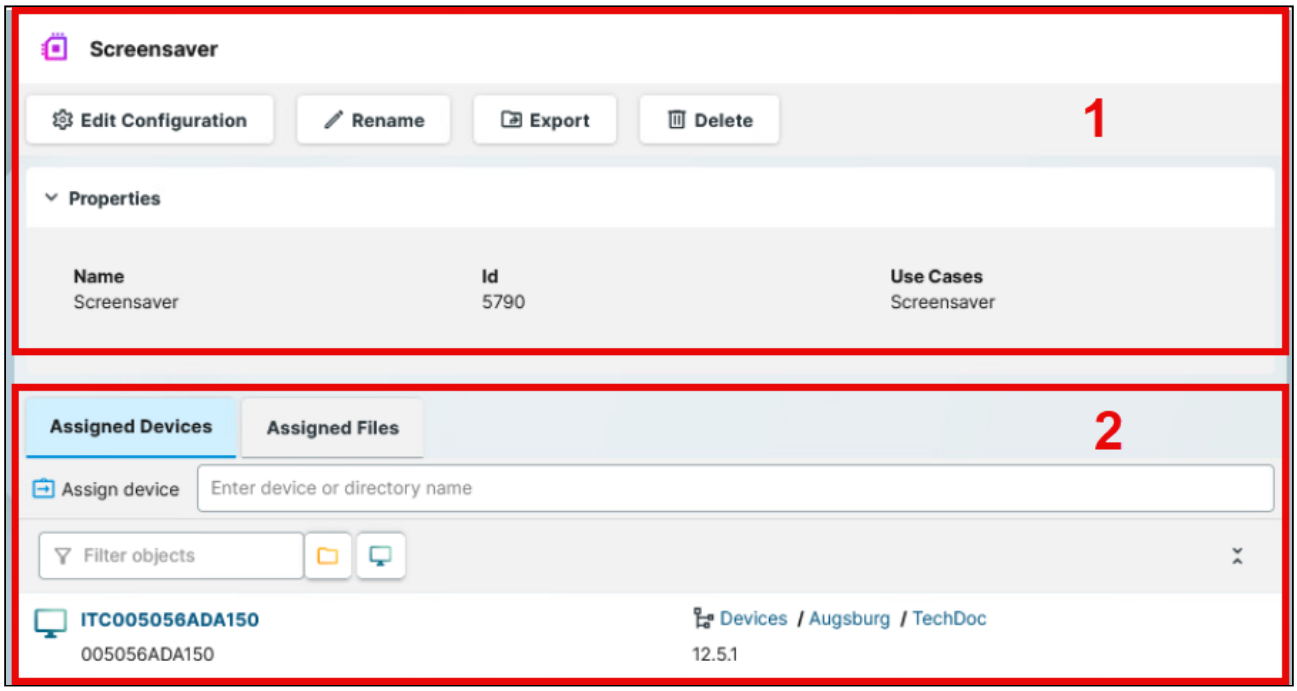
File Management Panel



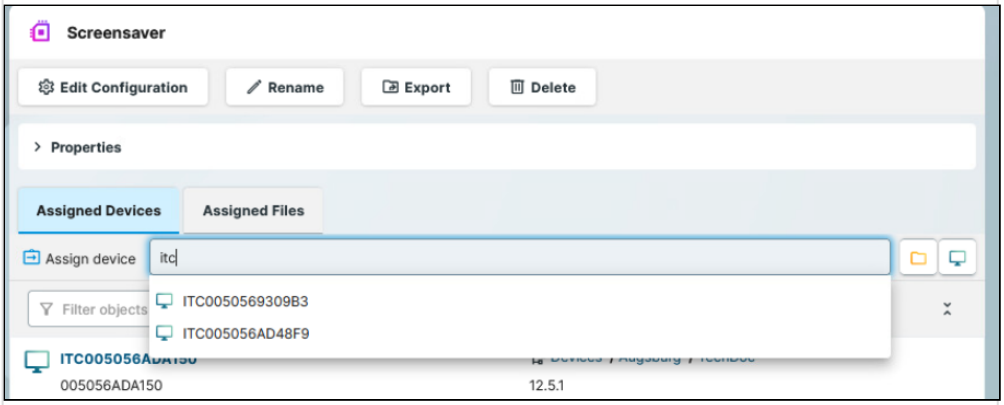
1	Action Buttons	→ To edit the properties and settings of the file, click **Edit**. → To delete a file, click **Delete**. If recycle bin is enabled, this will send the file to the recycle bin, where you can restore / permanently delete. For details, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).
2	File Information	For files, the information panel shows the **Properties** and **Settings** of the selected file, e.g. its **Name** or **Source URL**. The values are defined during the upload of the file, and can be edited later. For details on the settings, see Upload and Assign Files in the IGEL UMS Web App (see page 1290). When you upload a file with a filename that already exists, the new filename gets modified according to the format {filename}({n}), where n specifies how many files exist with the same name. For example, Logo(1).png, Logo(2).png. In the UMS Web App, this is only visible in the **Source URL** but not in the **Name** of the file.
3	Content	Displays a preview of the files uploaded through the UMS Web App. For example, an image preview or certificate content.
	Assigned Devices	Shows all the devices the selected file is assigned to. → To quickly assign the file to a device or a device directory, enter the name of the device or device directory and click the name in the list. For details, see Upload and Assign Files in the IGEL UMS Web App (see page 1290). → You can filter the devices / device directories assigned. The filter criteria are linked with the operator *AND*. Click  to remove all filters. → Detach the selected device / device directory by clicking  . → Click the name of the device in the list to jump to the corresponding device and see all **Assigned Objects** for it. → Click the name of the directory to jump to the corresponding device directory and see all **Assigned Objects** for it.
	Assigned CICs	Shows all corporare identity customizations the selected file is assigned to. → You can filter the list of the assigned CICs.

Corporate Identity Customizations

Using Corporate Identity Customizations (CICs) in the UMS Web App, you can customize the user interface of your IGEL OS devices to suit your corporate design. For details, see How to Use Corporate Identity Customizations in IGEL UMS Web App (see page 1279) .



1	CIC Information and Action Buttons	The information panel shows the **Properties** of the selected CIC, e.g. its **Name** and **Use case** and all available action buttons. → Click **Edit Configuration** to configure the CIC. → Click **Rename** to rename the CIC. → Click **Export** to export the CIC. For more information, see How to Use Corporate Identity Customizations in IGEL UMS Web App (see page 1279). → Click **Delete** to remove the CIC. If recycle bin is enabled, this will send the CIC to the recycle bin, where you can restore / permanently delete it. For details, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).

2	Assigned Devices	Shows all the devices the selected CIC is assigned to. → To quickly assign the CIC to a device, enter the name of the device or device directory and click the name in the list. You can also assign CICs just like any other objects in the **Devices** area. For more information on assigning objects, see How to Assign Objects in the IGEL UMS Web App (see page 1187) .  → You can filter the list of assigned devices / device directories. The filter criteria are linked with the operator *AND*. Click  to remove all filters. → Detach the selected device / device directory by clicking  . → Click the name of the device in the list to jump to the corresponding device and see all **Assigned Objects** for it. → Click the name of the directory to jump to the corresponding device directory and see all **Assigned Objects** for it.
	Assigned Files	Shows a list of files used in the selected CIC with size information. → You can filter the list of assigned files.

How to Create and Assign Profiles in the IGEL UMS Web App

In the IGEL UMS Web App, you can create profiles for configuring settings for your devices. For general information on profiles, see Profiles in the IGEL UMS (see page 695).

Menu path: **UMS Web App > Configuration**

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).

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 729).

Note 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.

Creating Profiles for IGEL OS 12 Devices

Before creating profiles for IGEL OS 12 devices, you have to import the required apps from the IGEL App Portal; see How to Import IGEL OS Apps from the IGEL App Portal (see page 1303).

Alternatively, at least one IGEL OS 12 device with the required apps has to be already registered with the UMS Server. IGEL OS Base System as well as all locally installed apps are then automatically recognized by the UMS. See e.g. (en) Installing IGEL OS Apps Locally on the Device .

As soon as there are apps listed under **UMS Web App > Apps**, you can create a profile to configure settings for your devices.

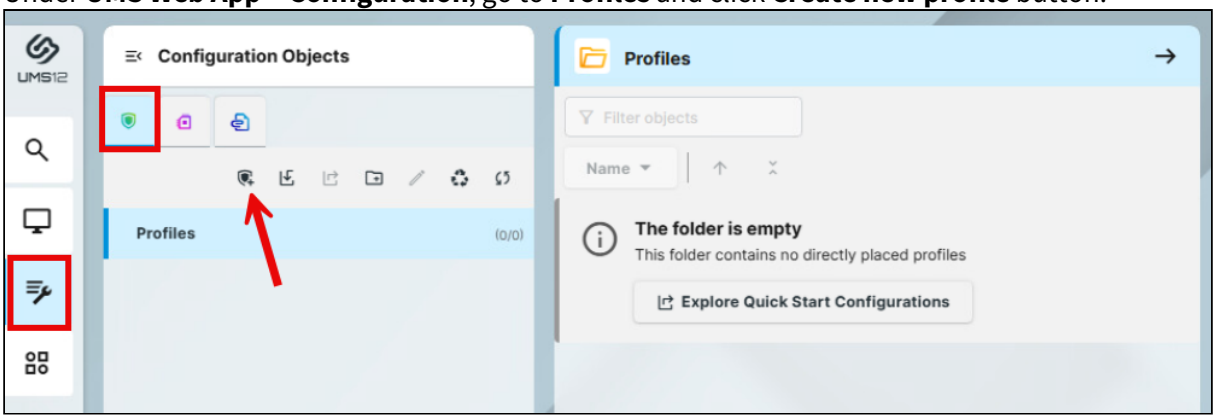
There are two methods to create a profile:

- Via **Configuration > Profiles > Create new profile** (used to configure one or several apps. A profile configures ALL versions of an app, unless the version is specified.)
- Via **Apps > Create new profile** (used to quickly configure a profile for the selected app.)

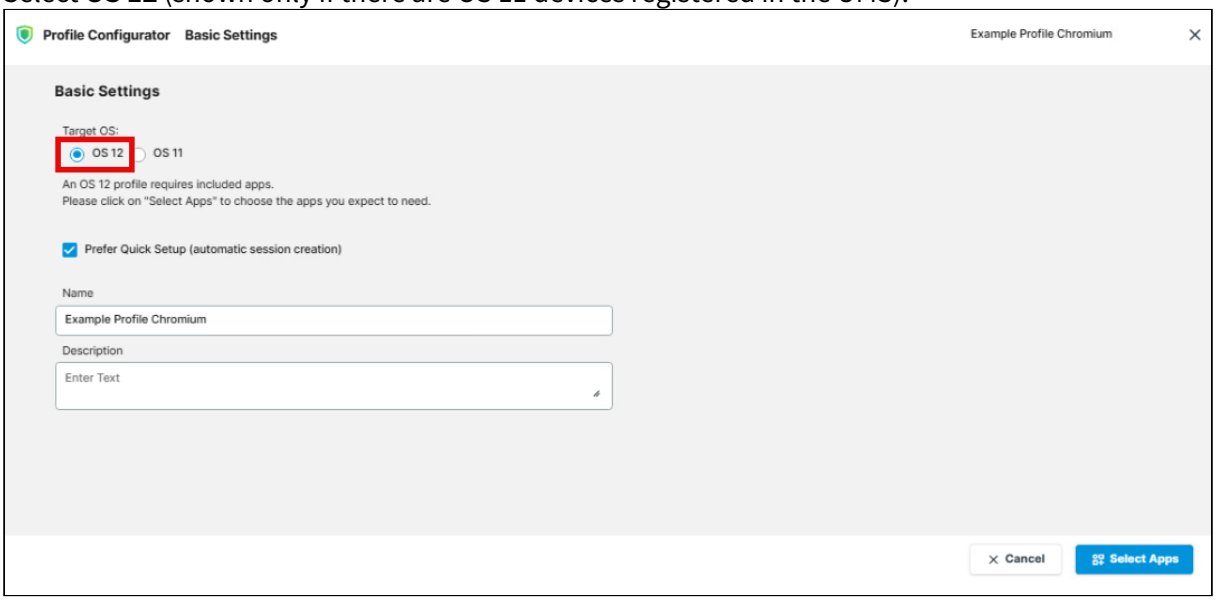
> For apps which have no configurable parameters (e.g. codecs), it is not possible to create a profile.

Option 1: Create an OS 12 Profile via Configuration

1. Under **UMS Web App > Configuration**, go to **Profiles** and click **Create new profile** button.



2. Select **OS 12** (shown only if there are OS 11 devices registered in the UMS).

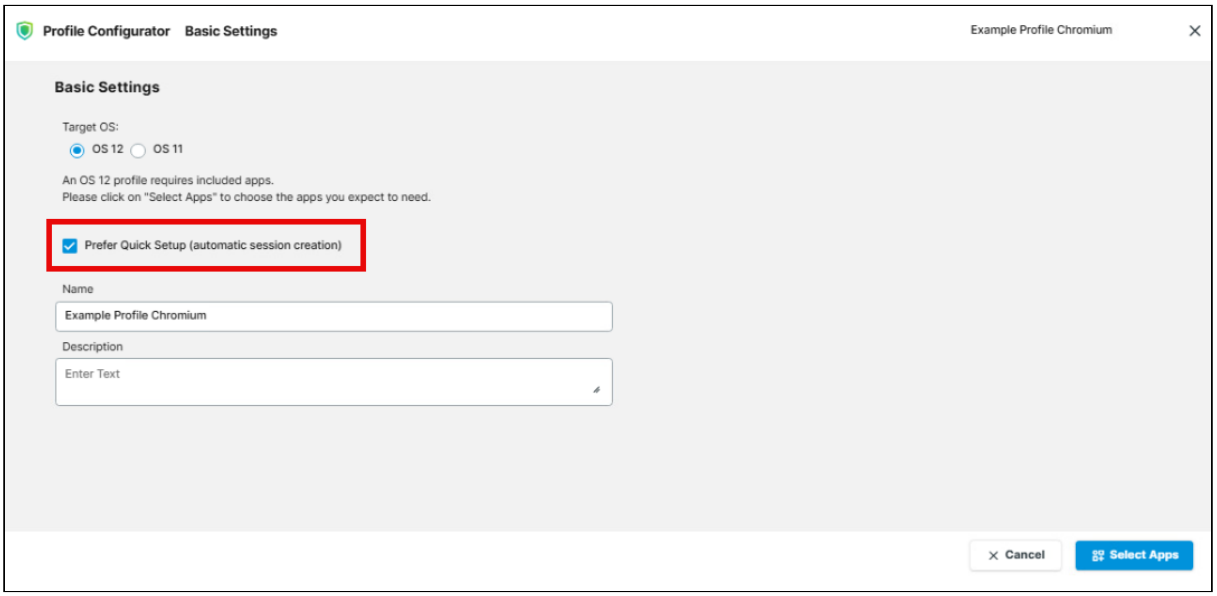


3. Optional (for a quicker profile creation): If you do not want to see all app settings available for configuration, but only those relevant for the quick start with the app, leave

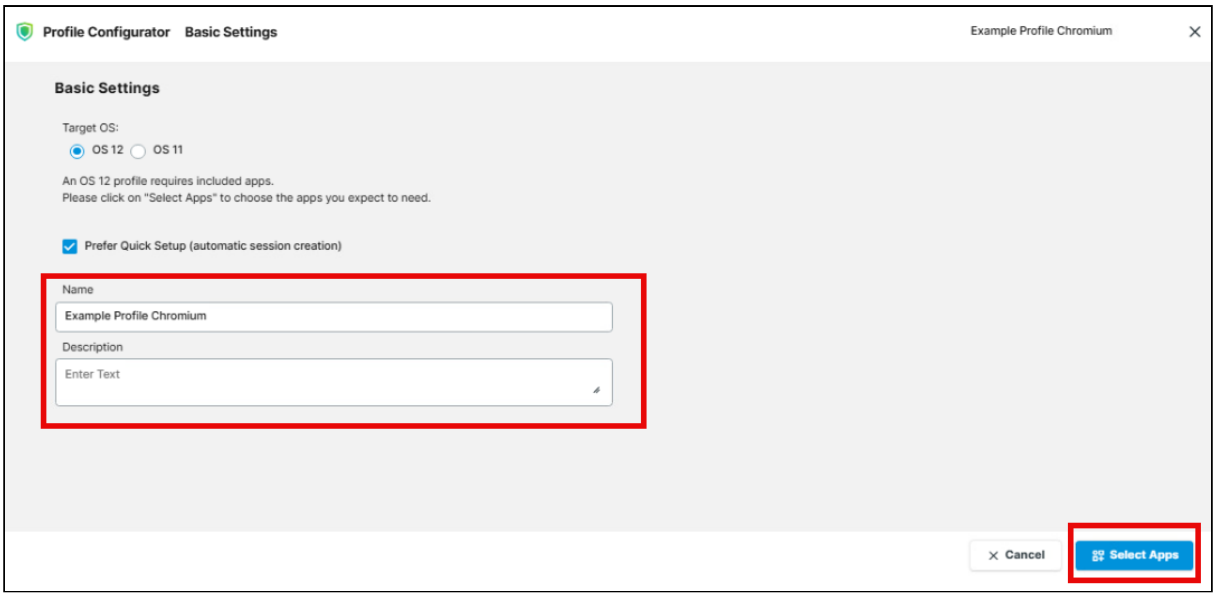
Prefer Quick Setup (automatic session creation) enabled.
Quick Setup mode for the configuration dialog will be opened if available.

Note the following:

- Quick Setup mode is currently available for specific apps only.
- Quick Setup mode is available only when creating a new profile, not while editing the existing profile.
- Quick Setup mode is available for OS 12 profiles only.
- Quick Setup mode is displayed only if one app supporting it is selected in the **App Selector**. In case multiple apps or an app not supporting the Quick Setup mode are selected, Advanced Setup with all available app settings will be displayed even if **Prefer Quick Setup (automatic session creation)** is enabled.

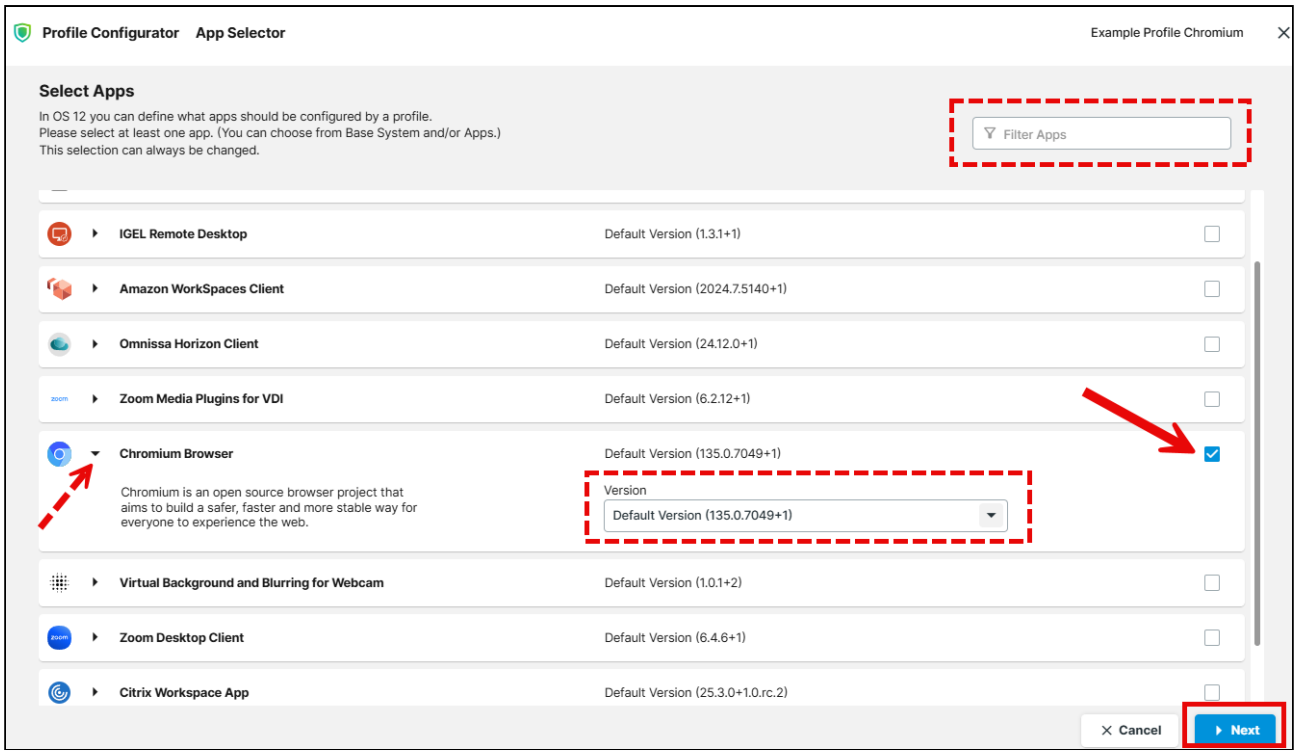


4. Enter the **name** of the profile and, if desired, the **description** for the profile.



5. Click **Select Apps**.
6. In the **App Selector**, select the app(s) you want to configure. It is ALWAYS necessary to select at least one app when creating a profile for IGEL OS 12 devices.
   To quickly find the required app, start typing its name under **Filter Apps**.

If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, SSO, accesories, etc.) before any of your IGEL OS 12 devices is registered with the UMS, import the IGEL OS Base System app. The latest app version is recommended. Alone for the purpose of profile creation, the subsequent assignment of the IGEL OS Base System app to a device / device directory is NOT necessary.



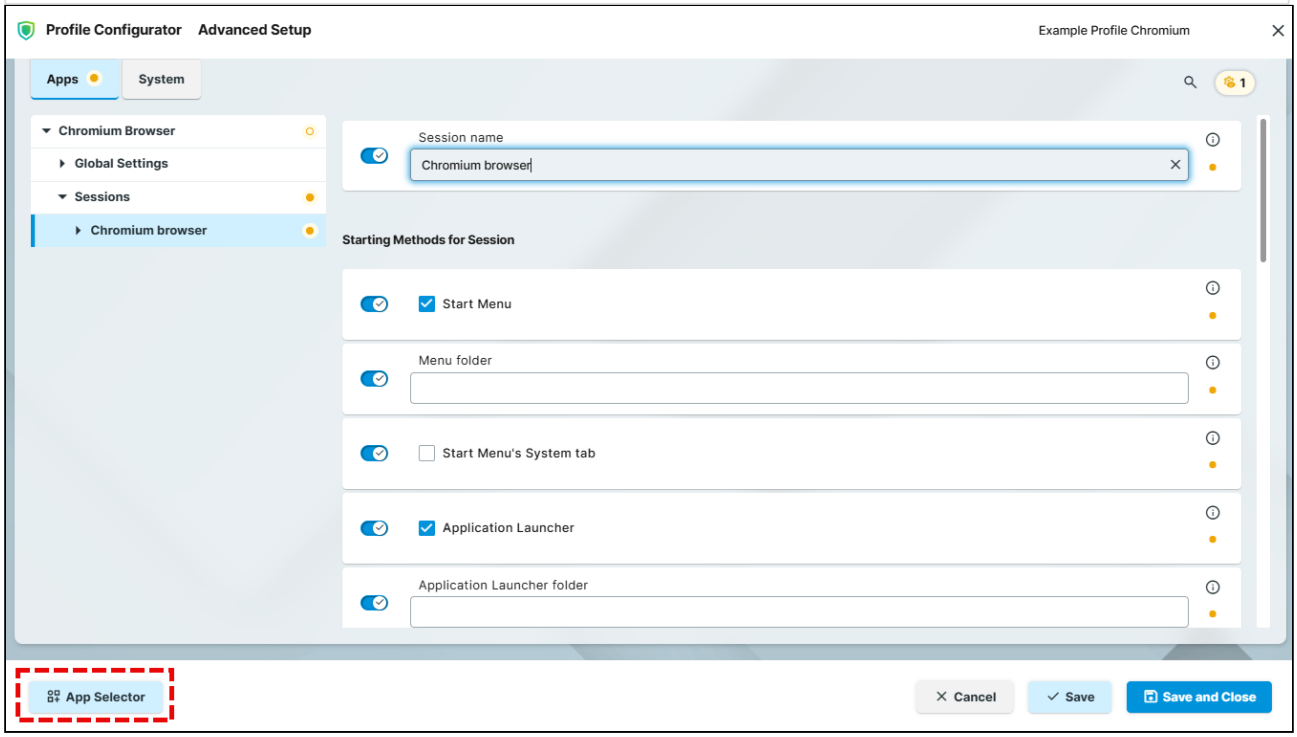
7. If you want to configure a profile for a specific app version, click ▸ and select the required app version under **Version**.

> An app version selected here will be assigned to a device, see Assigning OS 12 Profiles to Devices, or Implicit App Assignment via Profiles (see page 1261).
> The best practice is to use the **Default Version**, see How to Set a Default Version of an App in the IGEL UMS Web App (see page 1311) .

8. Click **Next**.
9. Configure the desired settings.
   The configuration dialog shows only those settings that can be configured for the selected app(s).
   If you want to change the scope of the profile (i.e. redefine which apps should be configured by the profile), click **App Selector**.

	The parameter is active and the set value will be configured by the profile.
	The parameter is inactive and will not be configured by the profile. **IMPORTANT**: When you deactivate the parameter, the value will be automatically set back to the default value.

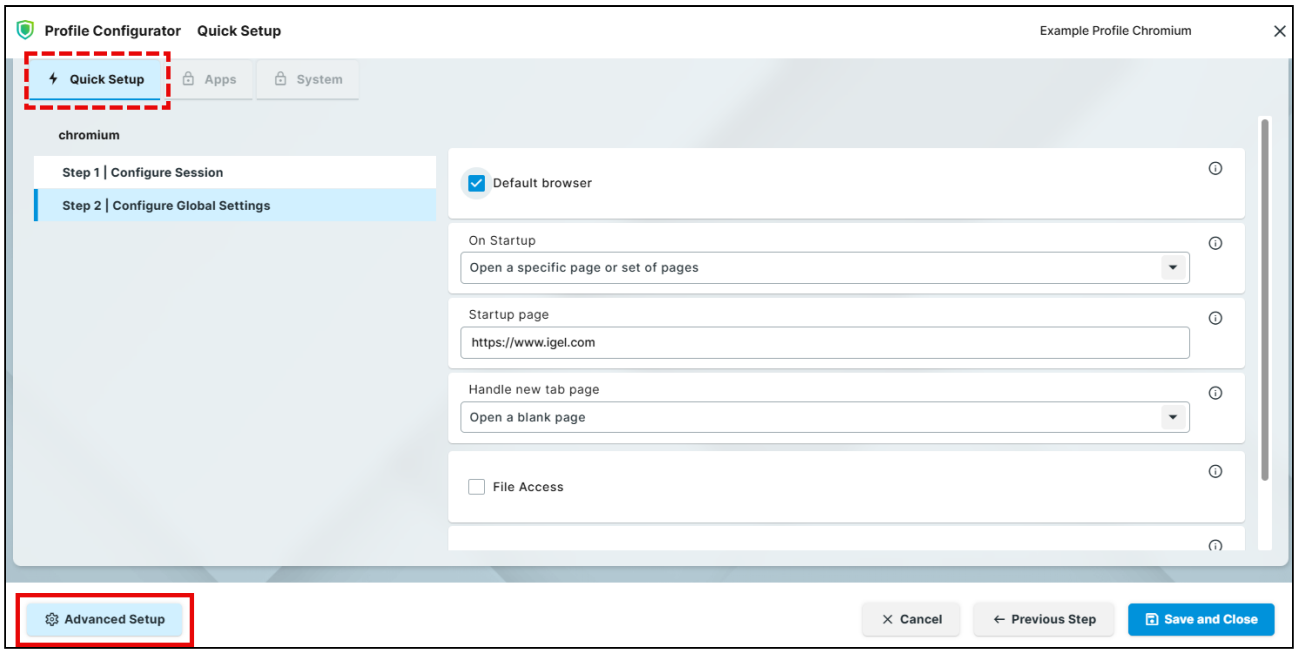
For information on the colored icons for tracking the changes, see Configuration of IGEL OS 12 Device Settings[206].



If the Quick Setup mode is displayed, click **Advanced Setup** to show all settings available for configuration or to open **App Selector** for changing the scope of the profile.
Note the following:

- If you navigate from Quick Setup to Advanced Setup, all changes are saved and, if relevant for the selected app, one app session is automatically created.
- If you click **Cancel** while in Quick Setup mode, the profile is permanently deleted straight away.

206. https://kb.igel.com/en/igel-os-base-system/12.6.1/configuration-of-igel-os-12-device-settings

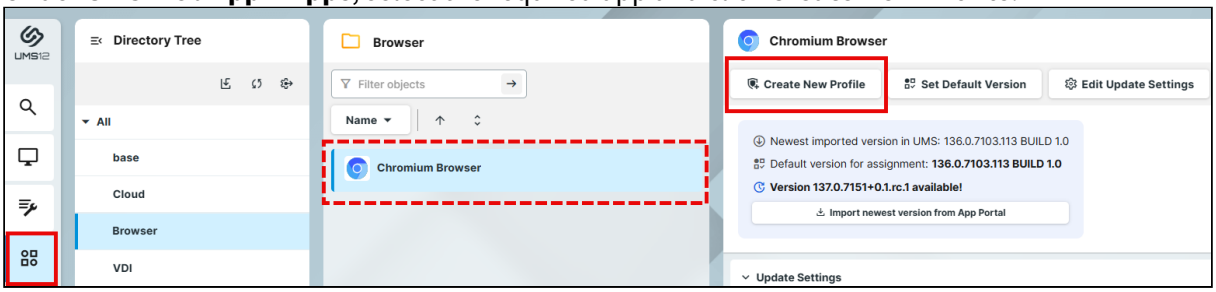


10. Save the changes.
11. Assign the profile to the required device / device directory. See Assigning OS 12 Profiles to Devices, or Implicit App Assignment via Profiles (see page 1261).

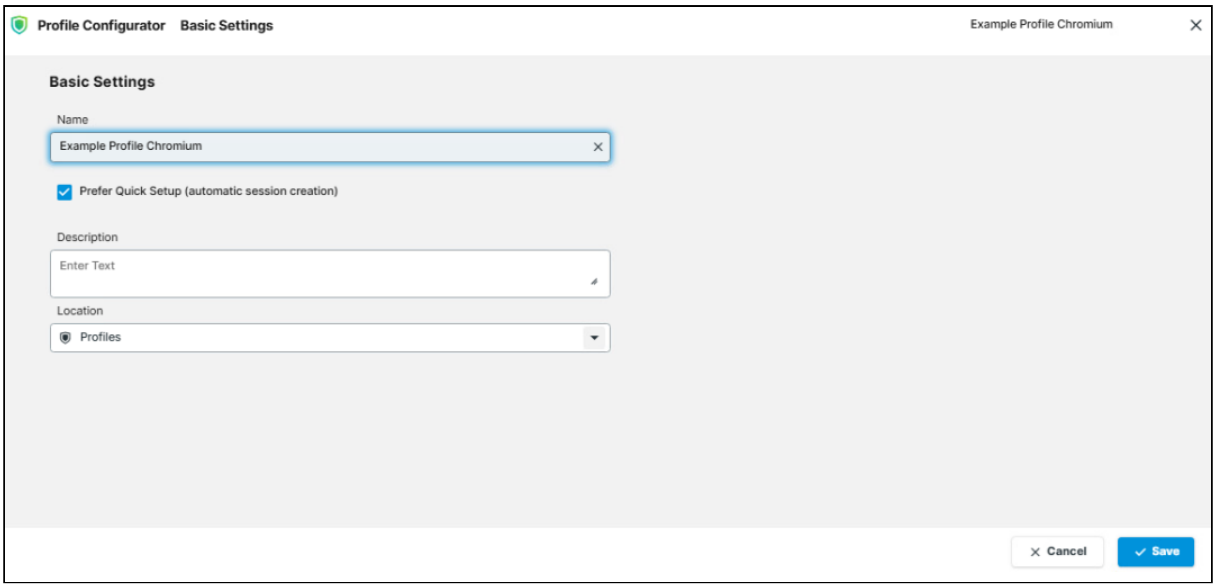
Option 2: Create an OS 12 Profile via Apps

To quickly create a profile for an imported app, proceed as follows:

1. Under **UMS Web App > Apps**, select the required app and click **Create New Profile**.



2. Enter the **name** of the profile and specify the desired directory for storing the profile under **Location**. If desired, add the **description** for the profile.

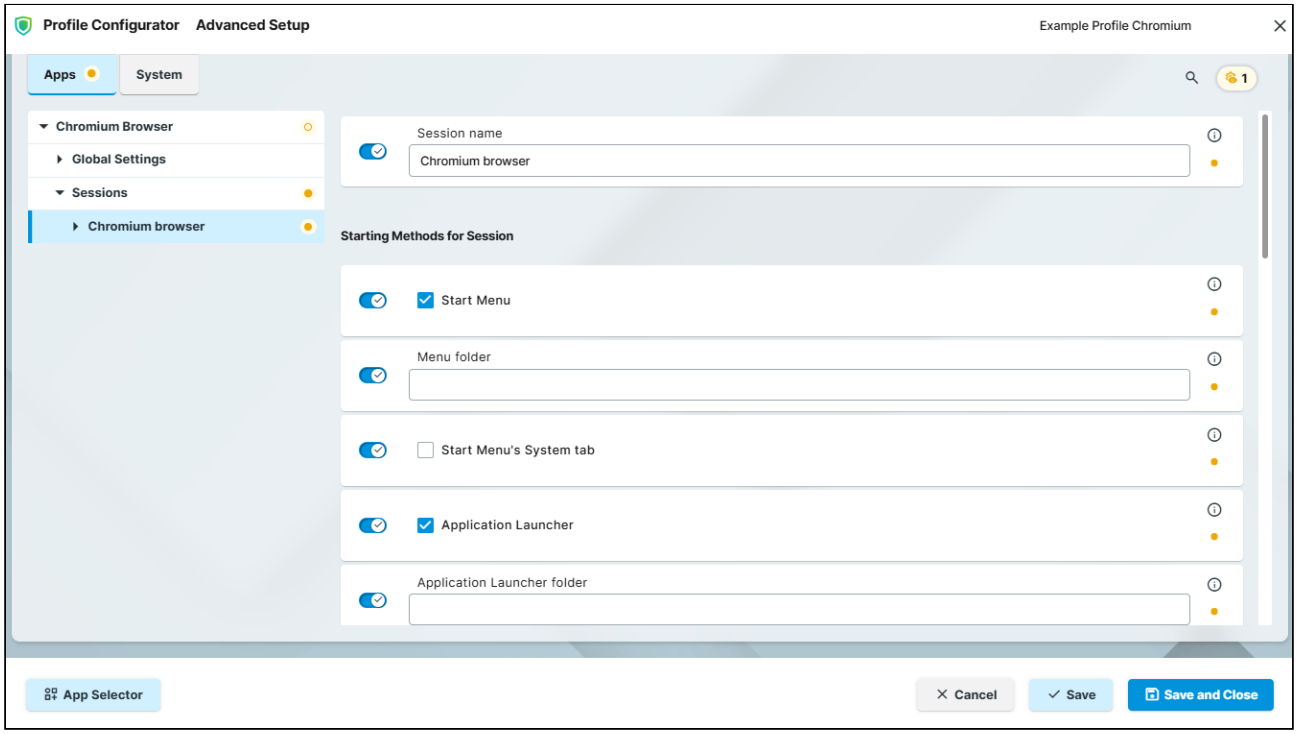


3. Optional (for a quicker profile creation): If you do not want to see all app settings available for configuration, but only those relevant for the quick start with the app, leave **Prefer Quick Setup (automatic session creation)** enabled.

   Quick Setup mode for the configuration dialog will be opened if available.
   Note the following:
   - Quick Setup mode is currently available for specific apps only.
   - Quick Setup mode is available only when creating a new profile, not while editing the existing profile.
   - Quick Setup mode is available for OS 12 profiles only.
   - Quick Setup mode is displayed only if one app supporting it is selected in the **App Selector**. In case multiple apps or an app not supporting the Quick Setup mode are selected, Advanced Setup with all available app settings will be displayed even if **Prefer Quick Setup (automatic session creation)** is enabled.
4. Click **Save**.
   The profile will be listed under **Configuration > Profiles**.
5. Configure the desired settings.
   The configuration dialog shows only those settings that can be configured for the selected app(s). If you want to change the scope of the profile (i.e. redefine which apps should be configured by the profile), click **App Selector**.

	The parameter is active and the set value will be configured by the profile.
	The parameter is inactive and will not be configured by the profile. **IMPORTANT**: When you deactivate the parameter, the value will be automatically set back to the default value.

For information on the colored icons for tracking the changes, see Configuration of IGEL OS 12 Device Settings[207].

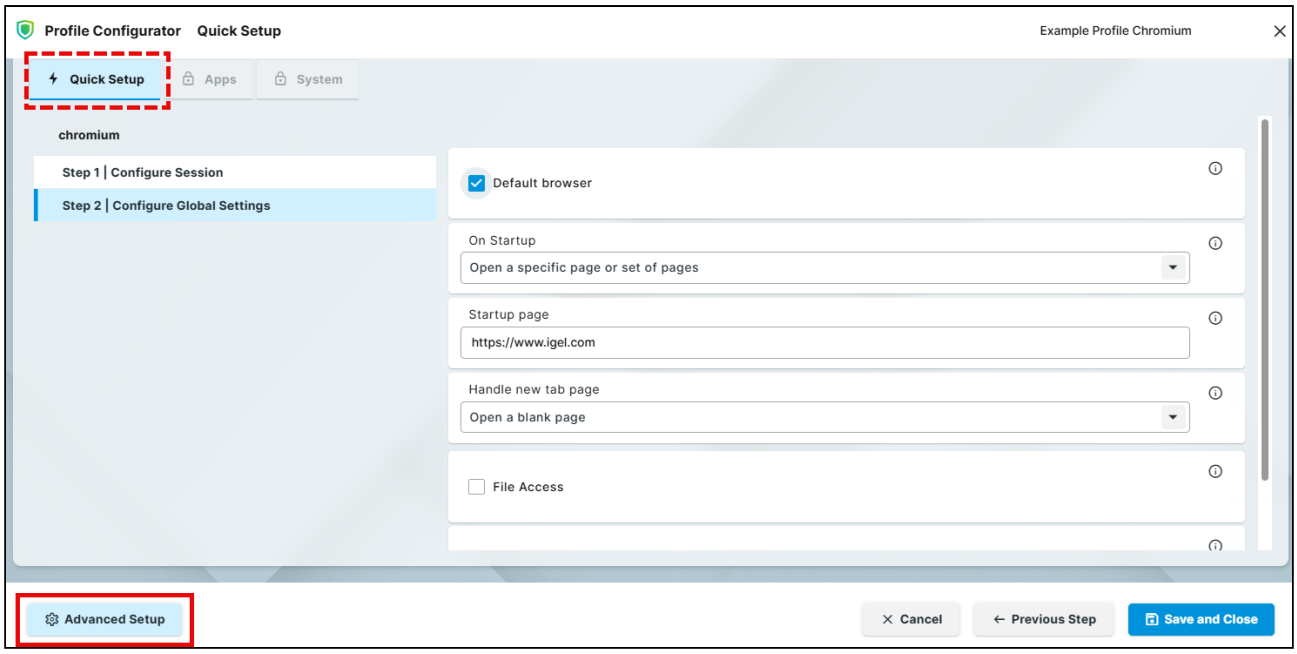


If the Quick Setup mode is displayed, click **Advanced Setup** to show all settings available for configuration or to open **App Selector** for changing the scope of the profile.

Note the following:

- If you navigate from Quick Setup to Advanced Setup, all changes are saved and, if relevant for the selected app, one app session is automatically created.
- If you click **Cancel** while in Quick Setup mode, the profile is permanently deleted straight away.

207. https://kb.igel.com/en/igel-os-base-system/12.6.1/configuration-of-igel-os-12-device-settings

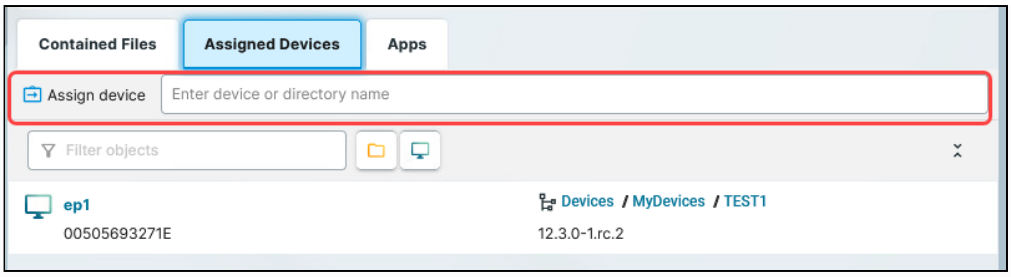


6. Save the changes.
7. Assign the profile to the required device / device directory. See Assigning OS 12 Profiles to Devices, or Implicit App Assignment via Profiles (see page 1261).

Assigning OS 12 Profiles to Devices, or Implicit App Assignment via Profiles

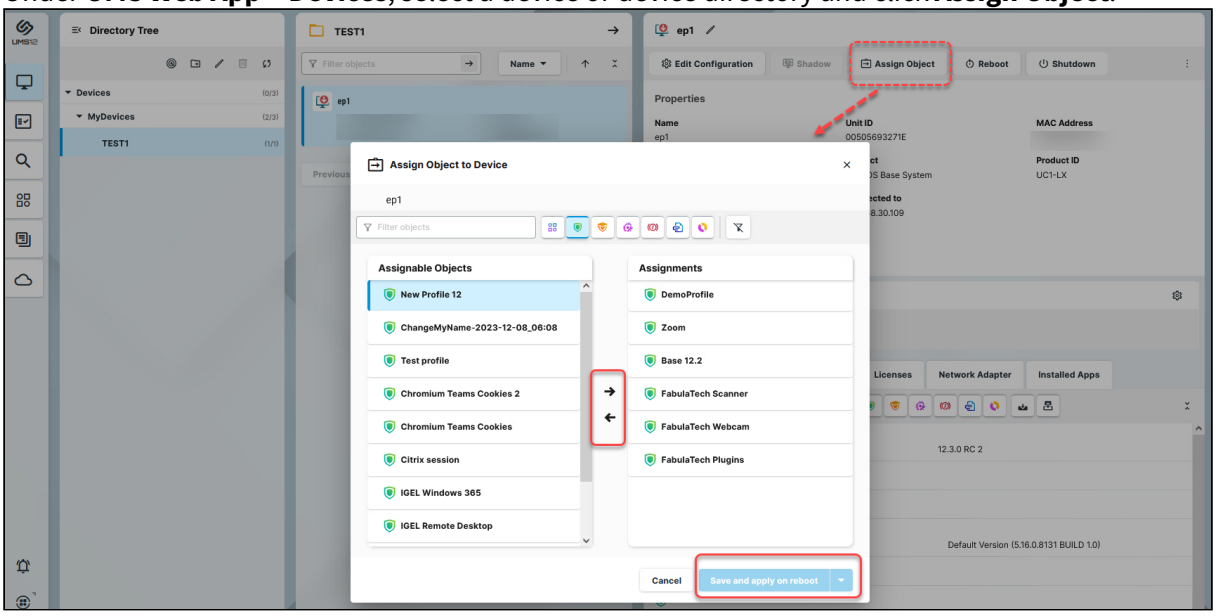
Implicit App Assignment via Profiles
An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app
The app version that will be installed on the device via the implicit assignment if several profiles configure this app (but in different versions) is defined by the priority rules for profiles, see Prioritization of Profiles in the IGEL UMS (see page 728) and Summary - Prioritization of IGEL UMS Profiles (see page 741). Note that the explicitly assigned app, i.e. app / app version selected as an object in the **Assign object** dialog, ALWAYS overwrites the implicitly assigned app. See How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).

To quickly assign a profile to a device / device directory, you can use the **Assign device** function under **Configuration > [name of the profile] > Assigned Devices**. To use this option, you should already know the name of the device / device directory or its part.



To assign profiles to a device / device directory, proceed as follows:

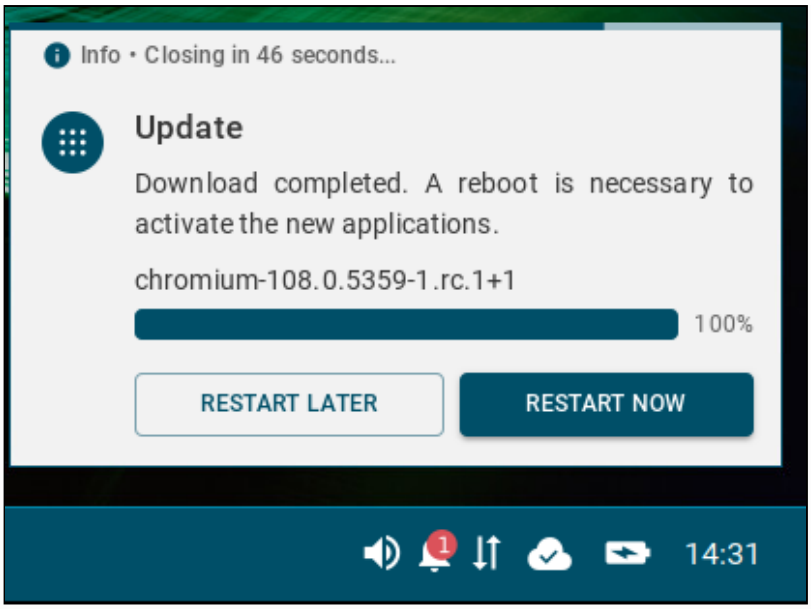
1. Under **UMS Web App > Devices**, select a device or device directory and click **Assign Object**.



2. Select the profile you want to assign to the device / device directory and use the arrow button or drag & drop.

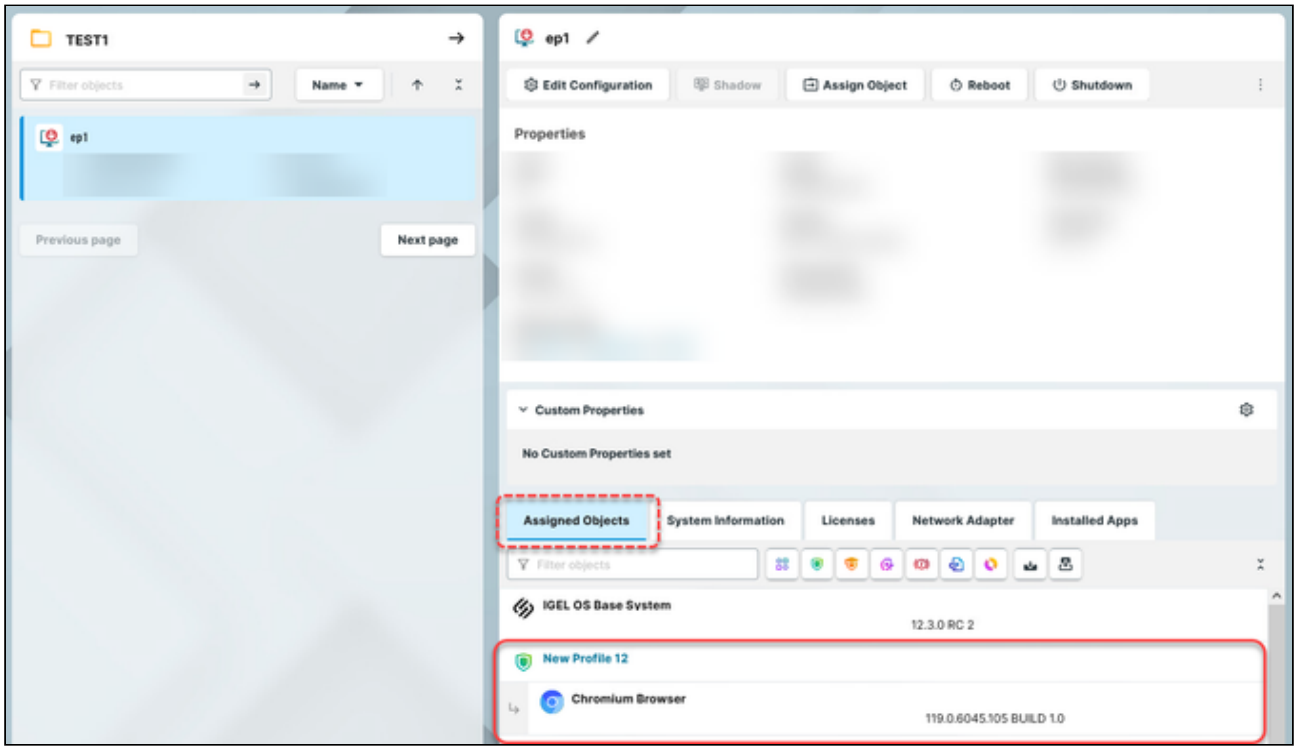
3. Decide when the changes should become effective, and save by selecting **Save and apply on reboot** or **Save and apply now**.
   An app assigned via the profile will be downloaded by the device.

By default, apps / app versions are automatically activated at the next reboot. The user will receive a corresponding notification.
Example:



If you have configured the background app update, an **Update** command must be sent, instead. For details, see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334).

The assigned profile and the app assigned to the device via this profile are displayed under **Devices > Assigned Objects**.



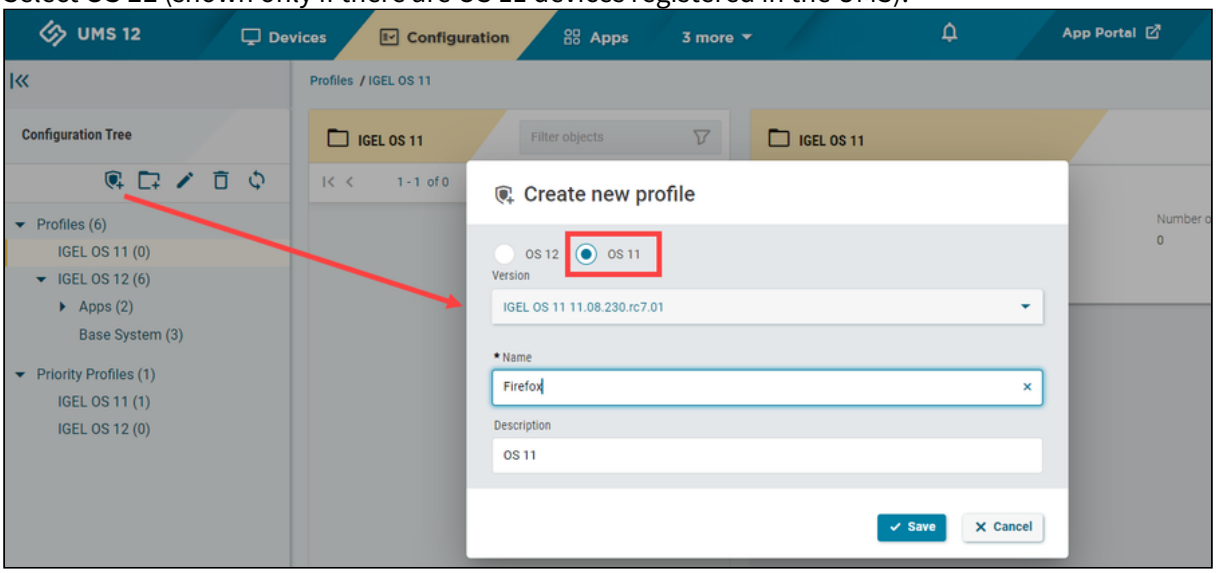
To check the installed apps on a device, go to **Devices > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App (see page 1317).

Creating Profiles for IGEL OS 11 Devices

For how to create IGEL OS 11 profiles in the UMS Console, see Creating Profiles in the IGEL UMS (see page 701).

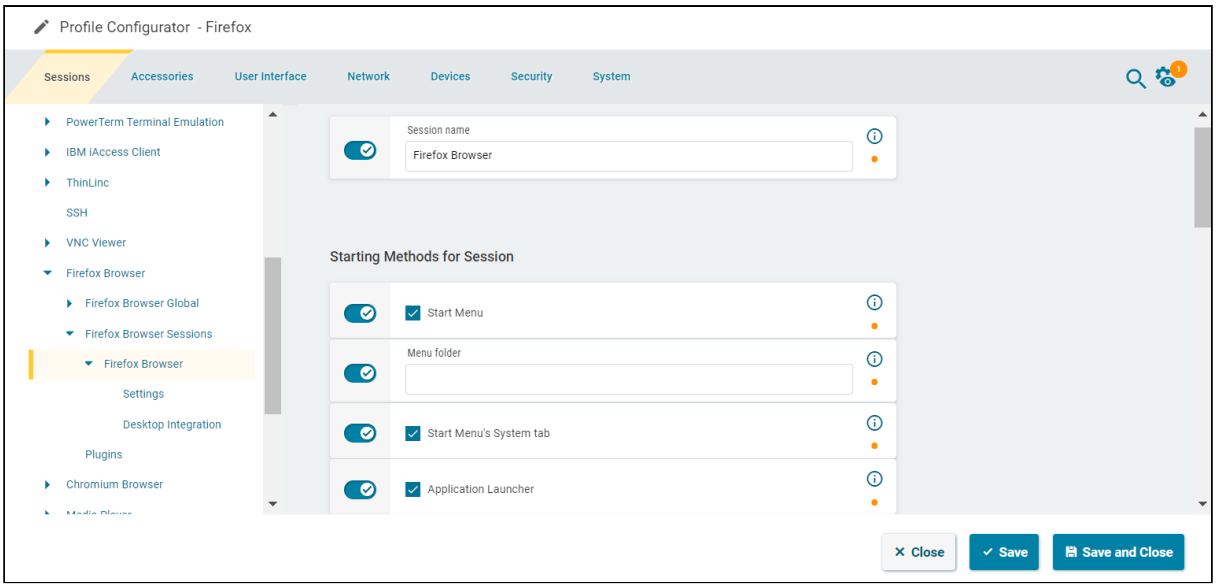
To create a profile for IGEL OS 11 devices via the UMS Web App, proceed as follows:

1. In the **UMS Web App > Configuration**, click **Create new profile** button.
2. Select **OS 11** (shown only if there are OS 11 devices registered in the UMS).



3. Select the firmware **version** the profile is based on.
4. Enter the **name** of the profile.
5. If desired, add the **description** for the profile.
6. Click **Save**.
   The profile will be saved and listed under **Configuration > Profiles**, even if you will not configure any settings in the next step.
7. Configure the desired settings.

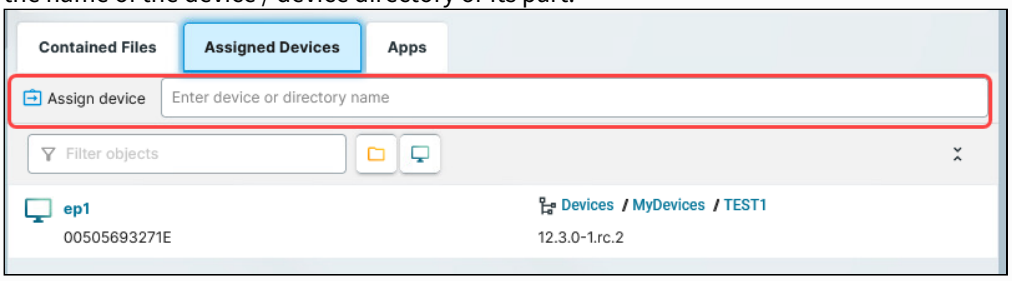
	The parameter is inactive and will not be configured by the profile. **IMPORTANT**: When you deactivate the parameter, the value will be automatically set back to the default value.
	The parameter is active and the set value will be configured by the profile.



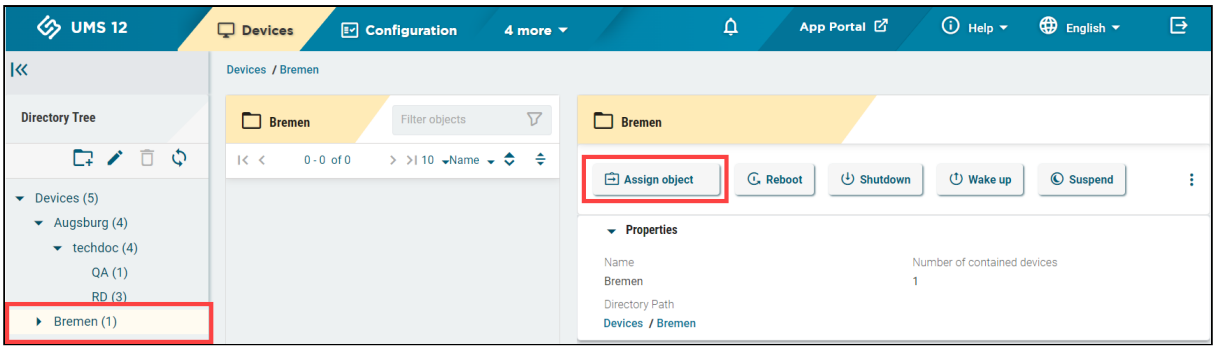
8. Save the changes.
9. Assign the profile to a device / device directory; see the instructions below.

Assigning OS 11 Profiles to Devices

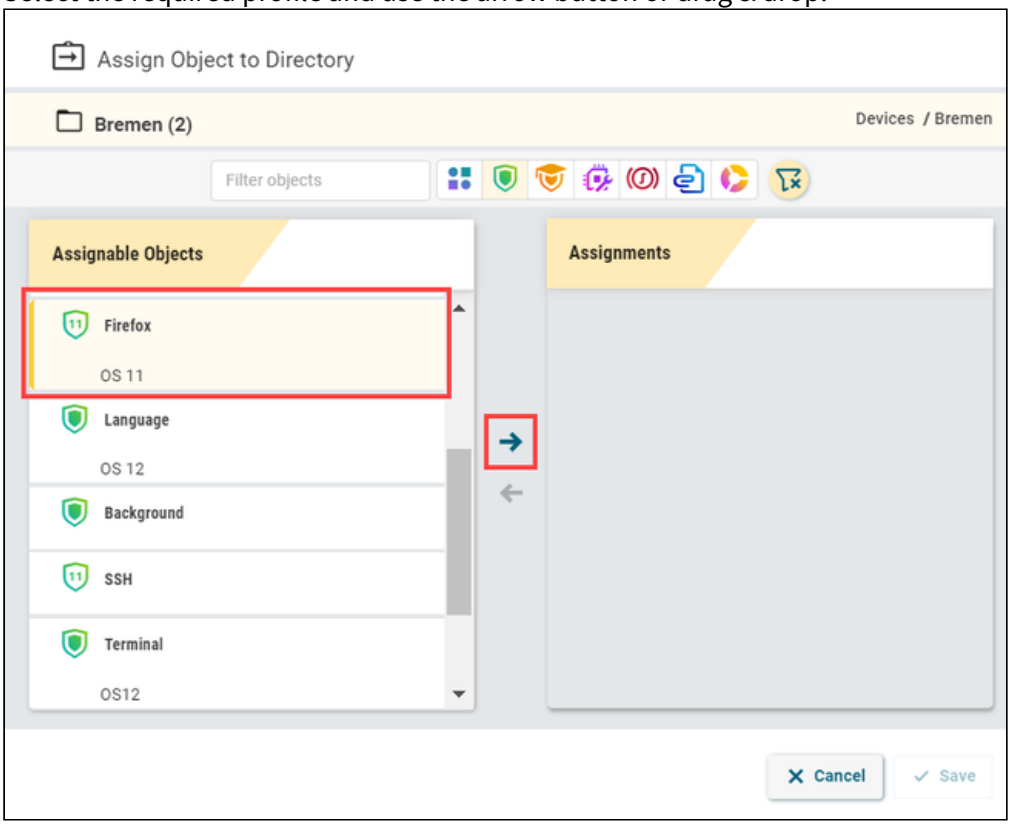
To quickly assign a profile to a device / device directory, you can use the **Assign device** function under **Configuration > [name of the profile] > Assigned Devices**. To use this option, you should already know the name of the device / device directory or its part.



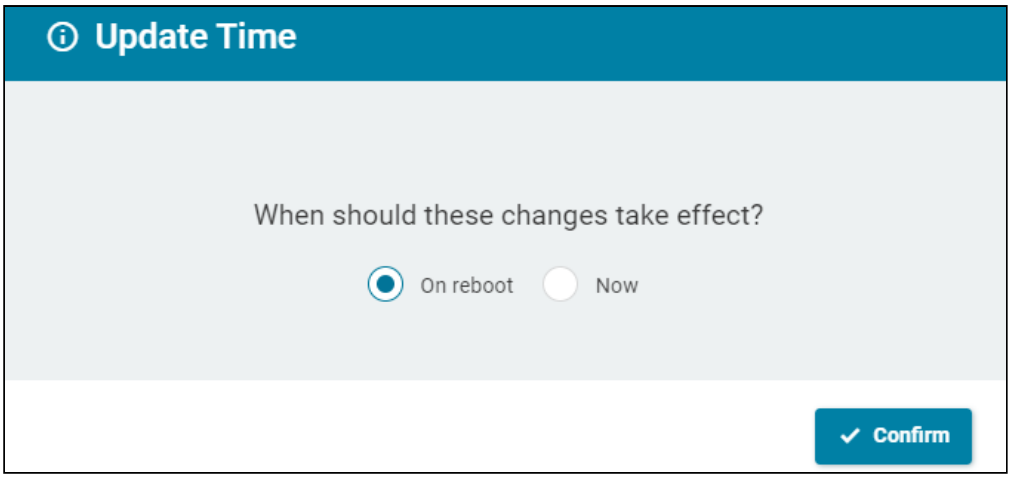
1. To assign a profile, go to **Devices > [name of the device / device directory] > Assign object**.



2. Select the required profile and use the arrow button or drag & drop.



3. Save the changes.
4. Decide when the changes should become effective.


Update Time
When should these changes take effect?
On reboot
Now
Confirm

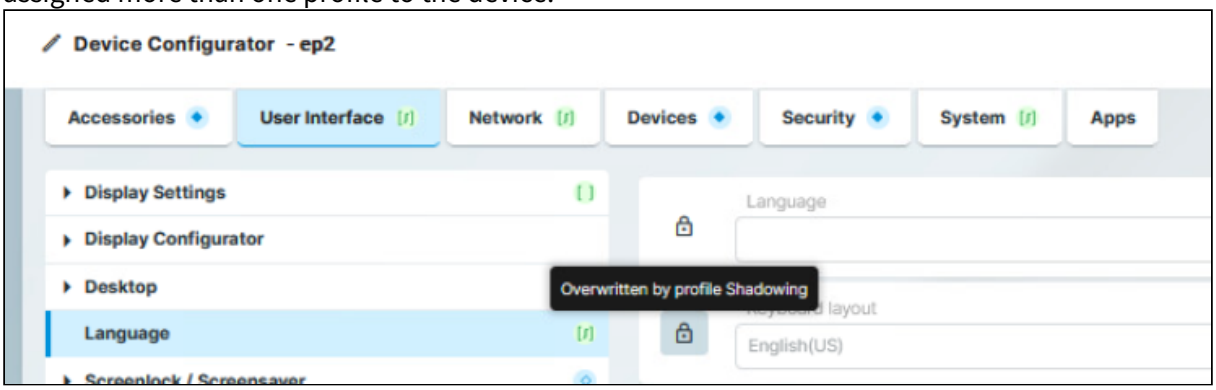
How to Check which Profiles Define Parameters in the IGEL UMS Web App

You can use profiles to define device parameters in the IGEL Universal Management Suite (UMS) Web App. When you use several profiles to define device parameters. you can check which profiles define a given parameter in the Device Configurator.

For information on how to do this in the UMS Console, see Checking Profiles in the IGEL UMS (see page 710).

You can check as follows:

1. In the UMS Web App, go to **Devices** and select the required device.
2. Click **[device's context menu] > Edit Configuration** or **Edit Configuration** in the device commands. Or you can simply double-click the device.
   The Device Configurator opens, showing the current configuration for the device. 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.
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 will be applied according to the prioritization described in Prioritization of Profiles in the IGEL UMS (see page 728).

Exporting and Importing Profiles in the IGEL UMS Web App

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 or support purposes or when importing the profile data from one UMS installation to another.

Alternatively, device settings can be exported and imported later as a profile, see How to Export Device Settings as a Profile in the IGEL UMS Web App (see page 1226).

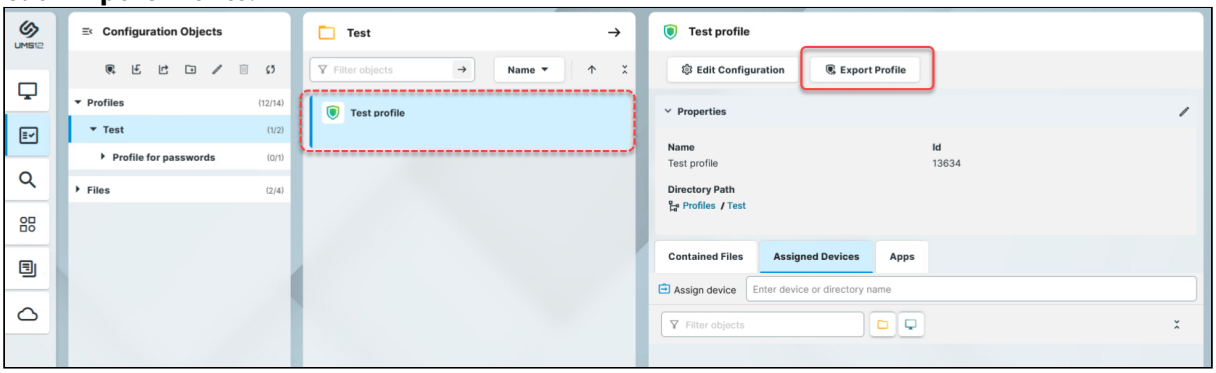
> In the UMS Web App, only OS 12 profiles can be exported or imported. If you need to export / import OS 11 profiles, see Exporting and Importing Profiles (see page 719).

Menu path: **UMS Web App > Configuration > Export Profile / Import Profiles**

Exporting Profiles

To export an individual profile, proceed as follows:

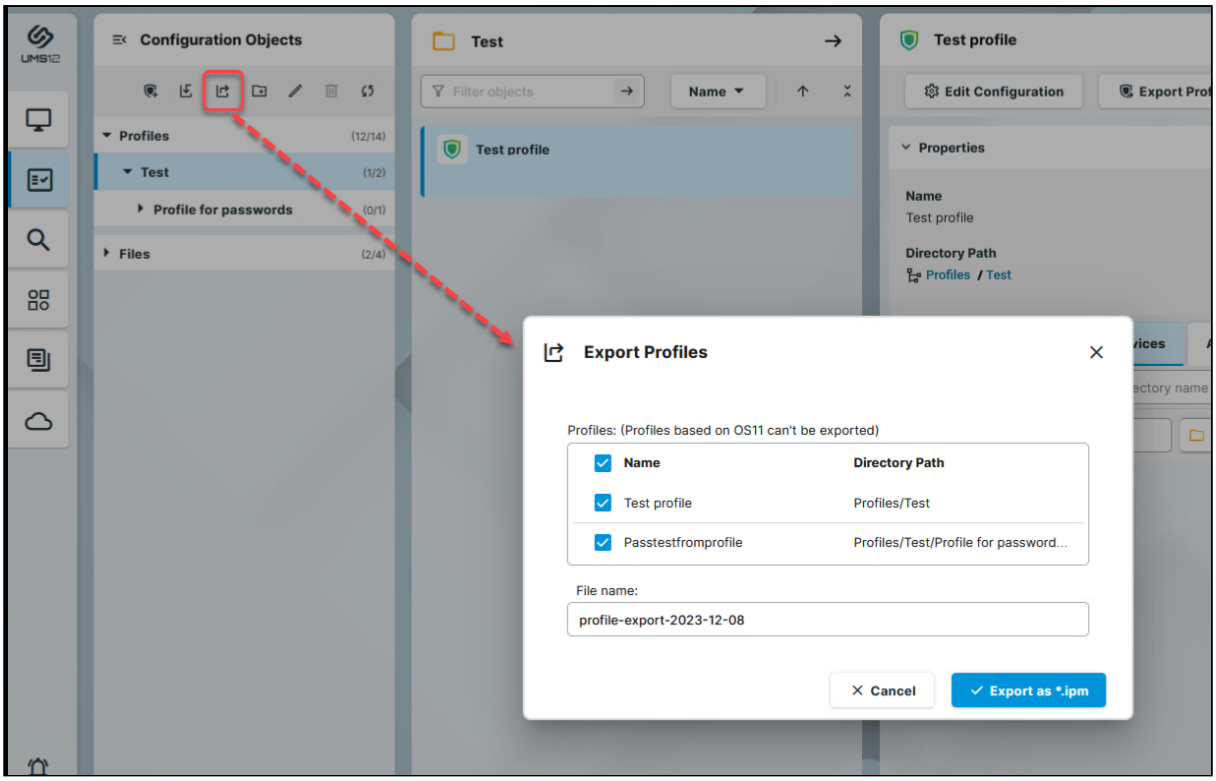
1. Under **UMS Web App > Configuration**, select the required profile.
2. Click **Export Profile**.



3. Specify the desired **file name**.
4. Confirm the export.

To export a number of profiles in one file, proceed as follows:

1. Under **UMS Web App > Configuration**, select the folder **Profiles** or the folder that contains the profiles you want to export.
2. Click **Export Profile** .
   The **Export Profiles** window will open.



3. Select the profiles you want to export.
4. Specify the **file name**.
5. Confirm the export.

The exported profiles are saved as an `.ipm` file, which also includes the metadata of IGEL OS Apps the profiles are based on. Therefore, it is not necessary to additionally import the required apps / app versions from the IGEL App Portal (or from the UMS).

> If the UMS to which you import the exported file has UMS as an Update Proxy feature activated but the fallback to the App Portal is disabled, you may nevertheless require the app binaries, see Configuring Global Settings for the Update of IGEL OS Apps (see page 1342).

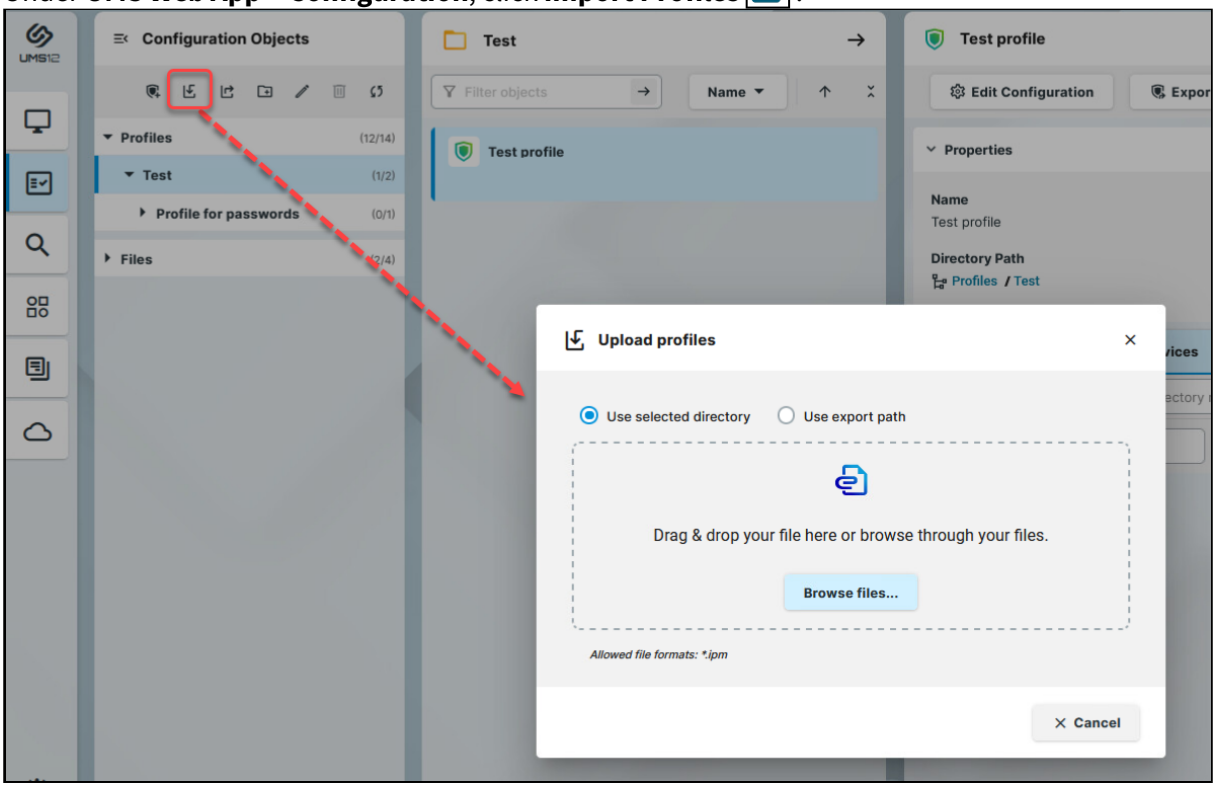
You can now import the exported file as described below.

> All passwords are excluded, i.e. replaced with a placeholder in the exported file. If you import the exported device settings later as a profile, no passwords will be included. You will have to set the passwords anew.

Importing Profiles

To import profiles, proceed as follows:

1. Under **UMS Web App > Configuration**, click **Import Profiles** .



2. Select if the profile(s) should be placed in the highlighted directory or if the original directory path of the profile(s) should be retained.
3. Select the file containing your profile(s).
4. When the upload is complete, confirm the import.
   The corresponding profiles will be imported to the UMS together with the metadata of IGEL OS Apps these profiles are configuring.
   If required, you can now assign the profiles to your endpoint devices.

Profiles can be imported as priority profiles (and vice versa).

How to Use Template Profiles in IGEL UMS Web App

You can use template keys in profiles to avoid having to set up numerous profiles which differ only in terms of a few points. The template keys contain parameters that are to receive divergent values for different devices. In addition, there are static template keys that receive their values from the device. The profiles containing template keys are called template profiles.

Template keys, values and template profiles created in the Console are also available in the UMS Web App, and vice versa. The following are only available in the UMS Console:

- Deleting template keys, template key directories and values
- Moving template keys from one directory to another
- Exporting and importing template keys
- Using Value groups

For details on the listed features, see Template Profiles in the IGEL UMS (see page 746).

Prerequisites

The **Enable template profiles** option is activated. For more information, see How to Activate Template Profiles in the IGEL UMS (see page 749).

Access the Template Keys Dialog

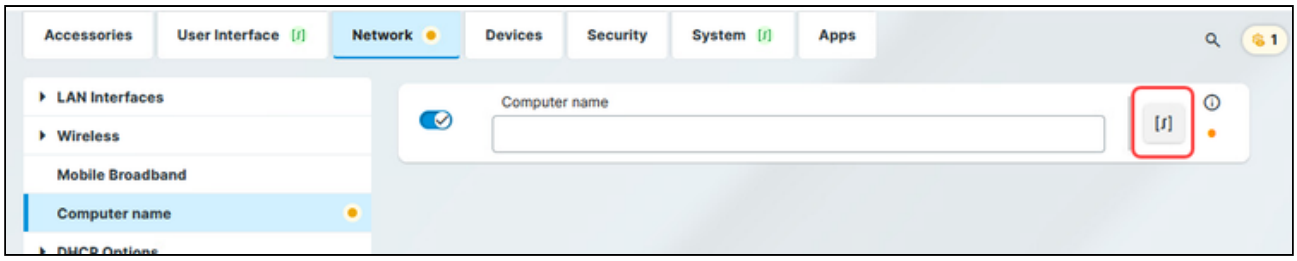
You can create template keys and values and apply them to the parameters in the Template Keys dialog. To access the dialog:

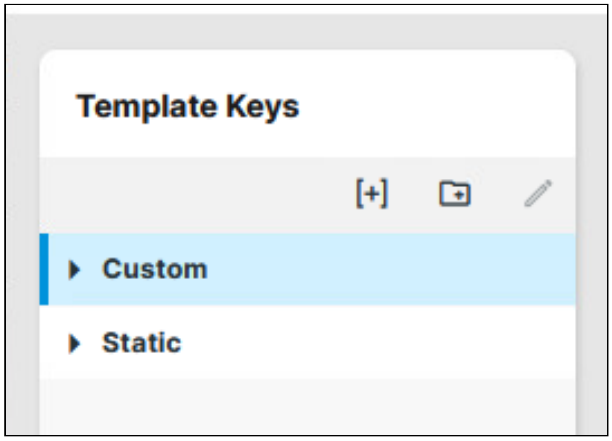
1. Edit an existing profile or create a new profile.

In the IGEL Web App we always use the Profile Configurator to create template keys and values. For more information on how to create profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).

2. In the Profile Configurator, go to the parameter for which you want to use the template key.
3. Activate the parameter and click the template key icon at the right side to open the **Template Keys** sidebar.

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.





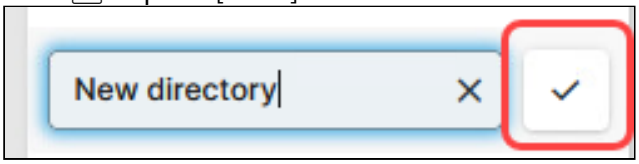
The following template key types are listed in the **Template Keys** tree node:

- **Custom**
  Here you can create your template keys and directories and template key values.
- **Static**
  The values of static template keys 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
  - **SERIALNUMBER**: Serial number of the device

Create Template Key Directories

To organize your template keys under directories, create the directories first:

1. Click **Create new directory**.
2. Give a name to your directory. The name cannot be empty and it cannot be more than 200 characters long.
3. Click ☑ or press [Enter] to save.

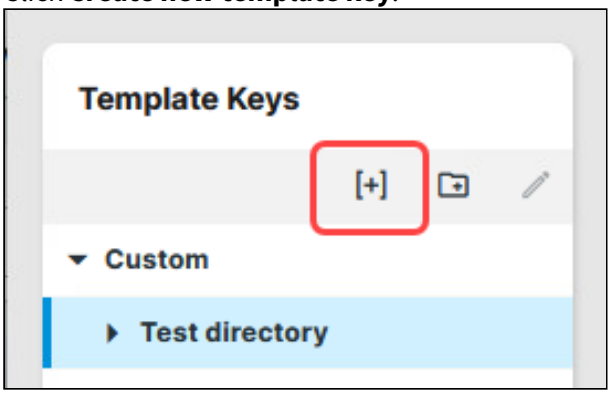


- You can only delete template keys, template key directories and values in the UMS Console.
- You can only move template keys from one directory to another in the UMS Console.

Create Template Keys

To create template keys:

1. Select the directory under which you want to create the template key.
2. Click **Create new template key**.



3. Give a **Name** to the key.
   The name:
   - cannot be empty.
   - has to be unique.
   - cannot be more than 200 characters long.
4. Optionally, give a **Description**.

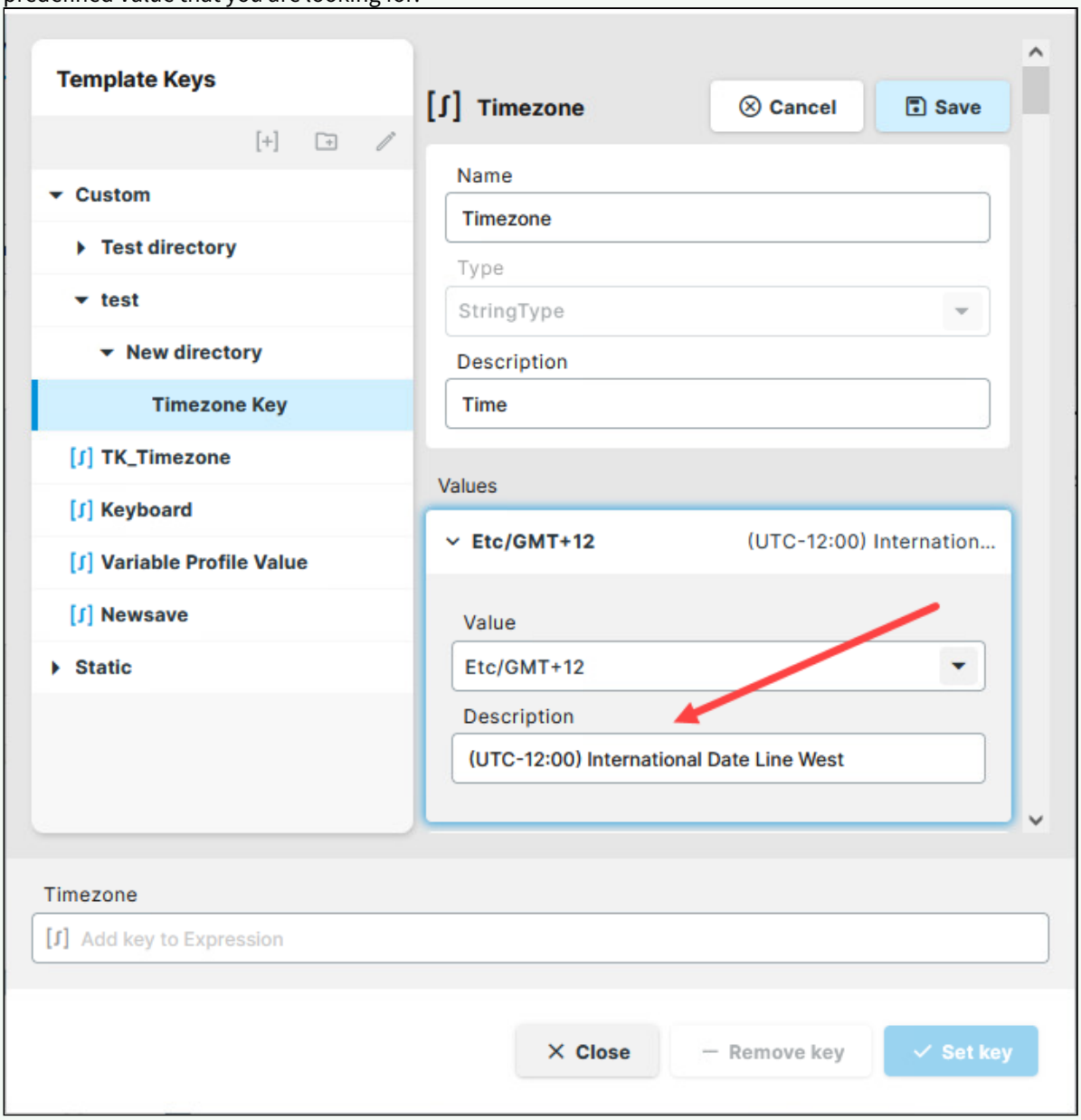
The **Type** for the key is stipulated by the selected parameter. For example, the type is going to be StringType for a parameter with a string field.

Add Template Key Values

To add values to the template keys:

1. Click **+ Add**.
2. Define the desired parameter value in the **Value** field, or in case of parameters with a fixed value range, select from the available value options.
   In case of parameters with a fixed value range such as selection menu or checkbox, the available options will be provided for selection. Click **Add all** to add all predefined values to the template key. You can change the predefined description of the parameters according to your needs.

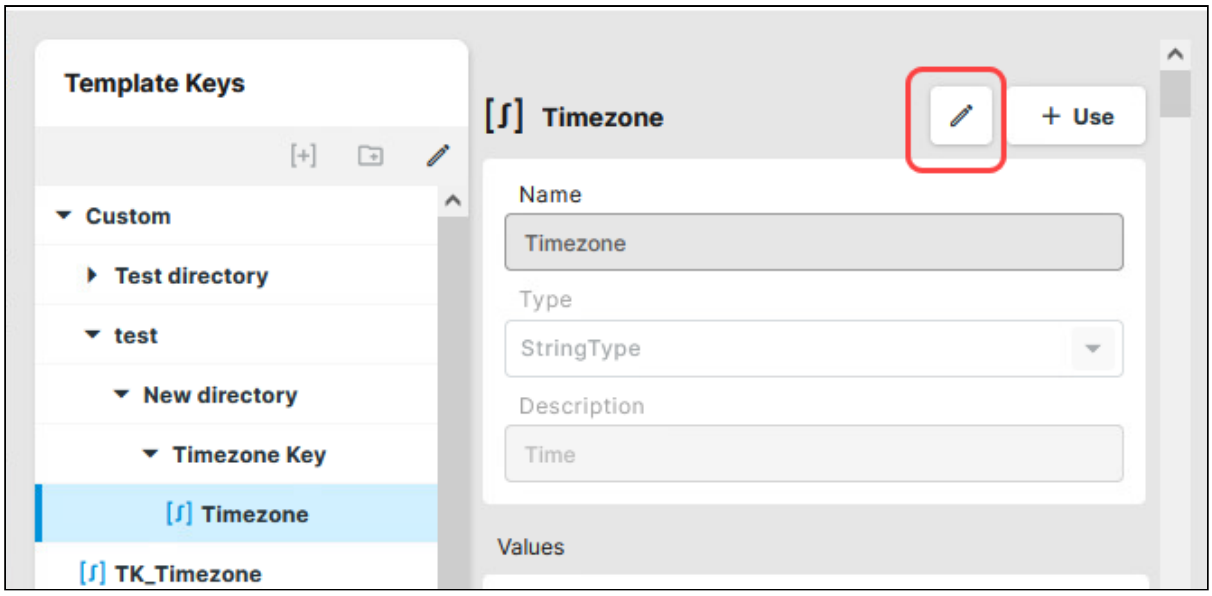
Using **Add all** can be helpful when parameters are known by their predefined Descriptions rather then their Values, for example, the **Timezone** parameter. With all the Descriptions listed, it is easier to find the predefined Value that you are looking for.



3. Define the **Description**.
4. Click **Save**.

If you do not want to save the template key, click **Cancel**.

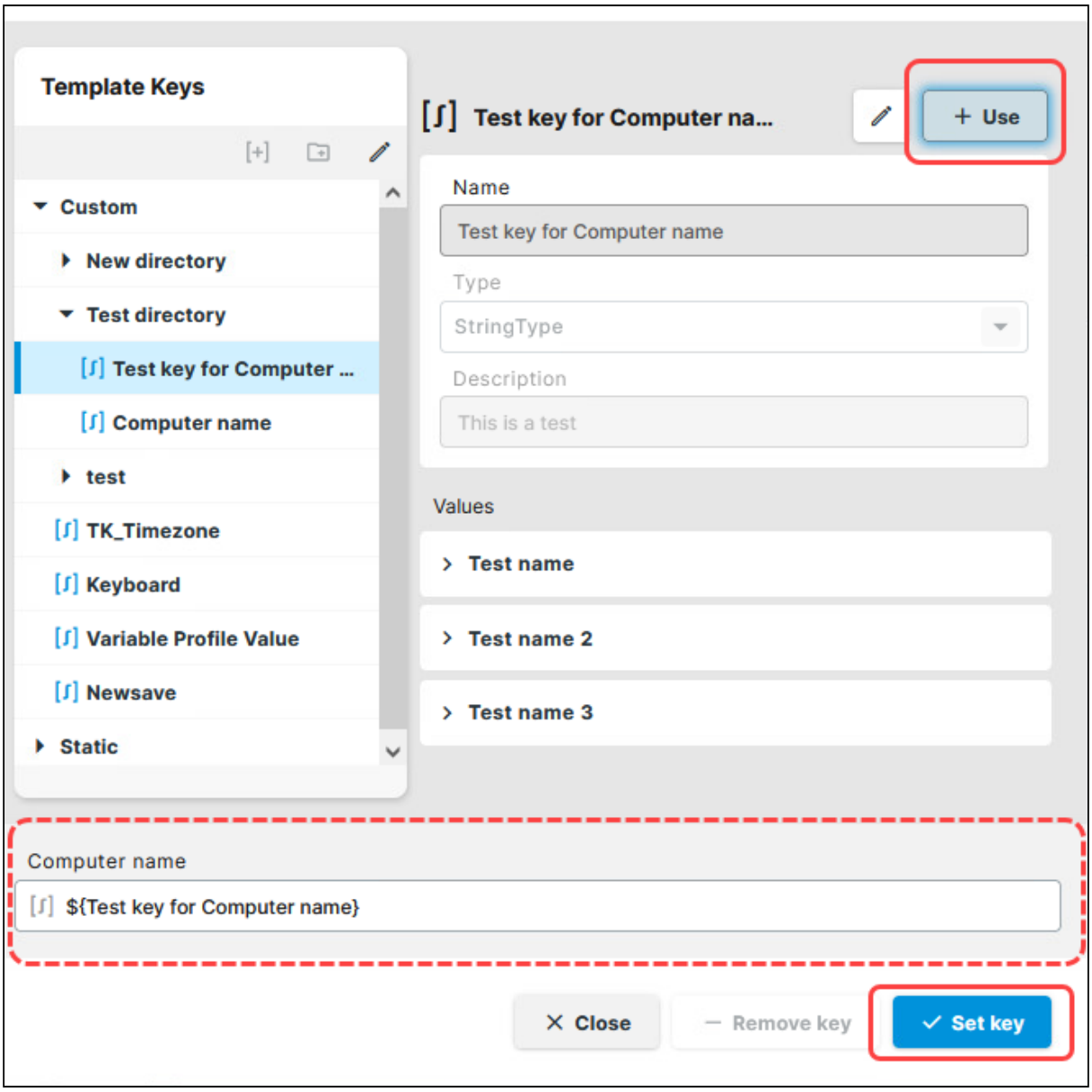
If want to modify an already saved template key, select the template key in the tree and click edit.



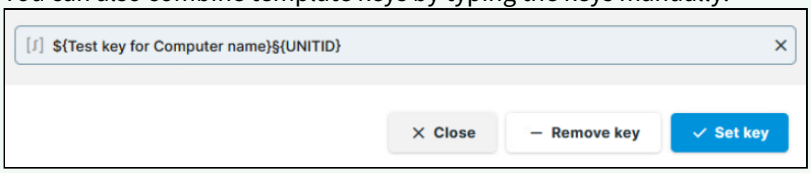
Template keys can be used in several profiles. Renaming a template key makes all profiles using the template key partly undefined. Check these profiles and deactivate or replace the edited template key there.

Apply the Key to the Parameter

1. Select the Template Key for the parameter and click **[+] Use.** The key is displayed at the bottom.

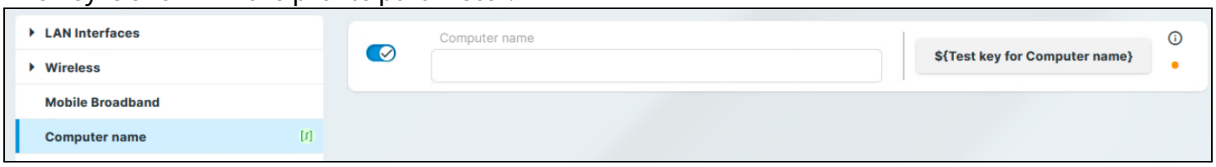


You can also combine template keys by typing the keys manually:



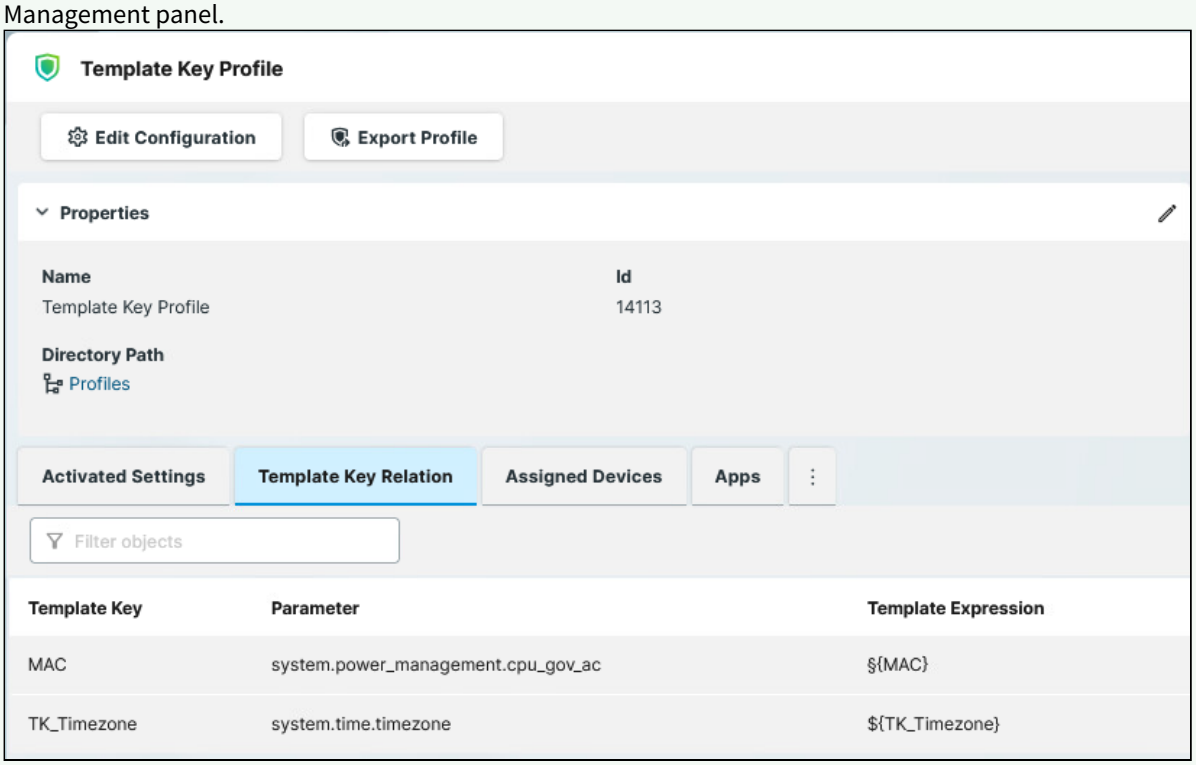
When you assign the values, both keys will be resolved and the displayed value will be a combination of both.

2. Click **Set key** to apply the key with its values and return to the profile.
   The key is shown in the profile parameter:



   When a template key is in use, it is marked in the Profile Configurator with the following symbols:
   [ ] - There is a saved template key change in one of the child pages.
   [ʃ] - There is a saved template key change in the page. / There is a saved template key change in the tab.
3. **Save** the template profile.

The template keys used in the profile are listed under the **Template Key Relation** tab of the Profile Management panel.



Assign Profile and Values to Devices

Assign the template profile and the template values in the **Devices** area to individual devices or device directories. For more information on how to assign them, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252) and How to Assign Objects in the IGEL UMS Web App (see page 1187).

How to Use Corporate Identity Customizations in IGEL UMS Web App

Using Corporate Identity Customizations (CICs) in the UMS Web App, you can customize the user interface of your IGEL OS devices to suit your corporate design. The same function was formerly called Firmware Customizations in the UMS Console. For details on CICs in the UMS Console, see Corporate Identity Customizations in the IGEL UMS (see page 764).

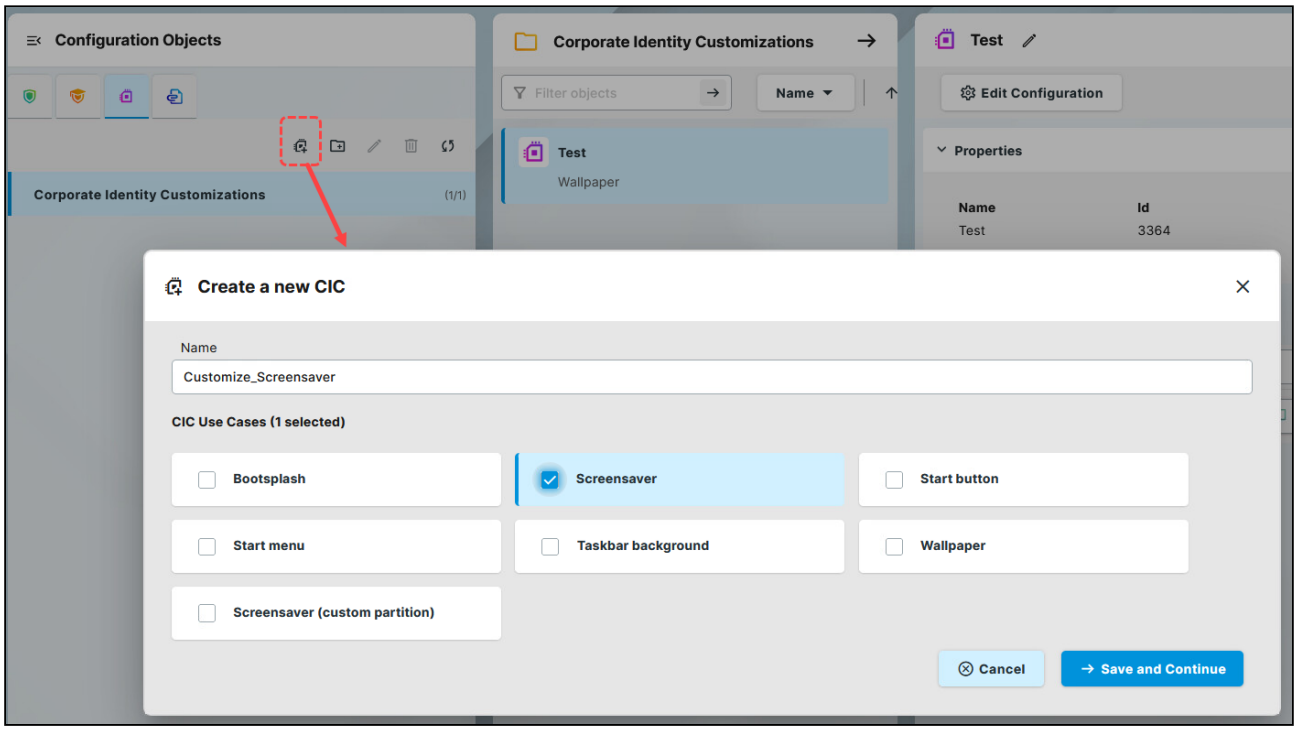
> The management of CICs is synchronized between the UMS Web App and UMS Console. If you create a CIC either in the UMS Web App or in the UMS Console you can later edit it both in the UMS Web App and UMS Console, except for CICs with multiple use cases. Multi-use CICs are only editable in the UMS Web App.

You can find instructions and detailed information in the following sections:

CIC Creation

To create a new CIC:

1. Go to the CIC tab in the **Configuration** area.
2. Click  .



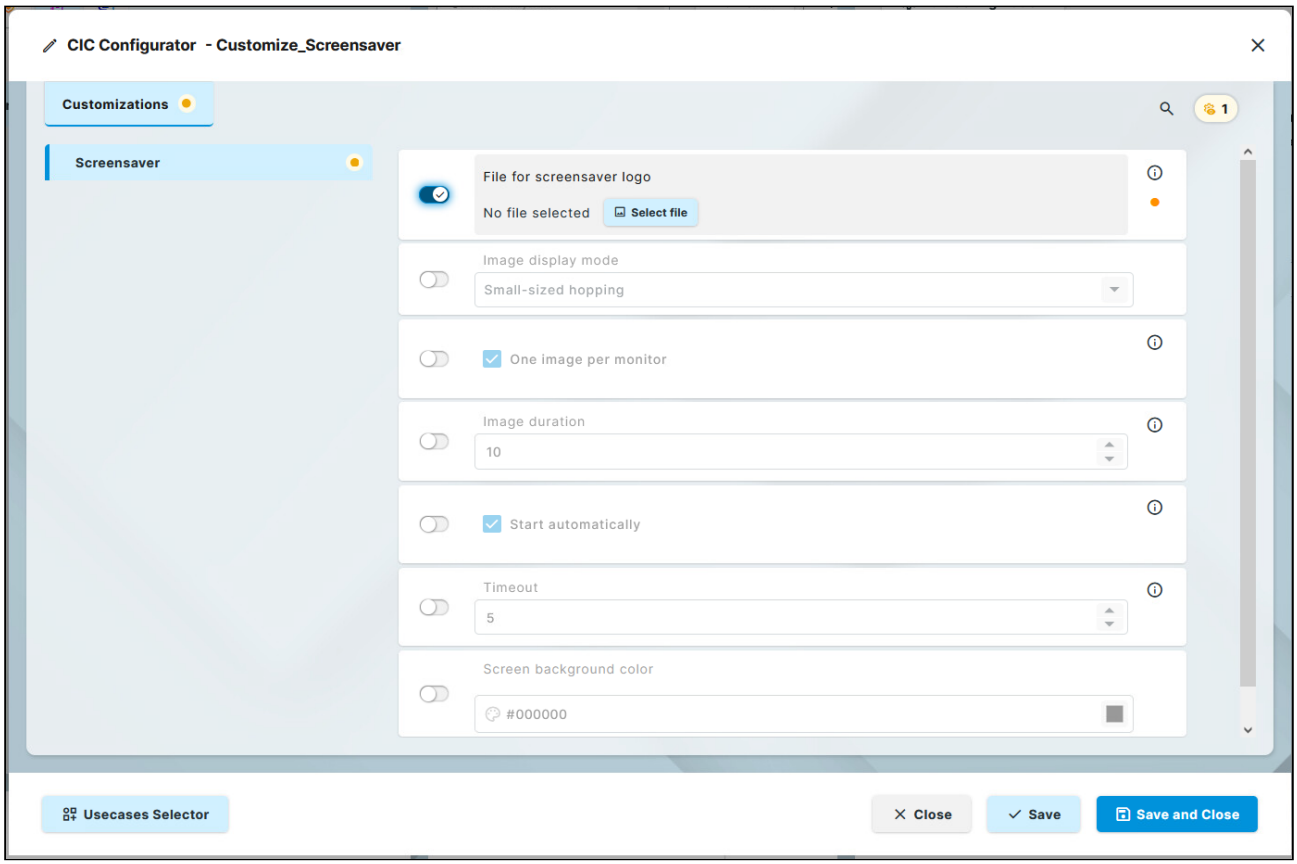
3. Give a Name to the CIC and select a use case or multiple use cases.

You can modify the selection later, by clicking the **Usecases Selector** at the bottom of the dialog.

Multi-Use CIC

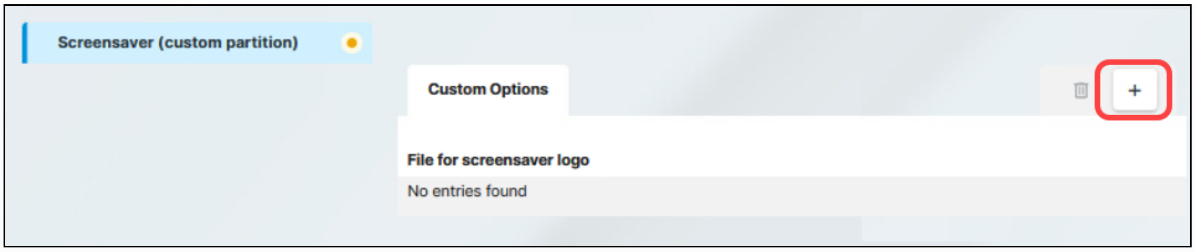
When selecting multiple use cases for the CIC, the CIC configuration will only be editable in the UMS Web App. You can still assign the CIC in the UMS Console, but cannot modify it.

4. Set the configurations. For details on the Use Cases and their configuration options, see CIC Use Cases and Configuration (see page 1282) further below.

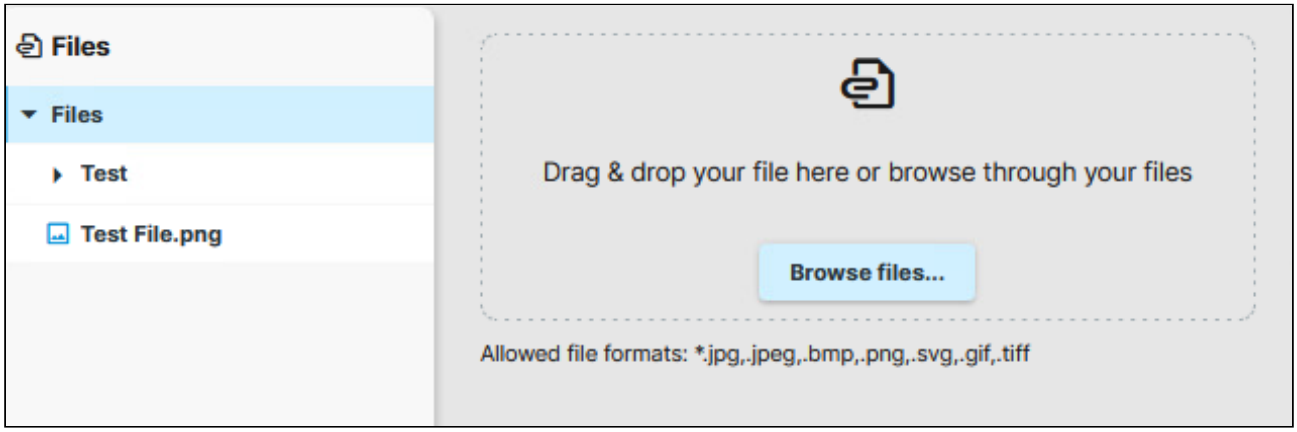


5. To add files, click **Select file**.

To add files to a **Screensaver (custom partition)**, first you need to click **+**.



6. Upload a new file through drag&drop or **Browse files...** or browse and select from the already uploaded files.



7. Save the CIC.

CIC Assignment

A CIC can be assigned to a device (both OS 11 and OS 12) or a device directory. Assigned CICs override standard profiles but in turn can be overridden by priority profiles. Further information regarding the prioritization of profiles can be found under Prioritization of Profiles in the IGEL UMS (see page 728) .

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 CIC assigned directly to the device has a higher priority than one which is assigned to the device directory. If both CICs have the same priority, the CIC with the higher ID will be effective.

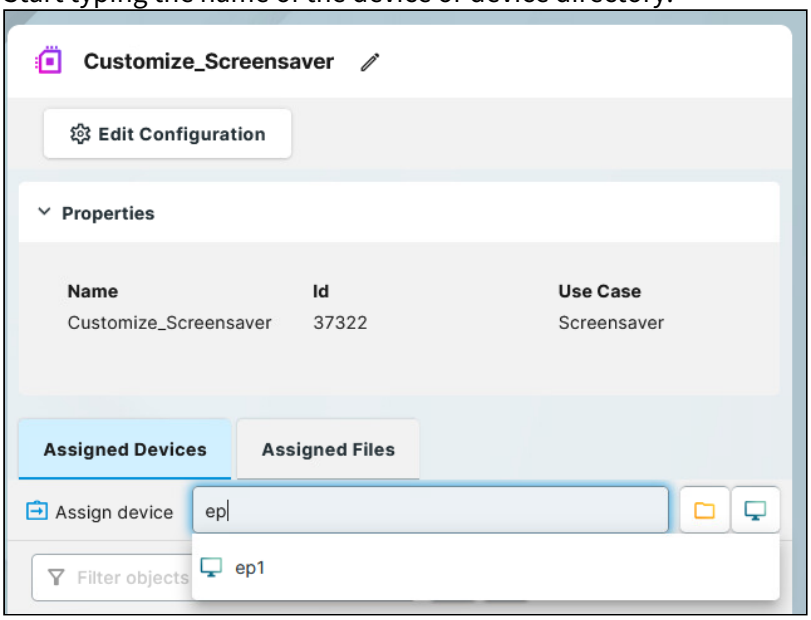
The ID of a CIC in shown under **Properties**.

In the **Configuration** area, you can quickly assign CICs through the **Assigned Devices** tab:

1. Select the CIC you want to assign.

2. In the information dialog, go to the **Assigned Devices** tab.

3. Start typing the name of the device or device directory.



4. In the displayed list, click on the device or device directory to assign the CIC

5. Confirm the assignment.

You can also assign CICs as any other objects through the **Devices** area. For more on object assignment, see How to Assign Objects in the IGEL UMS Web App (see page 1187).

CIC Use Cases and Configuration

Bootsplash

The assigned image file will be shown during the booting procedure.

You can set the horizontal and vertical alignment of the image and of the progress indicator.

Screensaver

The assigned image file will be shown when the screenlock/screensaver is activated.

You can set the following parameters...

Image display mode

Type of display. The following are available to choose from:

- **Small-sized hopping**: Small images are shown in changing positions. (Default)
- **Medium-sized hopping**: Larger images are shown in changing positions.

- **Full-screen center cut-out**: The images are shown in full-screen size. However, they may be clipped.
- **Full-screen letterbox**: The images are shown as large as possible in relation to the screen size.

One image per monitor

☑ If a number of monitors are used, a different image will be shown on each one. (Default)

☐ Images will be distributed over the monitors.

Image duration

Time in seconds until the image is changed. (Default: 10)

Start automatically

☑ The screenlock/screensaver starts automatically if there is no activity on the device within the **Timeout** period.

Timeout

Period of time in minutes before the screenlock/screensaver starts. (Default: 5)

Screen background color

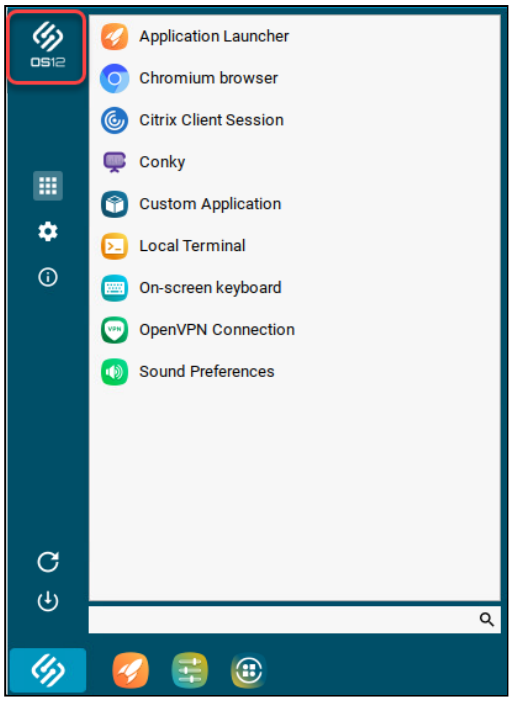
Color palette for determining the background color of the screen in screensaver mode. Click the color preview square to open the color selector.

Start Button

The assigned image file will be shown as the logo icon for the start menu in the taskbar. Size: 32x32 pixel

Start Menu

The assigned image file will be shown as the logo icon of the start menu window. Size: 64x64 pixels



Taskbar background

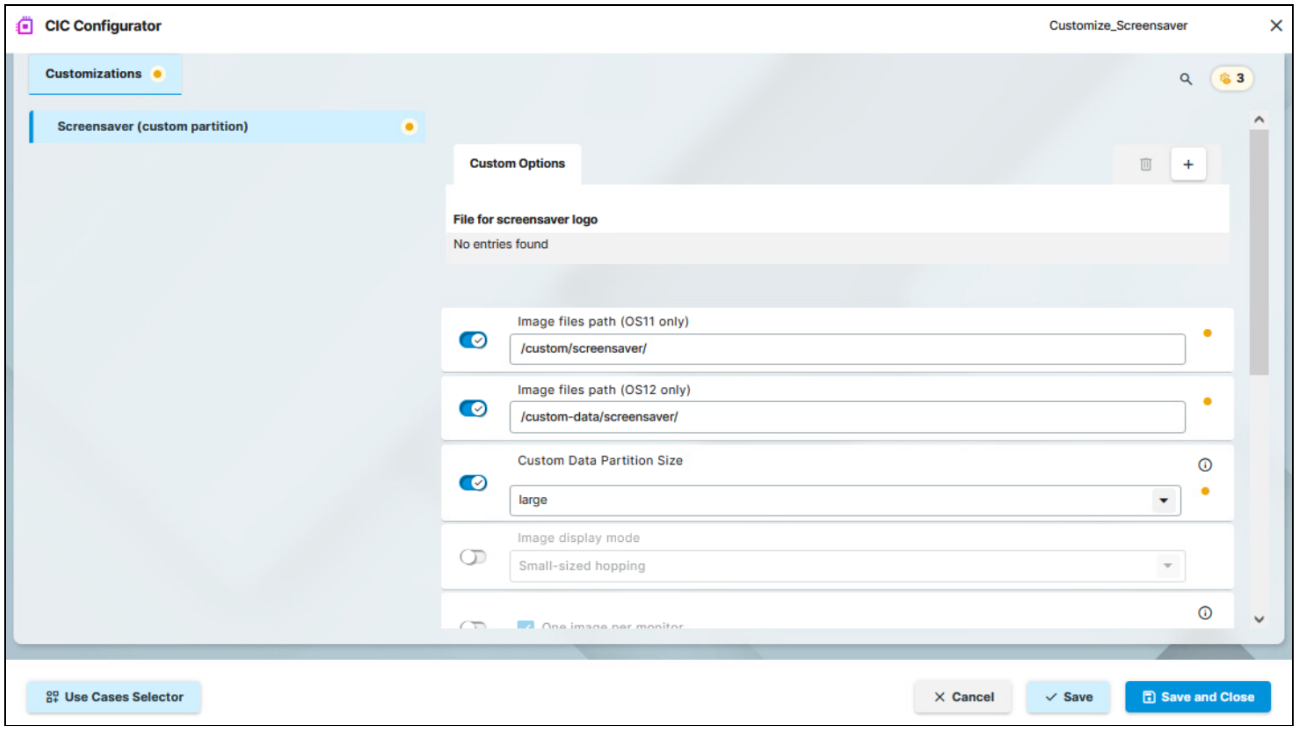
The assigned image file will be shown as the background of the taskbar in IGEL OS.

Wallpaper

The assigned image file will be shown as the background image of the desktop.

You can set up different background images for each monitor connected to the device.

Screensaver (custom partition)



You can set the following parameters...

Custom Options

List of configured image files.

Image file path (OS 11 only)

File path of a folder on the custom partition for OS 11 devices (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 at each boot.
> The folder does not need to be created beforehand. The path has to begin with a `/`.

Image file path (OS 12 only)

File path of a folder on the custom data partition for OS 12 devices (example: `/custom-data/screensaver`).

Custom Data Partition Size

You can use the drop-down to define the size. Available options:

- **small**
- **medium**
- **large** (Default)

You can also define the size of the custom data partition as a number followed by a multiplicative ending, without a space in between. Example: "100K" stands for 100 Kibibytes, that is, 100 * 1024 bytes.
The following multiplicative endings are possible (capital letters required):
K for kibibytes (number * 1024)
M for mebibytes (number * 1024 * 1024)
G for gibibytes (number * 1024 * 1024 * 1024)

Image display mode

Type of display. The following are available to choose from:

- **Small-sized hopping**: Small images are shown in changing positions. (Default)
- **Medium-sized hopping**: Larger images are shown in changing positions.
- **Full-screen center cut out**: The images are shown in full-screen size. However, they may be clipped.
- **Full-screen letterbox**: The images are shown as large as possible in relation to the screen size.

One image per monitor

- [x] If a number of monitors are used, a different image will be shown on each one. (Default)
- [ ] Images will be distributed over the monitors.

Image duration

Time in seconds that an image is shown before it switches. (Default: 10)

Start automatically

- [x] The screenlock/screensaver starts automatically if there is no activity on the device within the **Timeout** period.

Timeout

Period of time in minutes before the screenlock/screensaver starts. (Default: 5)

Screen background color

Color palette for determining the background color of the screen in screensaver mode. Click the color preview square to open the color selector.

CIC Export

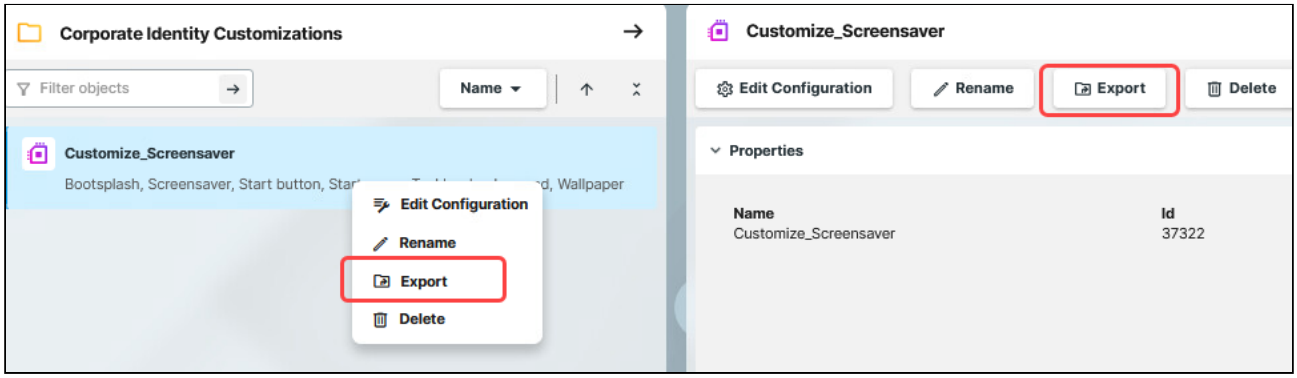
Export Single CIC

To export a single CIC, proceed as follows:

1. In the **UMS Web App** go to **Configuration > Corporate Identity Customizations** .

2. Select the CIC you want to export.

3. Click **Export**.



4. Specify the **File name**.

5. Confirm the export.

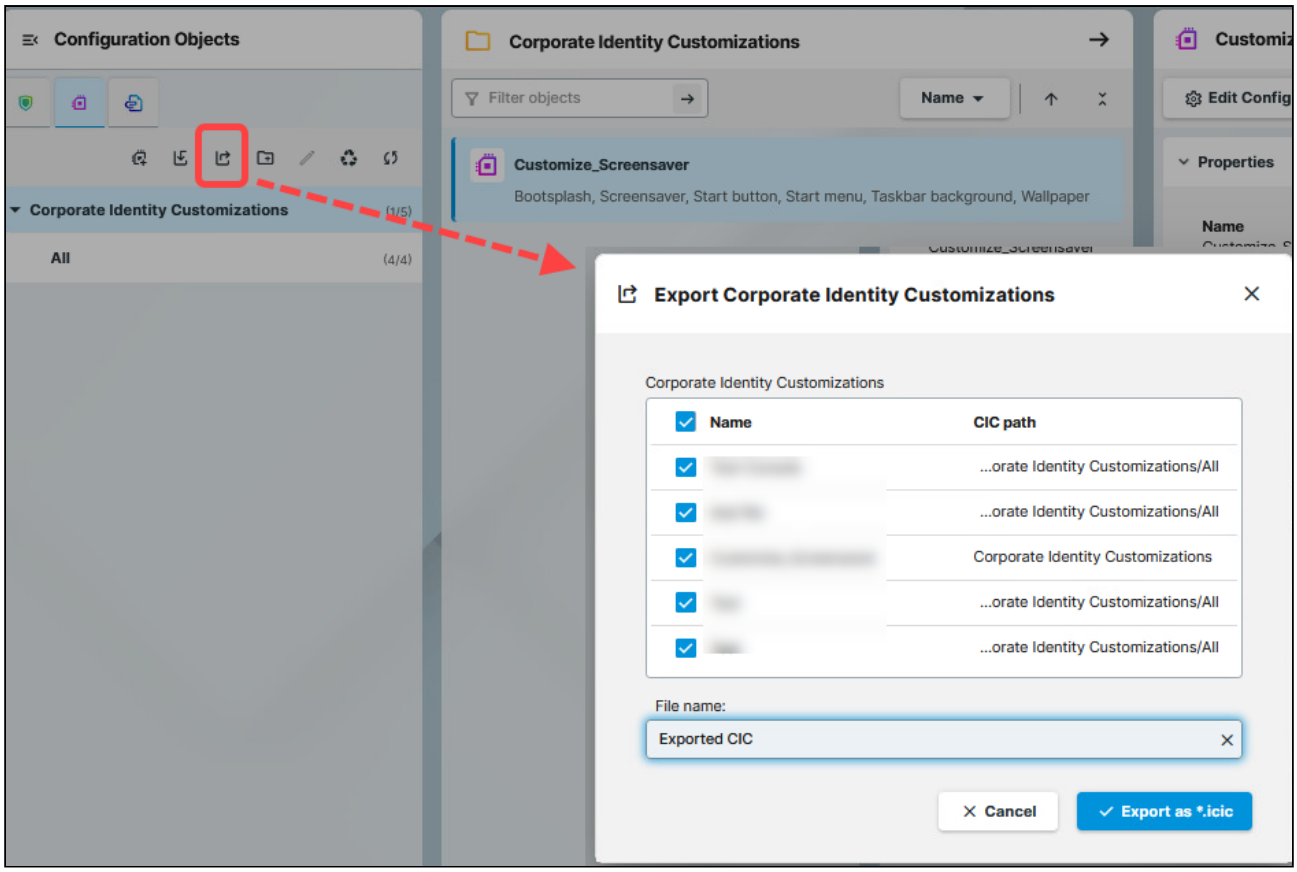
Export Multiple CICs

To export a number of CICs in one file, proceed as follows:

1. In the **UMS Web App** go to **Configuration > Corporate Identity Customizations** .

2. Select the root folder or the folder that contains the CICs you want to export.

3. Click **Export** .
   The **Export Corporate Identity Customizations** dialog opens.



4. Select the CICs you want to export.

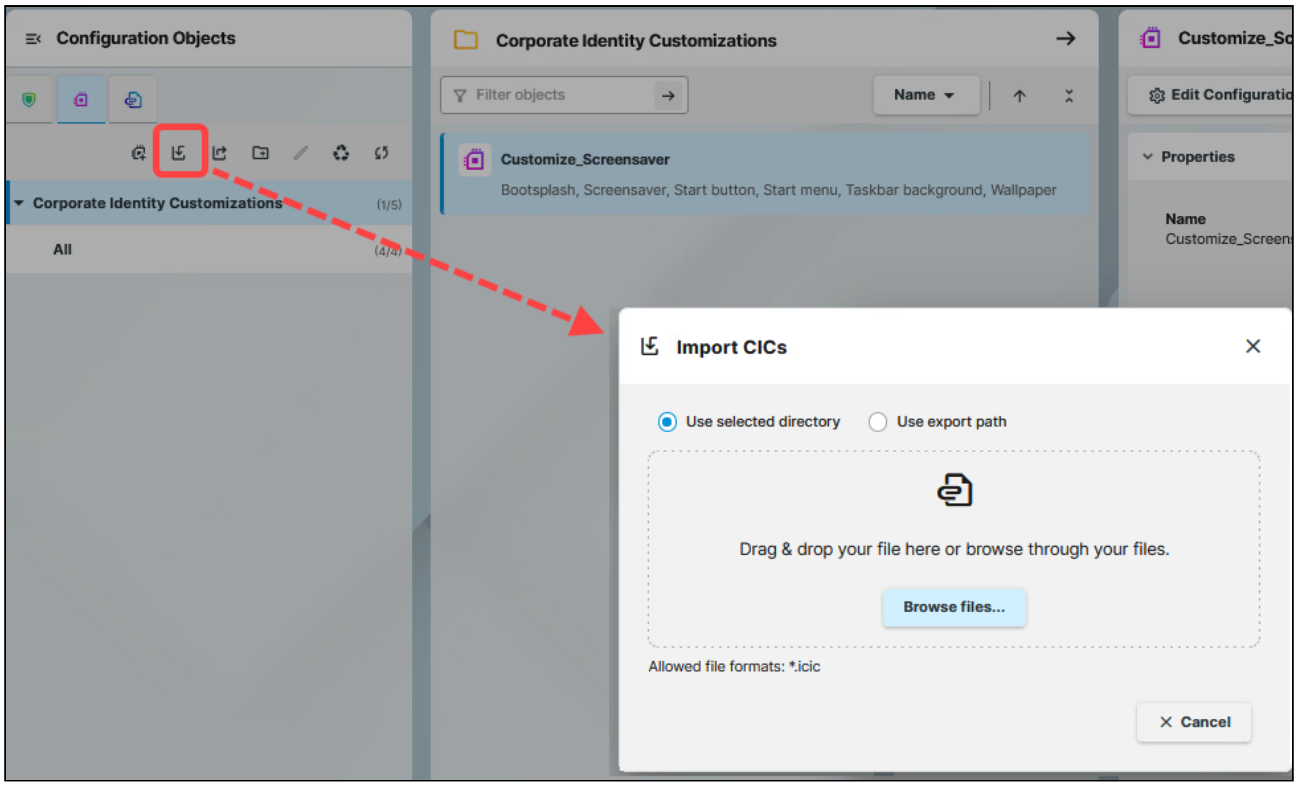
5. Specify the **File name**.

6. Confirm the export.
   The exported CICs are saved as an `.icic` file.

CIC Import

To import CICs, proceed as follows:

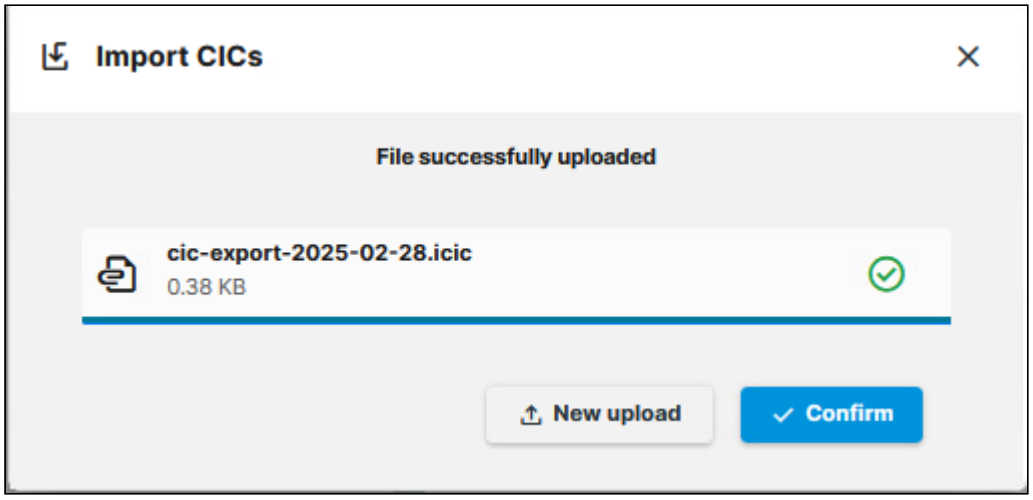
1. Under **UMS Web App > Configuration**, click **Import** .



2. Select if the CIC(s) should be placed in the highlighted directory (**Use selected directory**) or if the original directory path of the CIC(s) should be retained (**Use export path**).

3. Select the CIC file. The upload starts automatically.

4. When the upload is complete, confirm the import.



Upload and Assign Files in the IGEL UMS Web App

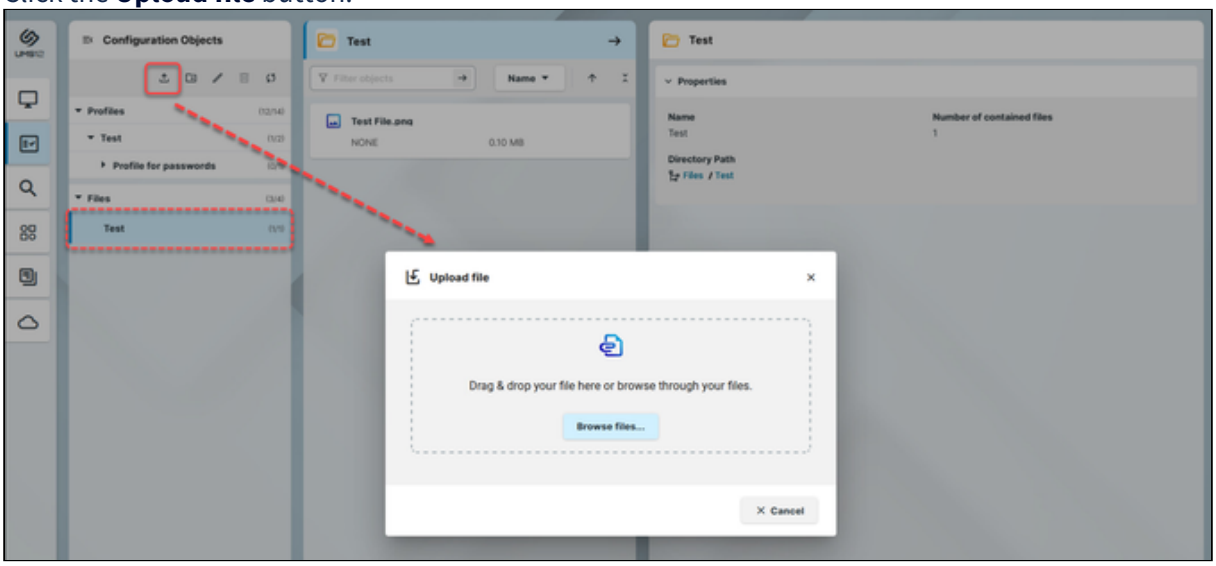
In the IGEL Universal Management Suite (UMS) Web App, you can upload files as configuration objects. Then, you can distribute these files to your devices through assignment. For information on configuration objects, see Configuration - Centralized Management of Device Settings in the IGEL UMS Web App (see page 1239).

> Files cannot currently be deleted in the UMS Web App. Use the UMS Console, instead.

Menu path: **UMS Web App > Configuration**

File Upload

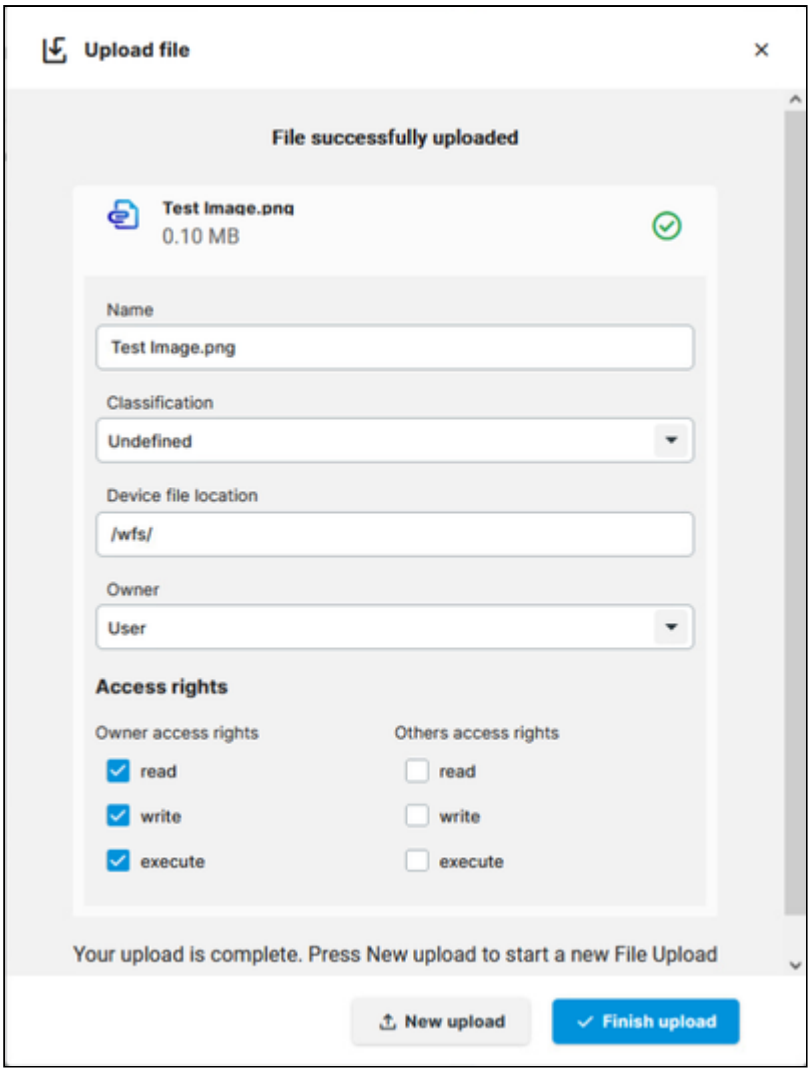
1. Select a folder under Files. The file will be uploaded here.
2. Click the **Upload file** button.



3. Browse or drag&drop the file.

> You can only upload one file at a time.

4. As soon as the file upload begins, you can edit the properties.

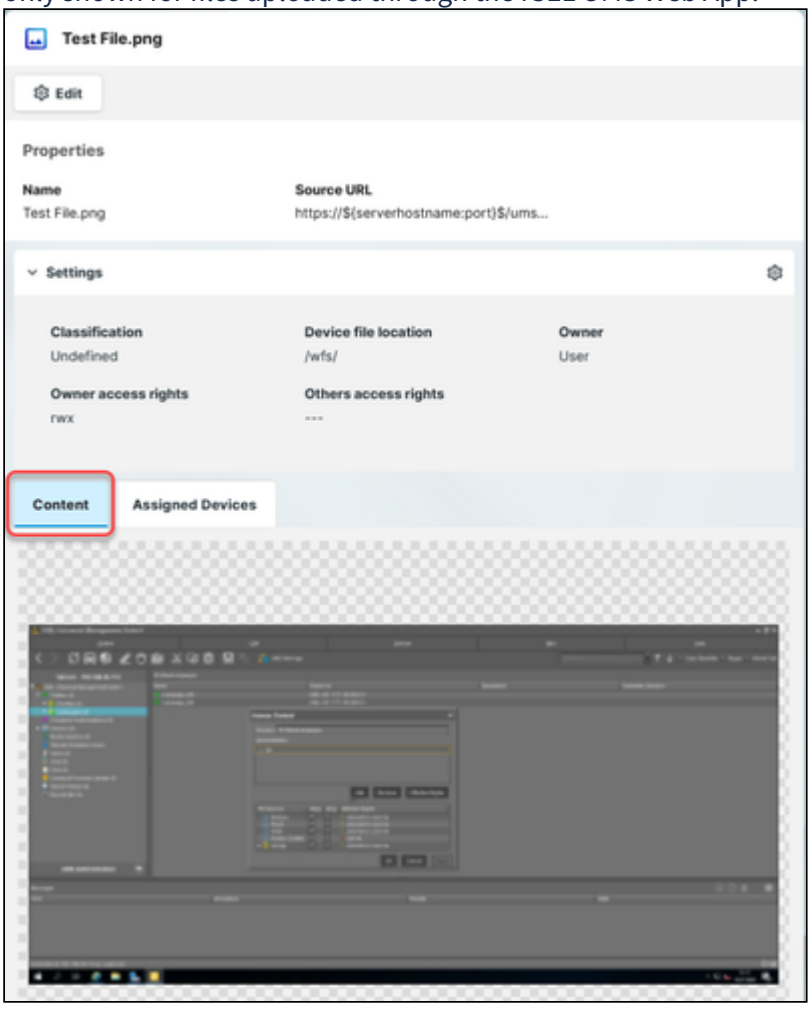


5. Under **Classification**, select the type of file. This serves to automatically establish suitable storage locations and file authorizations. Choose between:
   - **Undefined**
   - **Web browser certificate**
   - **SSL certificate**
   - **Java certificate**
   - **IBM iAccess certificate**
   - **App signing certificate**
   - **Common certificate**

   For information on certificate deployment, see the section *Deploying Certificates via the UMS* in *IGEL OS > Deploying Trusted Root Certificates in IGEL OS*.
6. If you set the classification to **Undefined**, specify the path in the devices's local file system under **Device file location**.
   Paths must end with a path separator – a slash "/" or a backslash "\". If you enter a directory which does not yet exist, it will be created automatically.

> Because of its space limit, the use of the `/wfs/` folder is NOT recommended for large files (>2 MB).

7. For the **Undefined** classification, set the **Owner** and the **Access rights**.
   These will be attached to the file when it is transferred to the device and will be used on the destination system.
8. Click **Finish upload** to confirm the settings and close the dialog or **New upload** to upload another file.
   Once the upload is finished, you can preview the uploaded file under the **Content** tab. A preview is only shown for files uploaded through the IGEL UMS Web App.



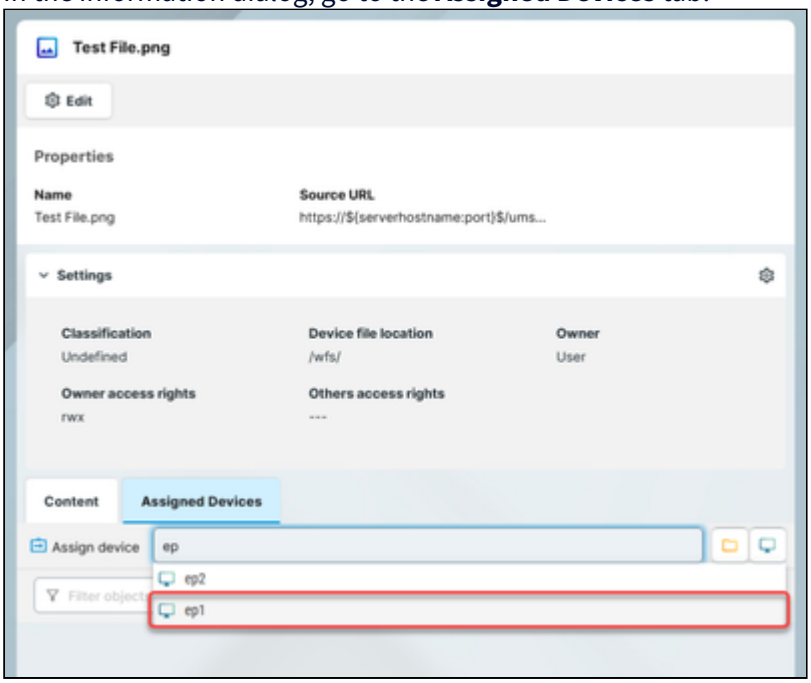
> When you upload a file with a filename that already exists, the new filename gets modified according to the format {filename}({n}), where n specifies how many files exist with the same name. For example, Logo(1).png, Logo(2).png. In the UMS Web App, this is only visible in the **Source URL** but not in the **Name** of the file.

Uploaded files can be managed both in the IGEL UMS Web App and UMS Console. For details on managing files in the UMS Console, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices (see page 1123).

File Assignment

In the **Configuration** area, you can quickly assign individual files through the **Assigned Devices** tab.

1. Select the file you want to assign.
2. In the information dialog, go to the **Assigned Devices** tab.



3. Start typing the name of the device or device directory.
4. In the displayed list, click on the device or device directory to assign the file.
5. Confirm the assignment.

You can also assign files as any other objects through the **Devices** area. For more on object assignment, see How to Assign Objects in the IGEL UMS Web App (see page 1187).

Apps - Import and Configure Apps for IGEL OS 12 Devices via the IGEL UMS Web App

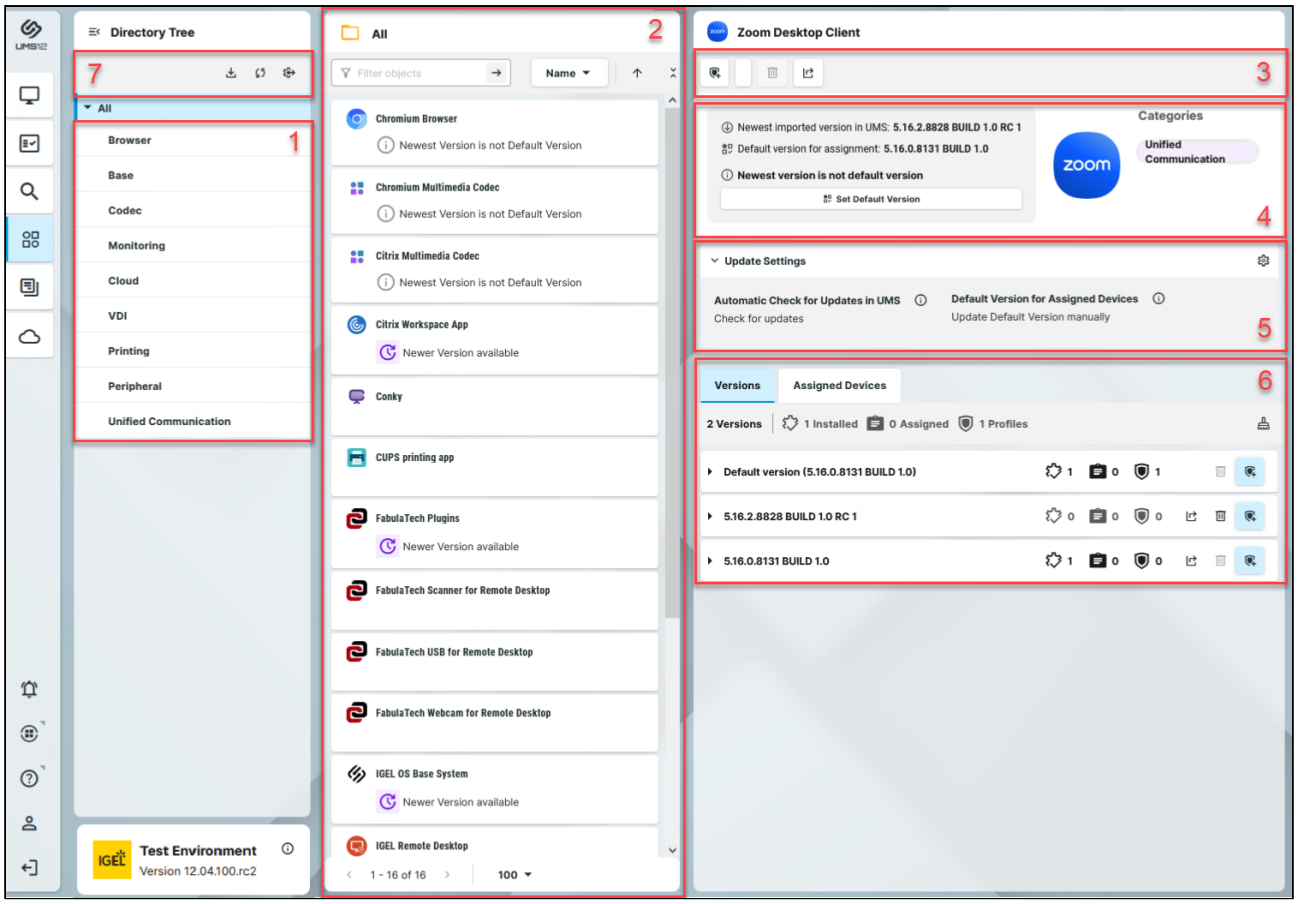
In the **Apps** area of the UMS Web App, you can manage apps imported to the IGEL Universal Management Suite (UMS) for configuring your IGEL OS 12 devices.

> To have access to the **Apps** area, you need **App Management** permission. You can set the permission in the **UMS Console > System > Administrator accounts**.
> For general information on rights and permissions, see How to Create Administrator Accounts in the IGEL UMS.

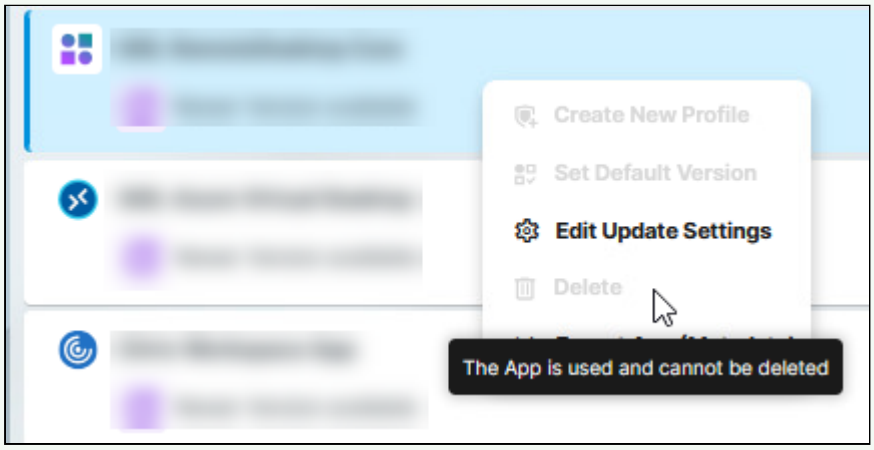
Menu path: **UMS Web App > Apps**

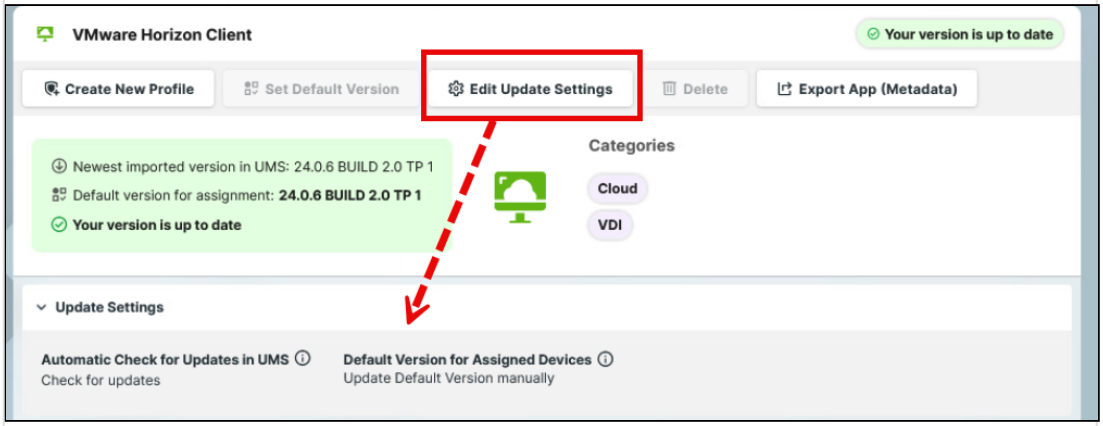
Under **Apps**, you can find

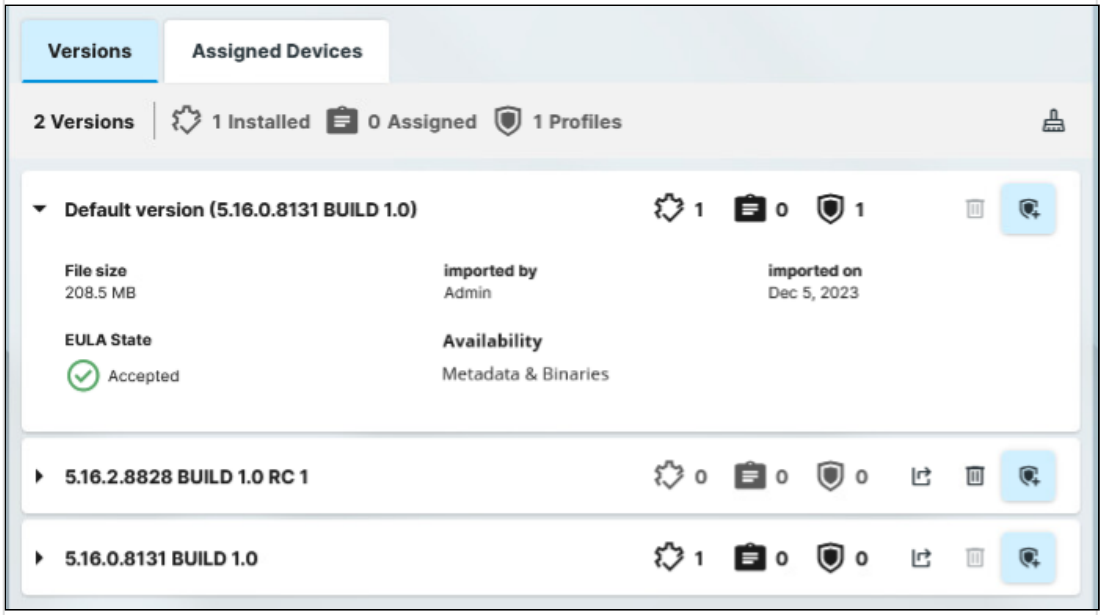
- apps imported from the IGEL App Portal
- automatically registered apps. The UMS automatically registers all apps available on the devices, e.g. IGEL OS Base System, locally installed apps, and dependent apps that are automatically installed on the device during the installation of the main app (e.g. Citrix Multimedia Codec as a dependent app for Citrix Workspace app)

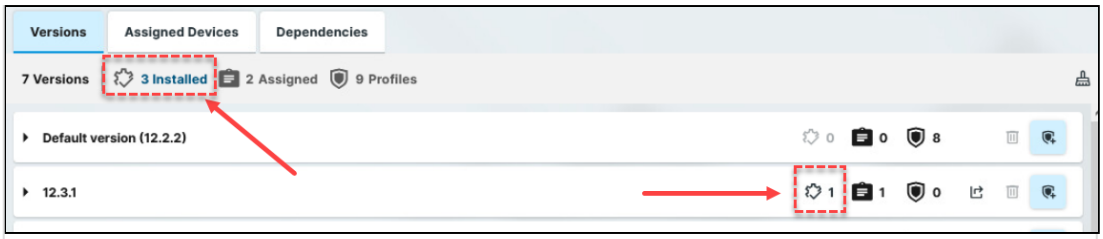


1	App categories	Shows all available app categories. → Click **All** to view apps from all categories. → Click a specific category to view all apps within this category.

2	App list	Shows apps contained in the selected category. → Right-click on the device to open a context menu with available commands. If a command is greyed out, hovering over it shows information on why the command is not available.  At the top of the app list, you can: • Filter and sort apps by **Name** • Collapse and expand the app details At the bottom of the app list, you can: • Set the paging for the navigation in the app list • Set the number of apps to be displayed on one page
3	Commands	**Create New Profile**: Creates a profile for the app selected in the app list. For more information on profile creation, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252). **Set Default Version**: Defines which app version will be assigned to a device / device directory if no specific app version is selected during the app assignment or the creation of a profile configuring this app. See How to Set a Default Version of an App in the IGEL UMS (see page 1311). **Edit Update Settings**: Allows you to change update settings for the app selected in the app list. See Configuring Update Settings for Individual IGEL OS Apps (see page 1337). **Delete**: Deletes an app selected in the app list if this app is nowhere used. See How to Delete Apps in the IGEL UMS Web App (see page 1324). **Export App (Metadata)**: Exports the metadata of an app selected in the app list, see How to Export and Upload Apps to the IGEL UMS (see page 1338).

4	App information	Details for the app selected in the app list such as **Newest imported version**, **Default version** that is selected under **Set Default Version**, availability of a newer version (depending on the configuration under **Update Settings**).
5	Update Settings	Shows update settings for the app selected in the app list. To make changes, click **Edit Update Settings**. 

6	Versions	Shows information on all available versions of the app, e.g. if and how an app version is used (installed, assigned, used in profiles). Under **Availability** you can check if the metadata and binaries of the app are available in the UMS. This is important when the UMS is used as an App Proxy. For details, see How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access (see page 1305).  → To export the selected app version, click  . → To delete a selected app version, click  . See How to Delete Apps in the IGEL UMS Web App (see page 1324). → To create a profile from the selected app version, click  . For details on profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).



→ To see the list of devices on which any version of the app is installed, click the link at the top of the tab. The list opens in a new tab as a search.

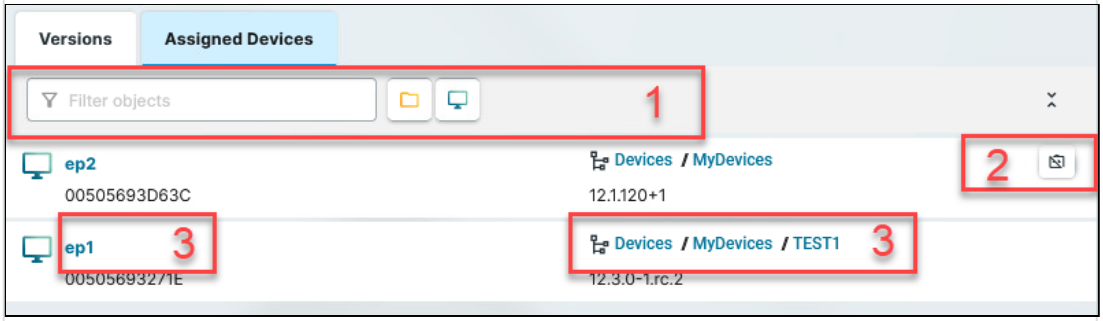
→ To see the list of devices on which the selected version of the app is installed, click the button in the row of the app version. The list opens in a new tab as a search.

An app version with End User License Agreement (EULA) not accepted is marked with an exclamation mark.

→ To accept the EULA for the app, click **Accept EULA**. This can be necessary, for example, for automatically registered apps (see page 1294) or if the EULA is changed. If not accepted in the UMS, the EULA can still be accepted by your users locally on the device via the corresponding notification dialog.

Assigned Devices

Shows all devices / device directories to which the selected app is assigned.



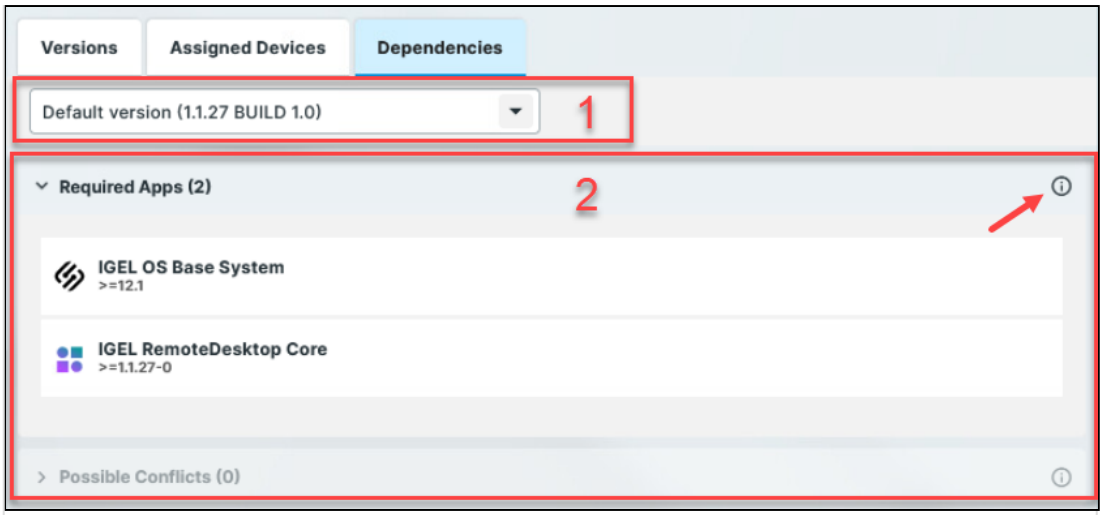
1: Filters the devices / device directories assigned to the selected app. The filter criteria are linked with the operator *AND*.

→ Click  to remove all filters.

2: Detaches the selected device / device directory from the app.

3: Jumps to the corresponding device / directory and shows all **Assigned Objects** for it.

	Dependencies	Shows information on how the selected app version relates to other apps.



1: Version selector

→ Select the version from the drop-down for which you want to see the dependency information.

2: Dependency information

→ Click the tooltip icon for the detailed descriptions:

Required Apps

The apps listed here are required for the app version in question to be fully functional.

If a required app is mentioned just as a name, any version of that app is sufficient.
If a specific version is mentioned, the required app is needed in that version.
If a max-value is given, the required app is needed in a version below that value.
If a min-value is given, the required app is needed in a version above that value.

If the admin does not actively assign a version of the required app to the device, the device will try to calculate the necessary version, and the required app will be installed in that version.

Possible Conflicts

The apps listed here cannot be installed on the device at the same time as the app version in question.

If a conflicted app is mentioned just as a name, no version of that app can be installed at the same time.
If a specific version is mentioned, only this version of the app cannot be installed at the same time.
If a max-value is given, the app cannot be installed in a version below that value.
If a min-value is given, the app cannot be installed in a version above that value.

7	Settings	Allows you to configure global settings for the app updates. See Configuring Global Settings for the Update of IGEL OS Apps (see page 1342).

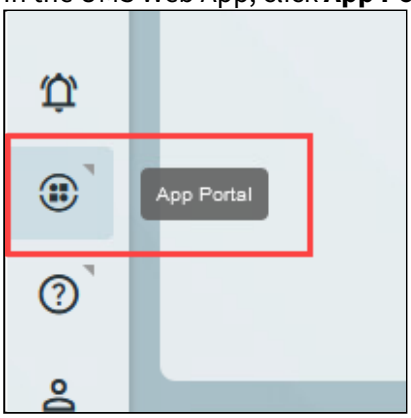
How to Import IGEL OS Apps from the IGEL App Portal

To manage IGEL OS 12 devices, you need to import IGEL OS Apps of your choice from the IGEL App Portal[208].

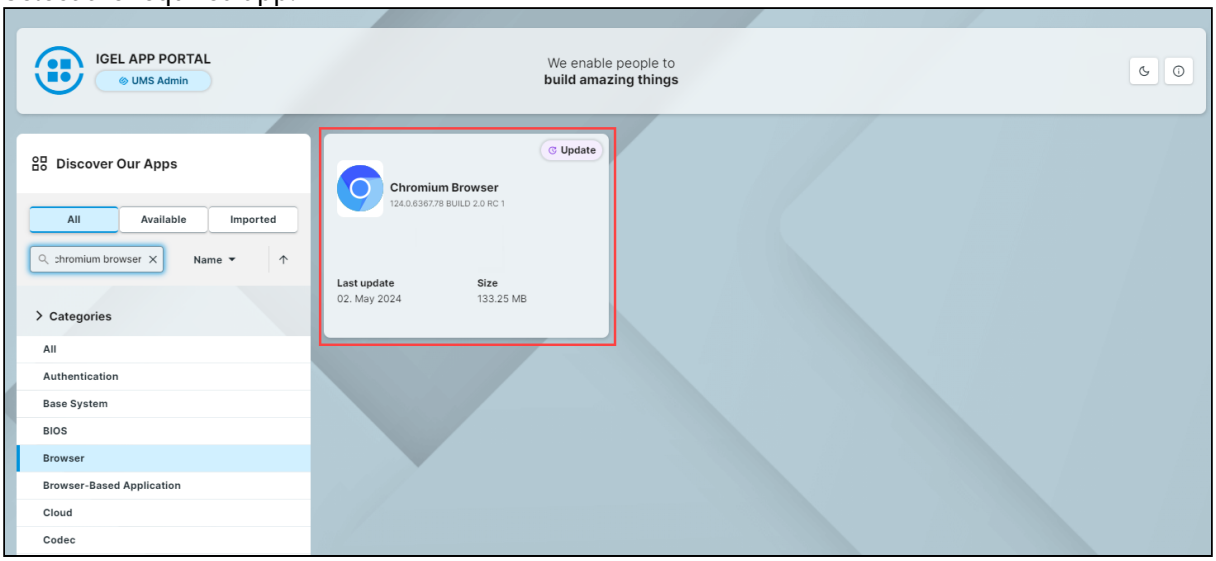
> To have access to the IGEL App Portal, you have to preliminary register your IGEL Universal Management Suite (UMS); see (en) Registering the UMS .
> For details on the IGEL App Portal, see (en) IGEL App Portal .

To import apps to the IGEL UMS, proceed as follows:

1. In the UMS Web App, click **App Portal**.

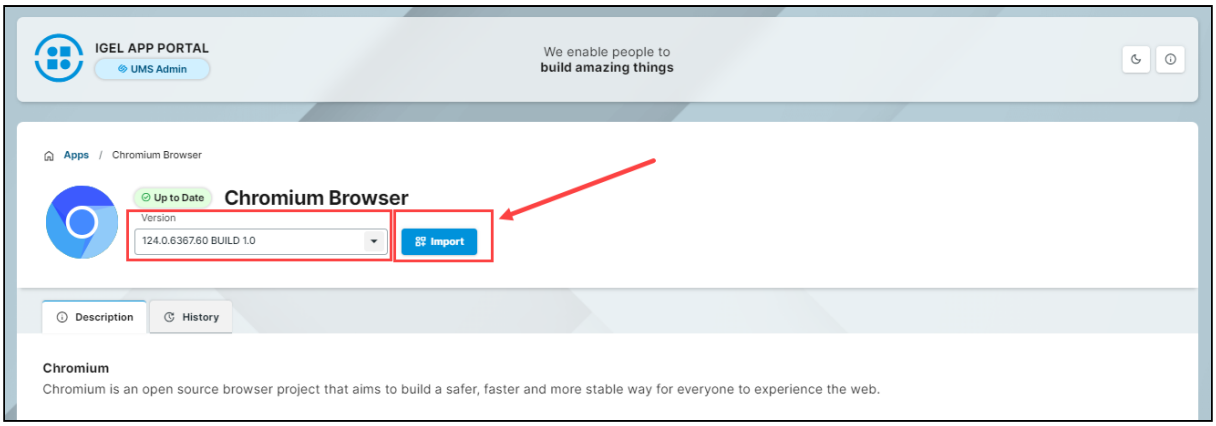


2. Select the required app.

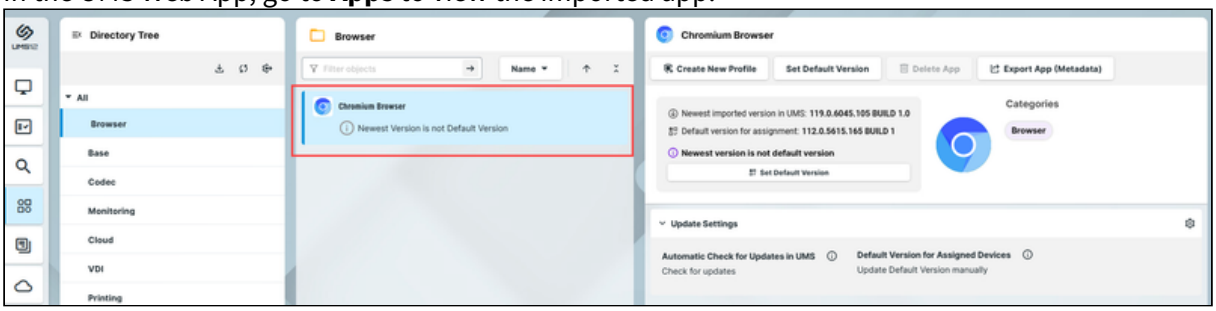


3. Select the required version and click **Import**.

208. https://app.igel.com/



4. Accept the End User License Agreement (EULA) and wait for the import to be finished.
5. In the UMS Web App, go to **Apps** to view the imported app.



How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access

If your IGEL Universal Management Suite (UMS) runs without internet connection and you want to use it to install apps on IGEL OS 12 devices, you can do that by manually uploading the apps to the UMS Web App before app assignment. If your OS 12 devices also run without internet connection, you also need to configure your UMS as an update proxy before app assignment.

No additional ftp server is required in any case, as everything is handled by the IGEL UMS and the IGEL OS.

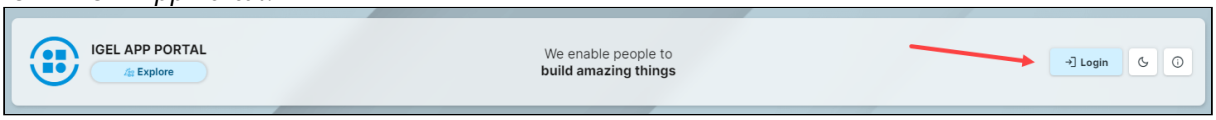
Direct Access to the IGEL App Portal

You need to access the App Portal to download the app packages for the manual upload. Since the UMS is not connected to the internet, you cannot access the App Portal from the UMS Web App. Instead, you need to access it by logging in directly to the App Portal. For more information, see the article *How to Start with IGEL > IGEL App Portal*.

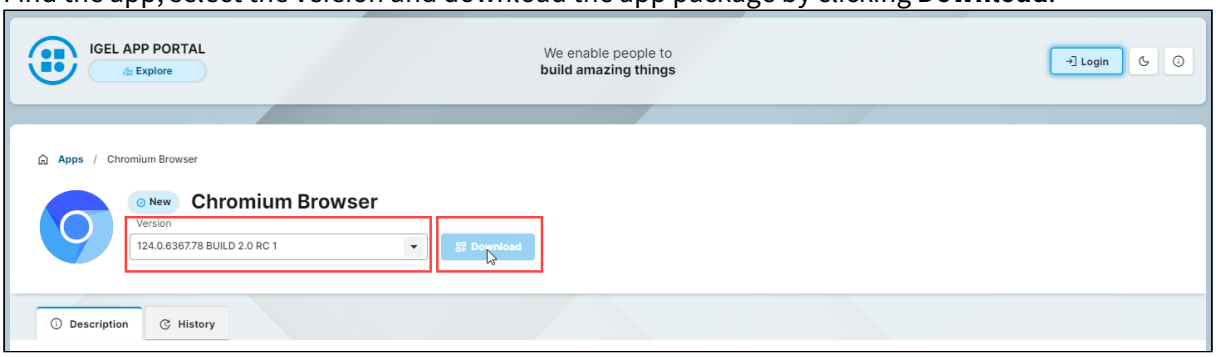
UMS without Internet Connection and OS 12 Devices with Internet Connection

When the UMS is not connected to the internet but the OS 12 devices are, you need to manually upload the apps to the UMS rather than importing them from the IGEL App Portal. Then the apps are assigned through the UMS and the devices get the app binaries from the Update proxy of the IGEL App Portal.
To install apps on OS 12 devices connected to the internet:

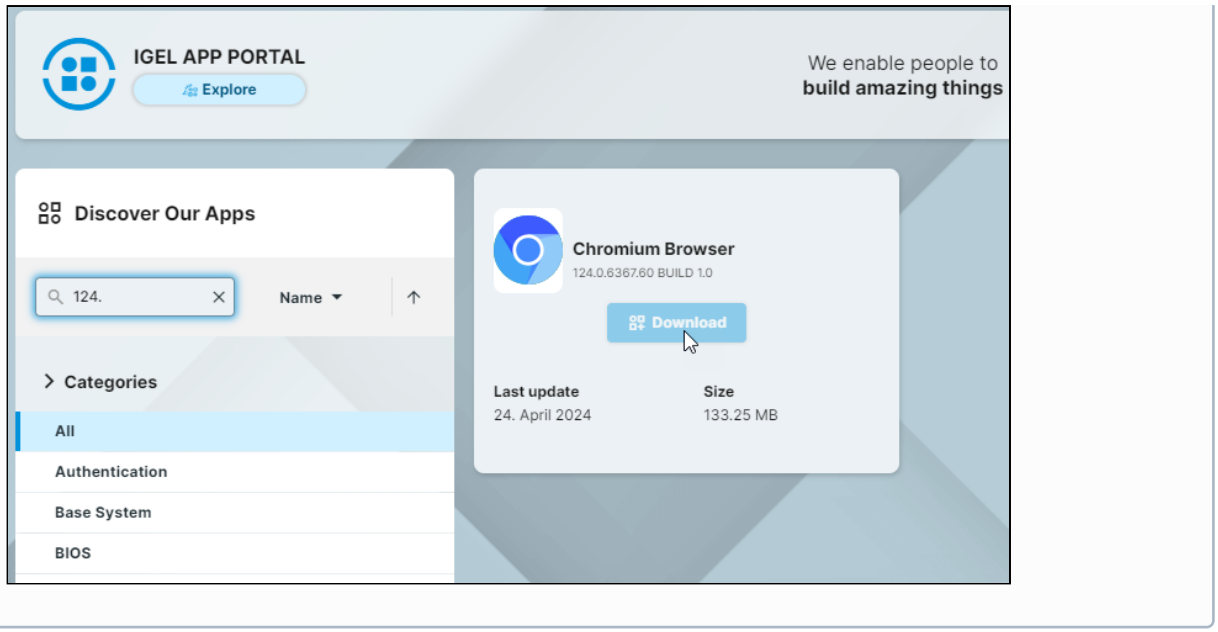
1. Log in directly to the https://app.igel.com/. For more information, see the article *How to Start with IGEL > IGEL App Portal*.



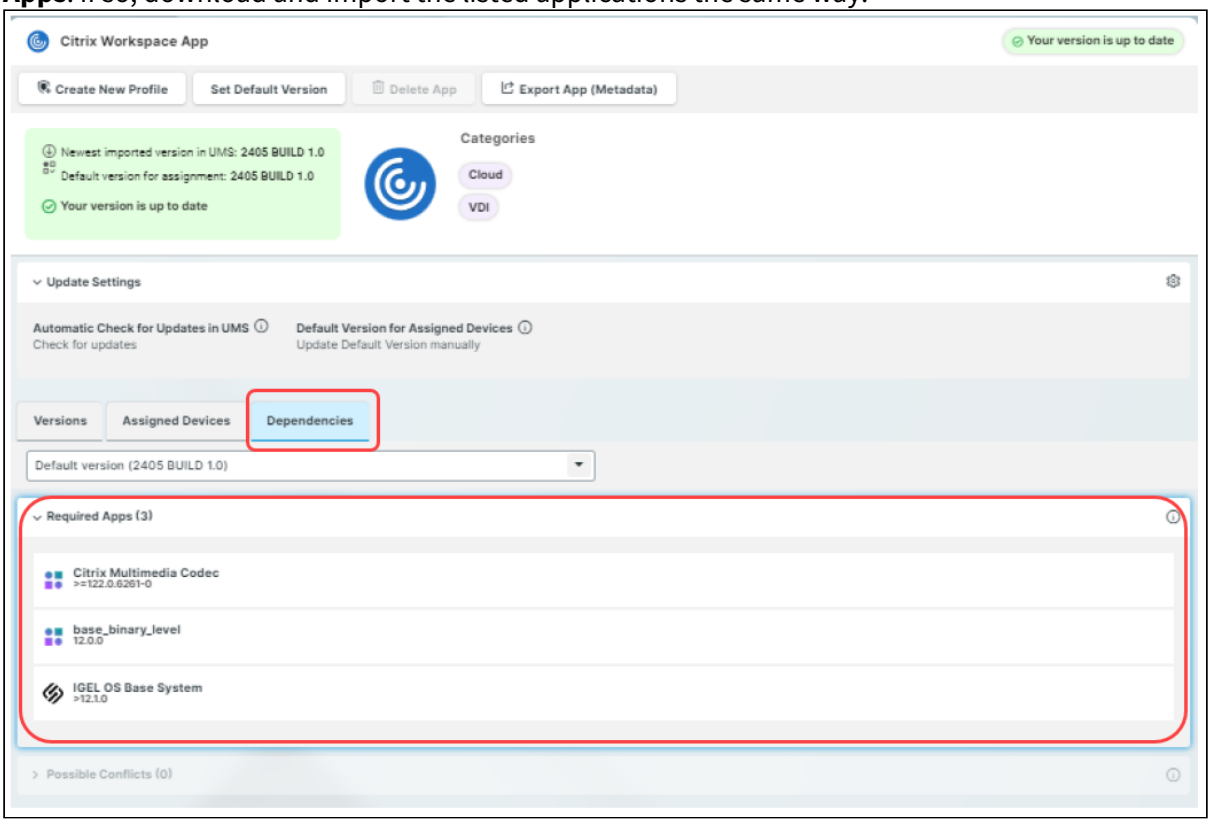
2. Find the app, select the version and download the app package by clicking **Download**.



If you click the **Download** action button in the cards view, you download the latest version of the app.



3. Import the downloaded `.ipkg` file to the UMS Web App as described in the Uploading Apps section under How to Export and Upload Apps to the IGEL UMS (see page 1338).
4. Check if the app requires any other applications to function under **Dependencies > Required Apps**. If so, download and import the listed applications the same way.



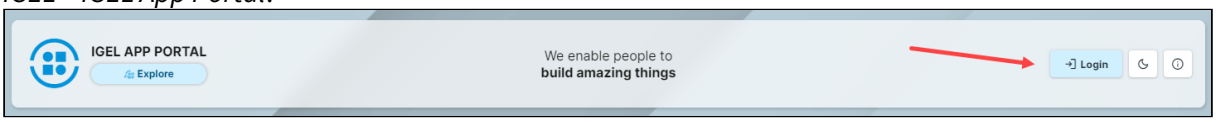
5. Assign the app to the devices. For detailed instructions, see How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).

   The devices will get the app meta data (`.iam`) from the UMS and the app binaries (`.ipkg`) from the IGEL App Portal by default.

UMS and OS 12 Devices both without Internet Connection

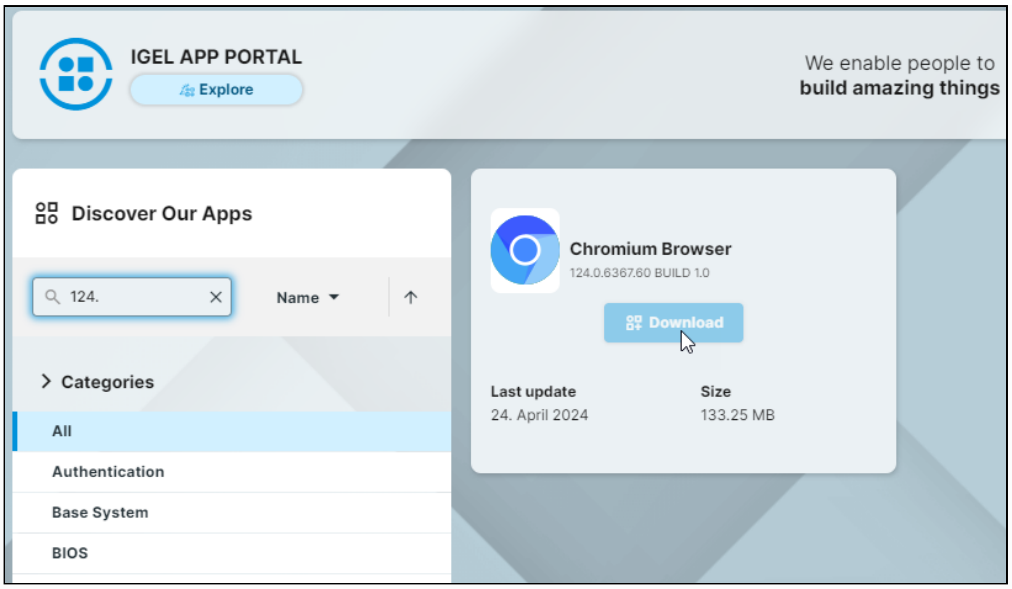
When both the UMS and the OS 12 devices are not connected to the Internet, you need to configure your UMS as an update proxy. This enables the devices to get the app binaries directly from the UMS.
To install apps on OS 12 devices without internet connection:

1. Log in directly to the https://app.igel.com/. For more information, see the article *How to Start with IGEL > IGEL App Portal*.



2. Find the app and download the app package by clicking **Download**.

If you click the **Download** action button in the cards view, you download the latest version of the app.

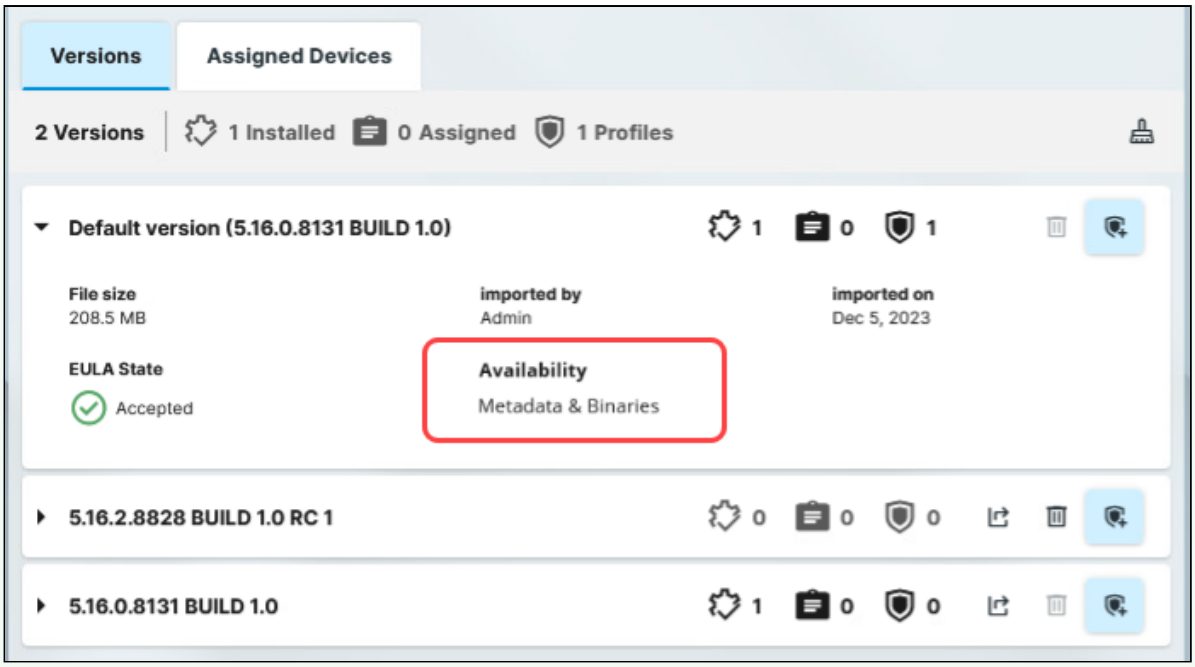


3. Set the UMS as the update proxy by selecting **Download from UMS** under **UMS Web App > Apps > Settings** > **UMS as an Update Proxy**. For details, see the UMS as an Update Proxy section under Configuring Global Settings for the Update of IGEL OS Apps (see page 1342).

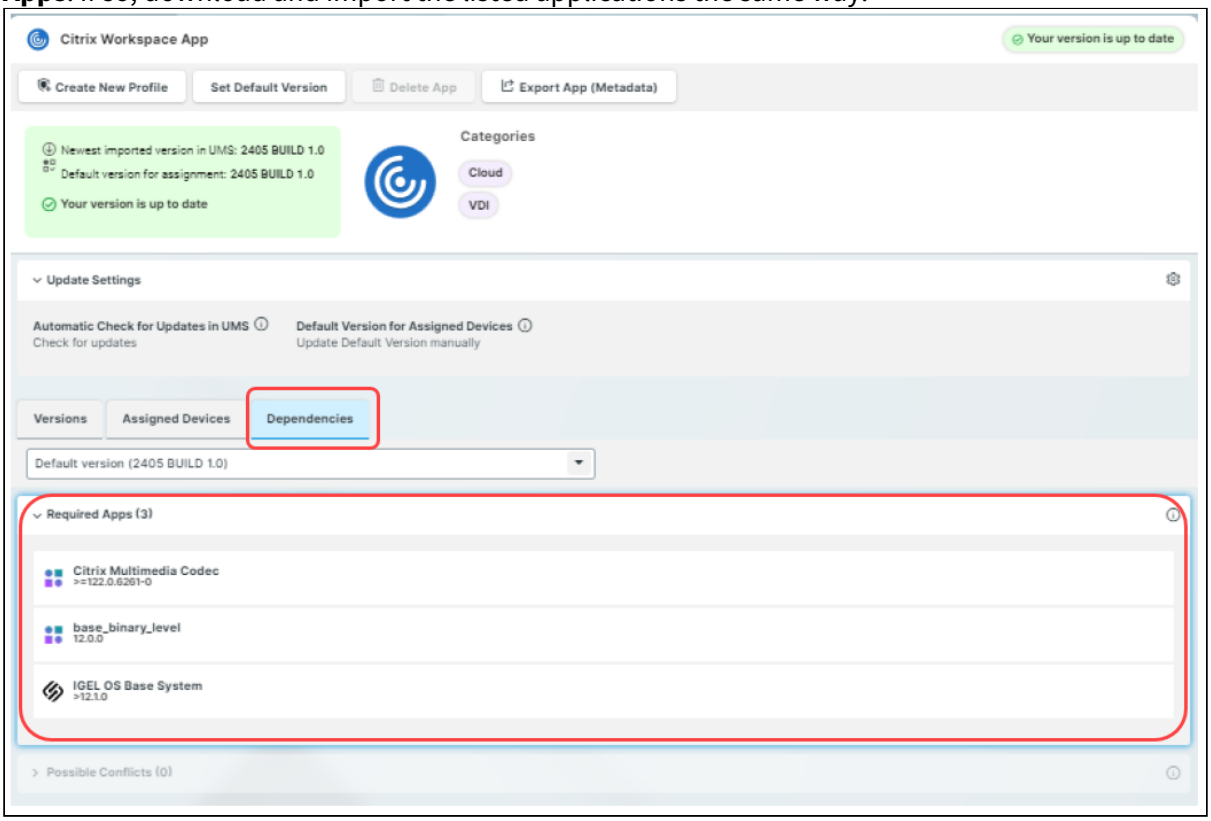
4. Optionally, configure distributed app repositories as described in How to Use Distributed App Repositories in IGEL UMS (see page 427) .
5. Import the downloaded `.ipkg` file to the UMS Web App as described in the Uploading Apps section under How to Export and Upload Apps to the IGEL UMS (see page 1338).

Check App Binary Availability

For a successful app deployment, both app binaries and app metadata need to be present in the UMS. You can check the availability for each app version in the **Versions** tab:



5. Check if the app requires any other applications to function under **Dependencies > Required Apps**. If so, download and import the listed applications the same way.



6. Assign the app to the devices. For detailed instructions, see How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).

The devices will get the app binaries directly from the UMS.

Troubleshooting

You get the following error message: "`Failed getting metadata from all APP Portals`".

Possible Reason

Microsoft Defender Antivirus blocked the UMS App Proxy functionality.

Solution

Create a local group policy or change the domain wide policy to exclude the `C:\Program Files\IGEL\RemoteManager` folder from Microsoft Defender Antivirus.

The policy can be found under: **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Exclusions > Path Exclusions**

The policy needs to be enabled and `C:\Program Files\IGEL\RemoteManager` to be added.

How to Set a Default Version of an App in the IGEL UMS Web App

If you have imported several versions of an app to the IGEL Universal Management Suite (UMS), you can define which version will be a **Default Version**.

Default Version is a version that will be assigned to a device / device directory if no version is specified during the assignment of an app (see How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313)) or during the creation of a profile configuring this app (see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252)).

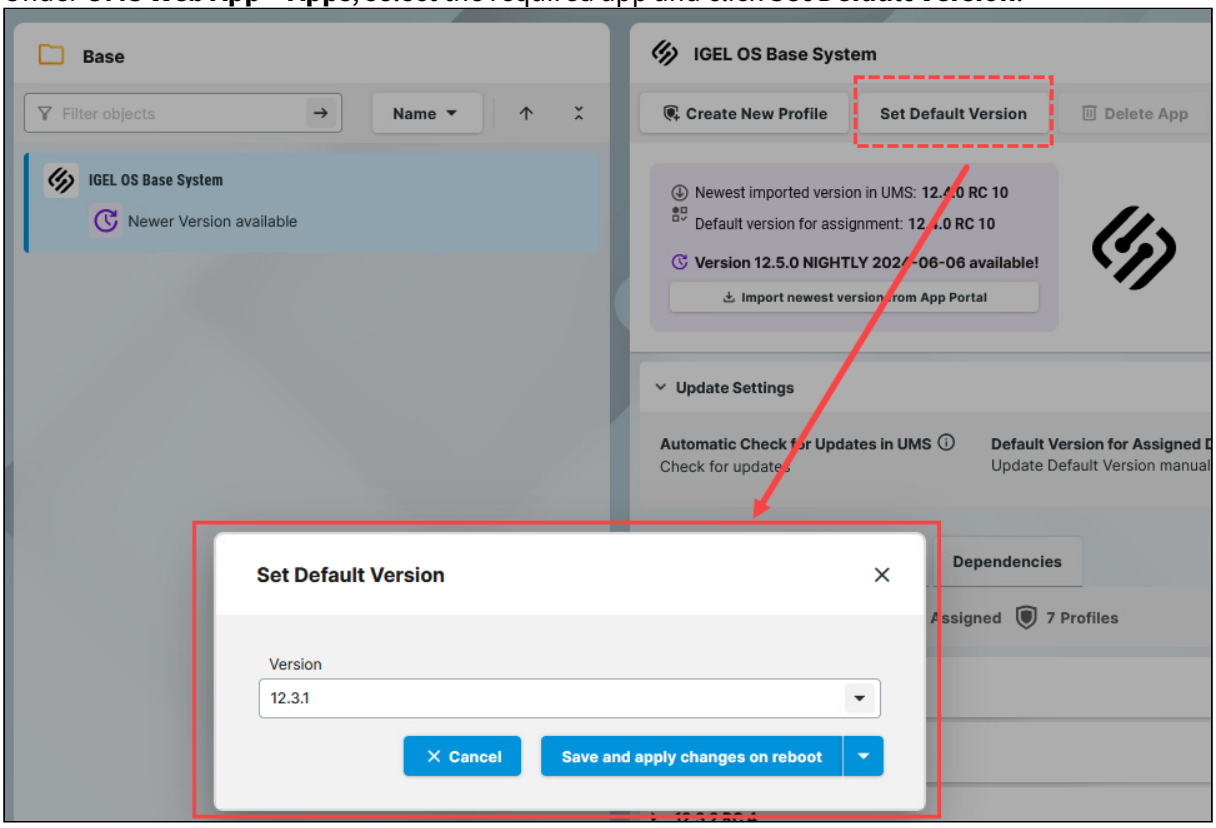
A **Default Version** is set globally: If changed, all assignments where no version was explicitly specified will change with it.

The best practice is to use the **Default Version** during the app assignment and profile creation.
The use of a specific version during the app assignment and profile creation is recommended for test purposes, e.g. to test app updates. After successful testing, you can change your Default Version.

Menu path: **UMS Web App > Apps**

To set a Default Version for an app:

1. Under **UMS Web App > Apps**, select the required app and click **Set Default Version**.



2. Select the desired Default Version.
3. Save the changes.

How to Assign Apps to IGEL OS Devices via the UMS Web App

In the IGEL Universal Management Suite (UMS), there are two methods to assign an app to your devices:

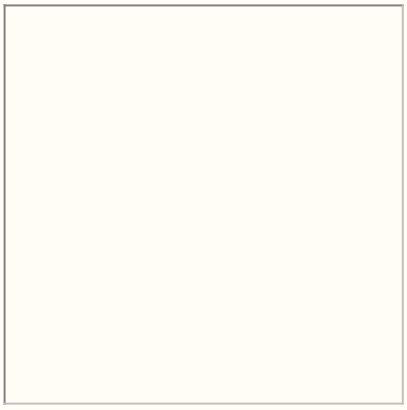
- Implicit app assignment via profiles: An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app. See How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).
- Explicit app assignment via the **Assign object** dialog, see below.

An explicitly assigned app ALWAYS overwrites an implicitly assigned app.

Explicit App Assignment

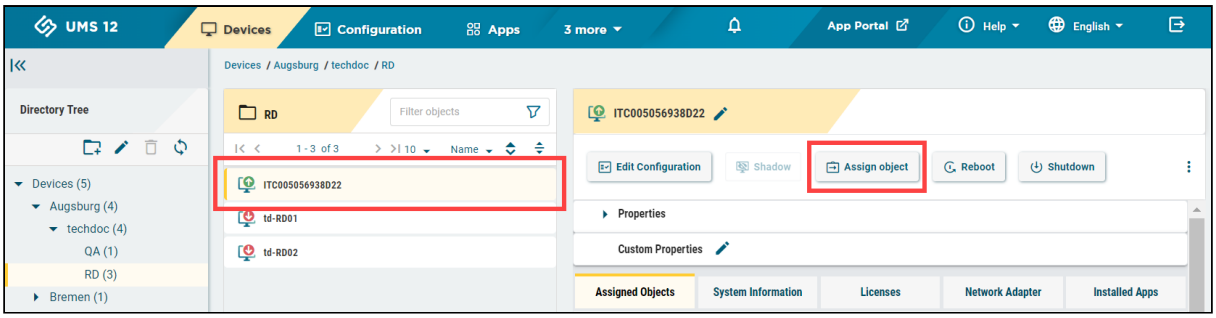
For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.
General information on rights and permissions can be found under How to Create Administrator Accounts in the IGEL UMS.

If various app versions have been assigned to a device (e.g. via direct and indirect assignment), the version which is closer to the device in the directory tree will have the priority and will be installed on the device.



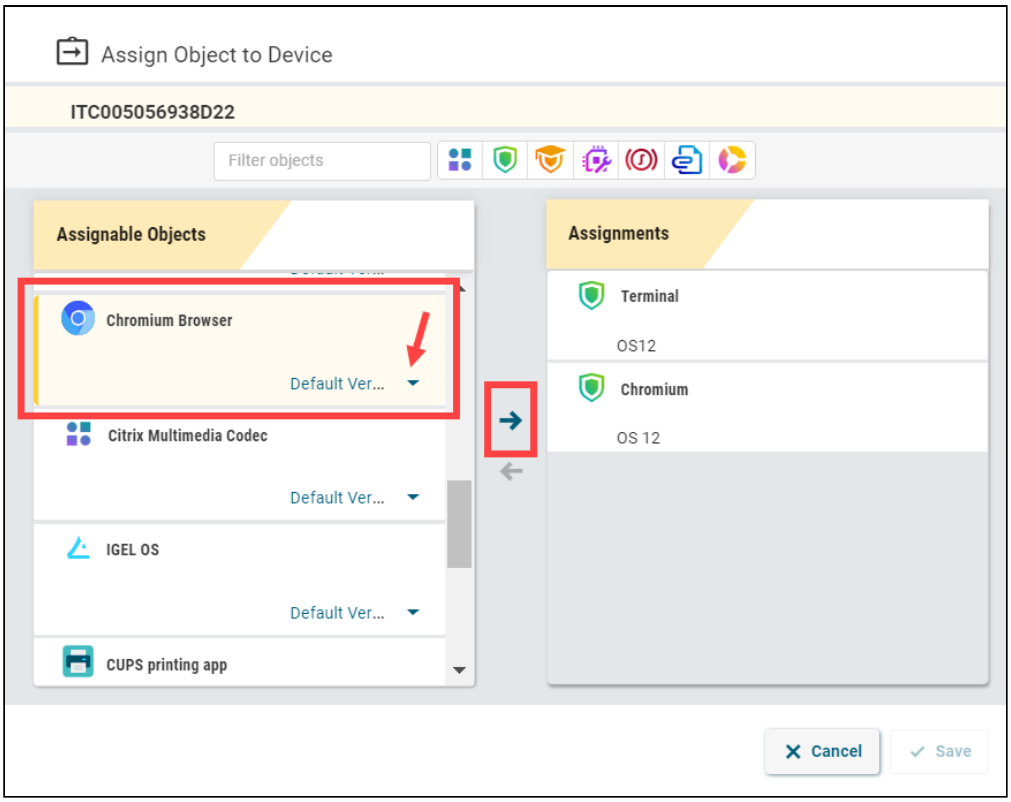
To assign apps to a device / device directory, proceed as follows:

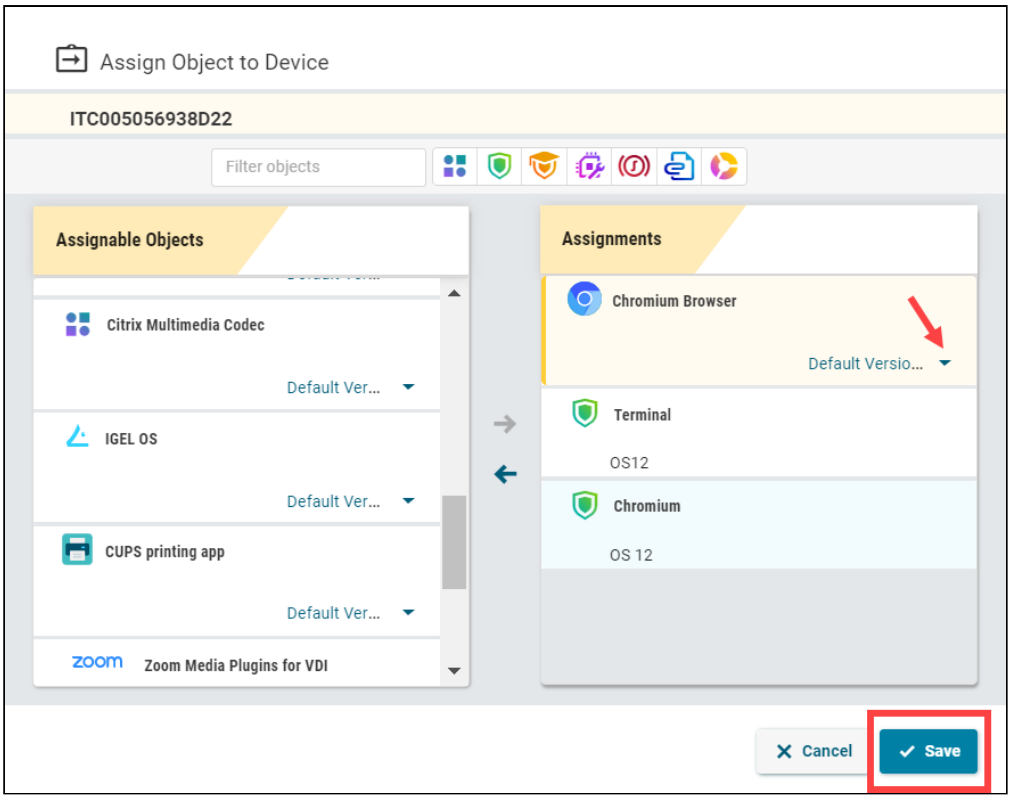
1. Under **UMS Web App > Devices**, select a device or device directory and click **Assign object**.



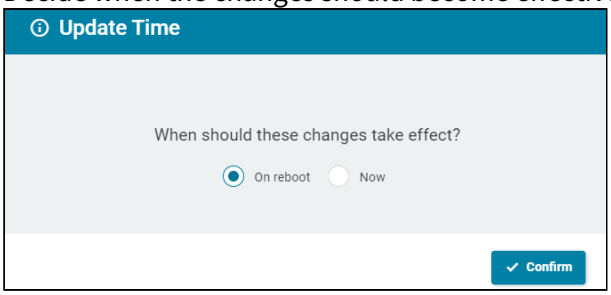
2. Select the required app (and its specific version, if necessary).

> If no version is specified for an app during the assignment, the Default Version (see page 1311) will be used. It is possible to select the version for an app in the **Assign Object** dialog either under **Assignable Objects** or under **Assignments**.



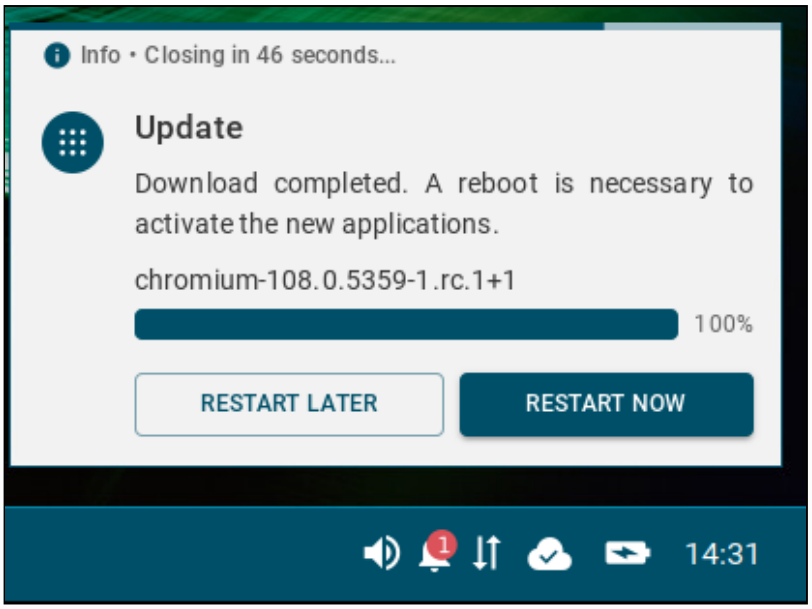


3. Save the changes.
4. Decide when the changes should become effective.



The app will be downloaded by the device.

By default, apps / app versions are automatically activated at the next reboot. The user will receive a corresponding notification.
Example:



If you have configured the background app update, an **Update** command must be sent, instead. For details, see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334).

The assigned app is displayed in the UMS Web App under **Devices > Assigned Objects**. To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App (see page 1317).

Checking Installed Apps via the IGEL UMS Web App

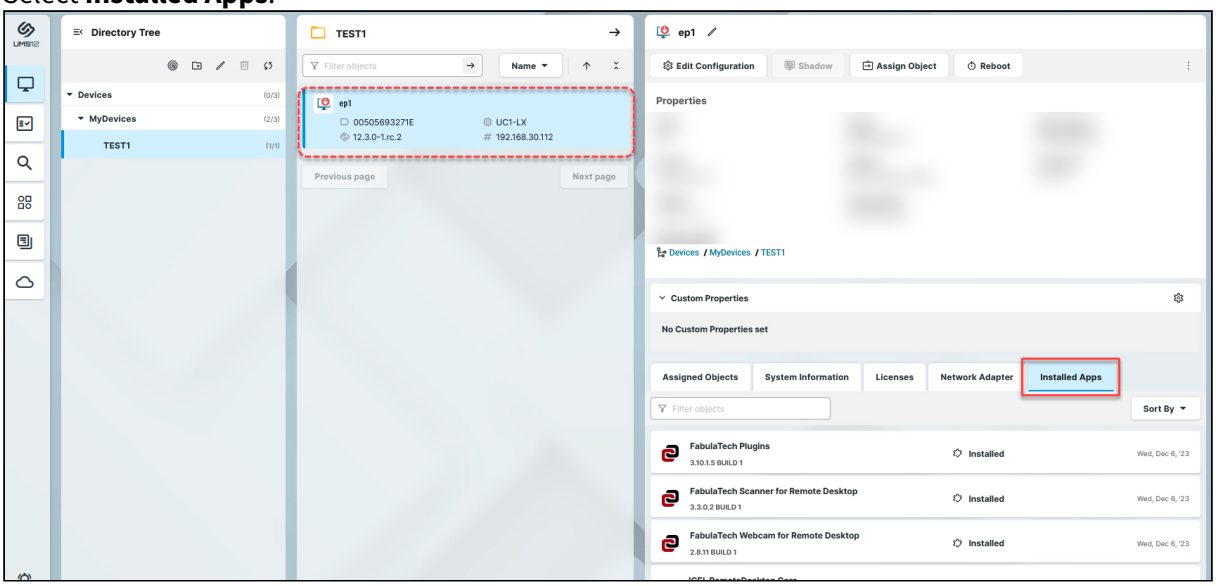
In the IGEL Universal Management Suite (UMS) Web App, you can view all apps installed on the IGEL OS device, their status and time when the message about the status is delivered.

Installed Apps ≠ Assigned Objects
Under **Installed Apps**, you may see apps that are not listed under **Assigned Objects**.
Typical examples:

- You have just onboarded your IGEL OS 12 device. The system will automatically recognize and show your IGEL OS base app under **Installed Apps**. You will not see this app under **Assigned Objects** unless you decide to assign, for example, a new version for it.
- Apps with no configurable parameters (e.g. dependant apps, codecs) such as Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec, are automatically installed on the device during the installation of the main app, e.g. Chromium Browser app, Citrix Workspace app. You will see them at first only under **Installed Apps**. However, if you decide to import another version of such an app and assign it to the device via the UMS, you will see it also under **Assigned Objects**.
- You decided not to use the UMS, but to install apps locally on the device. See e.g. (en) Installing IGEL OS Apps Locally on the Device.

To view the information about installed apps:

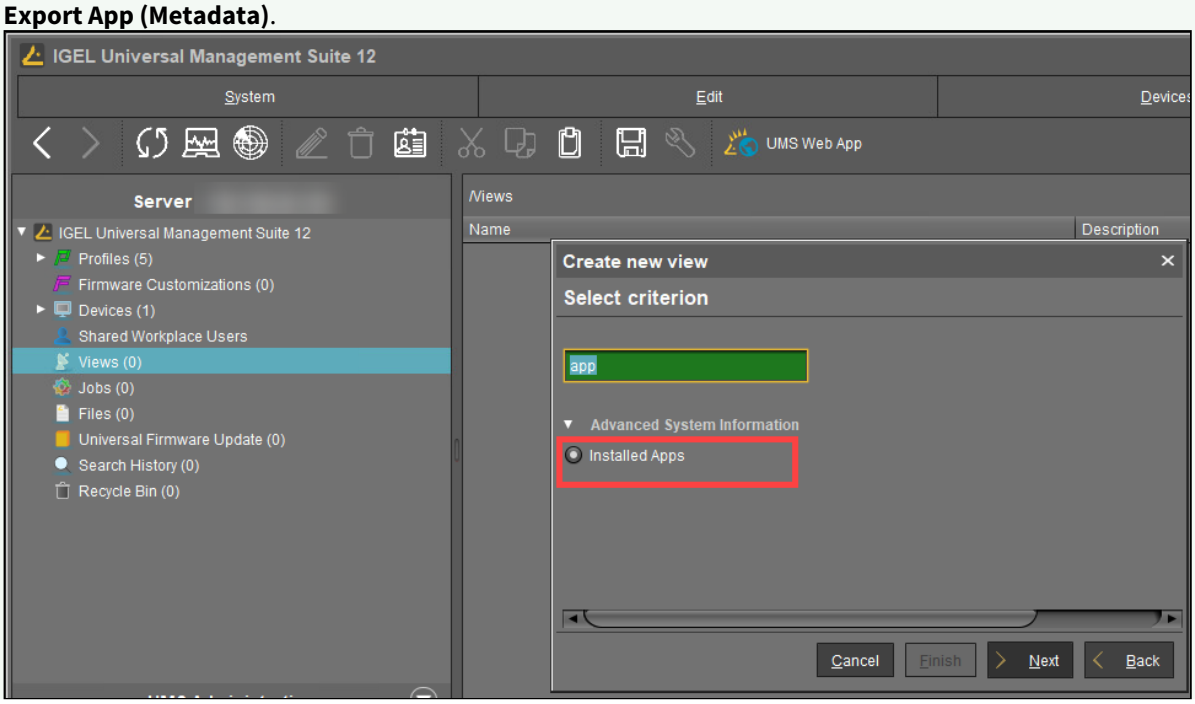
1. Under **Devices**, select the required device.
2. Select **Installed Apps**.

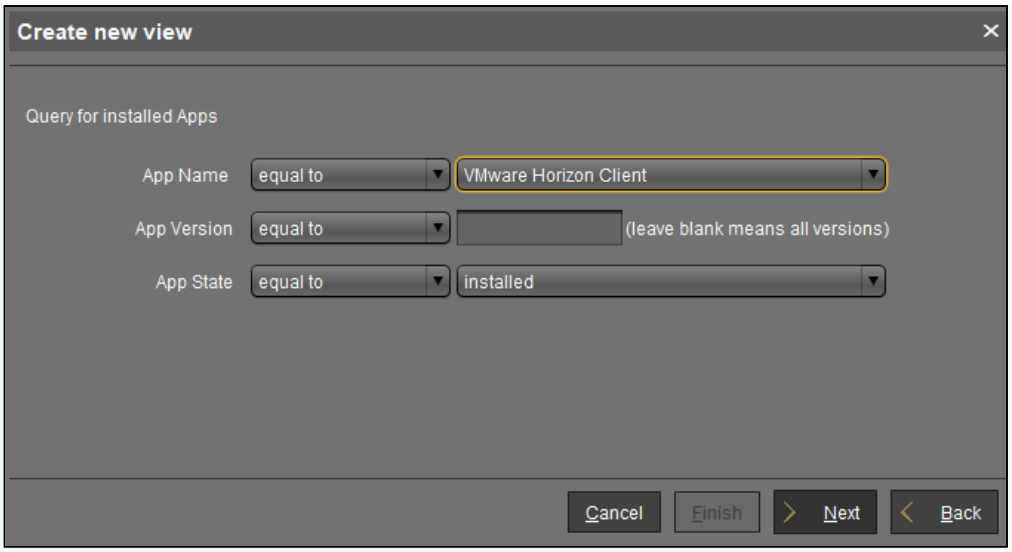


Status	Description
Installed	The app is currently installed and usable.
Downloaded	The app is successfully downloaded but needs manual activation. Use the **Update** command for this purpose.
Pending	The app download was requested but cannot be done because of the multistage update. The app will be downloaded in multiple stages. Trigger the process manually using the **Update** command.
Pending marked for installation	The app download was requested but cannot be done because of the multistage update. The app will be downloaded in multiple stages. The multistage update will be done on reboot.
Marked for installation	The app is successfully downloaded and will be activated on the next reboot.
Removal pending	The app has been removed but needs manual activation. Use the **Update** command for this purpose.
Marked for removal	The app will be removed on the next reboot.
Unusable	The app is installed but not usable. This can happen, for example, if the app requires a certain license, which the device does not have. Example: The device has a Starter license, and thus cannot use MMCP.
Download failed	Download of the app has failed. This can happen, for example, if the App Portal was not reachable or the device has no valid authentication token.
Activation failed	The app could not be activated because the multistage update was needed, but the App Portal was not available when activating the app. The device will repeat the app activation on the next reboot. If the background app update is configured, use the **Update** command, instead.
Limited functionality	The app partially works but some functionality is missing because of missing licenses. This can happen, for example, with the IGEL OS Base System app if a Starter license only or no license is available. As a result, multimedia codecs are disabled, and the base system is listed as limited functionality.
Dependency error	The app could not be installed because the dependencies are not met and could not automatically be resolved, for example, because a different version of IGEL OS Base System is required.

Status	Description
Note:	**Reboot** and **Update** commands can be found in the UMS Web App under **Devices** (see page 1176). The **Update** command is only required if the background app update is configured; see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334) .

To find out which devices have a certain app / app version installed or not installed, you can create a search in the UMS Web App (see page 1164), using the criterion **App Installed**.
You can also create a view in the UMS Console (see page 818) using the criterion **Installed Apps**. Under **App Version**, **you need to** specify a "technical" version of an app, e.g. `22.12.1-1.rc.2+1` (not `22.12.1 BUILD 1 RC 1`). The technical version can be found under **UMS Web App > Apps > [name of the app] > Export App (Metadata)**.




Create new view
Query for installed Apps
App Name
equal to
VMware Horizon Client
App Version
equal to
(leave blank means all versions)
App State
equal to
installed
Cancel
Finish
Next
Back

Detaching Apps from the IGEL OS Device in IGEL UMS Web App

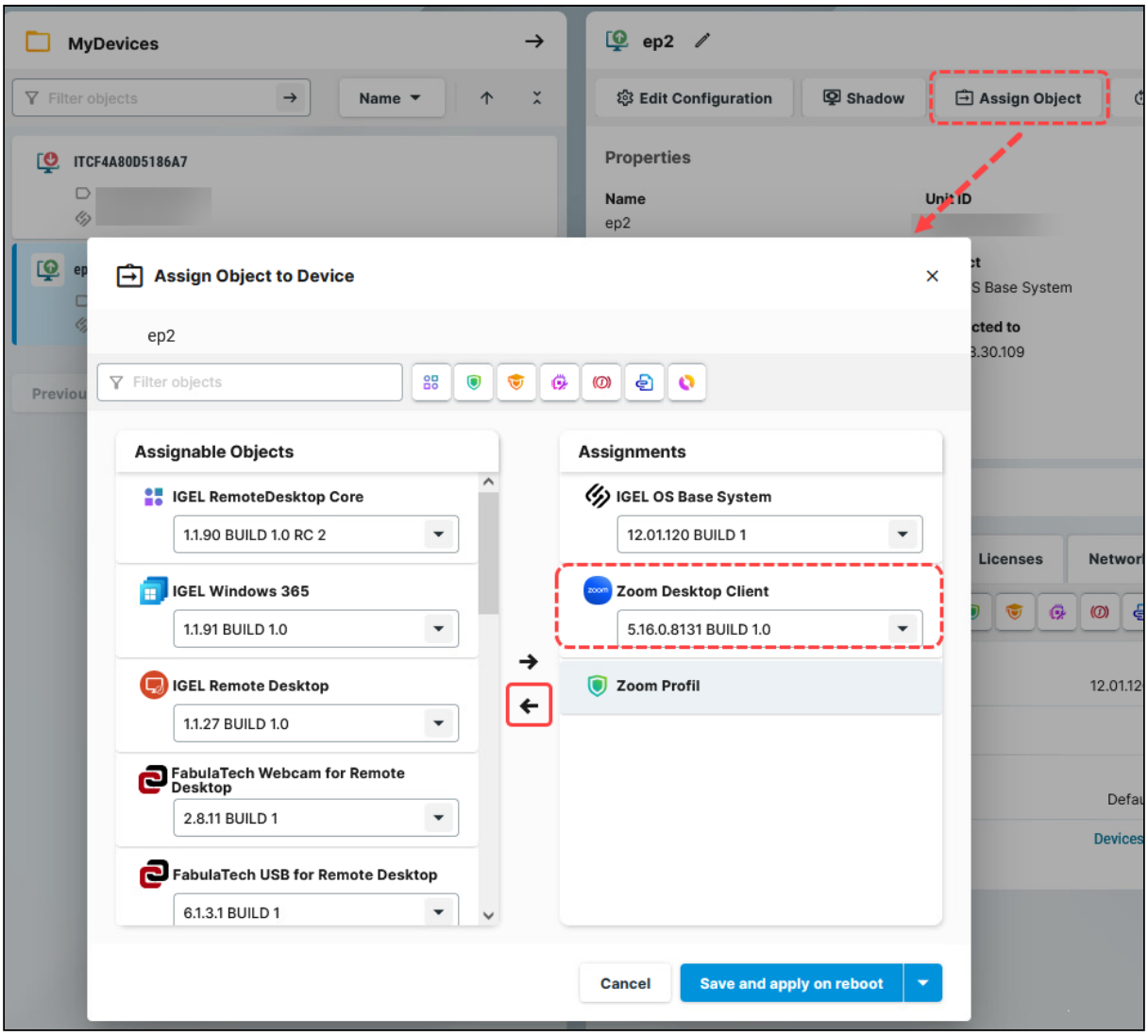
In the IGEL Universal Management Suite (UMS) Web App, you can detach apps that you no longer require.

> ⚠ In the case of the explicit app assignment: If you detach an app from a device, this app will be **uninstalled on the device**. Exception: IGEL OS Base System app is non-uninstallable.
> In the case of the implicit app assignment: If you detach a profile from a device, the app configured via this profile will be **uninstalled on the device**.
> For more information on implicit and explicit app assignment, see How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).

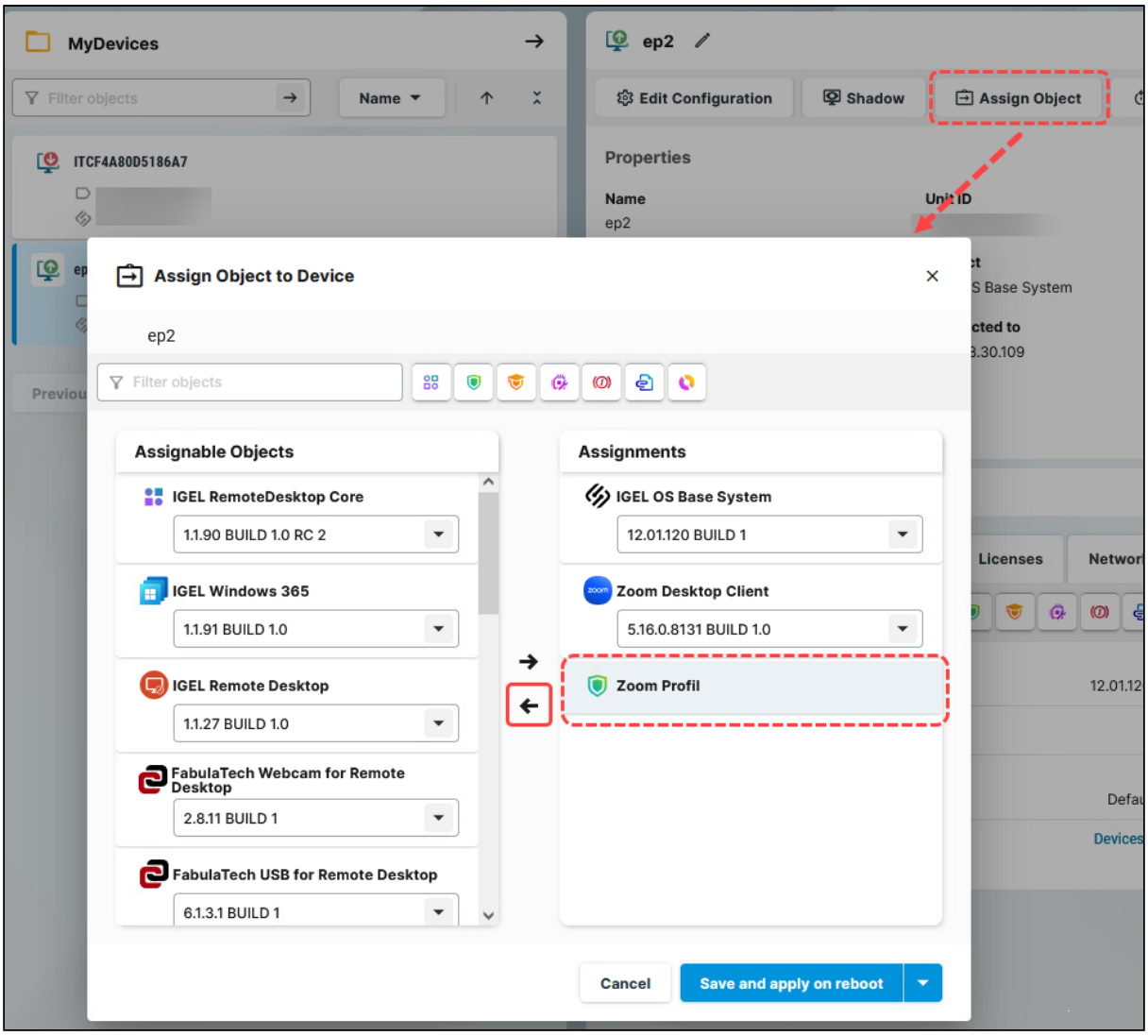
Menu path: **UMS Web App > Devices > [name of the device / device directory] > Assign object**

To detach an app from your device, proceed as follows:

1. Under **Devices**, select the device / device directory from which you want to detach an app and click **Assign object**.
2. Select the app to be detached or, in the case of the implicit app assignment, a profile via which this app is installed on the device, and click the left arrow button.
   In the case of the explicit app assignment:



In the case of the implicit app assignment:



3. Decide whether the new settings are to take effect immediately or at the next reboot of the device and save accordingly.
   If you have enabled the background app update (see page 1334), the **Update** command must be sent to activate the changes.

Quick Object Detaching

You can quickly detach objects from the devices through **Devices > [name of the device / device directory] > Assigned Objects** by clicking the **Detach object** button. For details, see How to Assign Objects in the IGEL UMS Web App (see page 1187).

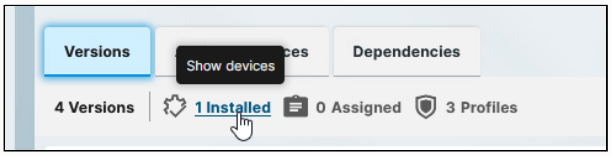
How to Delete Apps in the IGEL UMS Web App

In the IGEL Universal Management Suite (UMS) Web App, you can clean the app pool and delete apps and app versions that are no longer required.

Always follow the process described here for app deletion. Do not delete binaries directly from the cache of the UMS update proxy located in the folder `'rmguiserver/persistent/ums-appproxy/files'`.

Menu path: **UMS Web App > Apps**

Only unused apps / app versions can be deleted. You can check where the app is in use through the **Versions** tab.

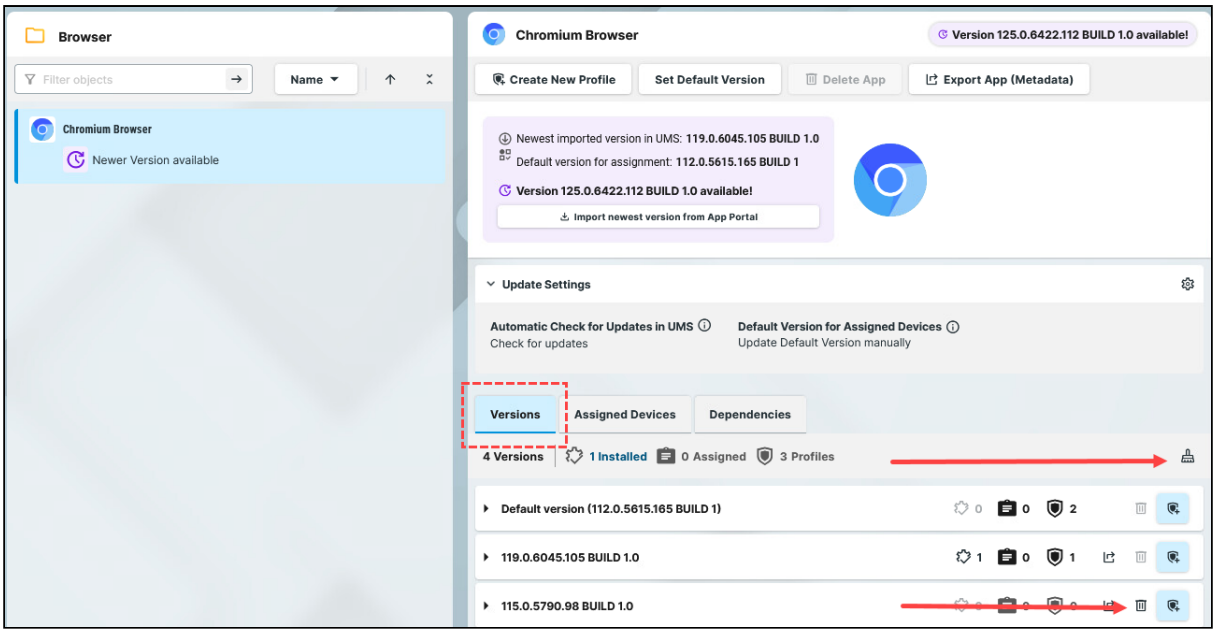


If you delete an app / app version, it will be immediately removed from the UMS, i.e. without moving to the recycle bin.
Tip: If all objects that use an app seem to be removed, but it is impossible to delete the app since the system declares it as used, check the recycle bin for devices and profiles that can still use the app and delete them. For more information on the recycle bin, see Recycle Bin - Deleting Objects in the IGEL UMS (see page 864).

Deleting an App Version

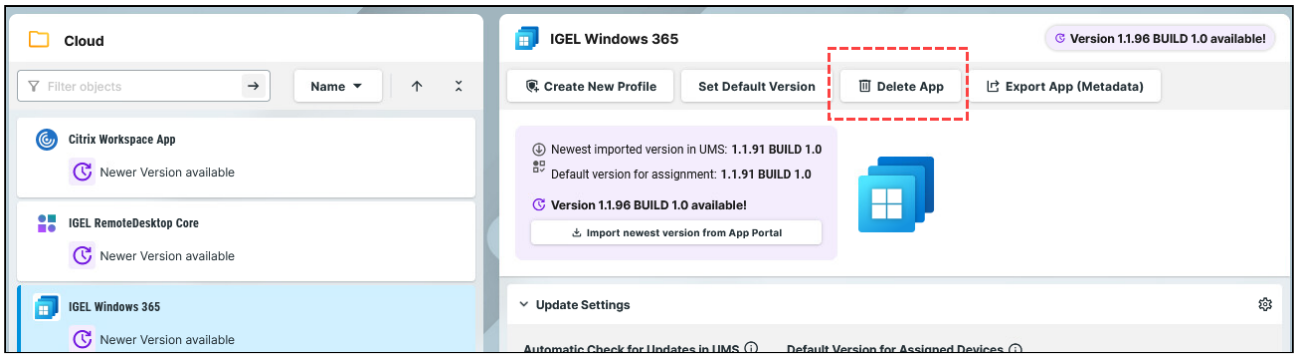
To remove an app version:

1. Go to the **Apps** and select the required app.
2. Click **Versions**.
   All available versions will be shown.



3. Click
   - the brush symbol to delete all unused versions, i.e. that are not installed, assigned, used in profiles, or set as a Default Version
   - [🗑] to delete a specific version

Deleting an App



To remove an app:

1. Under **Apps**, select the required app.
2. Click **Delete app**.
3. Confirm.

Updating IGEL OS Apps

The update procedure for the IGEL OS base system does not differ from the procedure for other apps. The update and downgrade procedures are also the same.

To update your apps, you have to

1. Configure global settings for app updates.
2. Configure update settings for individual apps.
3. Trigger the app update.

- How to Trigger the App Update in the IGEL UMS (see page 1327)
- Multistage Update of the IGEL OS Base System (see page 1331)
- How to Configure the Background App Update in the IGEL UMS Web App (see page 1334)
- How to Configure Update Settings for Apps in the IGEL UMS Web App (see page 1337)

How to Trigger the App Update in the IGEL UMS

IGEL Universal Management Suite (UMS) offers several possibilities to update your IGEL OS Apps. Generally, you can choose between changing the Default Version of an app or selecting a specific version.

The best practice is to use the **Default Version**.
Using a specific version is recommended for test purposes, e.g. to test app updates. After successful testing, you can change your **Default Version**.

The update procedure for the IGEL OS Base System does not generally differ from the procedure for other apps. The update and downgrade procedures are also the same.

For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.
For general information on rights and permissions, see How to Create Administrator Accounts in the IGEL UMS.

Options to Trigger the App Update

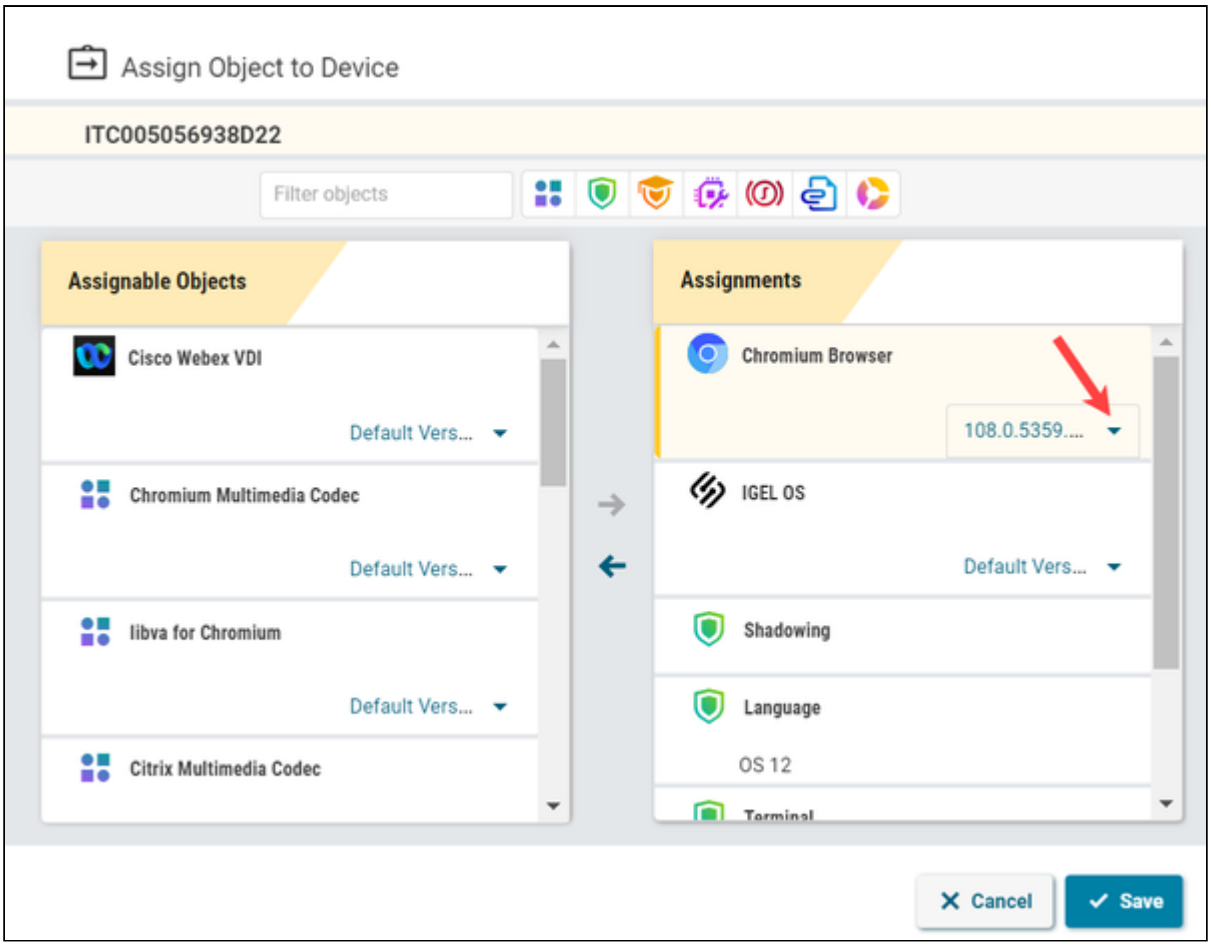
Remember that the app should already be assigned to the device. This fact can be forgotten, esp. if you update your IGEL OS Base System for the first time.

As soon as a new app version has been imported to the UMS, you can use one of the following options to start the app update:

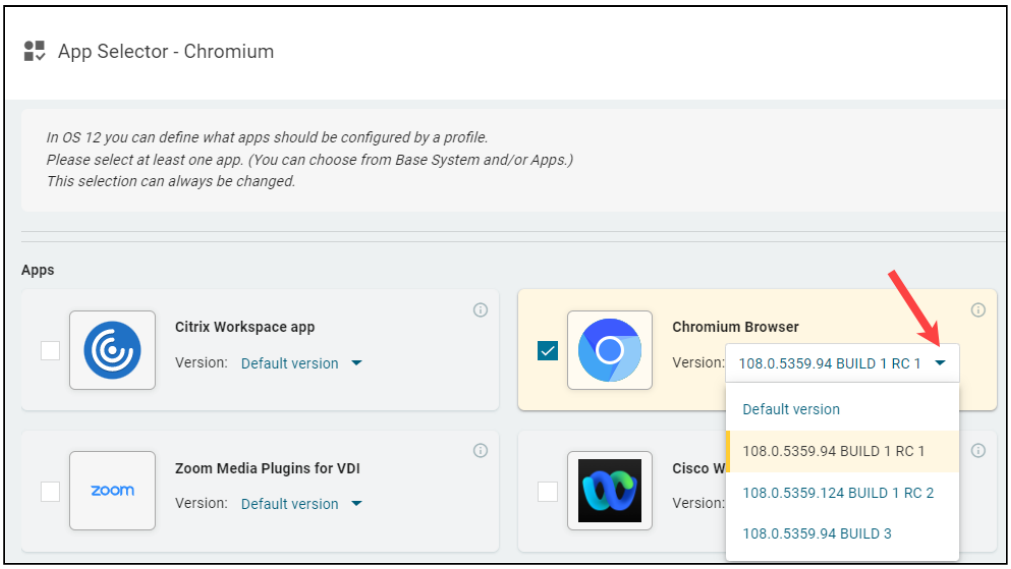
- Set manually the new version as a **Default Version** if you decided against **Auto-update Default Version to newest version** under **Apps > [name of the app] > Update Settings** (see page 1337).
  See How to Set a Default Version of an App in the IGEL UMS Web App (see page 1311)

Changing a **Default Version** should be a well-considered decision. Therefore, it is recommended to set a **Default Version** manually.

- In the case of the explicit app assignment: Go to **Devices > [device / device directory name] > Assign object** and select the new version under **Assignments**. For more information on the explicit app assignment, see How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).



- In the case of the implicit app assignment: Open a profile via which the app is assigned, click **Show Versions** in the upper right corner, and select the new version in the App Selector. For more information on the implicit app assignment, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).

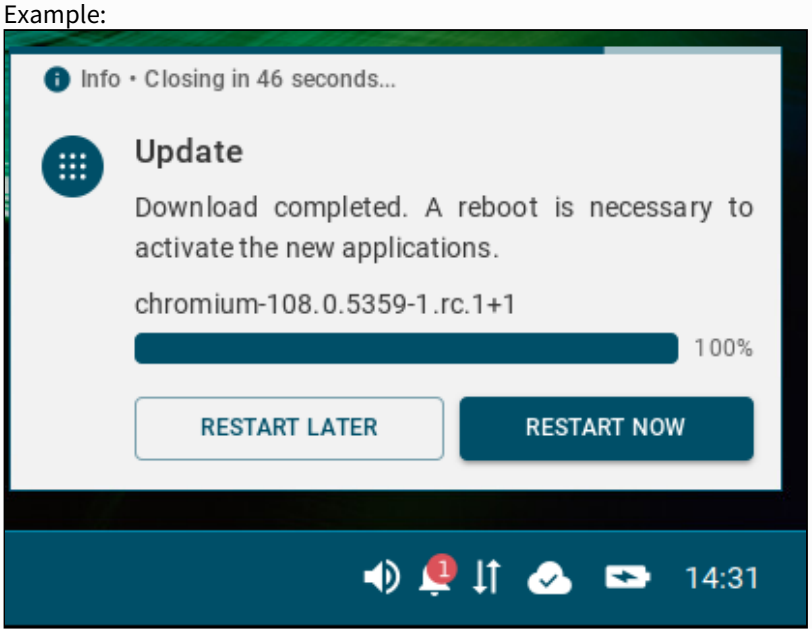


This method is NOT applicable to the IGEL OS Base System since the IGEL OS Base System app can only be assigned explicitly.

After the App Update Has Been Triggered...

After you have changed the Default Version or selected a specific version for the assigned app, this new version will be downloaded by the device.

By default, apps / app versions are automatically activated at the next reboot. The user will receive a corresponding notification.
Example:



If you have configured the background app update, an **Update** command must be sent, instead. For details, see How to Configure the Background App Update in the IGEL UMS Web App (see page 1334).

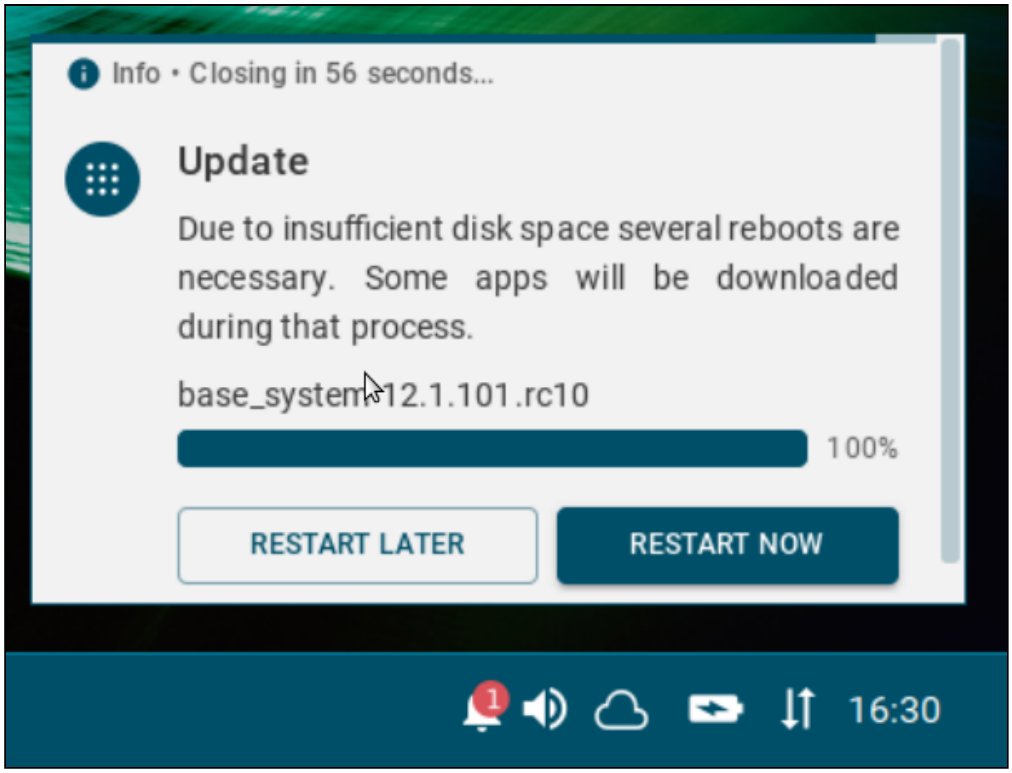
If there is not enough space for storing the new base system during the update of IGEL OS, the multistage update will be triggered. See Multistage Update of the IGEL OS Base System (see page 1331).

Multistage Update of the IGEL OS Base System

IGEL OS 12 supports the multistage update of the base system. During the multistage update, the device will automatically reboot multiple times.

> The multistage update is only triggered if there is not enough space for storing the new base system during the update of IGEL OS. This can happen, for example, on devices with small storage or with a large custom partition.

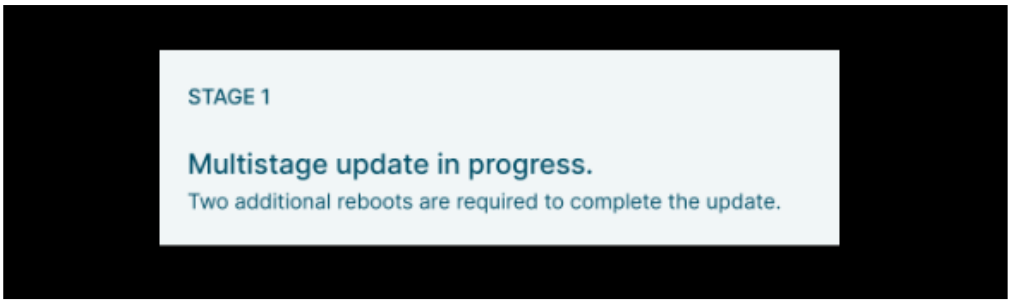
The user will receive a corresponding notification and can close opened applications to prevent data loss before the timeout for the restart is over. Alternatively, the user can postpone the reboot. For where to configure the timeout and reboot options for the app installation, see *How to Start with IGEL > IGEL OS Notification Center*.



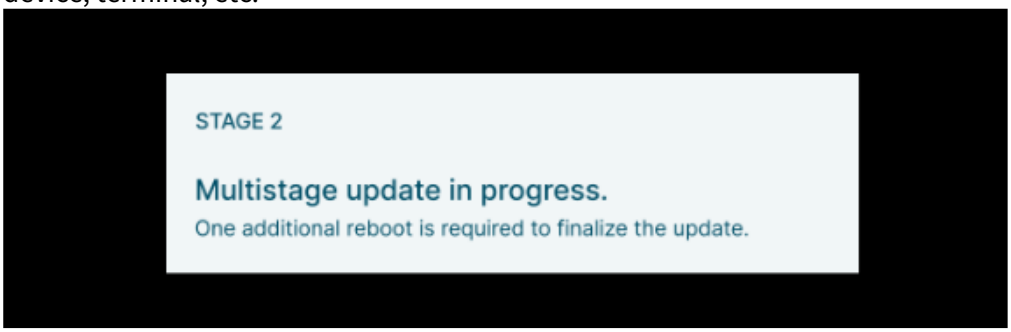
During the reboots, the user will be notified about each corresponding stage of the update process.

The multistage update includes the following stages:

- **Stage 1**: After the signal for the update is received, the system will reboot to the old system and will delete the installed apps and parts of the old base system to free as much space as possible. After that, the new base system will be downloaded.
  During this stage, the user will see only the following screen and cannot access the GUI of the device, terminal, etc.

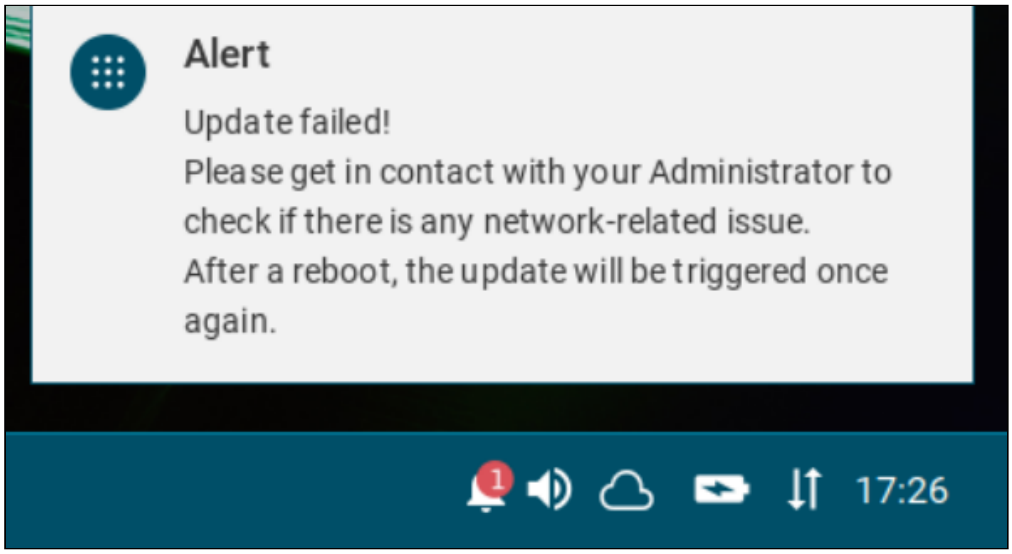


- **Stage 2**: The system will reboot to the new system and download the rest of the base system. During this stage, the user will see only the following screen and cannot access the GUI of the device, terminal, etc.



- **Stage 3**: The system will reboot to the new complete base system and will download all previously installed apps. The system will reboot and activate all apps.

If the multistage update fails for some reason, the system will boot again in the GUI with the minimal system required for that and will show the following message. Depending on the stage when the failure happens, apps may not be present in the system.



Possible reasons for the failure of the multistage update can be, for example:

- Unstable network connection during the update process.

> The network connection is checked only initially, i.e. before the multistage update starts: If no network connection can be established within 60 seconds, the multistage update will be aborted. You can change this parameter under **System > Update > Seconds to wait for network connection during a multistage update**.

- Expired license (no matter if it is a Starter, Demo, or Workspace Edition license) if the background app update (see page 1334) is enabled.

If the multistage update fails, it is recommended to check the log file `/wfs/update_<time>.log`.

You may find it also useful to activate debugging as described under *How to Start with IGEL > Debugging / How to Collect and Send Device Log Files to IGEL Support.*

How to Configure the Background App Update in the IGEL UMS Web App

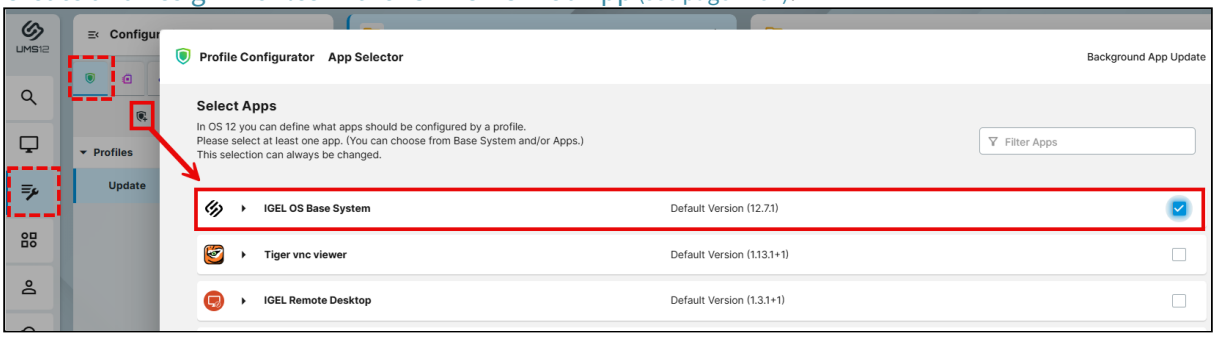
By default, apps / app versions assigned to the device will be downloaded and automatically activated at the next reboot. This is regulated by the IGEL OS setting **System > Update > Action after app assignment from UMS > Download and activate (Apps usable after reboot)**, see Update - App Update Settings in IGEL OS 12[209].

If you have a slow bandwidth connection or do not want the users to be disturbed while updates are being performed, you can activate the background app update. In this case, the manual app activation via the **Update** command in the UMS will be required.

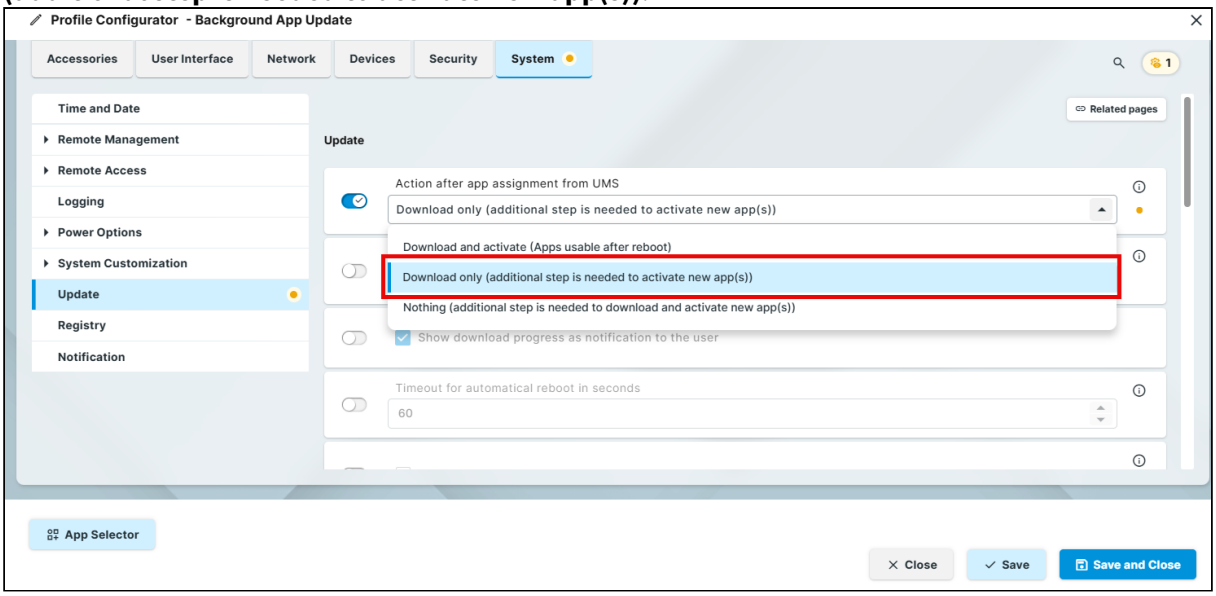
Alternatively, you can configure a timed update, see Custom CronJob/Systemd Timer in IGEL OS 12[210].

To enable the background app update:

1. Create a profile for the IGEL OS base system. For details on how to create profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).



2. Under **System > Update > Action after app assignment from UMS**, select **Download only (additional step is needed to activate new app(s))**.

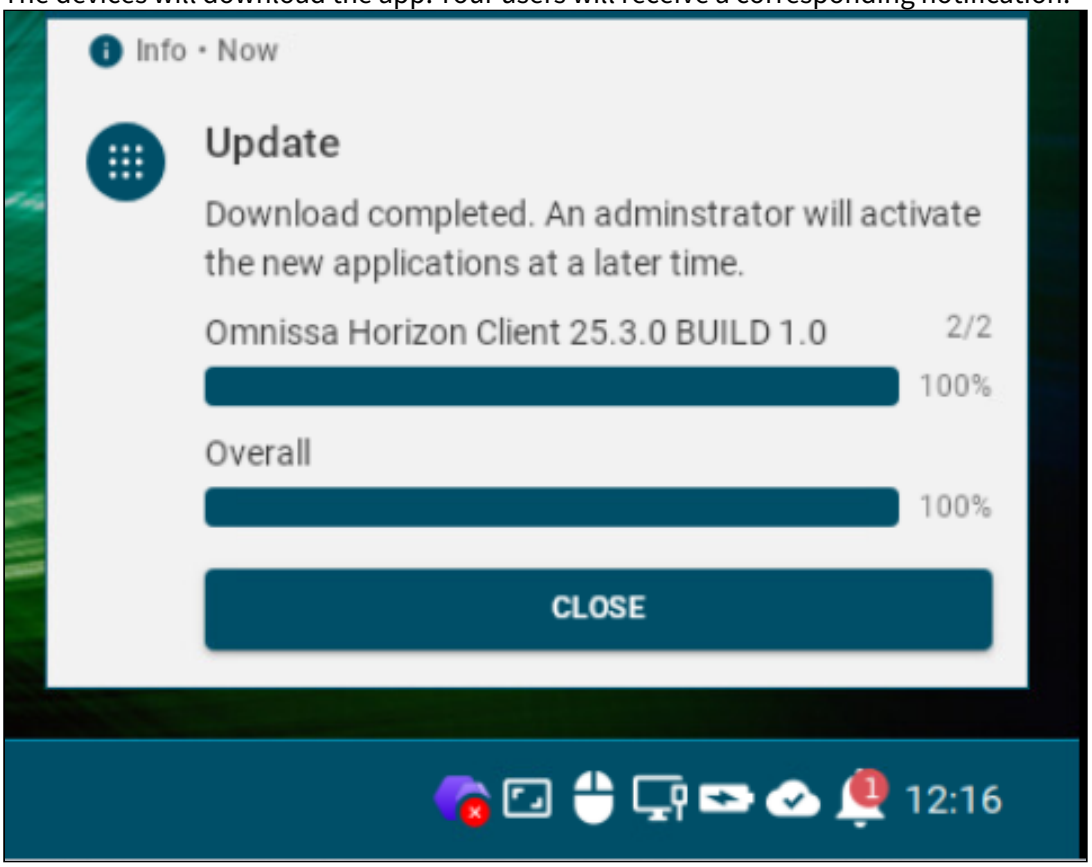


209. https://kb.igel.com/en/igel-os-base-system/current/update-app-update-settings-in-igel-os-12
210. https://kb.igel.com/en/igel-os-base-system/current/custom-cronjob-systemd-timer-in-igel-os-12

3. Optional: If you need to limit the bandwidth usage during the app download (e.g. if you see that updates affect the performance of the network), activate **Use a bandwidth limit while updating** and define the required limit under **Limit bandwidth used for updating**.

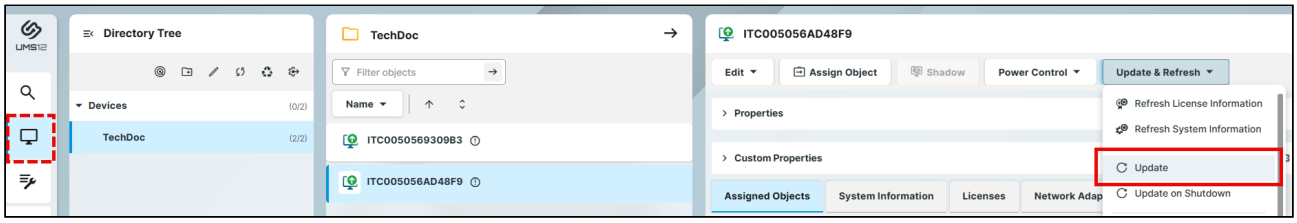
   When specifying **Limit bandwidth used for updating**, note the following:
   - Do NOT use spaces between the number and the unit.
   - Use only `KB`, MB, and `GB`.
   - If no unit is specified, megabytes (MB) will be used.
   - If the limit is specified incorrectly, the default value (`2MB`) will be used.

4. Save the settings.
5. Assign the profile to the devices under **Devices > [name of the device / device directory] > Assign object**. For details on how to assign profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).
6. Assign the required app / app version or a profile configuring the required app to your devices. See How to Assign Apps to IGEL OS Devices via the UMS Web App (see page 1313).
   The devices will download the app. Your users will receive a corresponding notification:



7. You can activate the apps at a later date by sending the **Update** command under **UMS Web App > Devices**.

Before triggering the **Update** command, you may want to check if all apps have been successfully transferred to the devices. You can find the status of apps under **Devices > [name of the device] > Installed Apps**, see Checking Installed Apps via the IGEL UMS Web App (see page 1317).



Alternatively, you can create a scheduled job for the **Update** command in the **UMS Console > Jobs** and assign it to the devices / device directory or a view. The app activation will be performed on the corresponding devices according to the schedule specified in the job. For more information on jobs, see Jobs - Sending Automated Commands to Devices in the IGEL UMS (see page 847) .

If You Want to Switch Back to the Default Behavior
Before deactivating the background app update, it is recommended to send the **Update command** to all devices and verify that apps have successfully been installed.

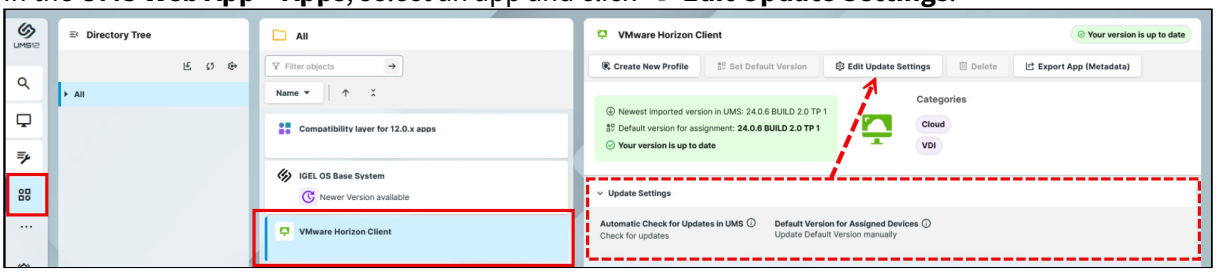
How to Configure Update Settings for Apps in the IGEL UMS Web App

For each app in the IGEL Universal Management Suite (UMS) Web App, you can define the update settings.

Menu path: **UMS Web App > Apps > [name of the app] > Edit Update Settings**

To configure the update settings for an individual app:

1. In the **UMS Web App > Apps**, select an app and click **Edit Update Settings**.



2. Select the required settings:
   Automatic check for updates in UMS
   - **Check for updates** (Default): The UMS automatically checks if a newer version of the app is available in the IGEL App Portal. The check is performed every 120 minutes (can be configured under **Apps > Settings > Automatic Updates** (see page 1342)). You can trigger the import into the UMS by clicking the **Import newest version from App Portal** button.
   - **Check for updates and auto-import into UMS**: If available, a newer version of an app will be automatically imported from the IGEL App Portal. The automatic check for updates is performed every 120 minutes (can be configured under **Apps > Settings > Automatic Updates** (see page 1342)).
   - **Do not check for updates**: It will not be automatically checked if a newer version of the app is available in the IGEL App Portal. You can manually check for updates by clicking the **Check for updates** button.

   Default Version for assigned devices
   - **Auto-update Default Version to newest version**: The newest imported version of an app will be automatically set as a **Default Version**. This does not apply to the already imported versions.

     > It is recommended to set a **Default Version** manually since a Default Version is set globally: If changed, all assignments where no version was explicitly specified will change with it.

   - **Update Default Version manually** (Default): You can manually select which version will be a **Default Version**, see How to Set a Default Version of an App in the IGEL UMS (see page 1311).

3. Save the settings.
   The configured settings can be viewed in the **Update Settings** area.

How to Export and Upload Apps to the IGEL UMS

In the IGEL Universal Management Suite (UMS) Web App, you can export apps and upload them. This can be helpful for support purposes or when transferring app data from one UMS installation to another.

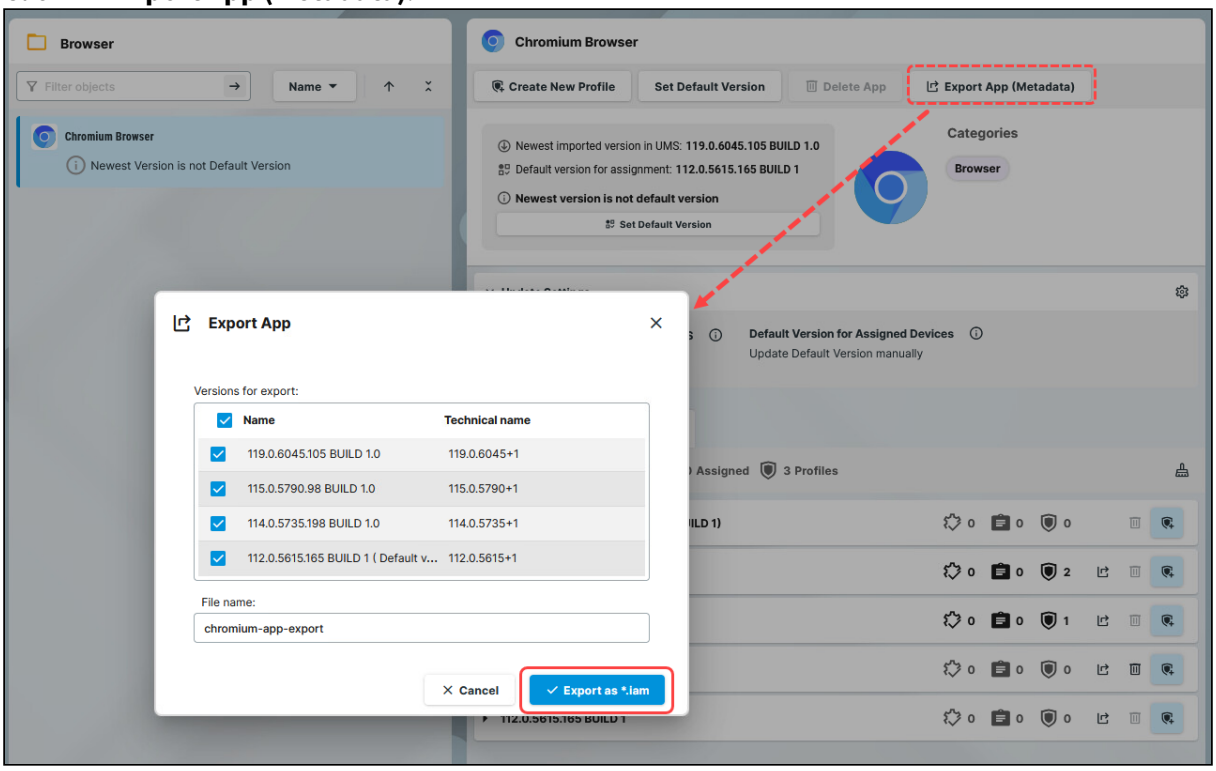
> Currently, it is possible to export only app metadata, i.e. no app binaries.

Menu path: **UMS Web App > Apps**

Exporting Apps

To export an app:

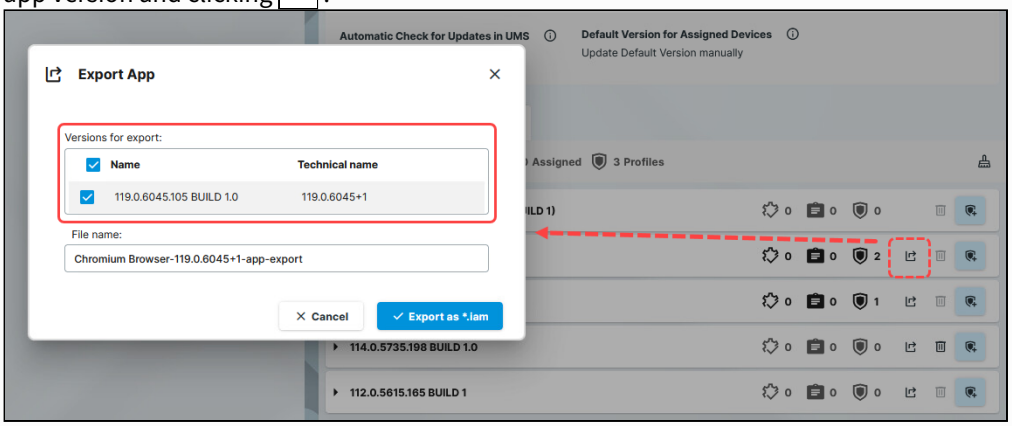
1. In the **UMS Web App > Apps**, select the required app.
2. Click **Export App (Metadata)**.



3. Select the app versions you want to export.
4. Specify the **file name**.
5. Confirm the export.

   The metadata of the selected app version(s) will be saved in an `.iam` file and can now be uploaded, for example, to another UMS installation.

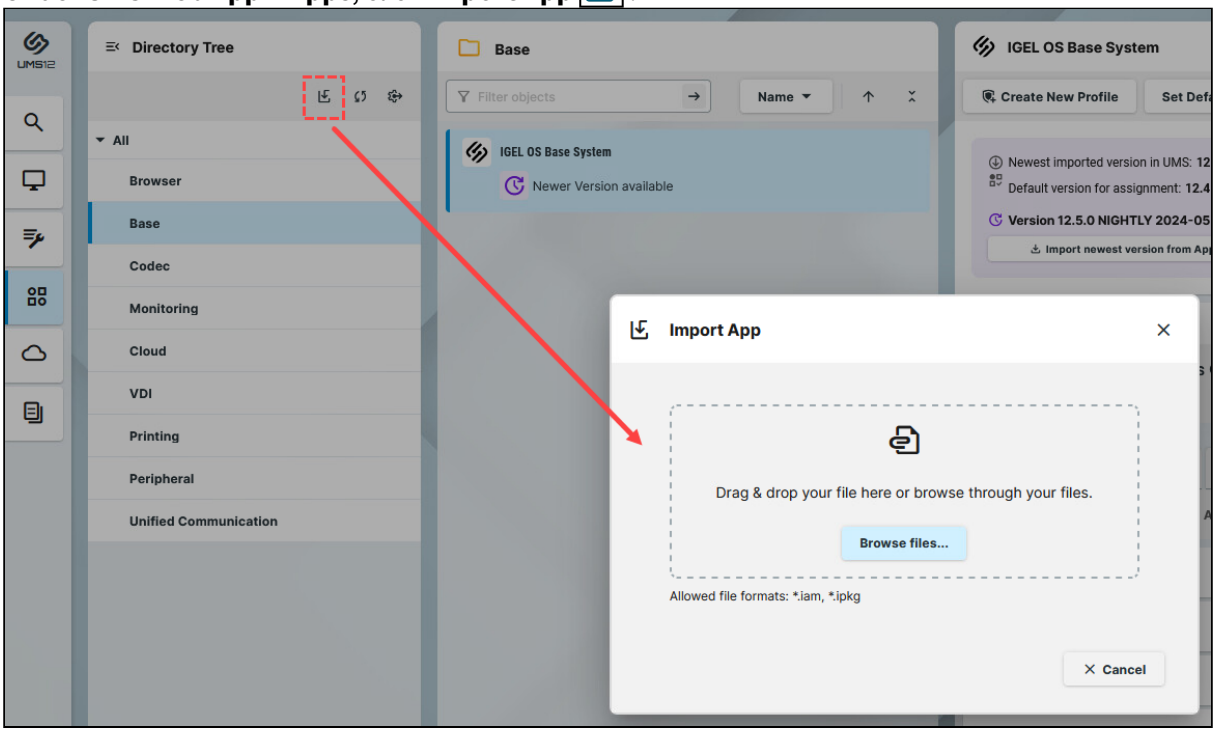
If you want to export a specific version of an app, you can also do that in the **Versions** tab by selecting the app version and clicking .



Uploading Apps

To upload an app to the UMS:

1. Under **UMS Web App > Apps**, click **Import App** .



2. Select the required file.

Only files in the `.iam` and `.ipkg` format can be uploaded. The `.iam` format includes the app metadata only, the `.ipkg` format includes the app metadata plus the app binaries.
In an air-gapped environment, always upload `.ipkg` files (i.e. metadata + binaries) because the UMS has no connection to the IGEL App Portal, and has no other way of downloading the app binaries. If you upload `ipkg` files, both the metadata and binaries of the imported apps are cached in the local cache of the UMS update proxy; the app binaries are cached in `[IGEL installation directory]/rmguiserver/persistent/ums-appproxy/files`.

3. Confirm the upload.
   You will receive a confirmation message and the uploaded app will be automatically placed in the corresponding app directory in the directory tree. You can now assign the app to your endpoint devices or create profiles that configure this app.

How to Make Devices Download from App Portal when UMS is Configured as the App Proxy as the Global Setting

When the global setting under **Apps > Settings > UMS as an App Proxy** is set to **Download from UMS**, that means that all devices managed by the UMS download the apps from the UMS server, see Configuring Global Settings for the Update of IGEL OS Apps (see page 1342). But if you would like to have certain devices download directly from the App Portal, you can do that through using a profile as described below.

Create the Profile

To create a profile that tells the devices to download directly from the App Portal, use the setting options on Update - App Update Settings in IGEL OS 12[211] :

1. Create a new profile. For more on profiles, see How to Create and Assign Profiles in the IGEL UMS Web App (see page 1252).
2. Under **System > Update > Repositories** set the following:
   Priority: 500
   Repository URL: https://app.igel.com/api
   Certificate: /etc/ssl/certs
3. In addition to this, if you have a cluster address configured, add the following to the profile mentioned above.
   Priority: 400
   Repository URL: https://<yourclusteraddress.domainname.com>:8443/ums-appproxy
   Certificate: /etc/ssl/certs

Test the Profile

To test the configuration:

1. After configuring the above, assign the profile to a test device.
2. Run the command `igelpkgctl update` on the test device.
   `http://app.igel.com` should get processed first.

Assign the Profile

Assign the profile to the devices that need to download directly from the App Portal.

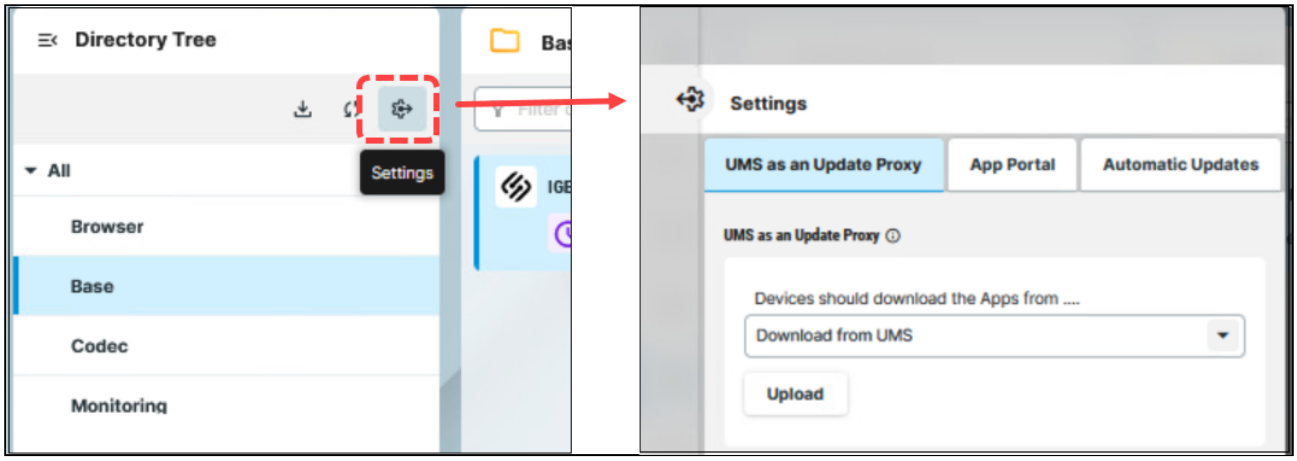
You can assign to the device directory that the devices register to through default directory rules.

211. https://kb.igel.com/en/igel-os-base-system/current/update-app-update-settings-in-igel-os-12

Configuring Global Settings for the Update of IGEL OS Apps

When preparing for updating your IGEL OS Apps, you have to first check if the global update settings set by default in the IGEL Universal Management Suite (UMS) suit your needs and, if not, adjust them accordingly.

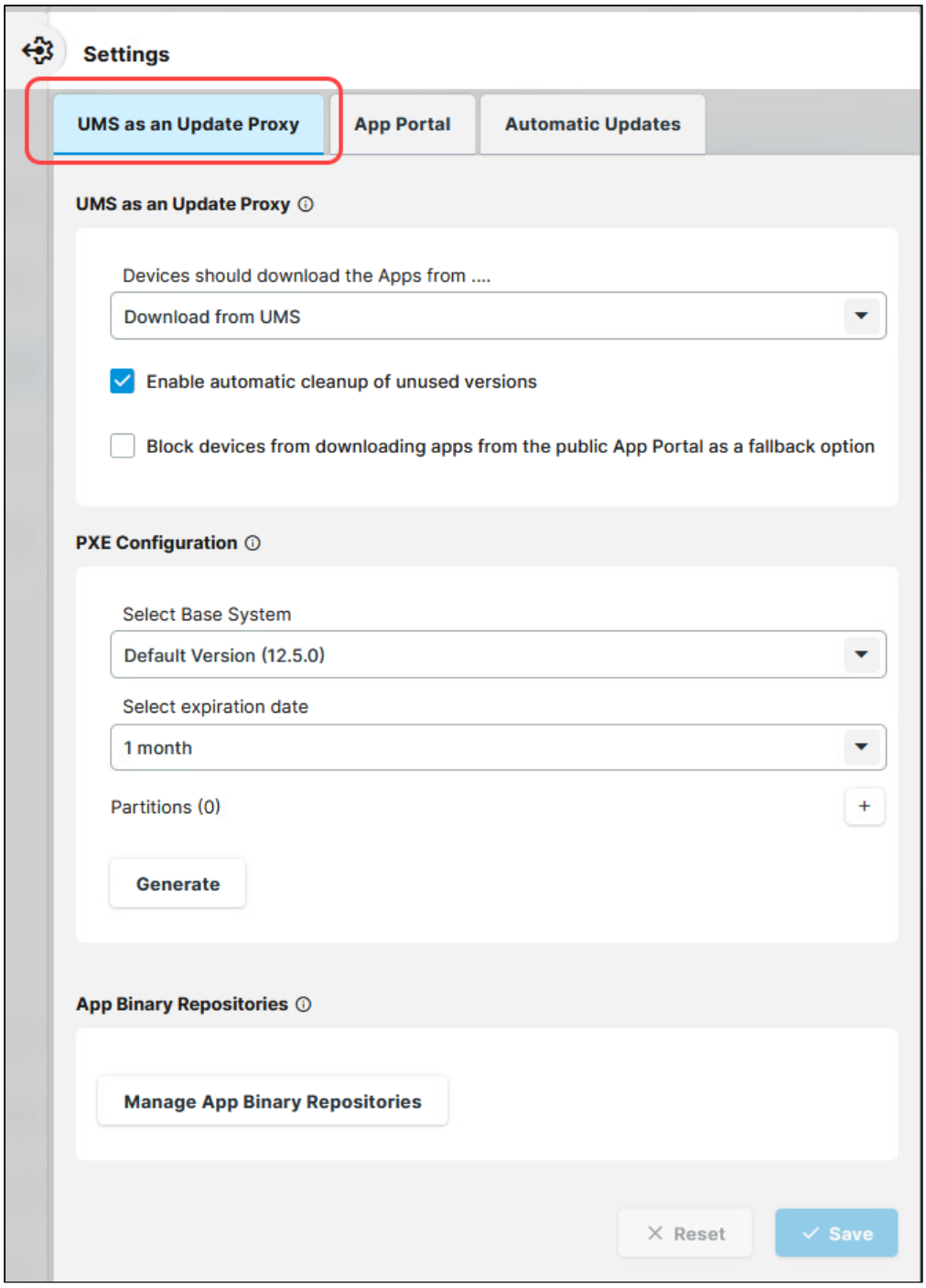
Menu path: **UMS Web App > Apps > Settings**



Permissions
To access the **Apps** area, **App Management** permission is required. You can set the permission in the **UMS Console > System > Administrator accounts**.
To access various tabs under **Apps > Settings**, set the following rights:

- **UMS as an Update Proxy**: Permissions for the node **UMS Features** under **UMS Console > UMS Administration > Global Configuration**
- **App Portal** and **Automatic Updates**: Permissions for the node **Server Network Settings** under **UMS Console > UMS Administration > Global Configuration**
  For how to set permissions, see Access Rights in the Administration Area (see page 1022).

UMS as an Update Proxy



UMS as an Update Proxy

Devices should download the apps from ...

Defines from where the IGEL devices should download the assigned apps / app versions:

- **Download directly from App Portal** (Default): The devices will download the assigned apps from the IGEL App Portal (defined in the tab **App Portal**).
  Only the metadata of the imported apps is stored in the UMS. The IGEL UMS will automatically check if a newer version of the imported app is available in the IGEL App Portal at regular intervals as defined under the automatic updates (see page 1342).

If you have enabled and defined the Distributed App Repository (see page 427), all binaries are uploaded to the configured Webdav servers. The devices will use the Distributed App Repository as a primary source in this case.

- **Download from UMS**: The devices will download the assigned apps from the UMS Server.
  The metadata of the imported apps is stored in the UMS. The IGEL UMS will automatically check if a newer version of the imported app is available in the IGEL App Portal at regular intervals as defined under the automatic updates (see page 1342).
  The binaries of the apps are cached in the local cache of the UMS update proxy; the app binaries are cached in `[IGEL installation directory]/rmguiserver/persistent/ums-appproxy/files`. The synchronization of app binaries with the App Portal is also performed at regular intervals as defined under the automatic updates.
  If the device requests an app before the synchronization (i.e. before the app binaries are available in the UMS), the app will be downloaded to the UMS Server just in time, so that the device can take the app from there.

If you have enabled and defined the Distributed App Repository (see page 427), all binaries are uploaded to the configured Webdav servers. The devices will use the Distributed App Repository as a primary source in this case.

For apps that are not imported from the IGEL App Portal, but manually uploaded (see page 1338), the metadata and binaries are stored in the UMS but never automatically updated.

If the app cannot be downloaded from the UMS for some reason (e.g. the UMS Server is unreachable), there is a fallback to the IGEL App Portal (defined in the tab **App Portal**) or to the hardcoded App Portal. If you want, however, to deactivate the fallback to the App Portal, you can enable the parameter **Block devices from downloading apps from the public App Portal as a fallback option**.

App synchronization between servers
Apps are automatically synchronized between the UMS Servers if you have an IGEL UMS High Availability or Distributed UMS installation. Note that a web certificate must be defined for all servers. It must contain the Cluster Address (if set) and all server addresses and be assigned to all servers. For detailed information on the Cluster Address and instructions on how to define a web certificate for all servers, see Server Network Settings in the IGEL UMS (see page 909) .

Enable automatic cleanup of unused versions

☑ The UMS update proxy does an automatic cleanup of the local cache once a week to keep the disc space used small. The cleanup checks all app versions in the cache against the app versions loaded in UMS. App versions which are used are excluded from the cleanup, for all others the binary files in the cache are deleted. The metadata of the apps in UMS is not changed.

⚠ Do not delete binaries directly from the cache of the UMS update proxy located in the folder `'rmguiserver/persistent/ums-appproxy/files'`. If you want to manually delete unused apps / app versions, follow the instructions in How to Delete Apps in the IGEL UMS Web App (see page 1324) .

ℹ **Which app versions are excluded from the automatic cleanup?**
An app version is declared as used and is excluded from the cleanup if any of the following conditions is true.
For the IGEL OS Base System app, the app version is excluded if

- it is the current default version of the app.
- it is assigned to a folder.
- it is explicitly assigned to a device.

For all apps other than the base system app, the app version is excluded if

- it is the current default version of an app.
- it is assigned to a folder.
- it is explicitly assigned to a device.
- it is assigned to a profile.
- it is installed on a device.
- it is a private app with binaries uploaded to the UMS update proxy.

Block devices from downloading apps from the public App Portal as a fallback option

☑ If the app cannot be downloaded from the UMS for some reason, devices will not try to download from the IGEL App Portal.

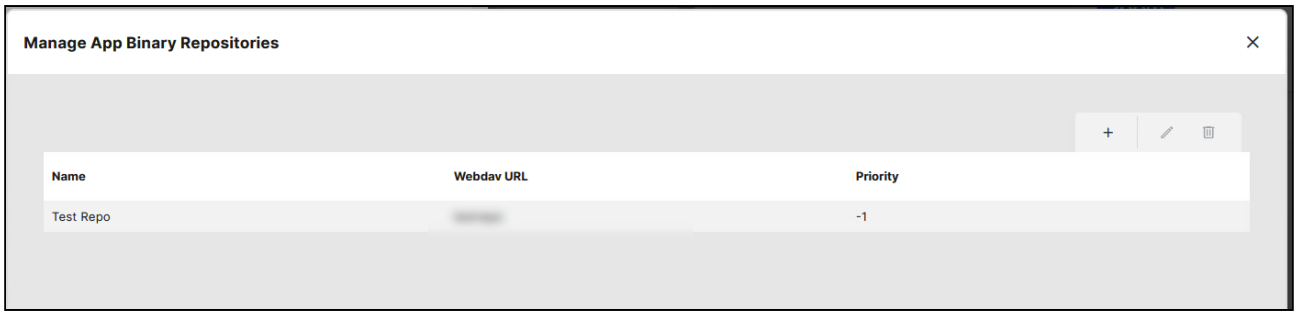
☐ If the app cannot be downloaded from the UMS for some reason (e.g. the UMS Server is unreachable), there is a fallback to the IGEL App Portal (defined in the tab **App Portal**) or to the hardcoded App Portal. (Default)

PXE Configuration

ℹ Deployment of IGEL OS via PXE is supported with IGEL OS 12.2.1 or higher. For details, see (12.4-en) How to Deploy IGEL OS 12 with PXE .

App Binary Repositories

Manage App Binary Repositories



Here you can configure the binary app repository for the distribution of apps to locations with no internet connection or low bandwith. You need to enable **Download from UMS**. For details, see How to Use Distributed App Repositories in IGEL UMS (see page 427).

Once an app is cached in the repository, synchronization is performed at the same intervals as defined for the automatic updates (see page 1342).

App Portal

App Portal base URL: Specifies which App Portal should be used for importing apps.

Make NO changes here unless you know exactly what you are doing!

Automatic Updates

Automatic Check for Updates

UMS will automatically check if a newer version of the app is available in the IGEL App Portal:

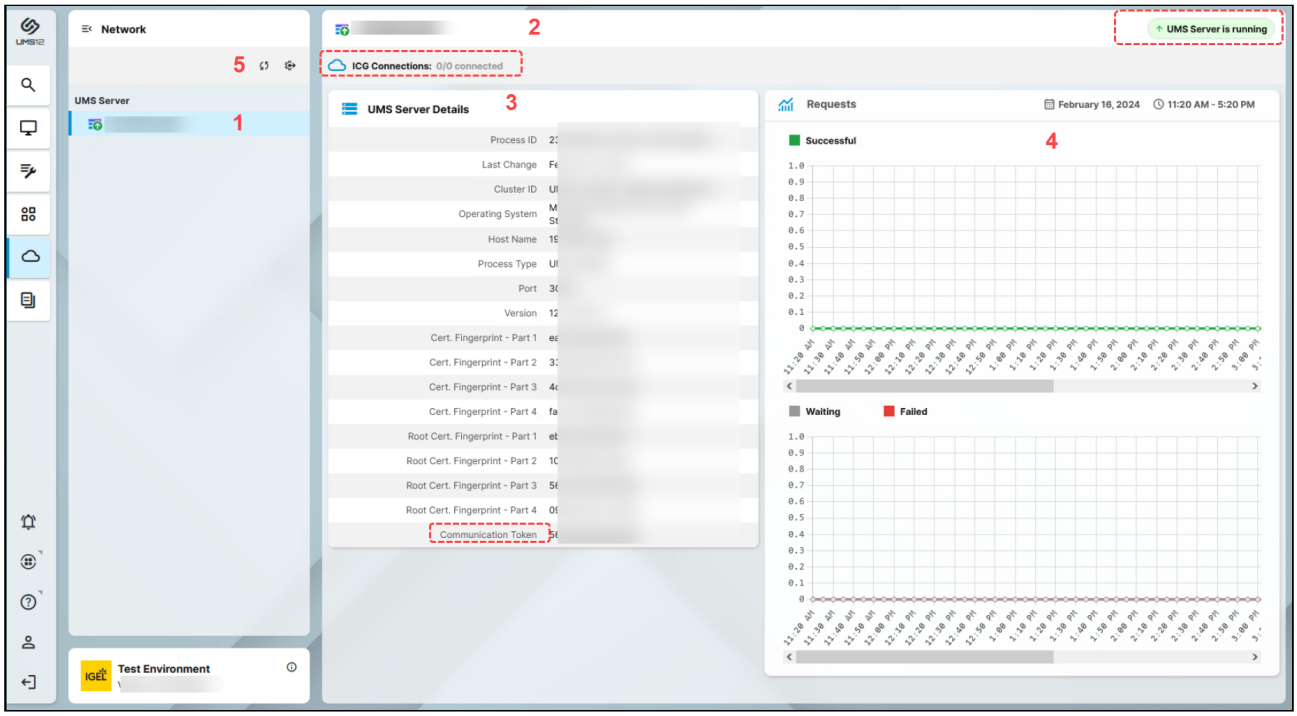
- **Updates will be checked every [number] minutes** (Default: Every 120 minutes)
- **Updates will first be checked [number] minutes after server startup** (Default: 17 minutes)

Settings specified here will be used for all apps for which **Check for updates** or **Check for updates and auto-import into UMS** is enabled in the **Update Settings** (see page 1337) area.

Network Settings in the IGEL UMS Web App

In the **Network** area of the IGEL Universal Management Suite (UMS) Web App, you can find information on all connected UMS Servers, UMS Load Balancers, and IGEL Cloud Gateways. You can also find here the OBS Routing details for IGEL Onboarding Service and specify the nickname for your UMS.

Menu path: **UMS Web App > Network**



1	List of all available UMS Servers / UMS Load Balancers / IGEL Cloud Gateways (ICG)
2	In the header, you can find the following: • Status of the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway, see "Status Displays" below. • Status of UMS Server / ICG connections (connected, disconnected, unknown) • Number of currently connected devices (only for the ICG)
3	Details for the selected UMS Server / UMS Load Balancer / IGEL Cloud Gateway You can find the Communication Token here. The communication token can be used during the onboarding process. For more information, see (en) Onboarding IGEL OS 12 Devices .

4	Statistics for the device requests
5	• Refresh network infromation. • Open the **Settings** area. See details below.

Status Displays

UMS Server

The following icons show the status of the installed UMS Servers.

	The UMS Server is running.
	The UMS Server is not running.
	The status of the UMS Server is unknown (e.g. when a new server is being propagated in the network) or has not yet been processed.
	The user is not authorized to view details for the UMS Server.
	The UMS Server is being updated.

UMS Load Balancer

The following icons show the status of the installed UMS Load Balancers.

	The Load Balancer is running.
	The Load Balancer is not running.
	The status of the UMS Load Balancer is unknown (e.g. when a new load balancer is being propagated in the network) or has not yet been processed.
	The user is not authorized to view details for the Load Balancer.

	The Load Balancer is being updated.

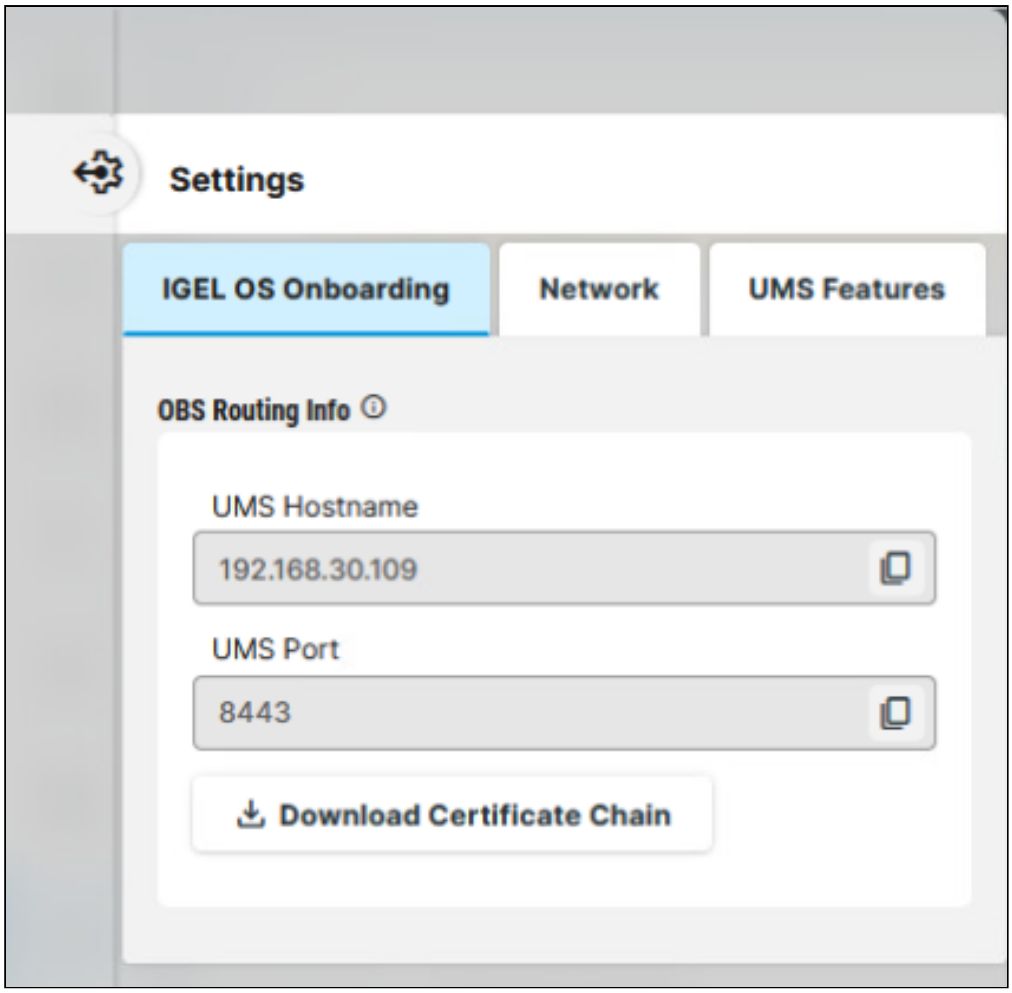
IGEL Cloud Gateway

The following icons show the status of the installed IGEL Cloud Gateways.

	The IGEL Cloud Gateway is running.
	The IGEL Cloud Gateway is not running.
	The status of the IGEL Cloud Gateway is unknown or has not yet been processed.
	The user is not authorized to view details for the IGEL Cloud Gateway.
	The IGEL Cloud Gateway is being updated.

Settings

Click  to open the **Settings** area.



IGEL OS Onboarding

Here, you can find **OBS Routing information** which is required if you use IGEL Onboarding Service. For details, see (en) Initial Configuration of the IGEL Onboarding Service (OBS) .

To copy the data, click .

UMS Hostname

Hostname (Fully Qualified Domain Name) or IP address of the UMS Server.

If configured, the Server Network Settings in the IGEL UMS (see page 909) or the Server - View Your IGEL UMS Server Information (see page 870) is used here (in the order given).

UMS Port

Port under which the UMS can be reached. The default port of the UMS web server is 8443. For details on the ports used by the UMS, see IGEL UMS Communication Ports (see page 256) .

If configured, the Server Network Settings in the IGEL UMS (see page 909) or the Server - View Your IGEL UMS Server Information (see page 870) is used here (in the order given).

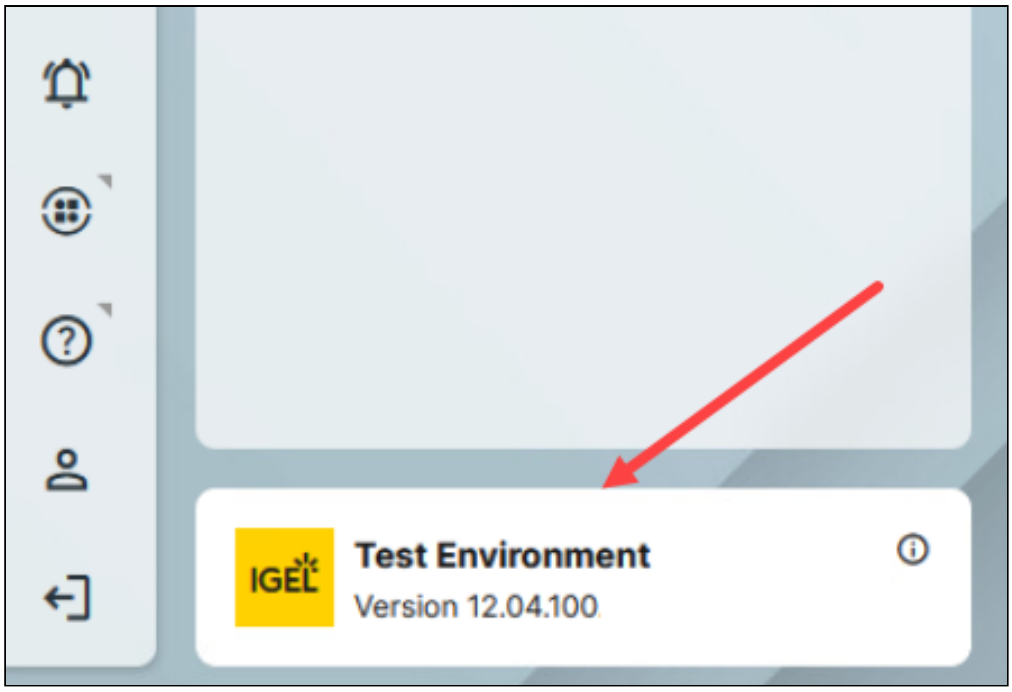
Download Certificate Chain

Downloads the UMS root certificate with `.crt` file extension.

Network

Nickname

A name specified here is displayed in the info box of the UMS Web App as well as in the browser tab and helps to distinguish one UMS instance from another.



To change the value, permission for the node **Server Network Settings** under **UMS Console > UMS Administration > Global Configuration** is required.
For how to set rights, see Access Rights in the Administration Area (see page 1022) .

Allowed Redirect URIs

If you use a URL to login to your UMS, which is not detected automatically, you can add additional redirect URIs here.

For details, see UMS Login Requirements[212] .

212. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

UMS Features

> Permission for the node **UMS Features** under **UMS Console > UMS Administration > Global Configuration** is required.
> For how to set rights, see Access Rights in the Administration Area (see page 1022) .

Enable Template Profiles

☑ Template profiles are enabled. For information on template profiles, see Template Profiles in the IGEL UMS (see page 746) .

Enable Priority Profiles

☑ Priority profiles are enabled. For information on priority profiles, see Priority Profiles in the IGEL UMS (see page 744) .

Enable Recycle Bin

☑ The recycle bin is enabled. Deleted items are moved to the recycle bin first. For information on the recycle bin, see How to Use the Recycle Bin in the IGEL UMS Web App (see page 1356).

☐ If the recycle bin is disabled, the items are deleted permanently straight away. The **Recycle Bin** button is not visible.

> The recycle bin is enabled or disabled globally for all UMS users.

Enable Insight Service

☑ Enables IGEL Insight Service if you accept the privacy policy in the consent dialog by clicking **OK**. When you activate the IGEL Insight Service, IGEL collects specific analytical and usage data listed under **Data collected by Insight Service**. For details, see (en) IGEL Insight Service .

☐ Disables IGEL Insight Service.

Logging in the IGEL UMS Web App

In the **Logging** area of the IGEL Universal Management Suite (UMS) Web App, you can activate logging and search for log messages according to the configured search parameters.

Not all actions performed in the UMS Console are displayed in the UMS Web App. Logs of the UMS Web App are not displayed in the UMS Console; for where to find them, see Logging (see page 987).

It is recommended to delete unnecessary logs regularly to avoid problems with insufficient disk space.

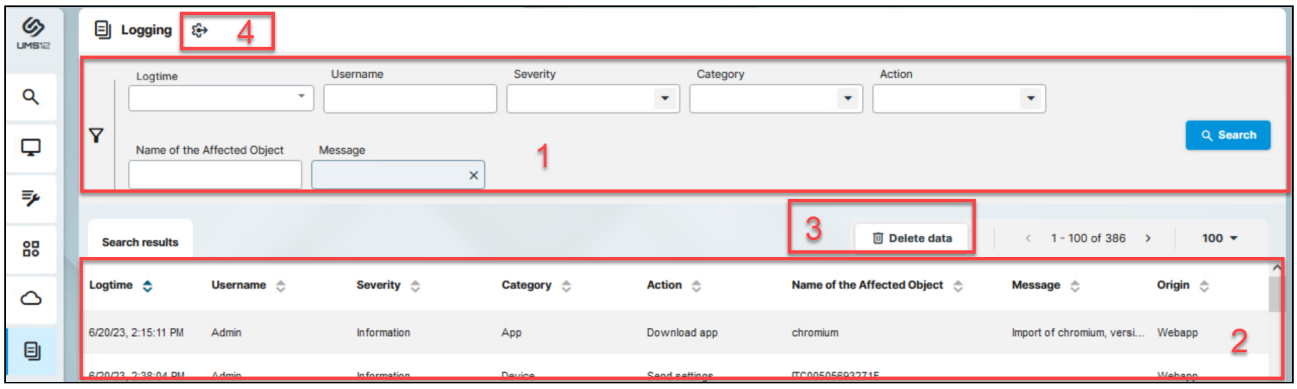
Menu path: **UMS Web App > Logging**

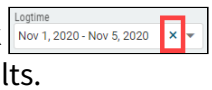
Log messages are available if:

- Logging is enabled either
  - under **UMS Web App > Logging > Settings** (see below)
    or
  - under **UMS Console > UMS Administration > Global Configuration > Logging** (see Logging (see page 987))
- A user has sufficient rights. For details on where you can define permissions, see General Administrator Rights (see page 1013) and Access Rights in the Administration Area (see page 1022).

The last search configuration is automatically saved and restored on the next visit of the **Logging** area.

When no values are specified in the search mask, all available log messages are shown.



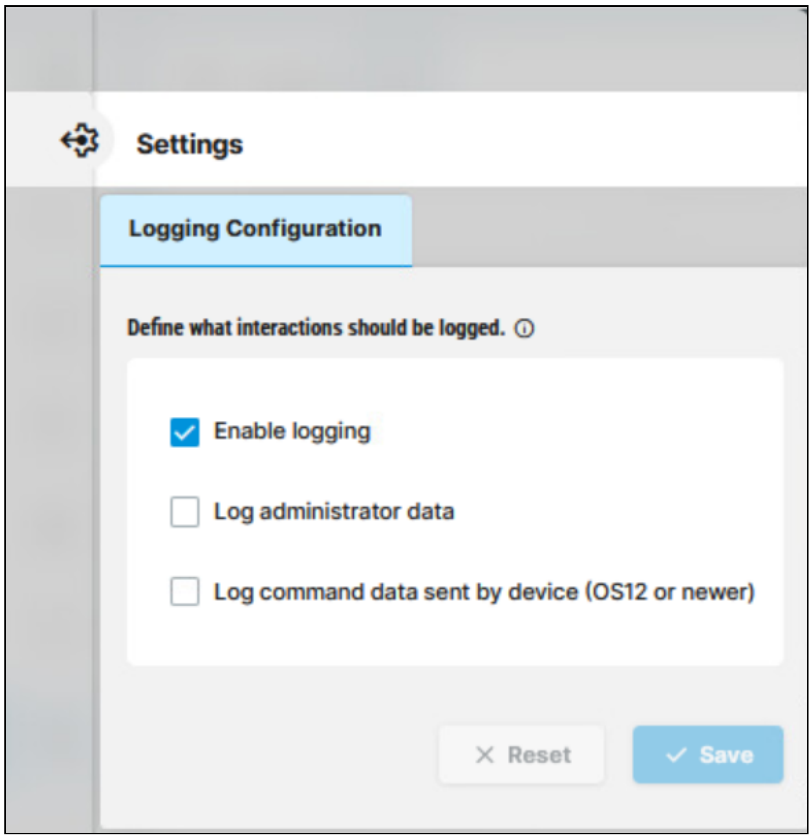
1	Search mask	Search criteria for the logs (linked with logical *AND*) To remove a value, click  and than **Search**. This updates the search results.

2	Log list	Shows all logs that match the search criteria. • Paging for the navigation in the log list • Defining the number of log messages to be displayed on one page • Sorting within any selected column • Tooltips, useful in case of truncations
3	Delete data	Deletes the logs that are older than the number of days set. ⚠ To delete the logs, a user must have the right "Delete Log Messages", see General Administrator Rights (see page 1013). Directly after the deletion of logs, a message "`No matching logs found`" appears. Wait for the next reindexing to view the updated list of the log messages. However, you can immediately view and search for new logs, i.e. logs for actions performed after the deletion procedure. ℹ To delete logs related to the UMS Web App and IGEL OS 12 device management, you can create an administrative task in the UMS Console starting from UMS 12.09.110. For details, see Delete Logging Data as an Administrative Task in the IGEL UMS[213].
4	Settings	Allows you to configure logging settings, see below.

Settings

→ Click ⚙ to open the **Settings** area.

213. https://kb.igel.com/en/universal-management-suite/current/delete-logging-data-as-an-administrative-task-in-t



Enable logging

☑ UMS user actions will be logged. This activates logging for the UMS Console and for the UMS Web App.

☐ UMS user actions will not be logged. This disables logging for the UMS Console and for the UMS Web App. (Default)

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. This activates the logging of the administrator name for the UMS Console.

☐ The name of the administrator who started the action will not be logged. This disables the logging of the administrator name for the UMS Console. (Default)

Log command data sent by device (OS 12 or newer)

☑ Actions initiated by a device, i.e. each command an IGEL OS 12 device sends to the UMS, will be logged.

☐ Actions initiated by a device will not be logged. (Default)

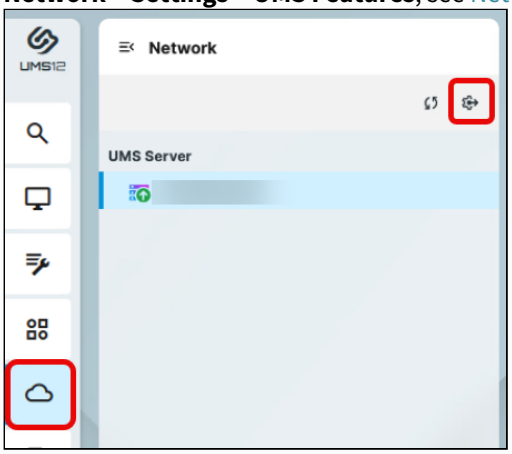
How to Use the Recycle Bin in the IGEL UMS Web App

In this article, it is explained how you can use the recycle bin and delete devices and configuration objects (that is profiles, files, and corporate identity customizations (CICs)) in the IGEL UMS Web App.

For details on how to use the recycle bin in the UMS Console, see Recycle Bin - Deleting Objects in the IGEL UMS (see page 864).

In the IGEL Universal Management Suite (UMS), objects are sent to the recycle bin when deleted by default. Elements in the recycle bin can be permanently deleted or restored.

If the recycle bin is disabled, objects are removed permanently straight away after you have confirmed the deletion. The recycle bin is enabled or disabled globally for all UMS users in the UMS Web App under **Network > Settings > UMS Features**, see Network Settings in the IGEL UMS Web App (see page 1347).



Important Information

In the UMS Web App, devices / device directories and configuration objects / their directories can be moved to the recycle bin. The highest nodes in the structure tree (the root directories) cannot be deleted.

Directories are moved to the recycle bin along with their subfolders and all contained objects. A deleted directory is handled as one item and can therefore be restored again or permanently deleted as a complete structure. If you delete a subfolder or contained objects first and then the parent folder as well, you will only see the parent folder in the recycle bin, but it will contain the previously deleted subfolder / objects as well.

Note the following:

- 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 configuration objects.
- Assigned profiles, files, and CICs in the recycle bin are not active. This means that the settings for devices may change by moving configuration objects to the recycle bin. Profiles previously assigned to devices will be reactivated if they are restored from the recycle bin.
- Objects in the recycle bin cannot be found via the search function (and views in the UMS Console) and cannot be addressed by scheduled tasks.

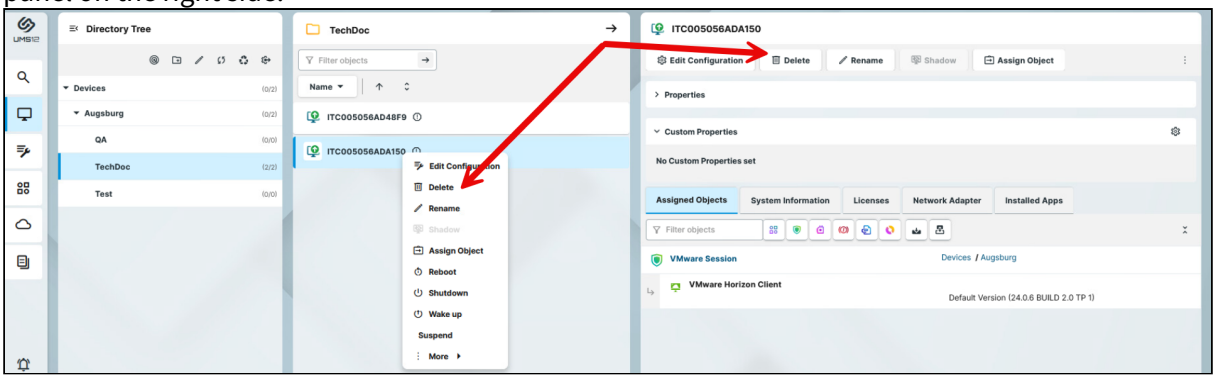
- In comparison to the UMS Console, the recycle bin in the IGEL UMS Web App only displays the deleted objects of the specific area / configuration tab.
  Example 1: If you open the recycle bin in the **Devices** area, you will only see the deleted devices/ device directories, but not profiles, files, etc.
  Example 2: If you open the **Configuration** area and click the **Recycle Bin** button while in the **Profiles** tab, you will only see the deleted profiles / profile directories, but not the deleted CICs or files.

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 (see page 533).

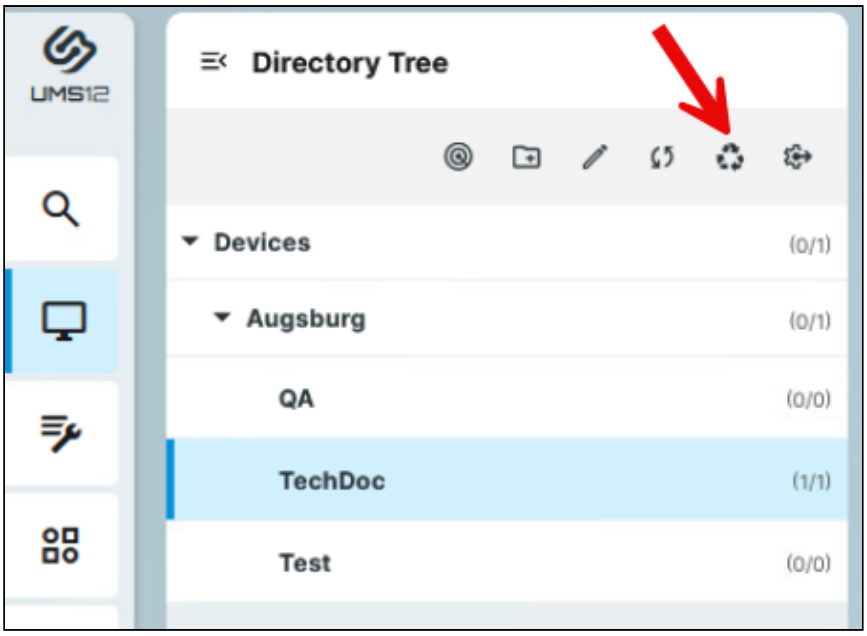
Deleting Devices from the UMS

To remove devices from the UMS:

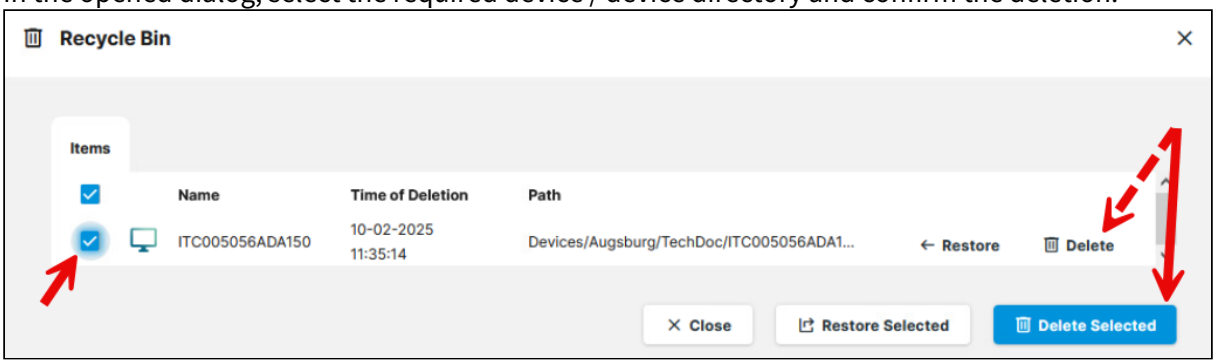
1. In the UMS Web App, go to **Devices** and select the device that you want to delete.
2. Click the **Delete** button or context menu item.
   If you want to remove the device directory, click the **Delete Directory** button in the management panel on the right side.



3. Confirm the deletion.
4. To see the items moved to the recycle bin and to permanently delete them, click the **Recycle Bin** button.



5. In the opened dialog, select the required device / device directory and confirm the deletion.



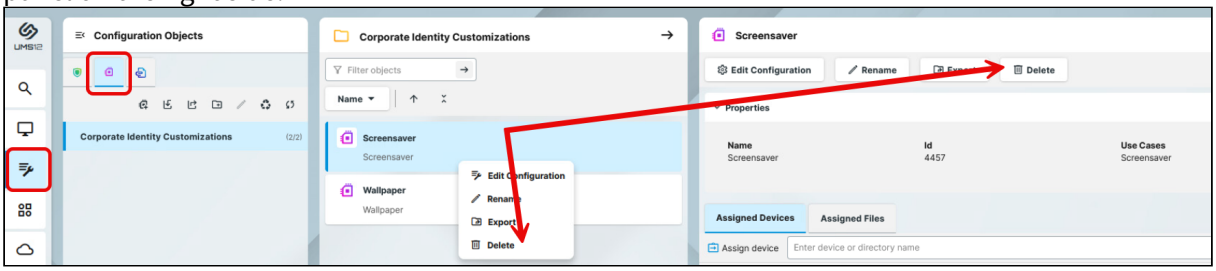
6. For IGEL OS 12 devices only: In the **Delete Items** dialog, specify whether the licenses should be deleted and accept the **Terms and Conditions**.
   If you enable **Delete Licenses** checkbox:
   - all licenses will be removed from the device if the device is online (Device level)
   - all licenses 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.

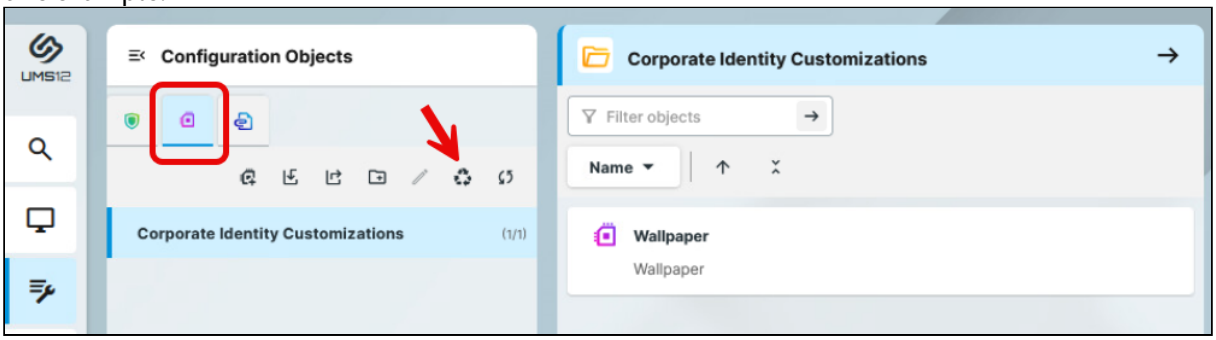
Deleting Configuration Objects from the UMS

To delete a configuration object:

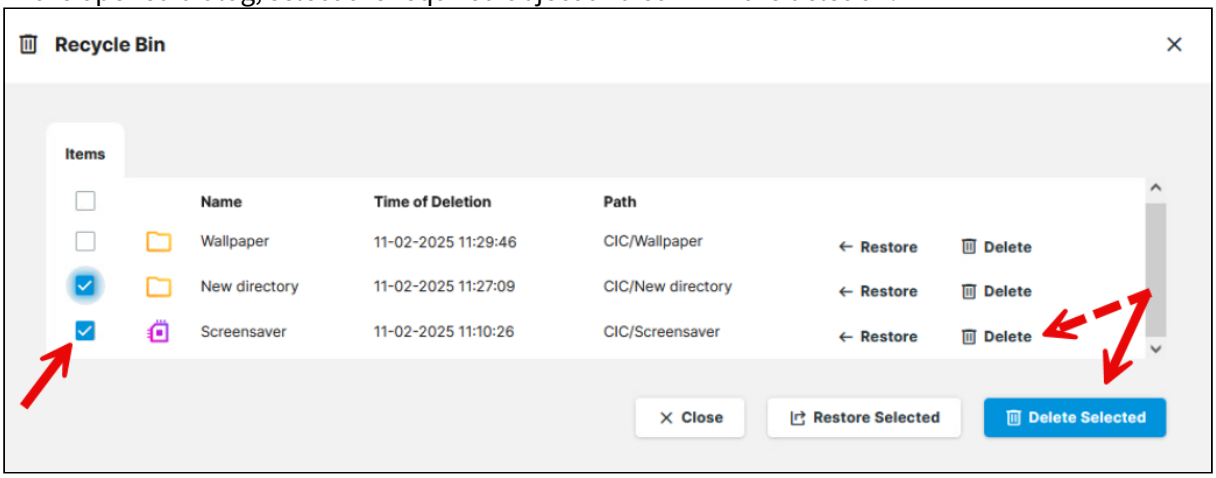
1. In the UMS Web App, go to **Configuration** and open the required tab, e.g. **Corporate Identity Customizations** (CICs) if you want to delete a CIC.
2. Select the CIC that you want to delete and click the **Delete** button or context menu item.
   If you want to remove e.g. a CIC directory, click the **Delete Directory** button in the management panel on the right side.



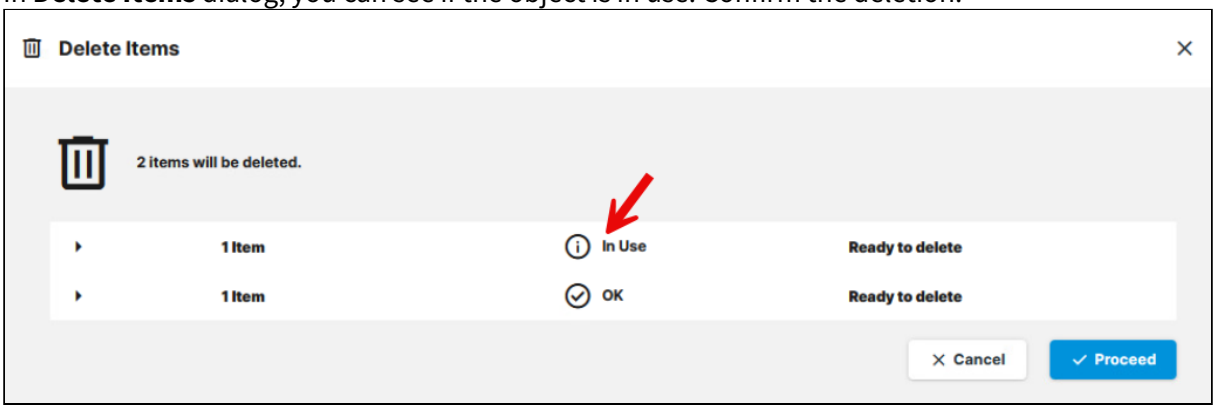
3. Confirm the deletion.
4. To see the items moved to the recycle bin and to permanently delete them, click the **Recycle Bin** button in the required tab.
   In the recycle bin, you can see the deleted objects only of the selected type, i.e. all removed CICs in this example.



5. In the opened dialog, select the required object and confirm the deletion.

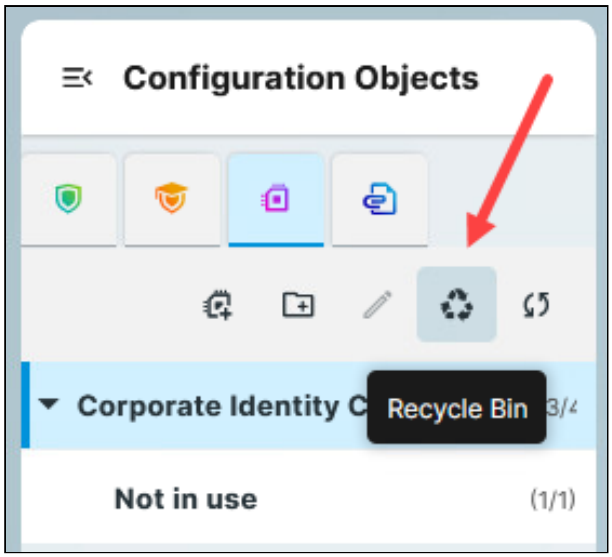


6. In **Delete Items** dialog, you can see if the object is in use. Confirm the deletion.



Restore from the Recycle Bin

→ To see the items moved to the recycle bin and to restore them, open the required area, e.g. **Devices** or **Configuration > specific configuration tab**, and click **Recycle Bin > Restore**.
Selected items will be restored without confirmation.



If you cannot see the **Recycle Bin** button, the recycle bin is probably disabled.

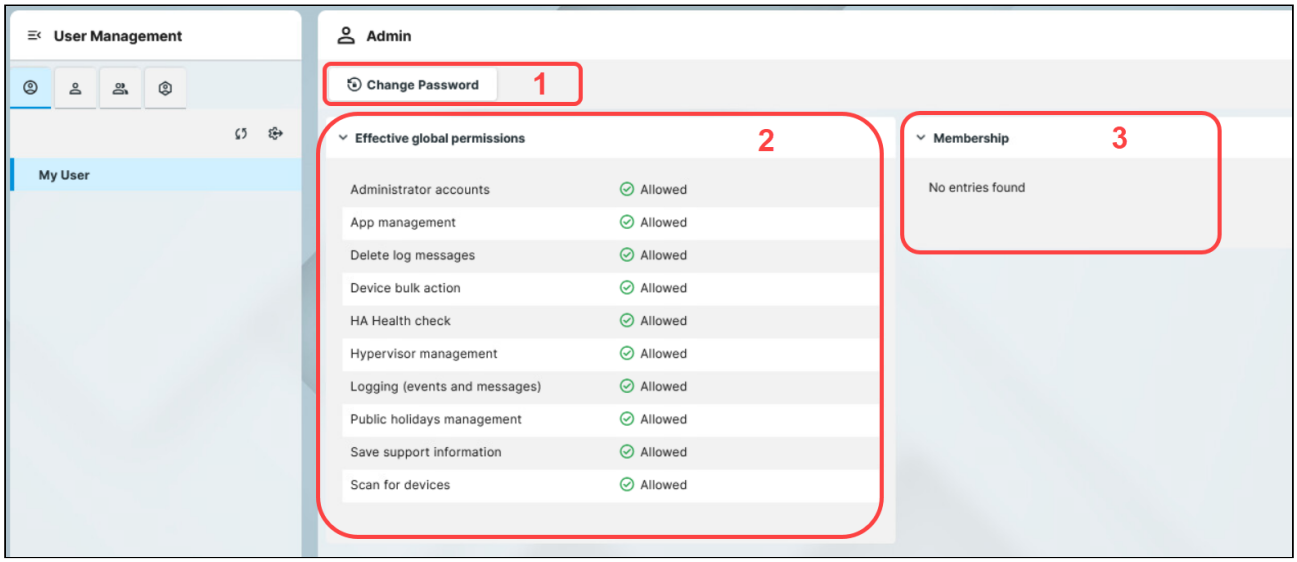
User Management and IdP Management in the IGEL UMS Web App

In the **User Management** area of the IGEL UMS Web App, you can manage your own user, and, depending on your permissions, other users and user groups. You can also configure Identity Provider (IdP) clients and manage IdP roles. The available features are grouped in tabs as described below.

Permission Dependant Tabs
The accessible tabs are defined by the permissions of the logged-in user:

- If the logged-in user does not have Administrator Accounts permission, they can only access the **My User** tab with their username, their effective permissions and membership.
- If the logged-in user user has Administrator Accounts permission, they can:
  - access all the tabs, including **Users**, **Groups** and **Identity Provider Roles** tabs
  - manage users, groups and IdP roles (for example, set passwords for users, set global permissions for users and groups)

My User Tab Overview

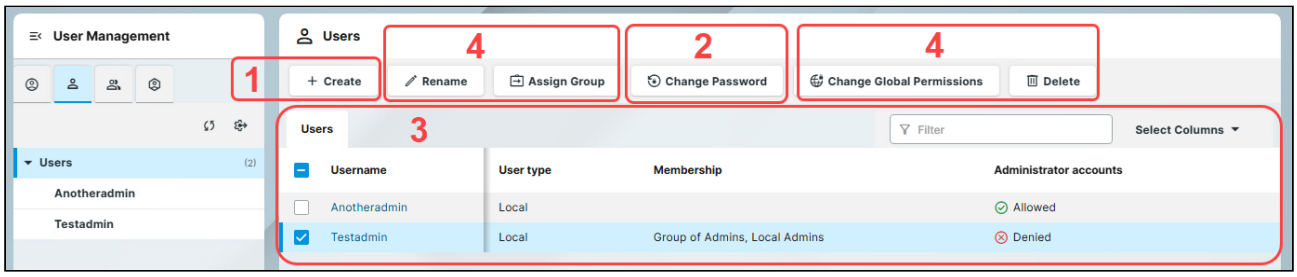


In the **My User** tab, you can manage the currently logged in user:

1. **Change Password** for the user, see How to Change User Password in the IGEL UMS Web App (see page 1379) .
2. Get an overview of the user permissions under **Effective global permissions** (see, Effective Rights in IGEL UMS (see page 1010))
3. Check which groups the user belongs to under **Membership**

Users Tab Overview

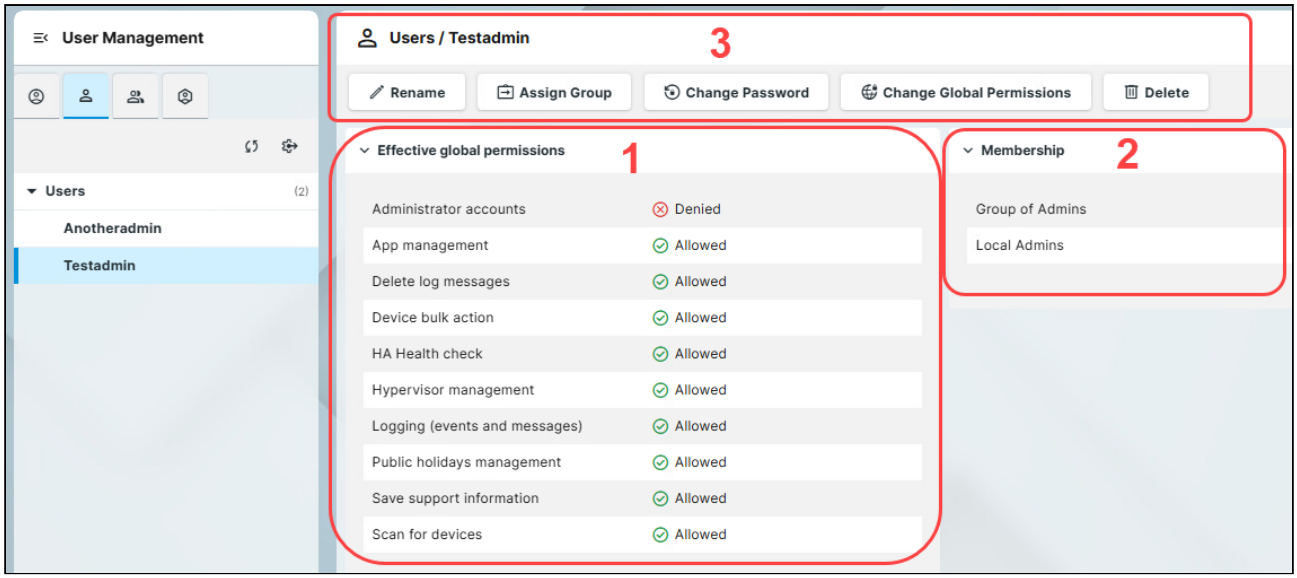
List View



If you select the root of the structure tree, you see the list view of the **Users** tab. In the list view you can:

1. **Create** user.
2. **Change Password** for the selected user, see How to Change User Password in the IGEL UMS Web App (see page 1379) .
3. Get an overview of all the users. You can use the text filter to find specific users.
4. Manage selected user accounts, that is, **Rename**, **Delete**, **Assign Group** and **Change Global Permissions**, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .

Details View

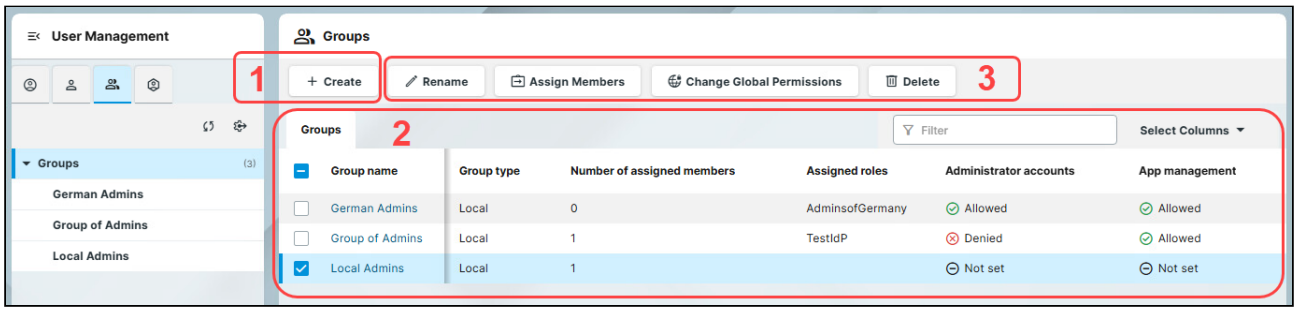


If you select a user from the structure tree, you access the details view of the **Users** tab. In the details view you can:

1. Get an overview of the **Effective global permissions** assigned to the selected user.
2. Check which groups the selected user belongs to under **Membership.**
3. Manage selected user accounts, that is, **Rename**, **Delete**, **Assign Group** and **Change Global Permissions**, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .

Groups Tab Overview

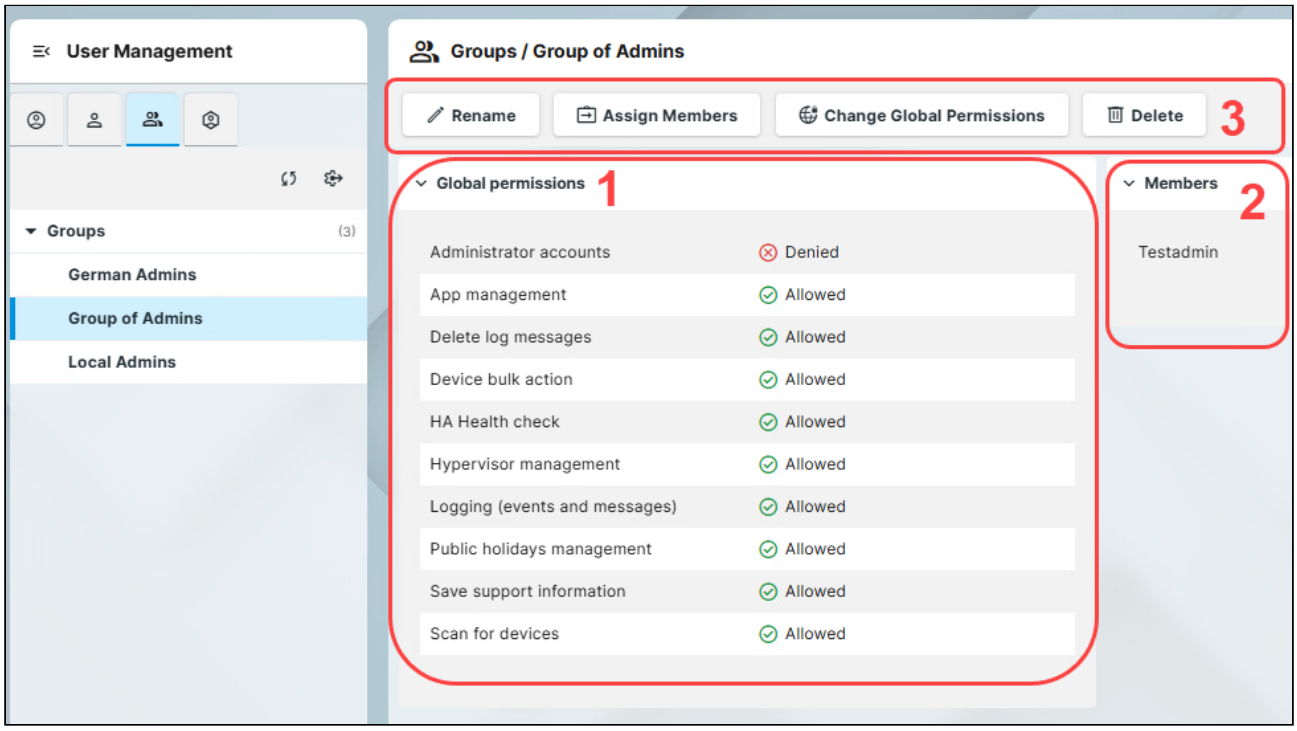
List View



If you select the root of the structure tree, you see the list view of the **Groups** tab. In the list view you can:

1. **Create** user groups, see How to Create User Groups in the IGEL UMS Web App (see page 1367)
2. Get an overview of all the groups. You can use the text filter to find specific groups.
3. Manage a selected group, that is, **Rename**, **Delete, Assign Member,** and **Change Global Permissions**, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .

Details View

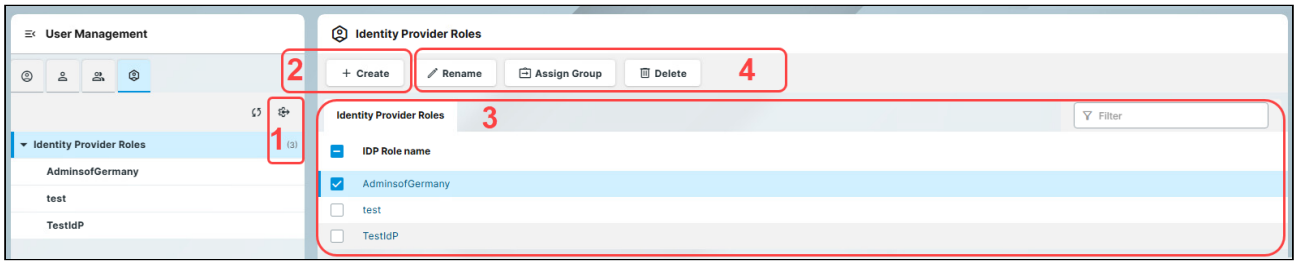


If you select a group from the structure tree, you access the details view of the **Groups** tab. In the details view you can:

1. Get an overview of the groups permissions under **Global permissions** (see, Effective Rights in IGEL UMS (see page 1010)).
2. Check the **Members** of the group.
3. Manage the selected group, that is, **Rename**, **Delete, Assign Member,** and **Change Global Permissions**, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .

Identity Provider Roles Tab Overview

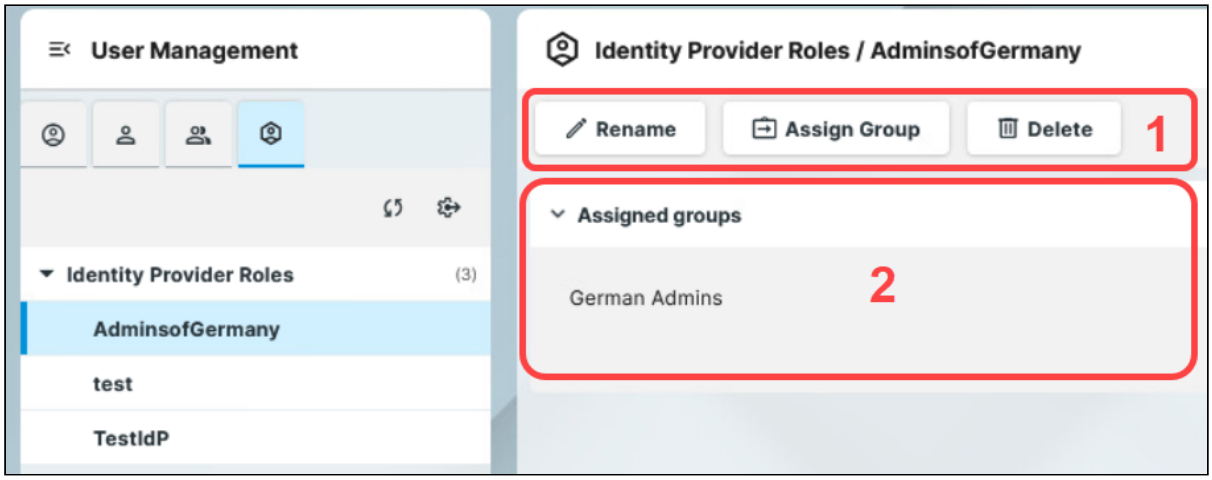
List View



In the **Identity Provider Roles** tab, you can:

1. Configure an IdP client in the UMS. For instructions on configuring the IdP client, see How to Configure an Identity Provider Client in the IGEL UMS Web App (see page 1373) .
2. **Create** IdP roles, see How to Map Identity Provider Roles in the IGEL UMS Web App (see page 1376).
3. Get an overview of all the roles. You can use the text filter to search for specific roles.
4. Manage selected IdP roles, that is, **Rename**, **Assign Group** and **Delete**.

Details View



If you select an IdP role from the structure tree, you access the details view of the **Identity Provider Roles** tab. In the details view you can:

1. Manage the IdP role, that is, **Rename**, **Assign Group** and **Delete**.

2. Check the **Assigned groups**.

How to Create User Groups in the IGEL UMS Web App

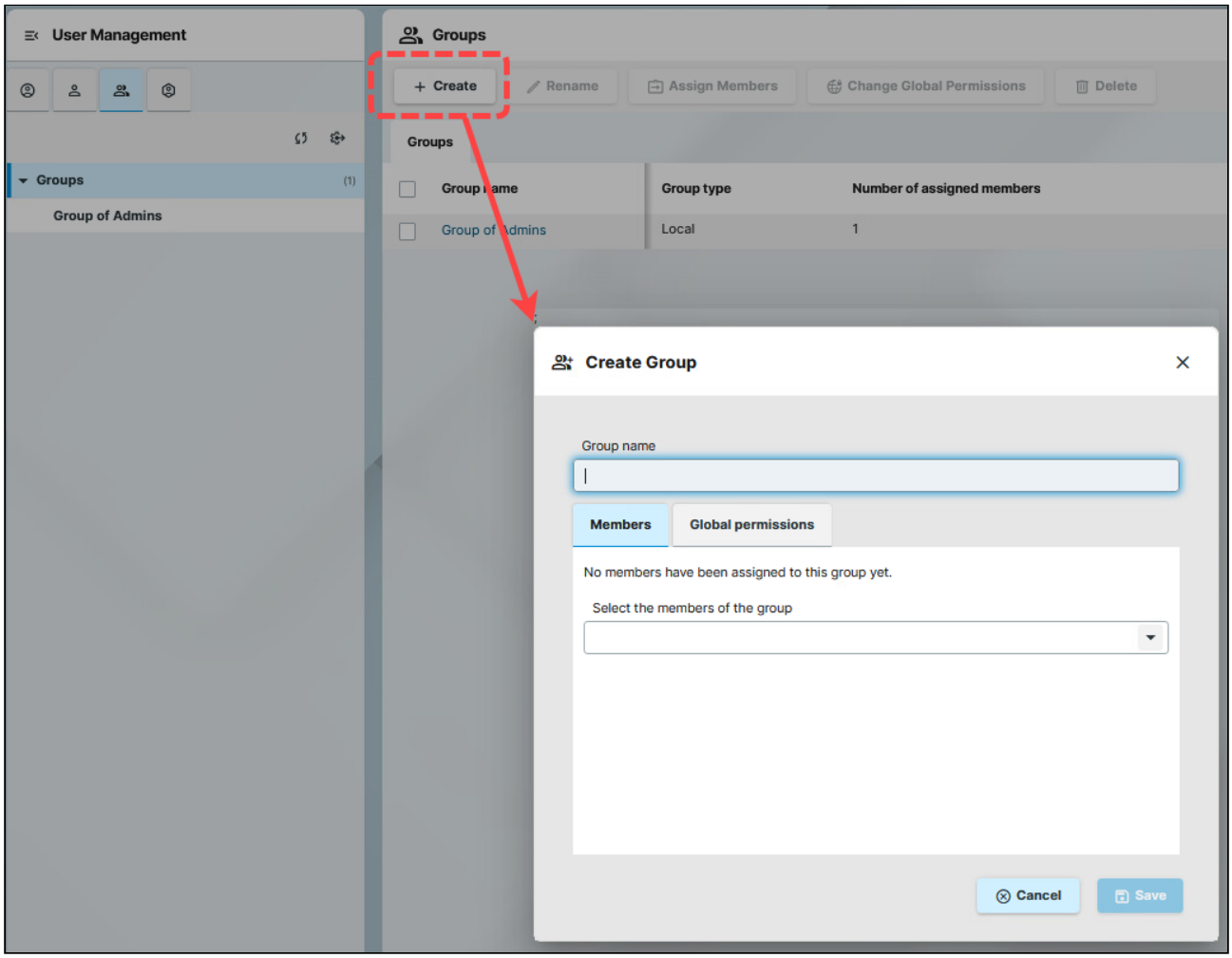
You can create user groups for easier user management in the IGEL UMS Web App. You can use these groups to grant permissions (see page 1370) or map Identity Provider (IdP) roles (see page 1376) to a set of users.

In the UMS Console you can do the same under Administrator Accounts in the IGEL UMS (see page 1007).

> **Permission Requirement**
> You need to have the Administrator accounts permission to manage user groups.

To create user groups:

1. Go to **User Management > Groups**.
2. Click **Create**.

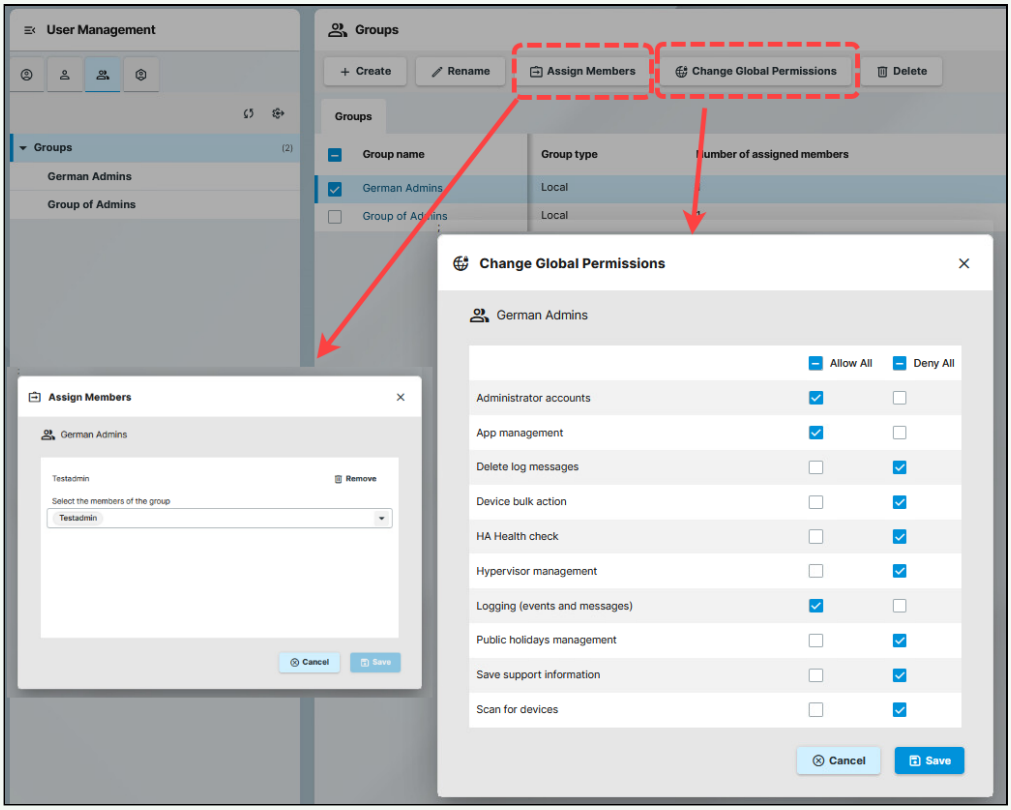


3. Add a name to the group.

4. You can assign users to the group under **Members**.

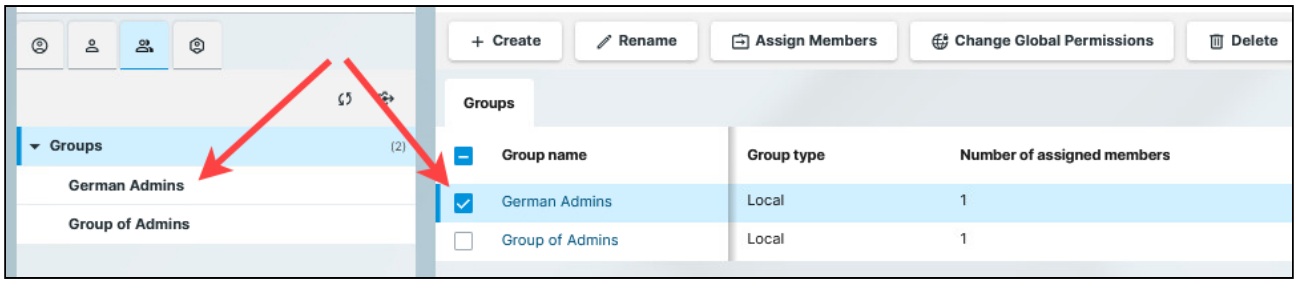
5. You can assign permissions to the group under **Global permissions**. For details on permissions, see Effective Rights in IGEL UMS (see page 1010) .

You can also assign members and edit permissions later through the **Assign Members** and the **Change Global Permissions** action buttons.



6. **Save** the group.

The new group gets listed under **Groups**. You can manage the group either by selecting it from the list in the main page or by navigating to it in the structure tree.


Create
Rename
Assign Members
Change Global Permissions
Delete
Groups
Groups (2)
German Admins
Group of Admins
Group name
Group type
Number of assigned members
German Admins
Local
1
Group of Admins
Local
1

How to Manage Global Permissions in the IGEL UMS Web App

An administrator can grant other administrators rights and take away those rights through permission assignment in the IGEL Universal Management Suite (UMS). These permissions are called administrator permissions or global permissions.

For the description of each permission, see General Administrator Rights in IGEL UMS (see page 1013) .

Permission Requirement
You need to have the Administrator accounts permission to access **Users** and **Groups** tabs and manage permissions.

Permissions Managed in the UMS Console Only

The following global permissions are only possible to change in the UMS Console:

- Firmware management
- License management
- WebDAV access
- Host assignment
- SQL console

For details on how to manage global permissions in the UMS Console, see General Administrator Rights in IGEL UMS (see page 1013) .

Direct and Indirect Permissions

A direct permission is a permission set for an individual user through directly changing the permisison of the user (see page 1371) in the **Users** tab.

An indirect permission is a permission set for user groups (see page 1371) in the **Groups** tab and, as a result, given to the members of that user group indirectly.

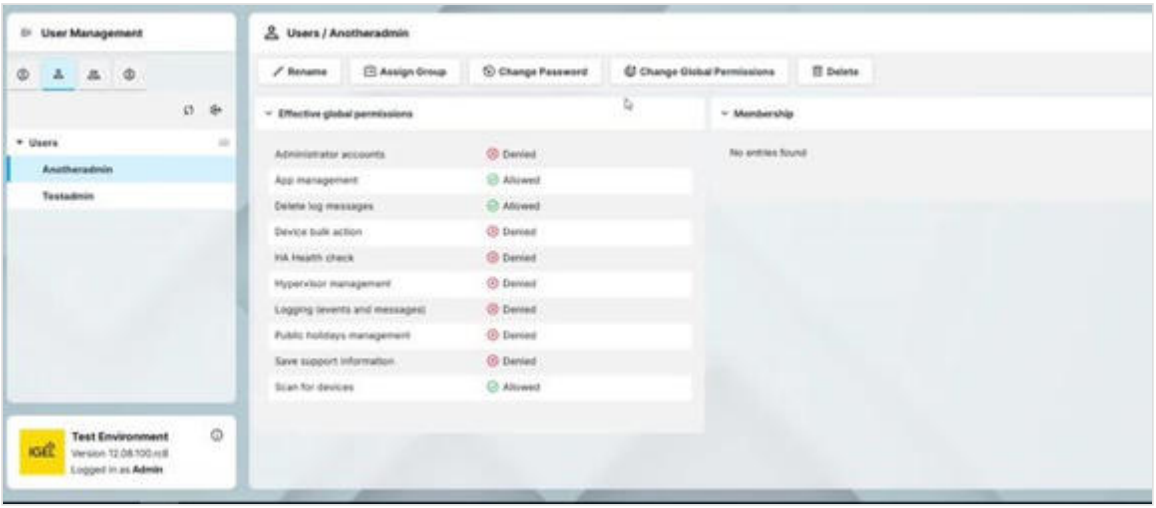
When direct and indirect permissions contradict each other, the following rules apply to calculate the actual permission of the user:

- Direct permissions have precedence over indirect permissions.
- Both deny and allow settings have precedence over not set permissions.
- If a permission is denied it always overrides the granting of the permission.
  For example, if the permission is granted to a user directly, but denied via a group membership, the permission is denied for that user.

For more information, see Effective Rights in IGEL UMS (see page 1010) .

You can always check which permissions are in effect for a user under **Effective global permissions** in the details view of the user selected from the structure tree.

Changing Global Permissions of a User



To grant or deny permissions per user:

1. Go **User Management > Users** tab.
2. Select a user from the list or from the structure tree.
3. Click **Change Global Permissions**.
4. Select the permissions you want to **Allow** or **Deny**.

> You can also use the **Allow All** and **Deny All** options at the top for bulk selection.

5. **Save** the configuration.

You can see the changed permissions listed under **Effective global permissions** in the details view of the user selected from the structure tree, or in the **Users** list view.

Changing Global Permissions of a Group

You can grant or deny permissions per group:

1. Go **User Management > Groups** tab.
2. Select a group from the list or from the structure tree.

3. Click **Change Global Permissions**.

4. Select the permissions you want to **Allow** or **Deny** for the member.

You can also use the **Allow All** and **Deny All** options at the top for bulk selection.

5. **Save** the configuration.

You can see the permissions listed under **Global permissions** in the details view of the group selected from the structure tree, or in the **Groups** list view.

You can see the effect of the change in the **Effective global permissions** of the members of the group. Some permissions might be overwritten following the rules of the direct and indirect permissions (see page 1370).

How to Configure an Identity Provider Client in the IGEL UMS Web App

You need to configure the Identity Provider (IdP) client and map IdP roles to user groups to enable Single Sign-On (SSO) for your IGEL Universal Management Suite (UMS). This article helps with configuring an IdP client using the IGEL UMS Web App.

You can also configure the IdP client in the IGEL UMS Console, see Identity Provider Configuration in IGEL UMS (see page 1001) .

Prerequisites

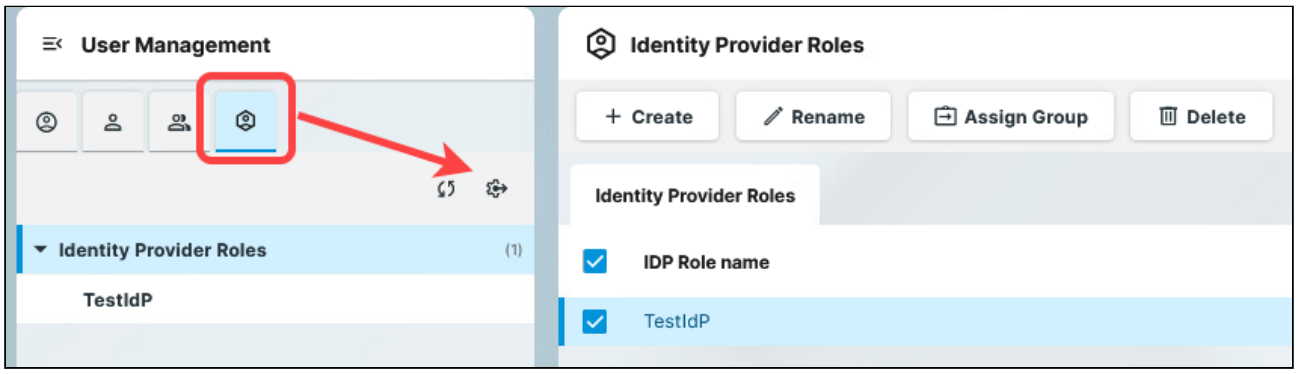
- You need to configure an application for the IGEL UMS in your IdP.

Permission Requirement

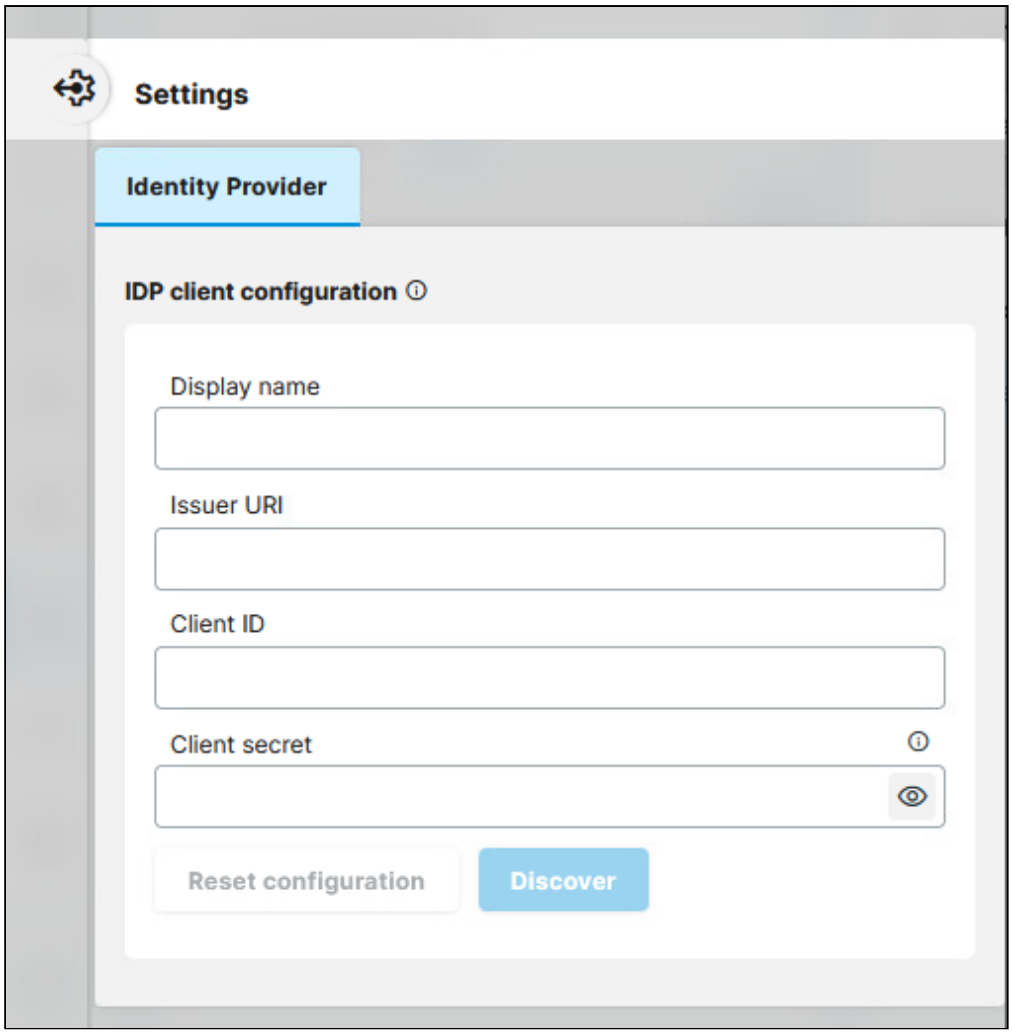
- The **Identity Provider** tab is only visible for users with the Administrator Accounts permission. This permission can be set both in the UMS Web App and UMS Console, see How to Manage Global Permissions in the IGEL UMS Web App (see page 1370) .
- The **Identity Provider client configuration** dialog is read-only for users with read permission for the **Identity Provider** node. You need write permissions for the **Identity Provider** node of the UMS Console to configure IdP clients in the UMS Web App. The permission can be set through the UMS Console structure tree. For details, see Access Rights in the Administration Area (see page 1022) .

Configuring the IdP Cient

1. Go to **User Management > Identity Provider Roles**.



2. Click the gear icon to open the **Settings** dialog.

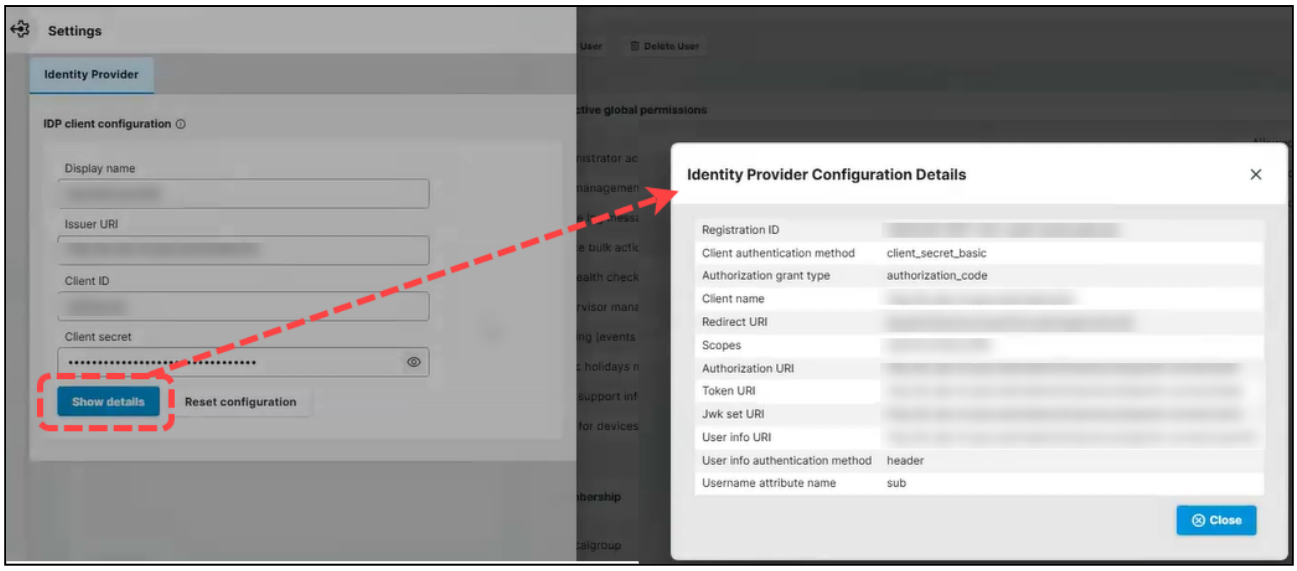


3. Enter the details to configure the IdP client:

- **Display name**: The name of your IdP client configuration, that will be displayed in UMS (e.g., “Okta SSO” or “Ping Configuration”).
- **Issuer URI**: The URL provided by your IdP (e.g. “https://auth.pingone.eu/…”).
- **Client ID**: The Client ID provided by your IdP.
- **Client secret**: The secret key provided when you registered your application with the IdP. Click the eye icon to toggle visibility if needed.

3. After filling in all fields, click **Discover** to establish the connection.

If the discovery is successful, and the IdP validates it, the button changes to **Show details**. Click to check the details of the configuration.



After the client is configured, you can assign IdP roles to user groups, see How to Map Identity Provider Roles in the IGEL UMS Web App (see page 1376).

4. You can click **Reset configuration** to clear the data and start over.

⚠ All users who log in through the configured IdP will not be able to access the UMS after the reset.

How to Map Identity Provider Roles in the IGEL UMS Web App

If you assign an Identity Provider (IdP) role to a user group in the IGEL Universal Management Suite (UMS), you can use this mapping to control permissions.

When a user logs in via Single Sign-On (SSO) and their IdP role matches the mapped role, they are automatically added to the corresponding UMS user group. The user then receives all permissions assigned to that group.

You can also map IdP roles in the UMS Console, see Administrator Accounts in the IGEL UMS (see page 1007) .

Prerequisites

- You need to configure the IdP client, see How to Configure an Identity Provider Client in the IGEL UMS Web App (see page 1373).
- You need to configure the roles in the IdP beforehand, to know the exact role values.
- You need to create the user groups in the UMS to which you will assign the IdP role. For details, see How to Create User Groups in the IGEL UMS Web App (see page 1367).

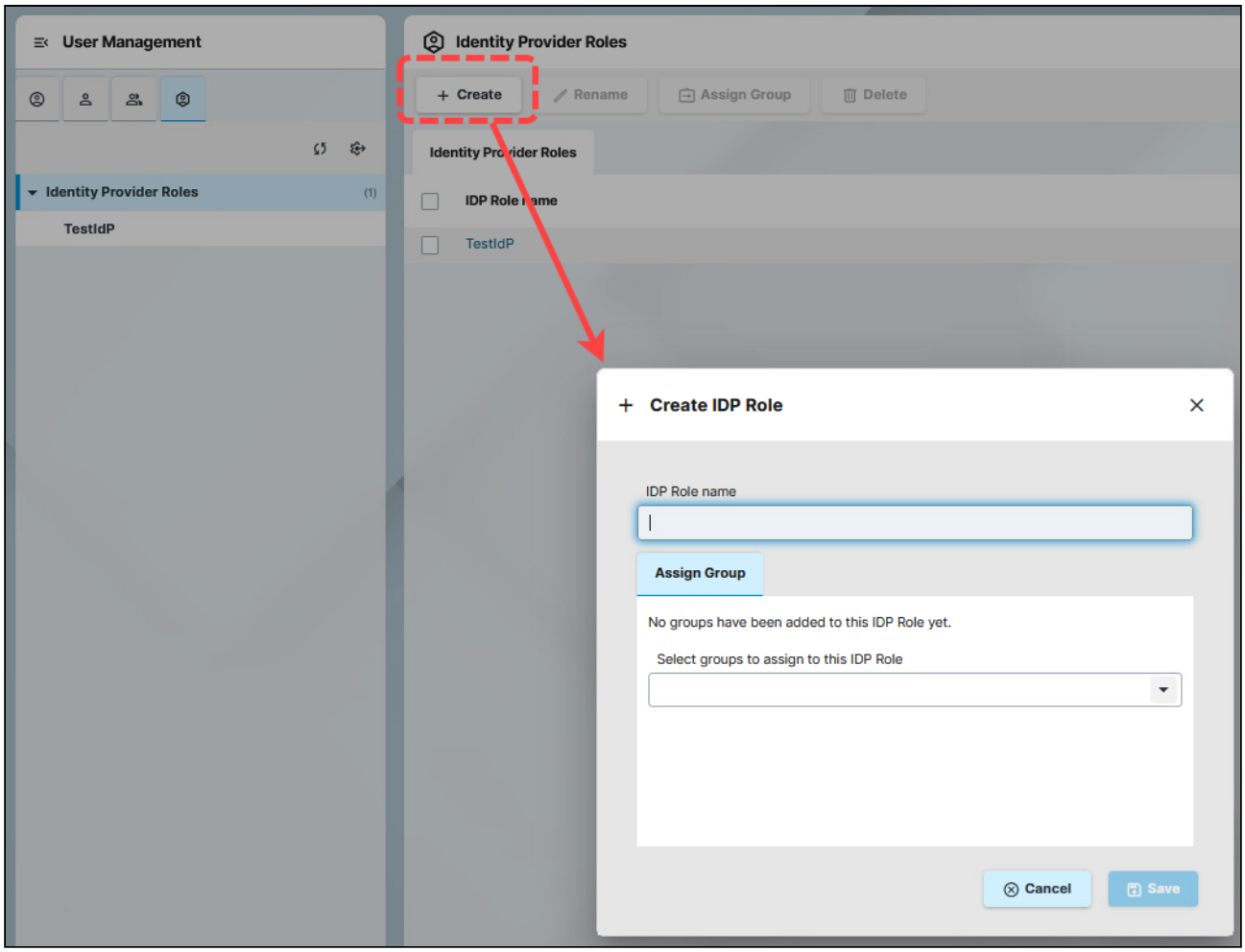
Permission Requirement
The **Identity Provider** tab is only visible for users with the Administrator accounts permission.

Mapping the IdP Roles

To map the roles created in your IdP to user groups in your UMS:

1. Go to **User Management > Identity Provider Roles**.

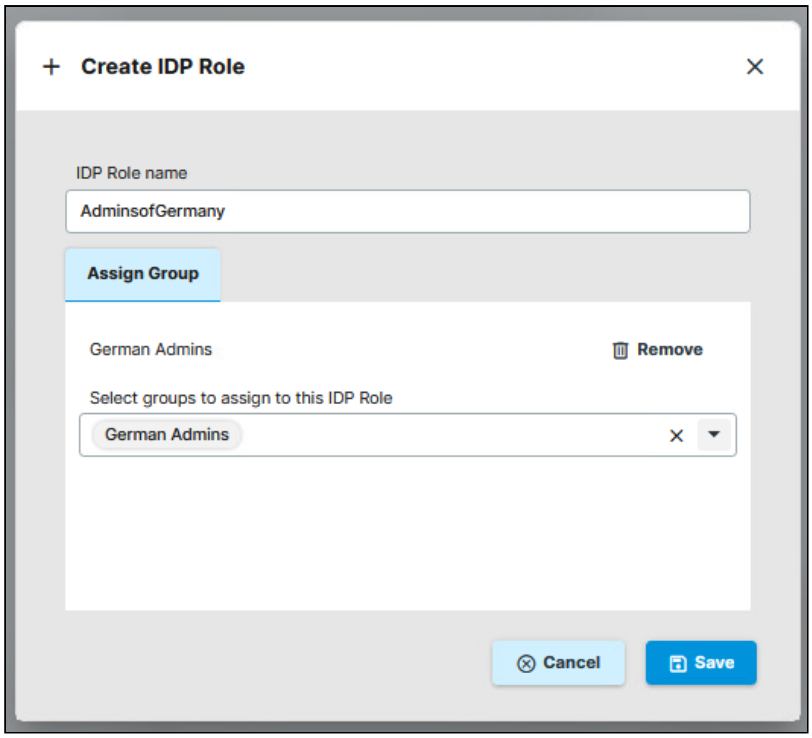
2. Click Create.



3. Under **IDP Role name**, add the value of the role configured in your IdP.

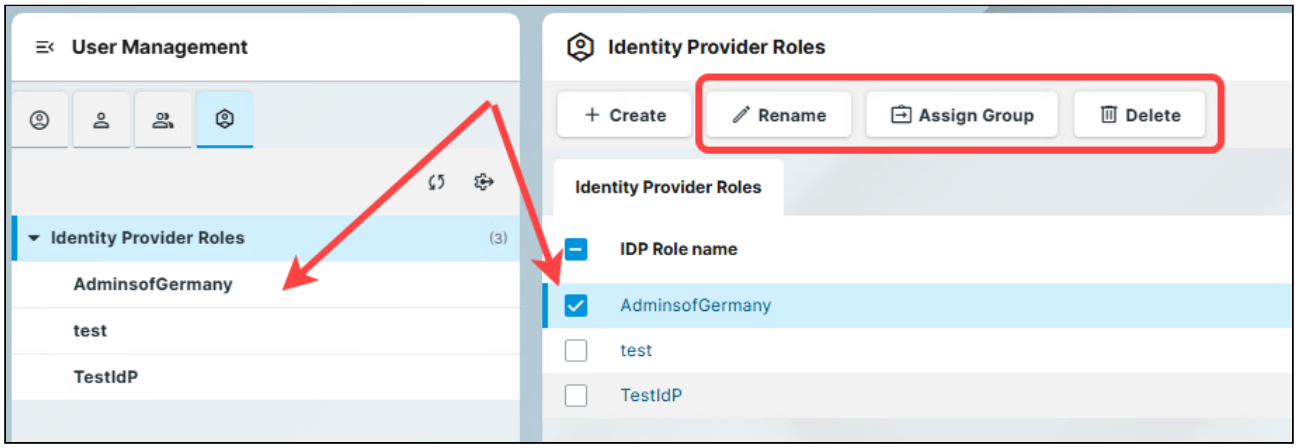
⚠ IdP Role names are case-sensitive, so the value should be exactly the same, as in your IdP client.

4. Select the groups to assign the IdP role.



5. **Save** the IdP role.

The new IdP role gets listed under the **Identity Provider Roles**. You can manage the role either by selecting from the list or by navigating to it in the structure tree.



How to Change User Password in the IGEL UMS Web App

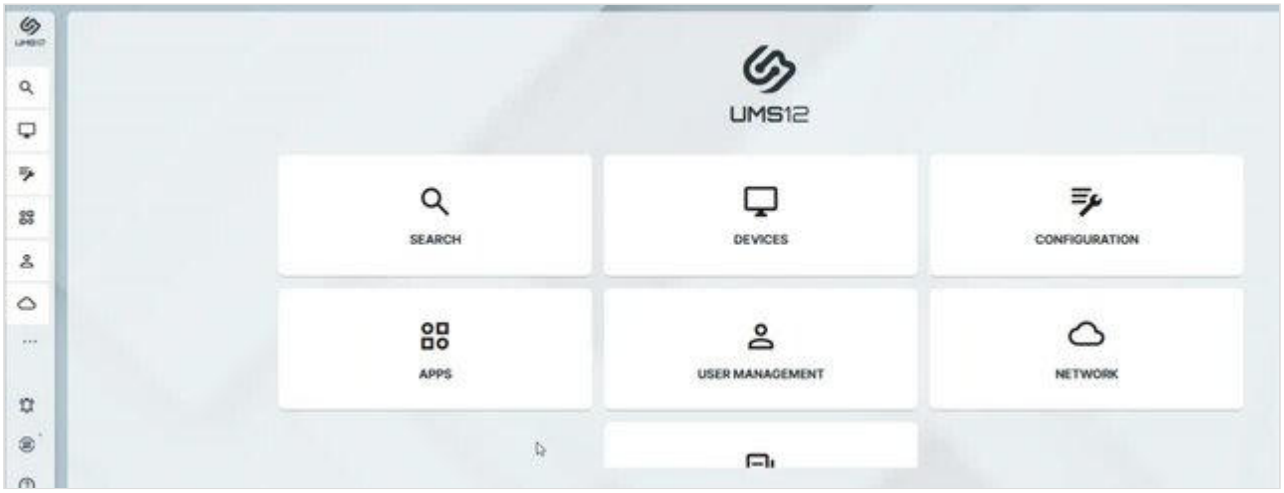
In the UMS Web App, you can change the password of the currently logged-in user, and other users as well.

In the UMS Console, you can do the same under **System > Administrator accounts**, see Administrator Accounts in the IGEL UMS (see page 1007).

> In the UMS Web App, unlike in the UMS Console, you can also change the password of the UMS superuser. You cannot change the password for Active Directory users and SSO users since these passwords are not managed by the UMS.

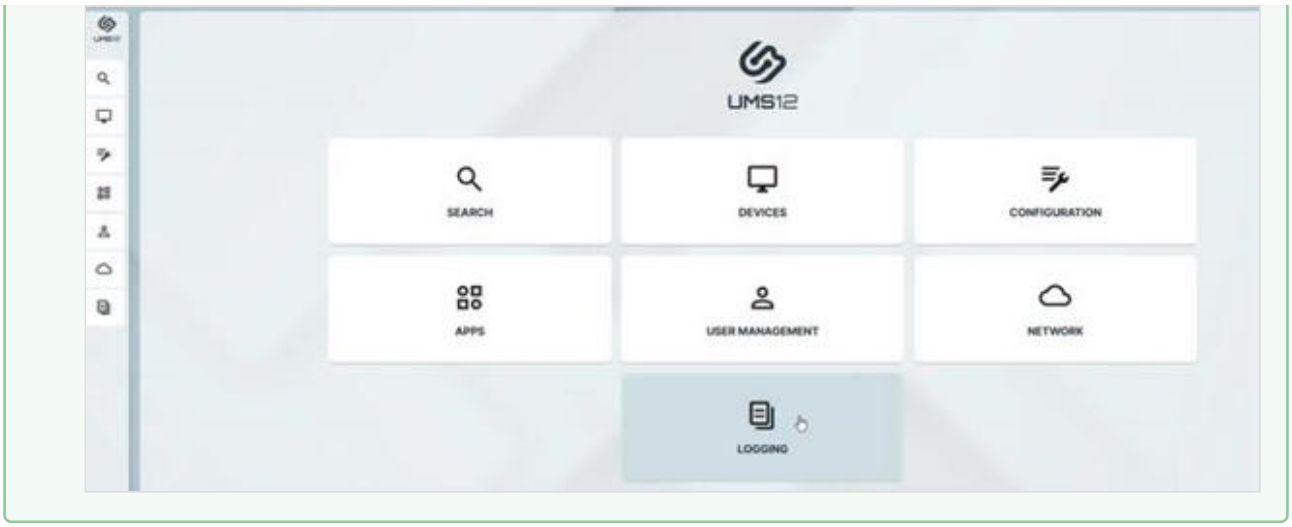
Changing Password of My User

To change the password of the currently logged-in user:



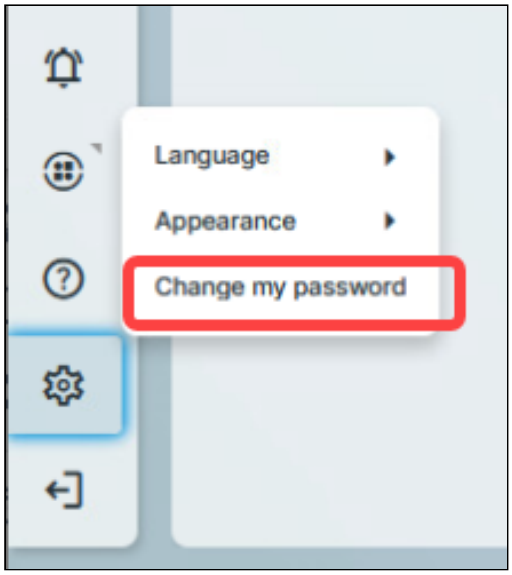
1. Go to **User Management > My User**.
2. Click **Change password**.
3. Change the password and click **Save**.

> In **Logging**, you can filter for **Change password** under **Action** to get password change logs.



Another way to change the password of the currently logged-in user:

1. Click the **Preferences** sidebar button.



2. Click **Change password**.

3. Change the password and save.

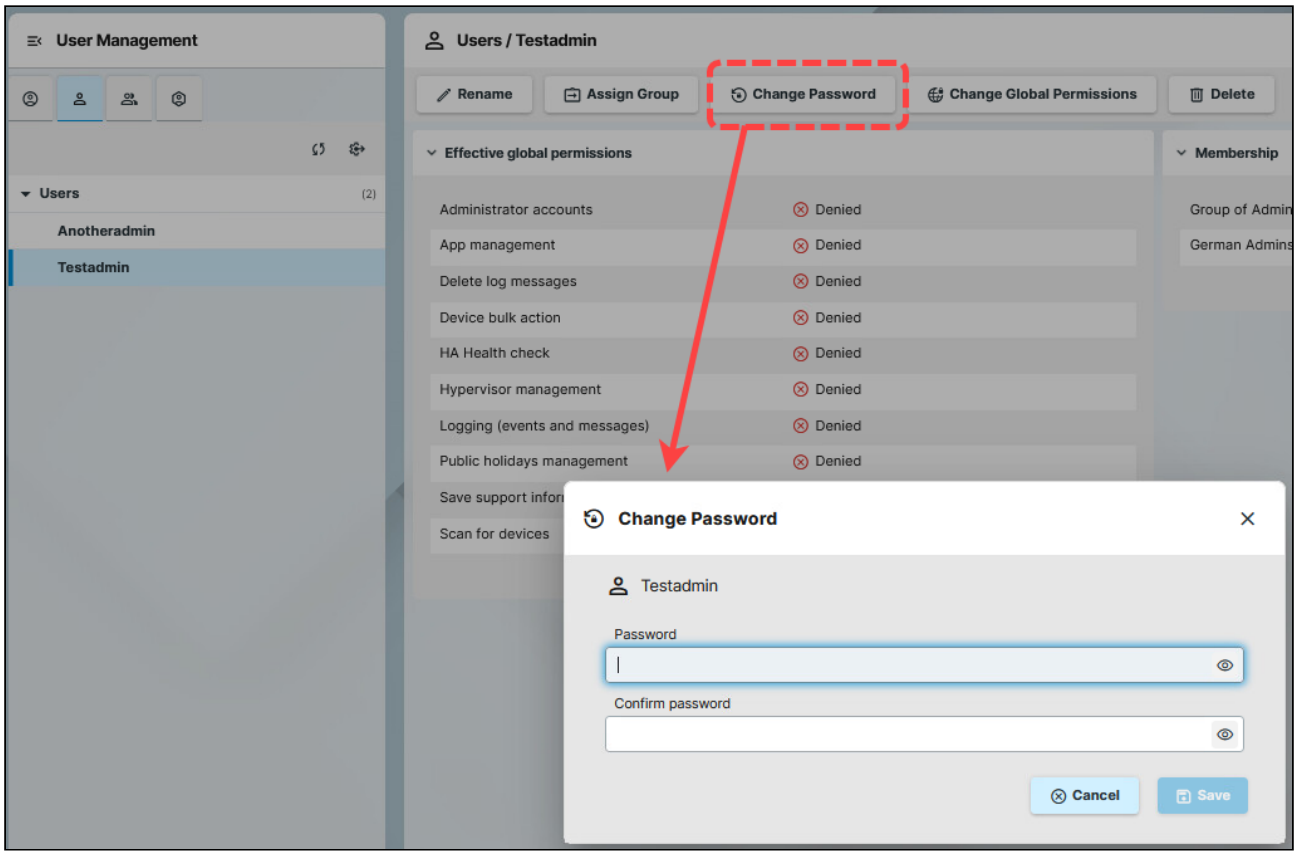
Changing Password of UMS Administrator Accounts

Permission Requirement

You need to have the Administrator accounts permission to change the password for other users.

To change the password for another user:

1. Go to **User Management > Users**.



2. Select a user.

3. Click **Change password**.

4. Change the password and save.

How to Save Support Information and Log Files in the IGEL UMS Web App

You can use the IGEL Universal Management Suite (UMS) Web App for collecting UMS and IGEL OS 12 device log files. These log files will be zipped, so you can easily send them to the IGEL Customer Support team via the IGEL Customer Portal[214].

Permission Required
The Save support information permission is required to generate the log files.

You can also use the UMS Console to collect log files. For more information, see Support Wizard - How to Send Log Files in the IGEL UMS[215] and Save Device Files for Support in the IGEL UMS[216] .

For more information on IGEL OS 12 debug settings, see Debugging / How to Collect and Send Device Log Files to IGEL Support[217].

How Can You Save Support Information from the UMS Web App?

As shown in the demo vide, you have the following options to save support information:

- You can save device logs files and/or IGEL UMS support information using the action menu in the **Devices** area.
- You can save IGEL UMS support information from the sidebar menu.

You can only save device logs from the **Devices** area. From the sidebar option, you can only save UMS support information.

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

https://www.youtube.com/watch?v=UOroSZw_Lf0

Saving Support Information of OS 12 Devices and IGEL UMS from Action Menu

In the UMS Web App, you can only save the log files of IGEL OS 12 devices. For IGEL OS 11, use the UMS Console, see Save Device Files for Support in the IGEL UMS[218] .

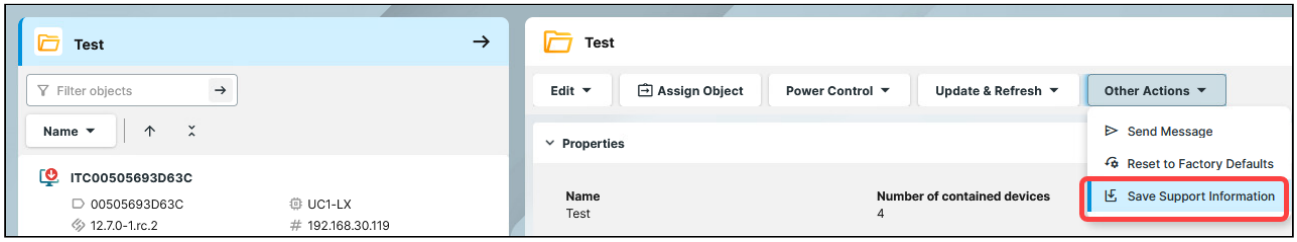
214. https://support.igel.com/
215. https://kb.igel.com/en/universal-management-suite/current/support-wizard-how-to-send-log-files-in-the-igel-u
216. https://kb.igel.com/en/universal-management-suite/current/save-device-files-for-support-in-the-igel-ums
217. https://kb.igel.com/en/how-to-start-with-igel/current/debugging-how-to-collect-and-send-device-log-files
218. https://kb.igel.com/en/universal-management-suite/current/save-device-files-for-support-in-the-igel-ums

To save support information of OS 12 devices as well as UMS:

1. Go to the device / device folder whose log files you want to save.

> When selecting a folder, you can later select from the devices of this folder in the **Save Support Information** dialog.

2. Click **Other Actions > Save Support Information** in the actions bar. For devices, you can also use the context menu.



The **Save Support Information** dialog opens.

3. Under **What to collect**, select what to include in the saved file. The action saves the selected information in a `ZIP` file. You can select if you want to save UMS support information, or OS 12 device support information, or both.
   System Information includes:
   - Summary of logs
   - Browser information
   - Log files from the UMS Server and UMS Console
   - Log files from the connected IGEL Cloud Gateway(s) and the basic information of the used ICG certificates, if present
   - API log file of the IGEL Management Interface (IMI), if used
   - Profiles and app metadata associated with the selected devices
   - Monitoring data of performance logging
     Only activate performance logging upon recommendation of IGEL Support; see Logging in the IGEL UMS (see page 987) .

   Logfiles from Devices includes:
   - Summary of logs
   - Browser information
   - Log files from devices

4. Under **Number of days included in the logfiles**, specify how many days of log data should be kept. Entries older than this will not be saved.

5. Optionally, enter the **Support Case Number** for your support case. This will be added to the name of the `ZIP` file.

6. Click **Next**.

7. Select which devices to include in the saved information.

8. Click **Next** to download the file.

You can monitor the progress of the file generation in the dialog. You can also close the dialog, the process will continue in the background.

The support information file is downloaded automatically with the naming convention: `igel-logs-<support case number>-<date>.zip`

Saving Support Information of the IGEL UMS from the Sidebar

The action saves the following information in a `ZIP` file:

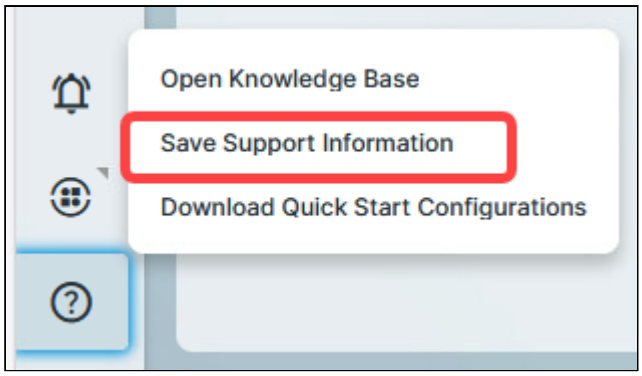
- Summary of logs
- Browser information
- Log files from the UMS Server and UMS Console
  For more on UMS log files, see Where Can I Find the IGEL UMS Log Files?[219]
- Log files from the connected IGEL Cloud Gateway(s) and the basic information of the used ICG certificates, if present
- API log file of the IGEL Management Interface (IMI), if used
- Monitoring data of performance logging
  Only activate performance logging upon recommendation of IGEL Support; see Logging in the IGEL UMS (see page 987) .

If you want to save the device logs, as well as additional information for the device (e.g. assigned profiles), see the Saving Support Information of OS 12 Devices and IGEL UMS from Action Menu (see page 1382).

To save support information of the UMS:

1. Click **Help > Save Support Information** in the sidebar.

219. https://kb.igel.com/en/universal-management-suite/current/where-can-i-find-the-igel-ums-log-files



The **Save Support Information** dialog opens.

2. Under **Number of days included in the logfiles**, specify how many days of log data should be kept. Entries older than this will not be saved.

3. Optionally, enter the **Support Case Number** for your support case. This will be added to the name of the `ZIP` file.

4. Click **Next**.

You can monitor the progress of the file generation in the dialog. You can also close the dialog, the process will continue in the background.
The support information file is downloaded automatically with the naming convention:
`igel-logs-<support case number>-<date>.zip`

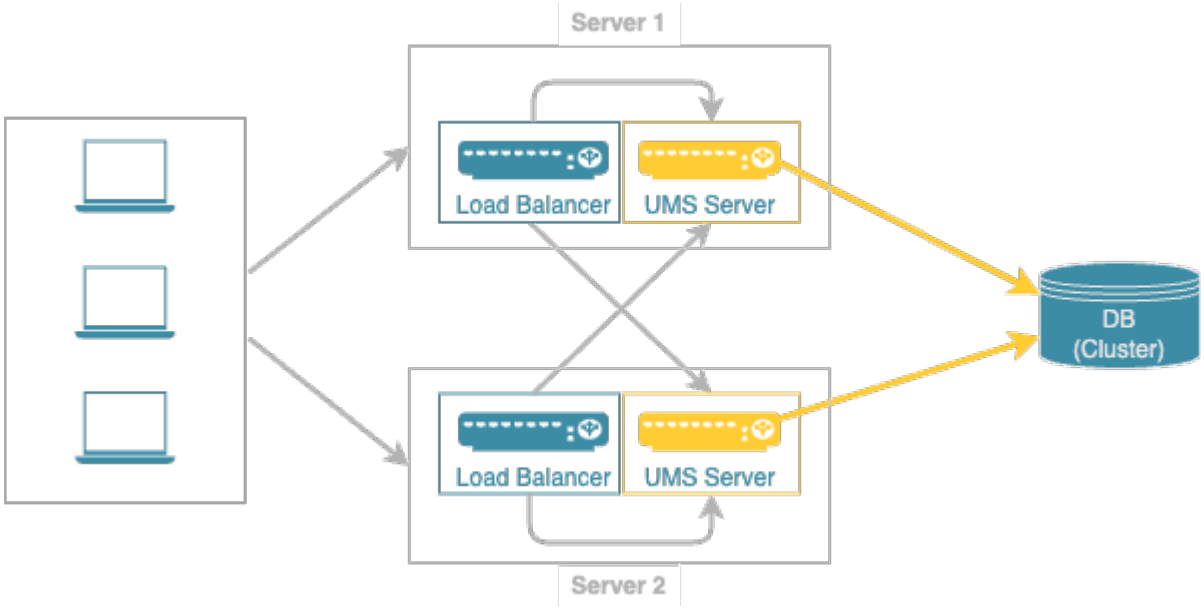
UMS Extensions

IGEL UMS High Availability (HA)

The optional High Availability extension is part of the IGEL UMS. It is designed to address the needs of large environments in which new settings need to be rolled out at once, or in which the fail-safe rollout of new settings is mission-critical for the organization concerned. The technical implementation is based on a network of several UMS Servers.

An upstream UMS Load Balancer takes over the load distribution and thus ensures that each device can receive new settings at any time – even at the start of a working day when a large number of devices log in to the UMS Server simultaneously and request new configuration profiles or firmware updates. To ensure maximum process reliability and high availability, IGEL also recommends that the UMS Load Balancer and the database have a redundant design.

Example:



See also IGEL UMS HA Configuration Options (see page 1389).

See also the collection of articles High Availability UMS (see page 512).

- UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems (see page 1420)
- IGEL UMS HA Services and Processes (see page 1425)

IGEL UMS HA Configuration Options

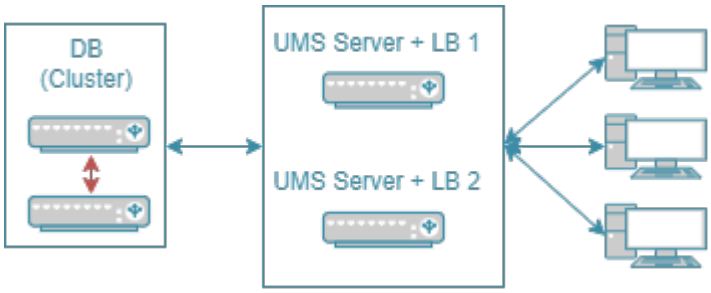
When planning the configuration of your High Availability (HA) network, you have to decide whether you want to install the UMS Server and UMS Load Balancer on the same host or on separate hosts. At the same time, there is a question how many UMS Servers and UMS Load Balancers are required. The following article describes the most common use cases and provides only general sizing recommendations. Your individual configuration may differ.

When deciding how many UMS Servers and UMS Load Balancers you need, simply counting your endpoint devices is not enough. Most importantly, you have to analyze the entire network environment as well as the other circumstances within your workplace. See Sizing Guidelines for IGEL UMS 12 and IGEL OS 12[220] and contact your IGEL reseller to get counsel.

UMS Server & UMS Load Balancer Are Installed on the Same Host Machine

The most common scenario when deploying UMS High Availability is to install the UMS Server and UMS Load Balancer on the same host machine. Both the UMS Server and the UMS Load Balancer offer redundancy and are installed on two servers. The database is ideally designed as a cluster.

Typical Use Cases	#UMS Server + UMS Load Balancer
The installation on the same host machine is suitable if • the number of devices < 50,000 • you use the Shared Workplace (see page 1427) feature	2 UMS Servers 2 UMS Load Balancers



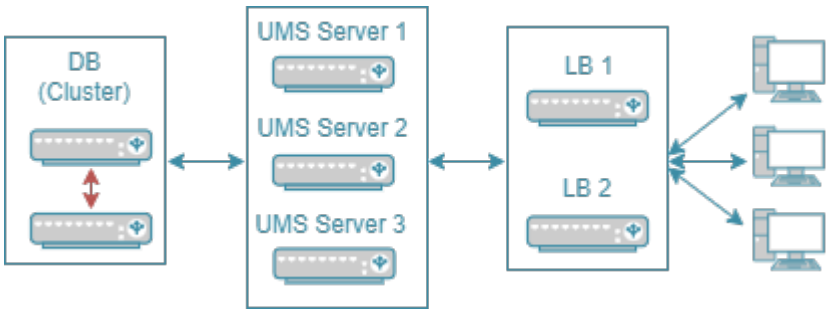
In this configuration, each of the two servers can also perform the tasks as a UMS Server alone. If both servers are active at the same time, this has a load-distributing effect. Note, however, that the load balancer generates extra load along with the actual UMS Server.

UMS Server & UMS Load Balancer are Installed on Separate Host Machines

If you need to manage a very large number of devices and/or do not want the server resources to be shared between the load balancer and the UMS Server, the installation on separate hosts should be considered.

220. https://kb.igel.com/en/universal-management-suite/current/sizing-guidelines-for-igel-ums-12-and-igel-os-12

Typical Use Cases	#UMS Server Standalone & Load Balancer Standalone
The installation of the load balancer on a separate host machine is • required if the number of devices > 50,000 • recommended if you do not want the load balancer to consume resources on the UMS Server host	Smallest typical configuration: 2-3 UMS Servers 2 UMS Load Balancers General sizing recommendations: • up to 6 UMS Servers • up to 3 UMS Load Balancers • 1 UMS Server per max. 50,000 devices • 1 LB per max. 3 UMS Servers

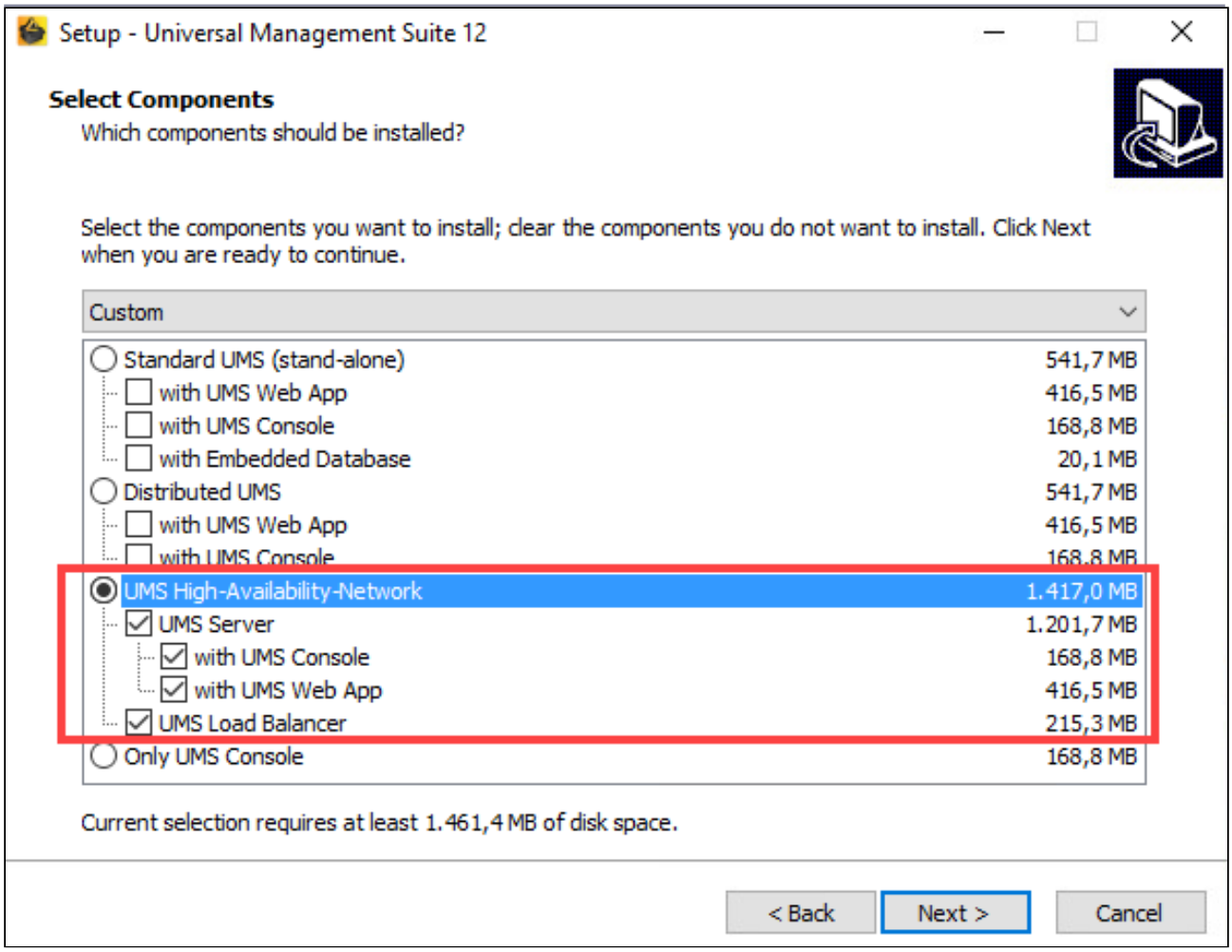


In the smallest typical configuration, queries from the devices are passed on to the UMS Servers by both load balancers. If one of the load balancers should fail, the other remains available and assumes responsibility for communications alone. A great number of UMS Servers could overload a single load balancer, which would then become itself a bottleneck. Therefore, there are provisions for no more than three UMS Servers in this configuration. For very large installations with more than three UMS Servers, the number of load balancers should be increased accordingly.

- 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 (see page 256).
- The network configuration on Windows Servers must have the TCP/IPv6 option enabled for UMS 12.
- 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.

HA Installation

To use the High Availability Extension, you have to select the option for installing the HA network components in the UMS installer.



When installing the High Availability Extension, it is important to differentiate between the installation of the first HA server and further HA servers.

During the installation of the first HA server (UMS Server obligatory), an IGEL network token is created. This network token allows the integration of new servers into the same HA network and, thus, must be used when installing all subsequent HA servers.

Follow these instructions to install the High Availability Extension:

- HA: Installation Requirements (see page 1392)
- Installing the First Server in an HA Network (see page 1394)
- Adding Further Servers to the HA Network (see page 1401)

For information on how to update the HA installation, see Updating the Installation of an HA Network (see page 1407).

HA: Installation Requirements

In order to install an IGEL UMS High Availability network, your hardware and software must meet the following minimum requirements.

The installation requirements can vary depending on how large your HA environment is. For more information, see Installation and Sizing Guidelines for IGEL UMS.

UMS High Availability Network: Minimum Requirements

UMS Server (includes UMS Server, UMS Administrator, and UMS Console)	UMS Load Balancer	UMS Web App	File System
UMS Server: • At least 4 GB of RAM • At least 2 GB of free HDD space UMS Console: • At least 3 GB of RAM • At least 1 GB of free HDD space UMS Administrator: • At least 1 GB of RAM	• At least 1 GB of RAM • At least 1 GB of free HDD space	• 1 GB of RAM • 1 GB of free HDD space	• 1 GB for the program files • Approx. 10 GB for each firmware update to be downloaded
For the supported operating systems, see the Supported Environment section of the release notes.[221]			

- The UMS Server must not be installed on a domain controller system!
- Manually modifying the Java Runtime Environment on the UMS Server is not recommended.
- Running additional Apache Tomcat web servers together with the UMS Server is not recommended either.

- 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 (see page 256).

221. http://www.igel.com/igel-ums-universal-management-suite/

- The network configuration on Windows Servers must have the TCP/IPv6 option enabled for UMS 12.
- 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.

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 909).

Database Systems (DBMS)

For details on the supported database systems, see the "Supported Environment" section of the release notes (see page 1440). Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

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

The database system must be accessible to all UMS Servers.

Installing the First Server in an HA Network

Prerequisites

- A set of servers with the operating system supported by the UMS; see the "Supported Environment" section of the release notes (see page 1440).
- A database system supported by the UMS; see the "Supported Environment" section of the release notes (see page 1440).
- All installation requirements described under HA: Installation Requirements (see page 1392) are fulfilled.
- The current version of the UMS is downloaded from the IGEL Download Server[222].

For the first installation, it is advisable to use a server without an existing UMS installation.

Instructions

To install the UMS High Availability (HA) Extension on the first server, follow the instructions in the order given:

1. Preparing the Database (see page 1394)
2. Preparing the Servers (see page 1394)
3. Starting the Installation (see page 1395)
4. Defining the Database Connection (see page 1398)
5. Checking the Installation (see page 1399)
6. Saving the IGEL Network Token (see page 1399)

Preparing the Database

→ Create a database schema and a user for the UMS. Use the relevant DBMS program and its documentation. See also Connecting External Database Systems (see page 63).

Preparing the Servers

1. Verify that each server can "see" the other servers via the network.

- 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 (see page 256).
- The network configuration on Windows Servers must have the TCP/IPv6 option enabled for UMS 12.

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

- 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.

2. Verify that the time on all servers is synchronized.

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

3. For Linux systems, make the directory `/root` writable for the user `root`.

Starting the Installation

1. Launch the UMS installer.

   ℹ You need administration rights to install the IGEL UMS HA.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.
5. Depending on your desired HA network configuration (see page 1389), select the components to be installed: **UMS Server + UMS Load Balancer** or **UMS Server**.

⚠

Installing UMS Server and UMS Load Balancer on Separate Servers

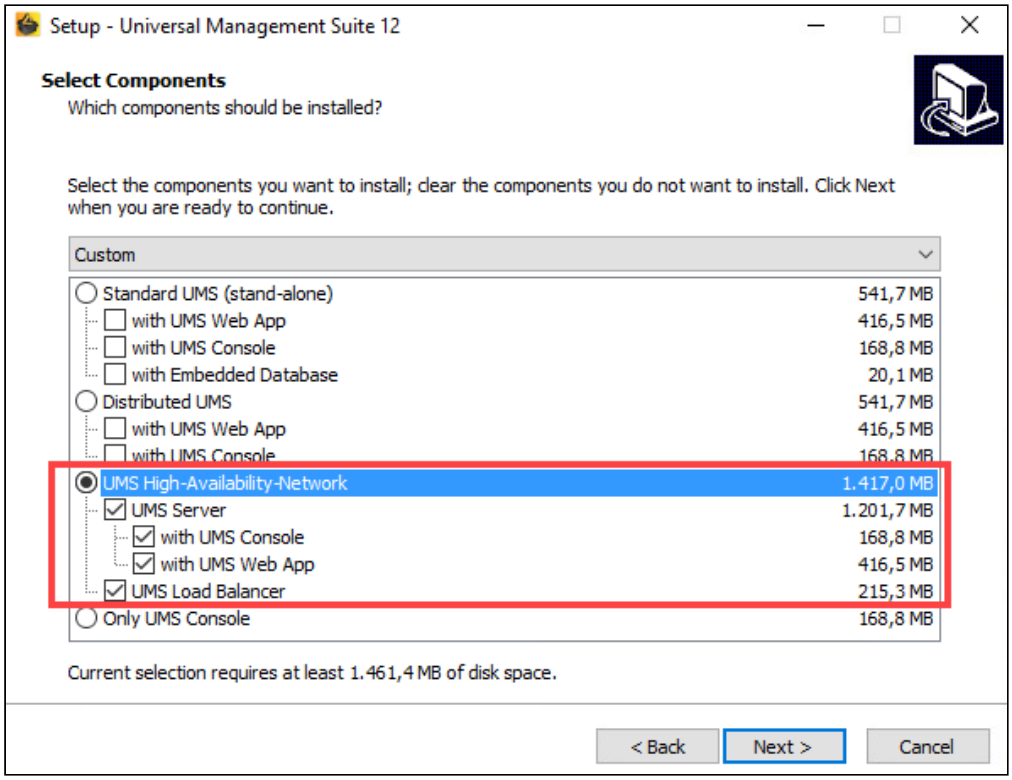
If you install HA network components on separate servers, **UMS Server** must always be installed first. In this case, the IGEL network token, which is required for the integration of further servers into the HA network, will be created. Additionally, the UMS Administrator application, necessary for the further management of the installation, will be installed too. After configuring and enabling the database via the UMS Administrator, the UMS Server will be available in the HA network.
If you install an individual UMS Load Balancer, neither the IGEL network token nor UMS Console nor UMS Administrator will be installed. Only the option for uninstalling the UMS will then be set up in the Windows start menu.

ℹ

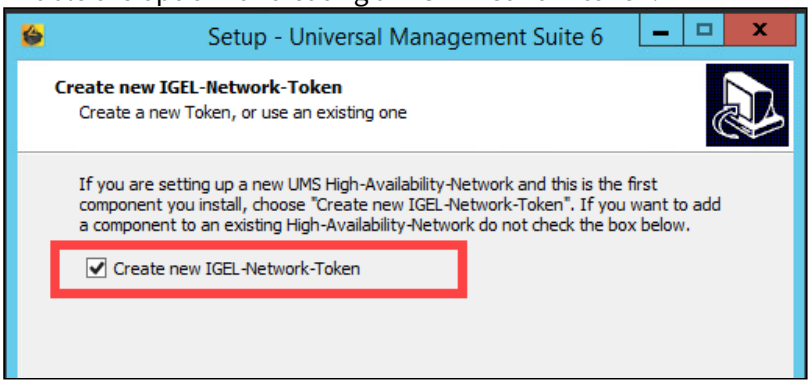
- For the management of the UMS installation, you require the UMS Console. In multi-instance installations, the UMS Console does not necessarily have to be installed on every UMS Server.
  Note: For security, performance, or other reasons, the UMS Console is often additionally installed on a separate 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 (see page 1155).
- 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 661).

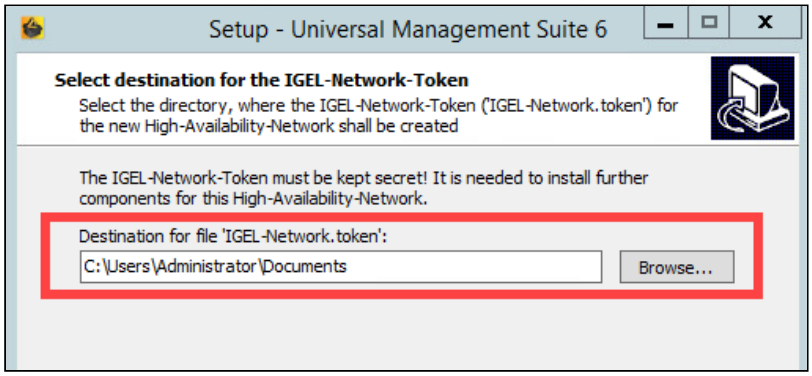


6. Confirm the system requirements dialog if your system fulfills them.
7. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.
8. Enable the option for creating an IGEL network token.



9. Specify a directory for saving the IGEL network token. The directory must be writeable for the administrator.

⚠ Keep the IGEL network token in a safe place! It will be needed for all subsequent server installations. If the IGEL network token is lost, the complete installation must be started again.



10. Optional: Under **Import existing keystore**, you can load the `tc.keystore` file from an existing UMS installation.

⛔ This function can destroy your UMS installation. Do not import this file unless you know exactly what you are doing.

11. 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 Universal Management Suite Network Configuration (see page 265)) 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 (see page 256) .

12. Under **Select Start Menu Folder**, specify a folder name for the shortcut.

13. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and UMS Administrator (see page 1037) on the desktop.
14. Read the summary and start the installation process.
15. Close the UMS installer once the installation is complete.
    The UMS installer creates entries in the Windows software directory and the start menu. If this was selected, shortcuts for the UMS Console and UMS Administrator will also be placed on the desktop.

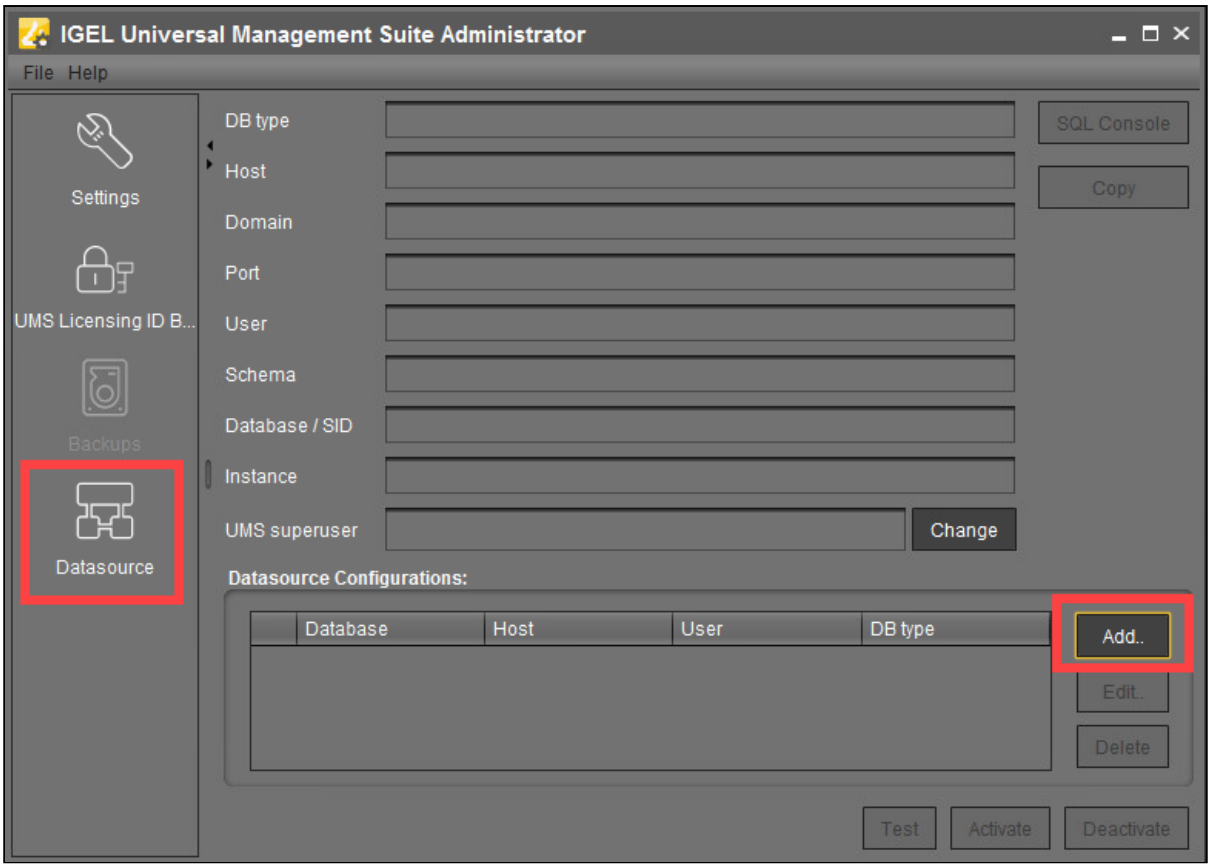
If SQL Server AD Native is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For more information, see Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84).

Defining the Database Connection

1. Open the UMS Administrator.

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

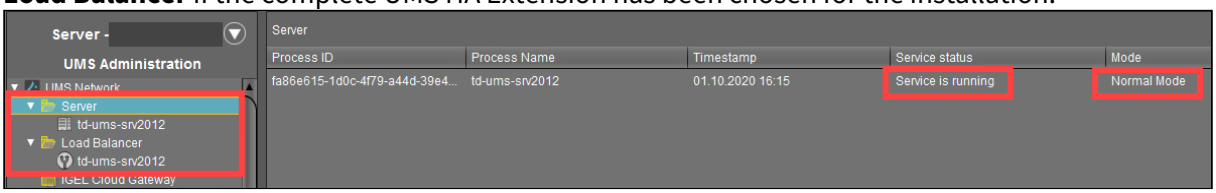
2. Select **Datasource > Add**.



3. Enter the connection properties of the prepared database schema. See also How to Set Up a Data Source in the IGEL UMS Administrator (see page 1073).
4. Click **Activate** to enable the data source. See also Activating a Data Source (see page 1062).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 1425).
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer** if the complete UMS HA Extension has been chosen for the installation.



Saving the IGEL Network Token

→ Save the IGEL network token, i.e. the file `IGEL-Network.token`, on a storage medium which will be accessible when installing further HA servers (e.g. on the network or on a portable storage medium such as a USB stick). Always keep the IGEL network token well protected.

Next Step

>> Proceed with adding a further server to the HA installation, see Adding Further Servers to the HA Network (see page 1401).

Adding Further Servers to the HA Network

Further HA servers – with UMS Server, UMS Load Balancer, or both – can be installed in the same way as the first one. However, you do not need to create a new IGEL network token. Instead, you must select the network token created previously during the installation of the first server in an HA network.

In addition, a connection with the same database that is used by the first server must be established. The UMS HA network only works if all servers are connected to the same database.

Prerequisites

- A High Availability (HA) installation with a configured database, see Installing the First Server in an HA Network (see page 1394) .

⚠ The database connection should be defined during the installation of the first UMS Server in an HA network. In this case, all relevant configuration information is automatically copied to the additional UMS Servers.

- The IGEL network token created during the installation of the first server in the HA network, see Installing the First Server in an HA Network (see page 1394) .
- A server with the operating system supported by the UMS; see the "Supported Environment" section of the UMS Release Notes (see page 1440) .
- All installation requirements described under HA: Installation Requirements (see page 1392) are fulfilled.
- The same version of the UMS as for the first HA server is downloaded from the https://www.igel.com/software-downloads/ .

Instructions

To add a new server to the UMS HA installation, follow the instructions in the order given:

1. Preparing the Server (see page 1401)
2. Preparing the IGEL Network Token (see page 1402)
3. Starting the Installation (see page 1402)
4. Checking the Installation (see page 1405)

Preparing the Server

1. Verify that the server can "see" the other servers via the network.

⚠
- 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 (see page 256) .
- The network configuration on Windows Servers must have the TCP/IPv6 option enabled for UMS 12.

- 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 IGEL UMS Installation (see page 13)) is, however, supported in cloud environments as of UMS version 6.10.

2. Verify that the time on all servers is synchronized.

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

3. For Linux systems, make the directory `/root` writable for the user `root`.

Preparing the IGEL Network Token

→ If you have not yet done so, save the IGEL network token created during the installation of the first HA server, e.g. on a portable storage medium.

ℹ If the path has not been changed, the file `IGEL-Network.token` can be found by default in the home directory of the administrator user on a UMS Server host.

⚠ If you have a fully functional UMS HA network already in use and simply want to enlarge it with one more HA server, make sure you use for the additional HA server installation the **current** IGEL network token.
If you have not saved it:
→ Restart the `IGEL RMGUIServer` service (for the instruction, see IGEL UMS HA Services and Processes (see page 1425)) and use in this case the network token created upon the UMS Server startup from the directory:
Windows: `C:\Windows\System32\config\systemprofile\IGEL-Network.token`
Linux: `/root/IGEL-Network.token`

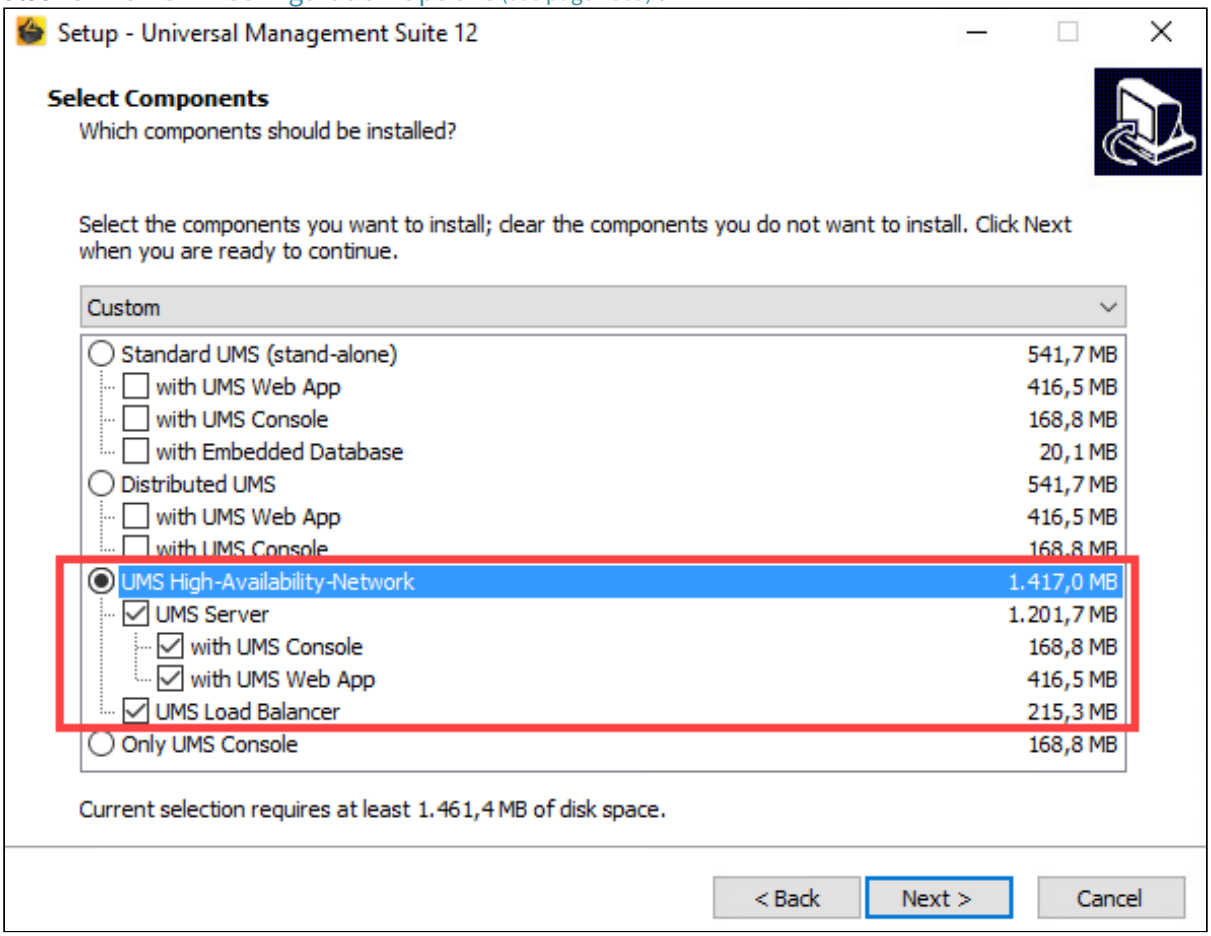
Starting the Installation

1. Launch the UMS installer.

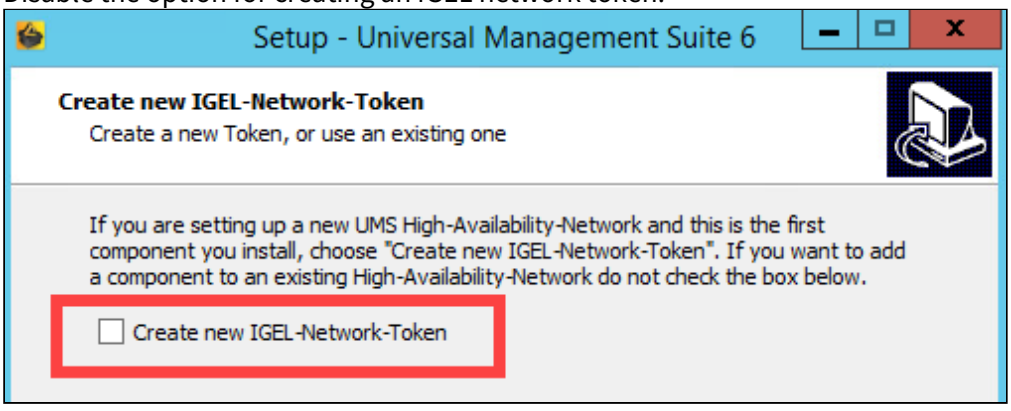
ℹ You need administration rights to install the IGEL UMS HA.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Select a path for the installation.

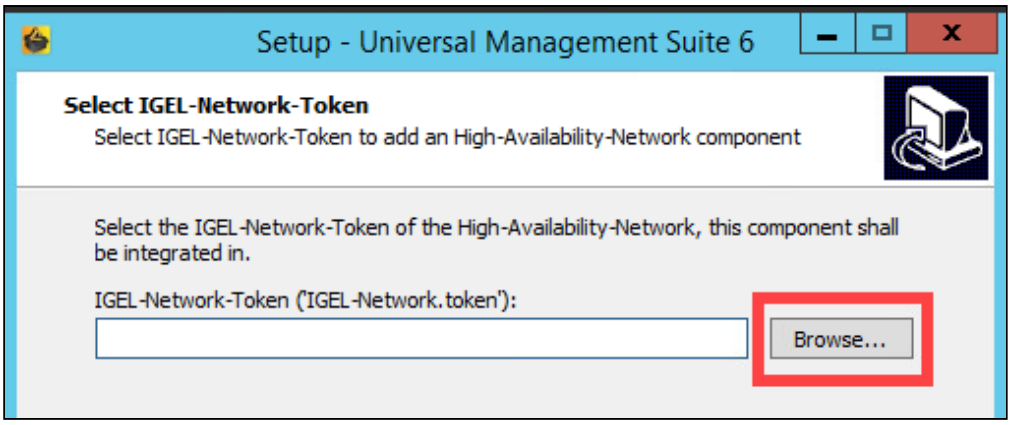
5. Select the components to be installed depending on your desired HA network configuration. See also IGEL UMS HA Configuration Options (see page 1389) .



6. Confirm the system requirements dialog if your system fulfills them.
7. Select the **UMS data directory**, in which Universal Firmware Updates and files are to be saved.
8. Disable the option for creating an IGEL network token.



9. Select the IGEL network token to be used.



10. 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 Universal Management Suite Network Configuration (see page 265)) 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 (see page 256) .

11. Under **Select Start Menu Folder**, specify a folder name for the shortcut.
12. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and UMS Administrator on the desktop.
13. Read the summary and start the installation process.
14. Close the UMS installer once the installation is complete.

If you have included a UMS Server in the installation, the UMS installer creates entries in the Windows software directory and the start menu. The UMS Console and UMS Administrator applications are installed, and, if this was selected, their shortcuts are placed on the desktop.

If you have installed an individual load balancer, only the option for uninstalling the UMS will be set up in the Windows start menu. No configuration on the load balancer is necessary. It connects automatically to the HA network during booting.

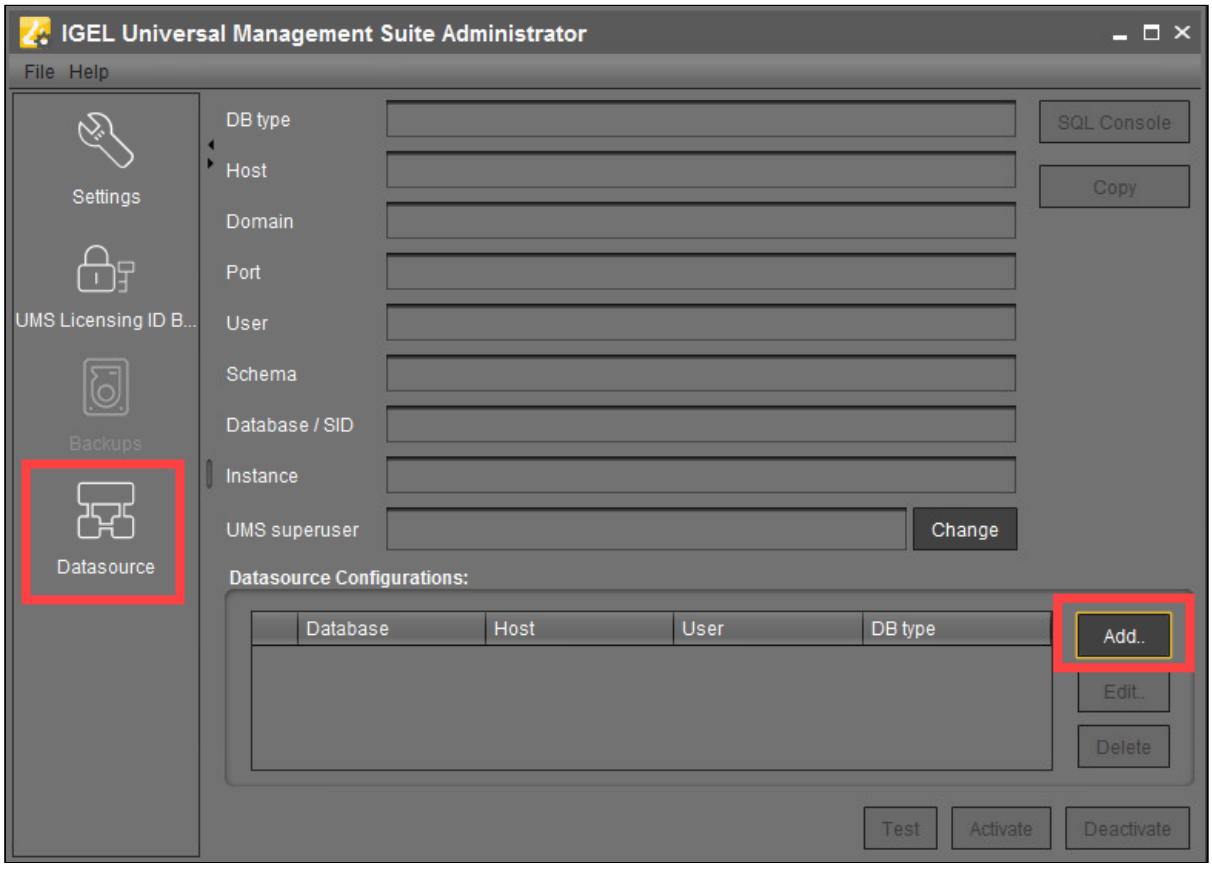
If SQL Server AD Native is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For more information, see Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84) .

Checking the Installation

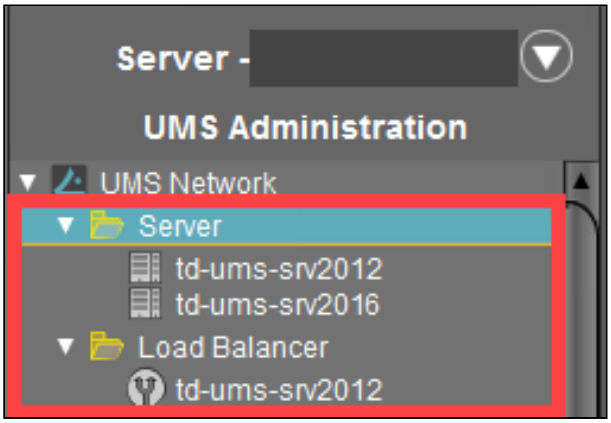
1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 1425) .
2. If you have included a UMS Server in the installation, open **UMS Administrator > Datasource** and verify that the database connection has been successfully transferred from the already running UMS Server.

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

If the database connection has not been defined automatically, enter under **UMS Administrator > Datasource > Add** exactly the same database parameters you used during the installation of the first HA server (see page 1398) and click **Activate**.



3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and/or **Load Balancer**.



Additionally, you can use the feature for checking the HA installation, see UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems (see page 1420) .

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 668).

For the future, you may also find it useful to read: Creating a Backup of the IGEL UMS (see page 1051) and Which Files Are Automatically Synchronized between the IGEL UMS Servers? (see page 514) .

Updating the Installation of an HA Network

Use Case

You have a UMS IGEL UMS High Availability (HA) (see page 1387) installation and need to update it.

General Overview

There are two possible HA update procedures:

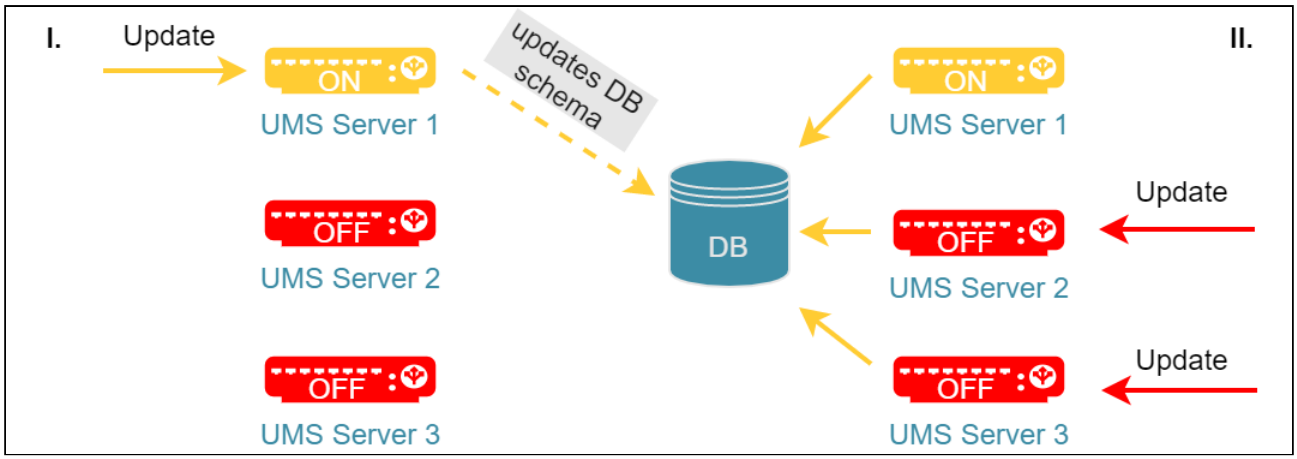
- With short downtime of the servers (see page 1407)(recommended)
- Without downtime of the servers, but with automatic copying the productive database to a temporary database (see page 1408), which generally results in longer update time

With Short Downtime

In this case, the update procedure generally looks as follows:

1. Stop all UMS Servers except one (verify this in the server list of the UMS Console connected to the last running server).
2. Update this UMS Server.
   As soon as the update is complete, the productive database will be updated upon server startup.
3. Update the remaining UMS Servers (simultaneously or one after another).
   When the update is complete, they will automatically connect to the productive database.
4. Update other components like separate UMS Load Balancers and/or UMS Consoles.

For detailed instructions, see How to Update a UMS HA Installation: With Downtime of the Servers (see page 1409).



IGEL recommends using this HA update method due to a number of advantages:

- The update procedure is much faster.

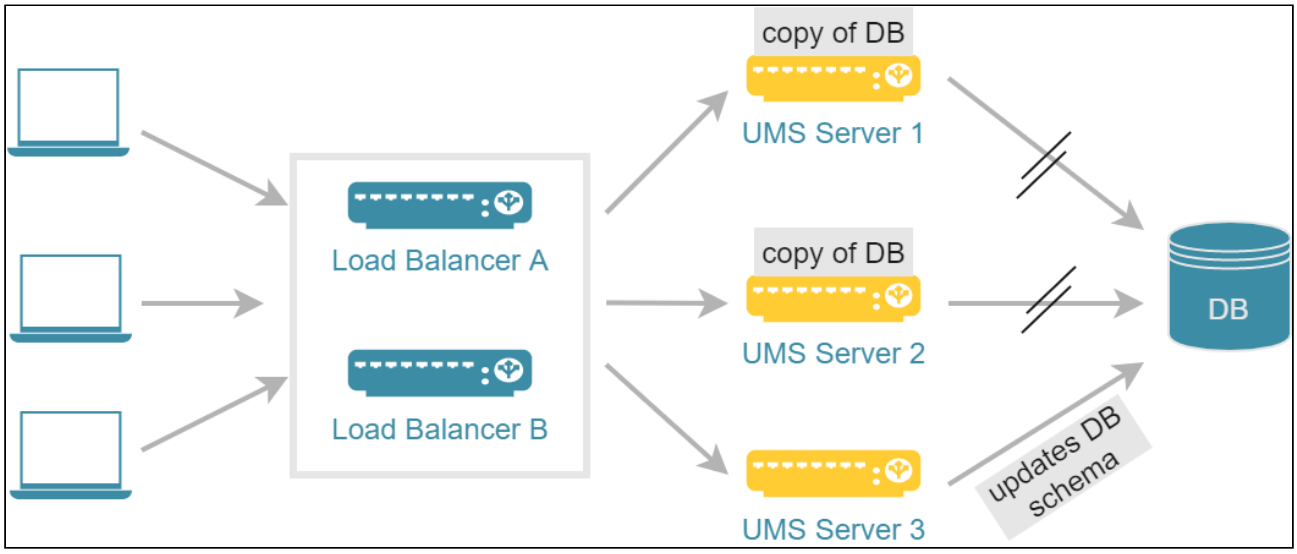
- No database inconsistencies since no other servers and processes use the database during the update.
- Only short downtime. Note: Since there is no communication between the servers and devices (during the update of the first UMS Server), user-specific profiles cannot be supplied (IGEL Shared Workplace).

Without Downtime

In this case, the update procedure generally looks as follows:

1. Update all UMS Servers to a new version, one server after another.
   While being updated, a UMS Server disconnects itself from the productive database and stores a copy of it locally in an embedded Derby database. The copy is created for each server except the last. The last UMS Server also updates the schema of the productive database. After this, all other UMS Servers connect themselves again to the original productive database.
2. Update other components like separate UMS Load Balancers and/or UMS Consoles.

For detailed instructions, see How to Update a UMS HA Installation: Without Downtime of the Servers (see page 1414).



⚠ By this update method, all UMS Servers can be addressed by the endpoint devices at any time during the update process, e.g. to supply user-specific profiles (IGEL Shared Workplace). However, note the following:

- The copying of the data from the productive database to the temporary database can take a lot of time.
- Requests from devices can interfere with the copying process.
- Changes in the temporary database are lost as soon as the servers switch back to the productive database when the update is complete.

- How to Update a UMS HA Installation: With Downtime of the Servers (see page 1409)
- How to Update a UMS HA Installation: Without Downtime of the Servers (see page 1414)

How to Update a UMS HA Installation: With Downtime of the Servers

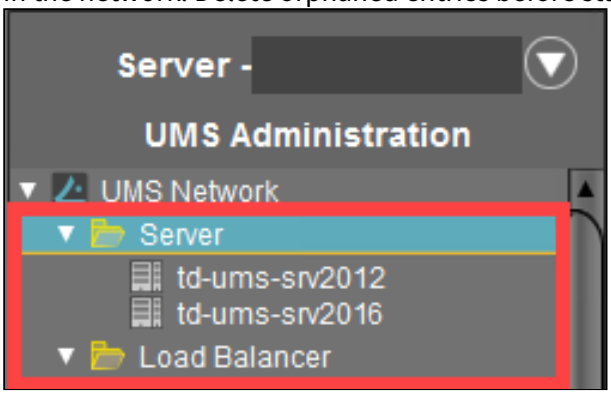
For a short overview of the High Availability (HA) update procedure, see Updating the Installation of an HA Network (see page 1407).

To update the HA installation, follow these instructions in the order given.

Preparing the Update

Perform the following steps before updating a server:

1. Download the current version of IGEL Universal Management Suite from the IGEL Download Server[223] and distribute the installer file to all systems with UMS components (UMS Server, UMS Load Balancer, UMS Consoles).
2. In the UMS Console, call up the list of UMS Servers and Load Balancers in the HA network under **UMS Administration > UMS Network** and check whether the listed components really exist in the network. Delete orphaned entries before starting the process for updating the components.



3. Create a backup of your database before starting the update installation. Use the backup procedures recommended by the DBMS manufacturer. See also Creating a Backup of the IGEL UMS (see page 1051).

> **Warning**
>
> It is not possible to install a UMS version which is older than the current one. If you want to change to an older version (e.g. from 6.10 to 6.09), you will need to install a separate HA network and restore a database backup of the corresponding schema. This is also one of the reasons why you should back up the running system before updating the UMS HA network.
> 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.

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

4. Verify that the time on all servers is synchronized.

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

Updating UMS Servers

The main feature of this update method is that it checks at the beginning how many UMS Servers are "online". If the server where the update has been started is the only one active, no temporary database with a copy of the productive database is created and the productive database is updated immediately, i.e. as soon as the UMS Server starts after the update is complete. Therefore, it is necessary to leave ONLY ONE UMS Server running, i.e. the one you start the update procedure with. This can be any UMS Server within your HA network.

1. Stop all UMS Servers except the one, on which you are going to start the update. You can stop UMS Servers in the UMS Console under **UMS Administration > UMS Network > Server > [Server name] > Stop service** or in Windows Services, see IGEL UMS HA Services and Processes (see page 1425).
2. Verify that only one UMS Server is running and the others are stopped:
   - by checking the list of servers in the UMS Console under **UMS Administration > UMS Network > Server**
     OR
   - with the following SQL statement:

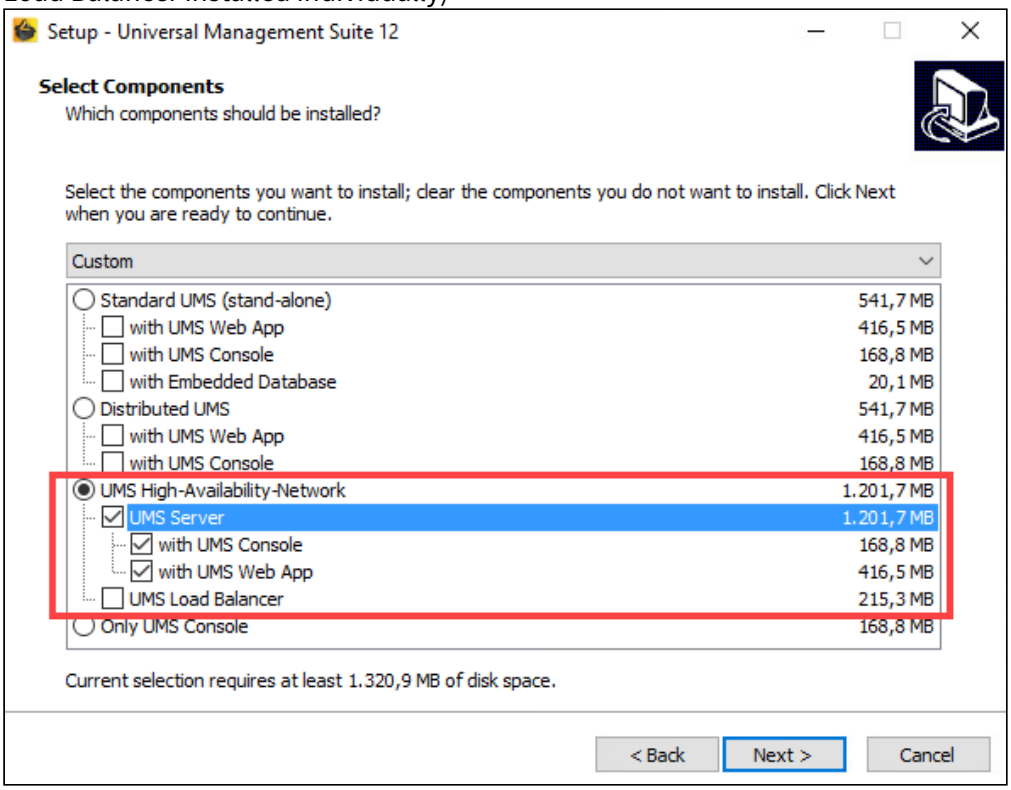
```
select
       ep.epr_process_id,
       ep.epr_process_host,
       ep.epr_process_mode,
       ep.epr_service_status
from
       epr_processes ep
where
       ep.epr_process_type = 'UMS_RMGUISERVER'
```

     `SERVICE_RUNNING` must be shown only for the server you are about to update.
     `SERVICE_STOPPED` must be shown for all the other servers.
3. Launch the UMS installer.

> ℹ You need administration rights to update the IGEL UMS HA.

When installing the UMS Server as a part of the HA network on Linux, the directory `/root` must be writable for the user `root`.

4. Read and confirm the **License Agreement**.
5. Read the **Information** regarding the installation process.
6. Verify the components to be installed. (In this example: HA network with UMS Server and UMS Load Balancer installed individually)



7. Confirm the system requirements dialog 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 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 Universal Management Suite Network Configuration (see page 265)) or at the UMS Server.

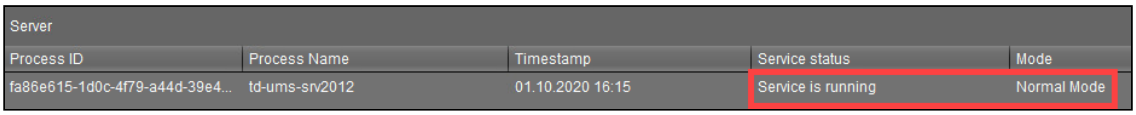
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL https://app.igel.com/ (TCP 443) is required.
- For the UMS Web App, TCP 8443 `/webapp/*` and `/wums-app/*` are required.
- For the UMS Console, the root is required, i.e. TCP 8443 `/*`
- For IGEL OS 11 devices, TCP 30001 and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

For more information on UMS ports, see IGEL UMS Communication Ports (see page 256) .

10. Read the summary and start the installation process.
11. Close the UMS installer once the installation is complete.
    The UMS Server will start and update the database.

If SQL Server AD Native is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For more information, see Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84).

12. Open the UMS Console and go to **UMS Administration > UMS Network > Server** to verify that the server is
    - successfully updated
    - running
    - in normal mode



13. Update the remaining UMS Servers, either simultaneously or one after another, by repeating steps 3-11.
    After the update, the servers will automatically start and connect to the productive database.

Updating Further Components

After updating the UMS Servers within the HA network, you have to update all other current UMS components, e.g. separate UMS Load Balancers and UMS Consoles.

1. In order to do this, run the UMS installer on the systems.
2. Verify the components to be installed.

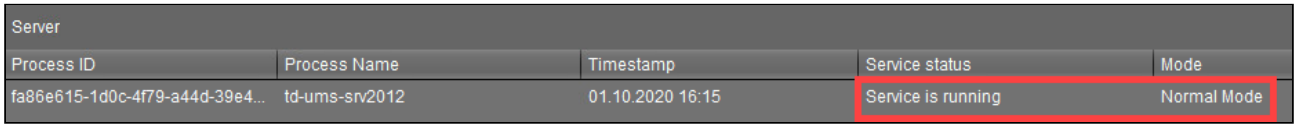
You cannot connect to the UMS Server with a console version that is older than the version of the UMS Server.

Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

See also Troubleshooting: Load Balancer Is Not Stopping during the Update of the HA Installation (see page 513).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 1425).
2. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer**.
   All servers and load balancers must be:
   - updated
   - running
   - in normal mode



How to Update a UMS HA Installation: Without Downtime of the Servers

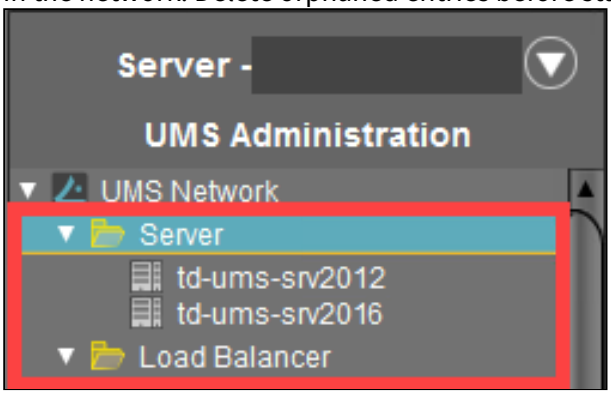
Before the update, see Updating the Installation of an HA Network (see page 1407).

To update the HA installation, follow these instructions in the order given.

Preparing the Update

Perform the following steps before updating a server:

1. Download the current version of IGEL Universal Management Suite from the IGEL Download Server[224] and distribute the installer file to all systems with UMS components (UMS Server, UMS Load Balancer, UMS Consoles).
2. In the UMS Console, call up the list of UMS Servers and Load Balancers in the HA network under **UMS Administration > UMS Network** and check whether the listed components really exist in the network. Delete orphaned entries before starting the process for updating the components.



3. Create a backup of your database before starting the update installation. Use the backup procedures recommended by the DBMS manufacturer. See also Creating a Backup of the IGEL UMS (see page 1051).

   Warning

   It is not possible to install a UMS version which is older than the current one. If you want to change to an older version (e.g. from 6.10 to 6.09), you will need to install a separate HA network and restore a database backup of the corresponding schema. This is also one of the reasons why you should back up the running system before updating the UMS HA network.
   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.

4. Verify that the time on all servers is synchronized.

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

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

Updating UMS Servers

In the update mode, the UMS Servers run with a local copy of the database. This ensures that they can answer requests from the devices and transfer configuration settings and profiles to the devices.

> In the update mode, you can connect to the servers via the UMS Console. All changes made in the UMS Console during this time will be lost after the update.

> Warning
>
> Do not make changes in the productive database during the update process. This is because decoupled servers work with a copy of the database schema in the meantime. For this reason, the update of all components within the UMS HA network should be carried out immediately. Implement a test system for the first installation of new IGEL UMS versions and check their processes before transferring them to the productive system. This also applies to hotfixes, patches, etc. for server systems and databases.

Updating the First UMS Servers

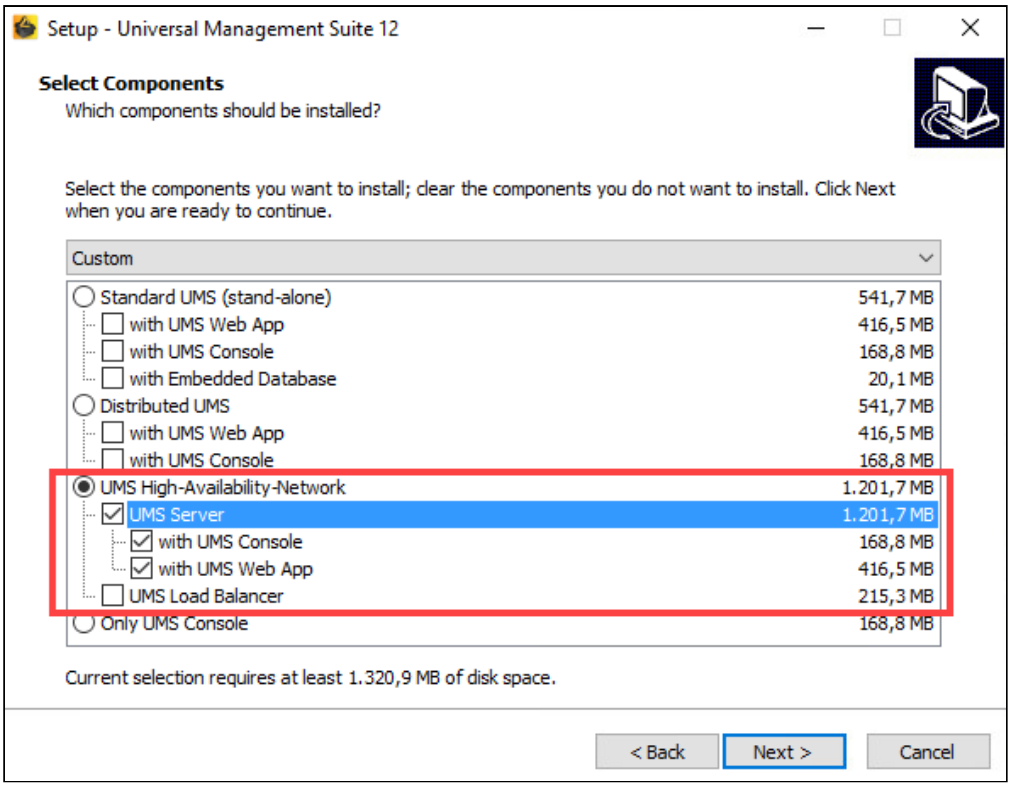
You can select any UMS Server within the HA network to start the update procedure.

1. Launch the UMS installer.

   > You need administration rights to update the IGEL UMS HA.

   > When installing the UMS Server as a part of the HA network on Linux, the directory `/root` must be writable for the user `root`.

2. Read and confirm the **License Agreement**.
3. Read the **Information** regarding the installation process.
4. Verify the components to be installed. (In this case: HA network with UMS Server and UMS Load Balancer installed individually)



5. Confirm the system requirements dialog if your system fulfills them.
6. Under **Select Additional Tasks**, specify whether you would like to create shortcuts for the UMS Console and UMS Administrator on the desktop.
7. 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 Universal Management Suite Network Configuration (see page 265)) 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 (see page 256) .

8. Read the summary and start the installation process.
   During the installation, the UMS Server switches to update mode.
9. Confirm the message `n of m servers updated`.
   Example:

10. Close the UMS installer once the installation is complete.

> If SQL Server AD Native is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. This must be done on **ALL** UMS Server hosts. For more information, see Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication (see page 84).

11. Continue with the update of the next UMS Server.

Updating the Last UMS Server

→ Repeat steps 1-9 (see page 1415) on the last UMS Server to be updated.

The last UMS Server updated renews the schema of the productive database after the installation. All other UMS Servers within the network which run in the update mode will be informed that the installation has finished. They will restart and reconnect themselves to the productive database. Afterwards, they will run in normal mode.

Updating Further Components

After updating the UMS Servers within the HA network, you have to update all other current UMS components, e.g. separate UMS Load Balancers and UMS Consoles.

1. In order to do this, run the UMS installer on the systems.
2. Verify the components to be installed.

> You cannot connect to the UMS Server with a console version that is older than the version of the UMS Server.

> Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

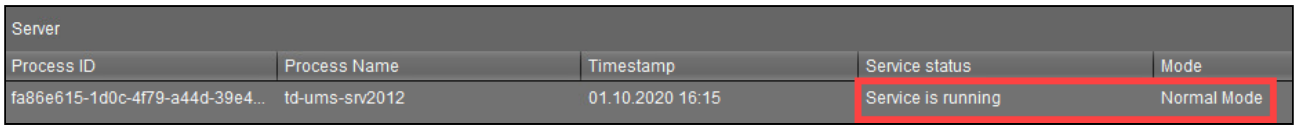
See also Troubleshooting: Load Balancer Is Not Stopping during the Update of the HA Installation (see page 513).

Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 1425).
2. In the UMS Administrator (see page 1037), go to **Datasource** to check if the database is activated.

   > If the server list has not been checked at the beginning of the update (see Preparing the Update (see page 1414), step 2) and there have been more servers registered in the database than actually running, it might be the case that there is a server within the HA network that did not reconnect to the productive database.
   > In this case, you have to switch over the data source manually to the productive database or you can use for this purpose the button **End update mode for local UMS Server** in the UMS Administrator > Distributed UMS (see page 1077).
   > The database schema will be renewed the first time an updated server connects to the productive database. Afterwards, all other servers within the network can be switched over to this database.

3. In the UMS Console, go to **UMS Administration > UMS Network** and check the items **Server** and **Load Balancer**.
   All servers and load balancers must be:
   - updated
   - running
   - in normal mode



Licensing the High Availability Extension

UMS Licenses

Starting from IGEL UMS version 12.07.100. the feature is only available with specific UMS Licenses. For details, see IGEL OS Editions[225].

IGEL OS Licenses

IGEL OS 11 and Higher

The IGEL UMS High Availability Extension no longer requires an additional license.

Before IGEL OS 11

The High Availability Extension comes in packages of 50 licenses. These licenses are installed in the UMS. The UMS checks if the number of licenses is at least as high as the number of devices connected to the UMS.

Each version of the IGEL UMS contains five test licenses allowing you to evaluate the function free of charge and without having to register.

→ Register the license file you receive in the UMS Console under **UMS Administration > Global Configuration > Licenses > UMS Licenses**.

An HA network only works with a license covering all managed devices registered in the UMS. A mixed mode (devices with HA support and devices without HA support) is not possible.

225. https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions

UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems

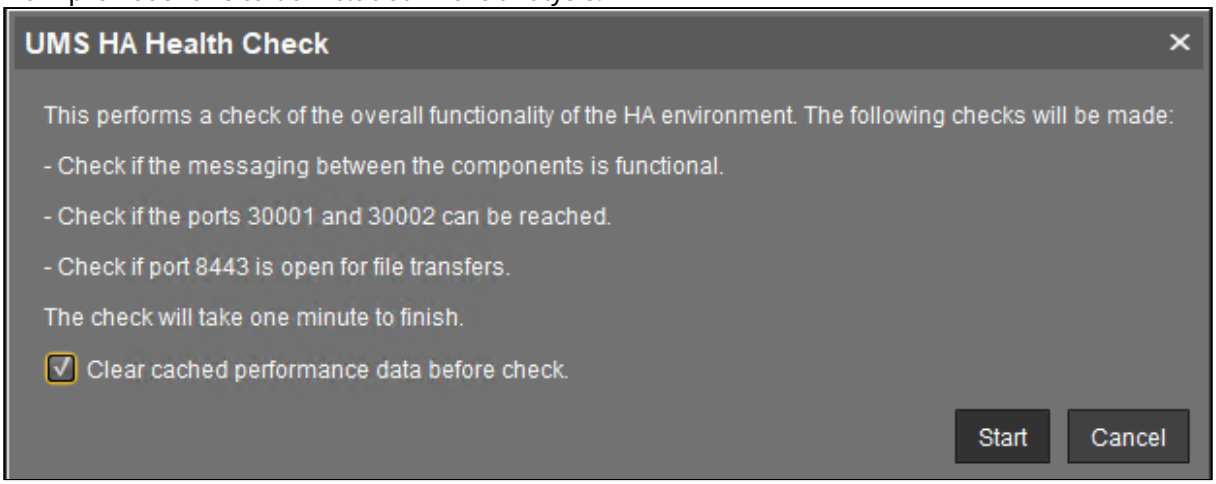
With the **UMS HA Health Check**, you can perform an overall check of your multi-instance IGEL Universal Management Suite (UMS) installations (see page 13). It checks whether the interaction between the components of the High Availability (HA) system or the Distributed UMS is working properly, in particular, whether the components can exchange messages and data:

> The permission to use the **UMS HA Health Check** feature can be set under **System > Administrator accounts**, see General Administrator Rights (see page 1013).

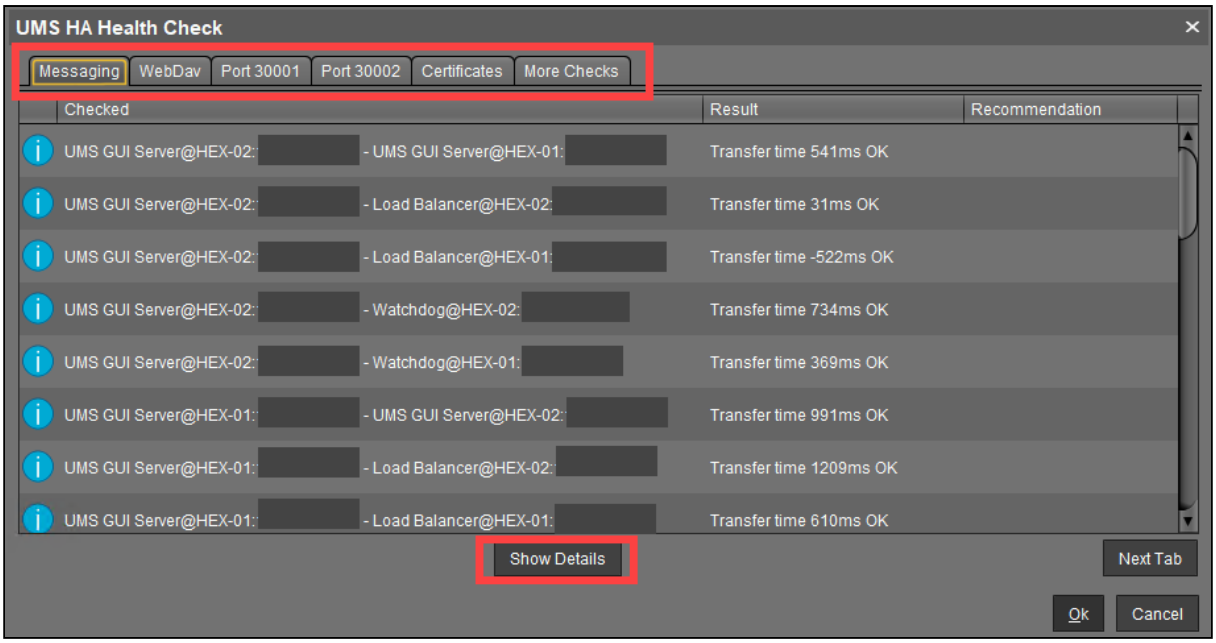
Menu path: Menu bar > **Help > UMS HA Health Check**

To check your HA environment / Distributed UMS, proceed as follows:

1. Make sure the servers and the components installed on them are in normal operational mode.
2. In the menu bar, go to **Help > UMS HA Health Check**.
3. Disable the checkbox **Clear cached performance data before check** if you want the cached data from previous runs to be included in the analysis.



After the necessary data are collected and analyzed, a window opens where the results and corresponding recommendations are presented in a number of tabs. Each tab has a **Show Details** button that opens a detailed analysis report in HTML format. The description of each tab and the HTML report can be found below.

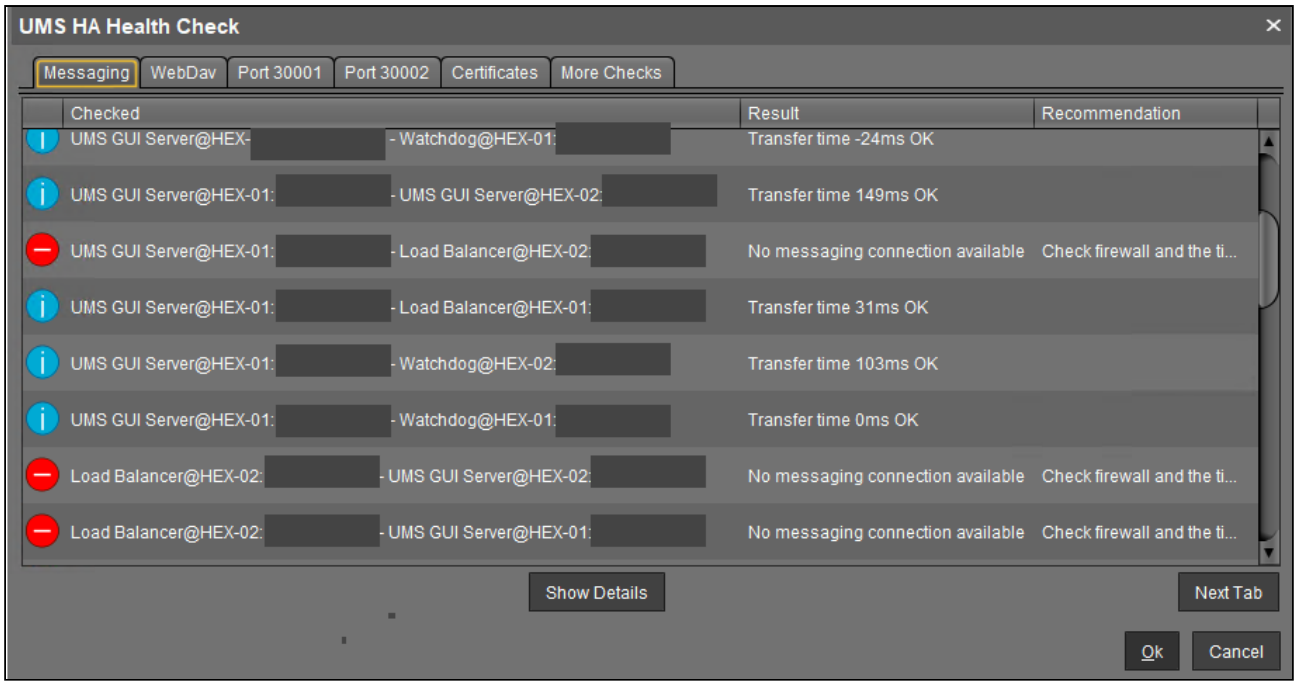


Messaging

This check detects whether the components are running and can exchange messages. It performs a ping test between the components of a High Availability installation on each server. The list shows the result with the indication of the transfer time for each combination of the components. The transfer time indicates for the UMS HA whether ActiveMQ messaging is working or not within the subnet.

If you have a Distributed UMS installation, the results displayed under **Messaging** can be ignored since the **UMS HA Health Check** mainly checks the performance of the ActiveMQ messaging of the UMS High Availability (within the subnet). For the Distributed UMS, **Messaging** tab shows the messaging delay over the database, which is approximately 30 seconds.
You can currently also ignore:

- the **Messaging** results of the UMS HA Health Check if your UMS HA without IGEL UMS Load Balancers is installed in different subnets / cloud environment
- error messages for Watchdogs if you have a UMS HA without IGEL UMS Load Balancers



The reasons why messaging between components is not possible are usually the following:

- One of the components is not running at all.
- The necessary ports, 61616 and 6155, are not open in the firewall. See IGEL UMS Communication Ports (see page 256).
- The system time on the servers differs a lot.

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

- The IGEL network token differs between the components. For example, this can happen due to the generating of a new IGEL network token, instead of using the network token initially created during the installation of the first UMS Server when further UMS Servers / UMS Load Balancers are installed within a HA network.

WebDav

This check examines whether the UMS Servers can exchange files via WebDav. WebDav is mandatory for the synchronization of files between the UMS Servers. See also Which Files Are Automatically Synchronized between the IGEL UMS Servers? (see page 514).

Possible reasons for failure are the following:

- One of the components is not running at all.
- WebDav port 8443 is not open in the firewall.

Port 30001

Port 30001 is used for connections between the devices and the UMS Load Balancer. As the test cannot mimic a device, the UMS Servers try to connect to the UMS Load Balancer via port 30001.

Possible reasons for failure are the following:

- One of the components is not running at all.
- Port 30001 is not open in the firewall.

Port 30002

Port 30002 is used by the UMS Load Balancer for forwarding requests from the device to the UMS Server.

Possible reasons for failure are the following:

- One of the components is not running at all.
- Port 30002 is not open in the firewall.

Certificates

This check compares the certificates stored on the UMS Server with those stored on the UMS Load Balancer.

A possible reason for failure can be the following:

- Failure in communication between the components due to the differing IGEL network tokens, see the above section "Messaging (see page 1422)".

More Checks

If other problems are detected, the corresponding results and recommendations are displayed here.

Detailed Report

A detailed report generated in HTML format upon the click on the **Show Details** button provides some additional information.

> Tip for Contacting IGEL Support
>
> If the recommendations provided did not help to resolve the problems, save the HTML report and send it to IGEL Support together with the archive with the support information, which can be created in the menu bar under **Help > Save support information**.

Roles: Based on the results, the check shows which roles are possible for the servers.

Example:

Process ID	Host	Roles
45ae09c1-4445-4ce1-a7a9-0125d353a480	HEX-01:	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
f427828d-fe9b-4445-abea-0b42382dee35	HEX-02:	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
ums-broker-49951-1592214135973-0-0	HEX-01:	[Server, HA, LoadBalancer, Client]
ums-broker-49993-1592214726620-0-0	HEX-02:	[Server, HA, LoadBalancer, Client]
ums-watchdog-49953-1592214138113-1-0	HEX-01:	[Server, HA, LoadBalancer]
ums-watchdog-49995-1592214730651-1-0	HEX-02:	[Server, HA, LoadBalancer]

Config Info: Shows the configuration information as provided by the processes. For a UMS Load Balancer, i.e. UMS broker process, the known servers of this Load Balancer are shown.

Process Info: Provides an overview of the processes.

Certificate Fingerprints: Shows fingerprints of the certificates stored in the database on the UMS Server and the tc.keystore file on the UMS Load Balancer.

IGEL UMS HA Services and Processes

The following article explains, which services and processes are running when you install the High Availability (HA) extension of the IGEL Universal Management Suite (UMS). However, it also provides a general overview of how you can restart services and processes for your UMS installation, not necessarily the UMS HA installation.

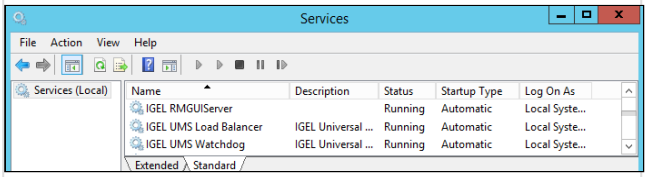
A High Availability (HA) installation consists of several processes: Each node of the HA network has either the UMS Server or the UMS Load Balancer or both running, depending on the configuration you have chosen during the installation process of the UMS HA, see also IGEL UMS HA Configuration Options (see page 1389). In addition, the UMS Watchdog always runs on each node.

UMS Server	• Handles all requests from the devices and the UMS Console. • Talks to the devices. • Executes jobs. • Acts as a message broker for internal messages.
UMS Load Balancer	• Forwards incoming requests from the devices to one of the UMS Servers with load balancing. The UMS Load Balancer has a list of running UMS Servers and distributes the requests to them sequentially.
UMS Watchdog	• Monitors the run status of the UMS Server and the UMS Load Balancer running on the same server and forwards it to the UMS Servers. • Starts or stops the UMS Server or the UMS Load Balancer on request from a UMS Server.

⚠ If both the UMS Server and the UMS Load Balancer are running on the same server, the UMS Server uses port 30002 and the UMS Load Balancer uses port 30001. If only the UMS Server is installed on a server, it always listens on port 30001. See IGEL UMS Communication Ports (see page 256).

The following table shows how you can find out which processes are running and how/where you can stop or start them.

Windows	Linux

Services:
 
 	
The processes are normally stopped here.
 	
Task Manager:
 
 	
Emergency stop if the process cannot be stopped in the **Services**.
 	
cmd / Command Prompt:
`sc queryex “IGELRMGUIServer”`
`sc queryex “IGEL UMS Load Balancer”`
`sc queryex “IGEL UMS Watchdog”`
Emergency stop if the process cannot be stopped in the **Services**:
• `taskkill /PID xxxx /F`
where the PID can be seen in the output of `sc queryex “Name of the process”`
	• For the list of running processes, use the command:
	`sudo ps -ef | grep RemoteManager`
	where `RemoteManager` is the last part of the installation path; Adjust it if the installation path is different.
	Each process has two entries on the list.
	• For stopping the processes, use:
	`sudo systemctl stop igel-ums-watchdog`
	`sudo systemctl stop igel-ums-broker`
	`sudo systemctl stop igel-ums-server`
	• For stopping the processes if the stop with the `init` scripts does not function:
	`sudo kill -9 xxxx`
	where the ID of the process can be seen in the output of
	`sudo ps -ef | grep RemoteManager`

You can stop / start the UMS Server service also in the **UMS Administrator > Distributed UMS**, see Distributed UMS - Perform Local UMS Actions in the IGEL UMS Administrator (see page 1077).

IGEL Shared Workplace (SWP)

IGEL Shared Workplace (SWP) allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters. You will find an overview of the parameters that can be individually configured for a user under Parameters Configurable in the User Profile (see page 1435).

IGEL SWP configuration is not available for OS 12 devices.

Licensing with IGEL OS 11

For use with IGEL OS 11 devices, Shared Workplace requires a valid license from the IGEL Enterprise Management Pack (EMP). This license must be present on every IGEL OS 11 device on which Shared Workplace is to be used. When the license expires, users will no longer be able to login to a Shared Workplace session.

Licensing with IGEL OS 10

For use with IGEL OS 10 devices, Shared Workplace requires an add-on license for Shared Workplace. This license must be present on every IGEL OS 10 device on which Shared Workplace is to be used. The license is perpetual.

Typical Uses for Shared Workplace

- Workstations used for shift work or in call centers, where different staff members at a workstation need their own individual settings, e.g. session types or mouse-button settings for right/left-handed operation.
- Roaming environments, where users frequently switch workstations, such as in hospitals and at service/ticket counters, checkouts, or reception areas. After a user has logged in, the endpoint device licensed for Shared Workplace automatically configures itself. It does this via the UMS server using the individual or group profile stored in the UMS database. These profiles can easily be assigned to a user with the help of the IGEL Universal Management console using a convenient drag-and-drop procedure.

In environments with an increasing number of Shared Workplace workstations, IGEL recommends using the UMS High Availability Extension (see page 1387). The high level of UMS server availability achieved ensures that users receive their user-specific profile at all times.

IGEL Tech Video

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

https://www.youtube.com/watch?v=opgVxN791Vg

- SWP Configuration in the UMS Console (see page 1429)
- Parameters Configurable in the User Profile (see page 1435)
- Display Configuration for Shared Workplace (SWP) (see page 1438)

SWP Configuration in the UMS Console

In order to be able to use IGEL Shared Workplace, the following requirements must be met:

- Users who are to be given a specific profile must be set up in a Microsoft Active Directory.
- Devices which are to allow user logins must have a license for the IGEL Shared Workplace function. This can be transferred to the devices via the IGEL UMS license management system.

> If a device has been given a license for IGEL Shared Workplace, this cannot be canceled. However, the function can be disabled via the list of available services in the device configuration. Login via IGEL Shared Workplace is then disabled.

- Although not absolutely necessary, the use of the High Availability Extension (see page 1387) for the IGEL Universal Management Suite is recommended for larger installations. This will ensure a high level of availability for the user profiles in the network.

> If you use IGEL Shared Workplace with IGEL Universal Desktop WES 7, bear in mind that the default password **"user"** must be set for the default user **"user"**, otherwise it will not be possible to log in.

See also Display Configuration for Shared Workplace (SWP) (see page 1438).

In this chapter, you can learn about:

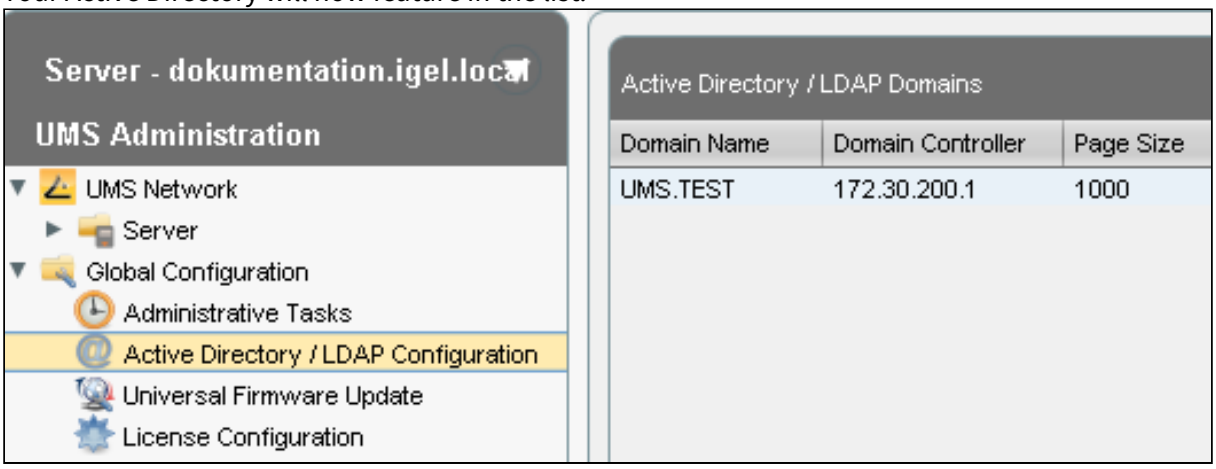
- How to Link an Active Directory in the IGEL UMS (see page 1430)
- How to Assign a User Profile in the IGEL UMS (see page 1431)
- How to Enable IGEL Shared Workplace on the Device (see page 1432)
- User Login (see page 1433)
- Logout and Change of User (see page 1434)

The priority of user-specific profiles is dealt with in Order of Effectiveness of Profiles in IGEL Shared Workplace (see page 732). See also Order of Effectiveness of Profiles (see page 729).

How to Link an Active Directory in the IGEL UMS

To link an Active Directory in the UMS, proceed as follows:

1. Click on **Active Directory** in the **UMS Administration** area.
2. Click on **Add**.
   The **Add Active Directory / LDAP Service** mask will open.
3. Enter the **domain name** and the access data.
4. Confirm your settings by clicking on **OK**.
   Your Active Directory will now feature in the list.



Other LDAP servers (*Novell eDirectory*, *OpenLDAP* etc.) cannot be used for *IGEL Shared Workplace* user authentication purposes.

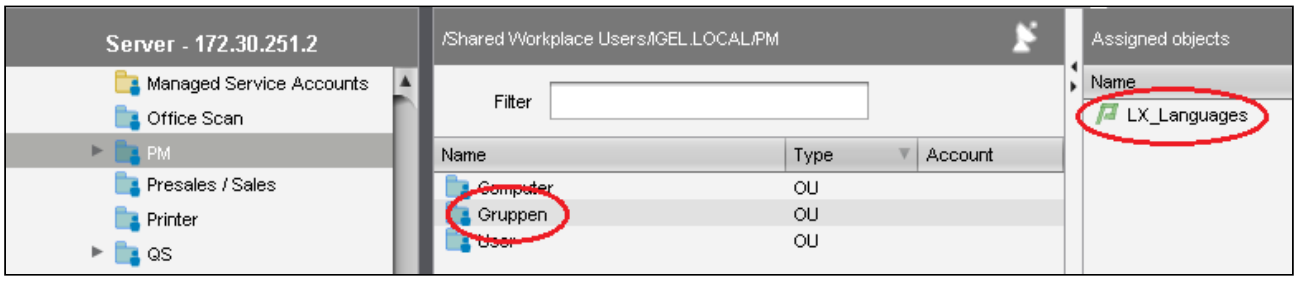
How to Assign a User Profile in the IGEL UMS

Go to your Active Directory in the UMS navigation tree under **Server > Shared Workplace User**.

You can browse it or search for it by using this symbol:  .

→ Select an object within the AD structure.
You will need to authenticate yourself vis-à-vis the Active Directory in order to do so.

→ Assign the desired user profile to this object:
Server > Shared Workplace User > [Active Directory] > [Object]



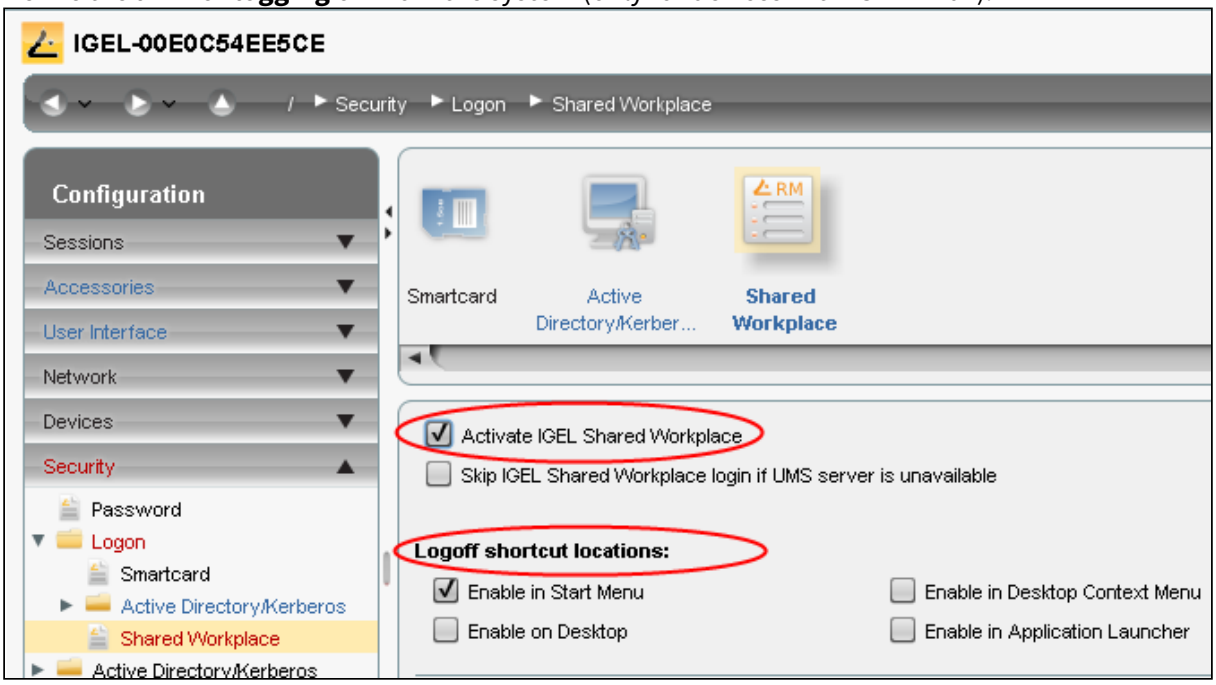
As with devices, a number of profiles can be assigned. In this case, indirectly as well as directly assigned profiles will be taken into account.

Right-click the name of a user account, to see the profile settings of the device.

How to Enable IGEL Shared Workplace on the Device

You can configure the settings for Shared Workplace from the IGEL Universal Management Suite (UMS) via a profile or directly in the setup of the relevant device.

1. Go to **Configuration > Security > Login > IGEL Shared Workplace**.
2. Enable the **IGEL Shared Workplace** function.
3. Define the **link for logging off** from the system (only for devices with IGEL Linux).



User Login

If you have a license, you can easily log in to an endpoint device with IGEL Shared Workplace:

1. Boot the device.
   A login window will appear.
2. Log in with your AD login data.
   You will receive the profile settings that are stored for you in the UMS.

> The device configuration which is active for the user logged in is the result of cumulating all profiles which have been assigned either directly or indirectly to the device or the user. See also Prioritization of Profiles in the IGEL UMS (see page 728) .

Logout and Change of User

Windows Embedded Standard

→ Log out via the start menu.

IGEL Universal Desktop Linux

Under Linux, you can set up the following logout options:

→ In the **Application Launcher**, define where you will place the buttons for logging off.

→ Under **Security > Login > IGEL Shared Workplace** in the IGEL Setup, define a hotkey for logging off.

Parameters Configurable in the User Profile

Not all parameters available in an item of firmware can be configured on a user-specific basis.

The system settings which cannot be configured effectively by a user-specific profile are described below.

> The UMS does not check whether the settings are effective.

The device-specific system settings for the IGEL operating systems which **cannot be configured effectively** are listed below. No check takes place in the IGEL UMS.

- Universal Desktop Linux (see page 1436)
- Universal Desktop Windows Embedded Standard (see page 1437)

UD Linux Device-specific Parameters

The following system settings are **not** configurable in the user profile:

- Network settings including those for the network drives
- Screen configuration for IGEL Linux v5 to 5.05.100 and for IGEL Linux v4 to 4.13.100.

  > Depending on the hardware used, display errors may occur if the user changes the resolution or rotates the screen even under IGEL Linux from Release 4.14.100. See the How-To document Display Configuration for Shared Workplace (see page 1438).

- Touchscreen configuration
- Update settings
- Security settings
- Remote management
- Customer-specific partition
- Server for background images

  > With IGEL *version 10.03.500* or higher, background images and the custom wallpaper server can be defined for each individual user via Shared Workplace.

- Customer-specific bootsplash
- Browser plug-ins
- SCIM entry methods, however, these can be enabled on a user-specific basis
- Three-button mouse emulation
- Appliance Mode (VMware View, Citrix XenDesktop and Spice)

UD W7 Device-specific Settings

The following system settings cannot be configured in the user profile:

- Language, standards and formats
- Network settings including those for the network drives
- Active Directory login
- USB device configuration
- List of the available features and Windows Services
- Update settings
- Setup session
- User and security settings
- File Based Write Filter
- Energy options
- Remote management
- Appliance Mode (VMware View and Citrix XenDesktop)

Display Configuration for Shared Workplace (SWP)

As of IGEL Universal Desktop Linux *version 4.14.100* and *version 5.06.100*, Shared Workplace allows user-specific screen resolutions and configurations. Resolution, layout, refresh rate, rotation, number of screens, monitor connectors (DVI, VGA, ...) can be set per user, but color depth cannot.

There are technical limitations to user-specific settings: For VIA graphics drivers/hardware, the maximum desktop size is set in the `Screen` section of the X configuration file. The name and location of the X configuration file depend on the firmware version:

- IGEL Linux *version 10*: `/config/Xserver/xorg.conf-0`
- IGEL Linux *version 5*: `/config/Xserver/xorg.conf-0` or `/etc/X11/xorg.conf` (this is a symbolic link that points to `/config/Xserver/xorg.conf-0`)

  In the `Screen` section of the above-mentioned configuration file, you can find a line such as `Virtual 1920 1200`. The size defined here cannot be changed dynamically; it is a hard limit for the overall desktop size.

Best Practice

It is recommended to set the initial desktop configuration to the maximum number of screens and the resolutions to A `utodetect`. This way, the user-specific resolutions will not be restricted.

Debugging

If the total framebuffer size of the user-specific resolutions exceeds the limits of the `Virtual [width] [height]` setting from `/config/Xserver/xorg.conf-0` (or `/etc/X11/xorg.conf`), the user-specific resolutions cannot be activated and the screen configurations are not changed dynamically.

There is no warning dialog or anything else to alert the user to this restriction. But you can find related log messages via `journalctl` or in `/var/log/messages`:

```
XRANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XRANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

Asset Inventory Tracker (AIT)

For details, see Asset Inventory (see page 781).

UMS Release Notes

Notes for Release IGEL UMS 12.09.110

Software:	Version 12.09.110
Release Date:	2025-09-23
Release Notes:	RN-1209110-1

Resolved Issues IGEL UMS 12.09.110

AD / LDAP Integration

- Fixed: AD group membership stored in database could cause problems if an AD user creates a job.

Administrator Application

- Changed: Misleading message when an external database is activated and no valid Enterprise license is present.

DB Commandline Tools

- Fixed: The import of Web Certificates via IGEL UMS Administrator command-line interface was no longer possible.

Device Service

- Fixed: Custom values for instances defined in profiles not applied to device.
- Fixed: OS12 configurations with template key HOSTNAME used device name instead of network name as value. Now OS12 uses the network name as OS11 does.

Views

- Fixed: Superfluous errors were logged during calculation of view results.

UMS Common

- Fixed: Issue where ICG installation could fail if the UMS web port was set to something other than the default (8443).

UMS Web App

Devices

- Fixed: The icon in CA Proxy settings showed an incorrect state for the configuration and the uploaded keystore.
- Fixed: Devices could not be unassigned from a profile via the profile page.

Search

- Fixed: Message was delayed or not shown immediately when clicking the "Reindex all" button.

Important Notice IGEL UMS 12.09.110

With IGEL UMS 12.08.100, the login process has changed, which entails new requirements for your environment.

Before upgrading to IGEL UMS 12.09.X please read the related Knowledge Base article:
UMS Login Requirements[226]

226. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Supported Environment IGEL UMS 12.09.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser:

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

New Features IGEL UMS 12.09.110

Admin Tasks

- Added: Admin task to export / delete OS12 logging messages.

DB Commandline Tools

- Added: Export of the UMS ID is now possible with a new command in the IGEL UMS Administrator command-line interface.

Devices

- Added: Advanced System Information section now shows the information whether a device is currently routed through a reverse-proxy connector.

IGEL Management Interface (IMI)

- Added: IMI / Device Details: the response now contains a new field `connectedViaReverseProxy` that indicates whether the device is currently routed through a reverse-proxy connector.

Installer (Windows)

- Added: Option to manually search for a user during installation to run the services with.

Unified Protocol

- Added: The CA Proxy Feature now supports a CA Label as defined in RFC 7030.
- Tested: Compatibility with AWS ALB.
- Added: New configuration option to support the encoding type of client certificates forwarded by AWS ALB.

Views

- Added: New view criterion 'Connected via Reverse Proxy'.

UMS

- Added: Admin task to export/delete OS12 logging messages.

UMS Web App

Devices

- Added: Device connection via reverse proxy is now displayed in the device details.
- Added: Optional CA Label for CA Configuration

Search

- Added: Reverse Proxy Connection is now available for the search in the UMS Web App.

Automation

- Added: New Admin task: "Delete logging data (OS 12 and Web App)".

Notes for Release IGEL UMS 12.09.100

Software:	Version 12.09.100
Release Date:	2025-08-26
Release Notes:	RN-1209100-1

Important Notice IGEL UMS 12.09.100

With IGEL UMS 12.08.100, the login process has changed, which entails new requirements for your environment.

Before upgrading to IGEL UMS 12.09.X please read the related Knowledge Base article:
UMS Login Requirements[227]

227. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Supported Environment IGEL UMS 12.09.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser:

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

New Features IGEL UMS 12.09.100

Administrator application

- Added: UMS Admin CLI Commands
  - `ums-license state`
  - `ums-license register -f=<path to .lic file>`
  - `ums-license deleteall`

Cloud IdP / SSO

- Added: Content Security Policy (CSP) to enhance browser security to protect against cross-site scripting (XSS).
- Added: Translations for `Authorization failed` message in UMS Console.

Default Directory Rules

- Added: New default directory rule / view criterion **Connected via Reverse Proxy**.

UMS common

- Updated: Apache Tomcat from version 10.1.41 to 10.1.43
- Added: New feature to enable the UMS to act as a CA Proxy, allowing devices to request client certificates directly through UMS. These certificates will be signed by an external CA via the EST protocol.

Web App

Configuration Dialog

- Changed: The modal dialogs are no longer being closed and reopened on profile creation. The content of the dialogs is updated instead.
- Changed: Replaced badge with chip for Adjustments to make it accessible via keyboard.

Users

- Added: Button to create a user was added to the Users tree toolbar.
- Added: Button to create a group was added to the Groups tree toolbar.
- Added: Button to create an Identity Provider Role was added to the IDP Roles tree toolbar.

Misc

- Added: CSP Header Filter to WUMS-UI (security improvement)
- Updated: Angular was updated from v18 to v19 to include the latest security patches.

Resolved Issues IGEL UMS 12.09.100

AD / LDAP integration

- Fixed: AD logon support in an environment where the Domain Name System (DNS) cannot map to Key Distribution Centers (KDCs).

Administrator application

- Fixed: umsadmin-cli.sh now working.

Cloud IdP / SSO

- Fixed: Effective Rights Dialog doesn't show Permissions for currently logged on AD/IdP user.
- Fixed: Support for external IdP role claims that may return either a single string or a list of strings.

Console, common

- Fixed: Memento feature was not working when the user logged out.

IGEL Cloud Gateway (ICG)

- Fixed: The input field in ICG installer no longer overflows the dialog window.

Installer (Linux)

- Fixed: umsadmin-cli.sh now working.

Jobs

- Fixed: Job Execution for OS12 device connected to an ICG in a distributed UMS environment.

UMS common

- Fixed: The profile settings for assigned objects could not be opened initially after starting the UMS Console.
- Fixed: Device list “Show unlicensed devices” displayed incorrect devices.
- Fixed: Public Web port was not used for initial UMS ID sync if public address was set for existing servers.
- Fixed: Devices with low memory entered into an infinite boot loop if they got a firmware update.

Unified Protocol

- Fixed: Job Execution for OS12 device connected to an ICG in a distributed UMS environment.

UMS

- Fixed: Superadmin could be attached to a group in administrative accounts UI.

UMS Web App

Apps

- Fixed: Versions in app details card were not properly aligned.

Devices

- Changed: Due to recent implementation changes, the following actions for IGEL Managed Hypervisor Devices have been temporarily removed from the UI: Backup, Restore, Re-Image, and Wipe.
- Changed: The device details section has a single scroll bar that affects the entire height of the component.
- Changed: The UI for the First Authentication Keys was improved.
- Changed: Global Permission for the Save Support Information workflow is now checked before UI is opened.
- Fixed: Date-type fields in device attributes, accessed through the "Edit custom properties" button, were previously all labeled as "Date input" instead of displaying their actual field names
- Fixed: It was not possible to edit or create a device attribute of list type.
- Fixed: Check for global permissions in Recycle bin was added.
- Fixed: The Save Support Information command for a device directory could be executed when the directory did not contain OS12 devices.
- Fixed: After the deletion of a device the tree is now properly reloaded.
- Fixed: Added missing translations for scheduler commands.
- Fixed: Mass deployment key is now still properly focused after opening its details.
- Fixed: Assigned object tab information was not aligned.
- Fixed: First Authentication Keys tab was not shown in the settings if user had no permission for device attributes.

Configuration

- Changed: The display name of a file is now shown in all places, instead of the technical name.
- Fixed: Incorrect message was displayed in the dialog for confirming the assignment of a device to a profile.
- Fixed: Template-key assignment errors occasionally blocked profile assignment.

Configuration Dialog

- Fixed: Changes indicators in Device Configuration were shown for some cases when no changes were made.
- Fixed: Unnecessary parameter "Multiple images" was removed from the CIC screensaver (custom partition) use case.
- Fixed: Dependent parameters were not enabled when a template key was set for a parameter.

Devices

- Fixed: Broken "Save Support Information" workflow.

Network

- Changed: UI for Redirect URIs now recognizes http://hostname as valid input.

Search

- Changed: Instead of a popup, now a clear message is presented on the top of the result-table.
- Fixed: Reindex messages were not always properly translated.
- Fixed: Users without permission could close the EPR Settings sidebar.
- Fixed: Some columns broke the Search export.
- Fixed: Regression bug causing unauthorized access in AD user search results.

Users

- Fixed: Information about effective permissions was not updated on My User page without refreshing the page or logging out and logging in.
- Fixed: The order of displayed columns in Groups and Users overview was not consistent.
- Fixed: Breadcrumbs and links in User Management were not visually intuitive and accessible.

Logging

- Changed: Loging-UI was updated to utilize new components.
- Fixed: Origin field on logging table displayed "Webapp" instead of "Web App".
- Fixed: Log entries could be added to the table without a message parameter.

Misc

- Changed: All dialogs are now closable via "ESC".
- Changed: Expired license dates now display in red for quick identification
- Changed: In all applicable dialogs the primary action button is now focused.
- Changed: Added spinner for better log-in experience.
- Fixed: Fixed an issue where the user was logged out (both at the UMS Web App and at the UMS Console) if the refresh token (Web App) was expired.
- Fixed: Removed unnecessary calls for a faster login-experience.
- Fixed: Highlight style was overlapping with the next column for tables with sorting.

- Fixed: Checkbox column was not fixed for tables with fixed first text column.

Notes for Release IGEL UMS 12.08.130

Software:	Version 12.08.130
Release Date:	2025-07-14
Release Notes:	RN-1208130-1

Important Notice IGEL UMS 12.08.130

With IGEL UMS 12.08.100, the login process has changed, which entails new requirements for your environment.

Before upgrading to IGEL UMS 12.08.X please read the related Knowledge Base article:
UMS Login Requirements[228]

228. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Supported Environment IGEL UMS 12.08.130

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser:

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

New Features IGEL UMS 12.08.130

Cloud IdP / SSO

- Added: Discovery of Cloud IdPs use the configured default proxy.

Unified Protocol

- Added: In some cases, the Client Certificate renewal could fail for old devices (devices with base_system ≤ 12.4.0)
  A configuration was added to switch off the Client Certificate Expiration check to further manage the devices and start reenrollment. For details, see Troubleshooting: IGEL OS 12 Devices Failing to Connect to UMS Due to Expired Client Certificates (see page 557) .

UMS Web App

Other

- Added: If the Client Certificate Expiration check is switched off a warning dialog is added to highlight the potential security and compliance risk.

Known Issues IGEL UMS 12.08.130

UMS Common

- AD logon will fail in an environment where the Domain Name System (DNS) cannot map to Key Distribution Centers (KDCs). This mapping is crucial for the UMS to locate the KDC responsible for a specific realm when authenticating.

Firmware Update of OS 11 versions

OS 11 devices with only a small amount of free space on the disc are using a multi-reboot workflow for an OS 11 firmware update. This workflow is broken if the UMS has version 12.08.xx. As a result, these devices will enter an infinite boot loop.
If you have devices with low disc space, either:

- update the devices before switching to UMS 12.08.xx if you have UMS 12.07.xx or lower installed.
- test with single devices before updating a larger number of devices. If your devices are affected, update to UMS 12.09.100 or higher before updating the device firmware.
- use an alternative source for firmware update instead of UMS (for example, external WebDAV or FTP).

Affected environments:

- UMS versions 12.08.100, 12.08.110, 12.08.120, 12.08.130
- Firmware update of any OS 11 version

Resolved Issues IGEL UMS 12.08.130

WebDAV

- Fixed: Findings from penetration test commissioned to a third party.

UMS

- Fixed: Findings from penetration test commissioned to a third party.

UMS Web App

Configuration Dialog

- Fixed: Parameters of type `parameterGroup` could not be activated in Quick Setup mode.
- Changed: Initial checkbox to prefer Advanced Setup was changed to **Prefer Quick Setup (automatic session creation)** when creating an OS12 profile.

Notes for Release IGEL UMS 12.08.120

Software:	Version 12.08.120
Release Date:	2025-06-30
Release Notes:	RN-1208120-1

Important Notice IGEL UMS 12.08.120

With IGEL UMS 12.08.100, the login process has changed, which entails new requirements for your environment.

Before upgrading to IGEL UMS 12.08.X please read the related Knowledge Base article:
UMS Login Requirements[229]

229. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Supported Environment IGEL UMS 12.08.120

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser:

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

New Features IGEL UMS 12.08.120

IMI, server

- Added: Direct authorization for IMI calls.
- Added: Possibility to wrap results of IMI thinclients call with a `results` tag.

Resolved Issues IGEL UMS 12.08.120

Admin Tasks

- Fixed: Monitor information was not included in view **Export to CSV by E-Mail**.

UMS Web App

Configuration Dialog

- Fixed: Uses of `innerhtml` assignments that could lead to XSS were removed

Known Issues IGEL UMS 12.08.120

UMS Common

- AD logon will fail in an environment where the Domain Name System (DNS) cannot map to Key Distribution Centers (KDCs). This mapping is crucial for the UMS to locate the KDC responsible for a specific realm when authenticating.

Firmware Update of OS 11 versions

OS 11 devices with only a small amount of free space on the disc are using a multi-reboot workflow for an OS 11 firmware update. This workflow is broken if the UMS has version 12.08.xx. As a result, these devices will enter an infinite boot loop.
If you have devices with low disc space, either:

- update the devices before switching to UMS 12.08.xx if you have UMS 12.07.xx or lower installed.
- test with single devices before updating a larger number of devices. If your devices are affected, update to UMS 12.09.100 or higher before updating the device firmware.
- use an alternative source for firmware update instead of UMS (for example, external WebDAV or FTP).

Affected environments:

- UMS versions 12.08.100, 12.08.110, 12.08.120, 12.08.130
- Firmware update of any OS 11 version

Notes for Release IGEL UMS 12.08.110

Software:	Version 12.08.110
Release Date:	2025-06-17
Release Notes:	RN-1208110-1

Important Notice IGEL UMS 12.08.110

With IGEL UMS 12.08.100, the login process has changed, which entails new requirements for your environment.

Before upgrading to IGEL UMS 12.08.X please read the related Knowledge Base article:
UMS Login Requirements[230]

230. https://kb.igel.com/en/universal-management-suite/current/ums-login-requirements

Supported Environment IGEL UMS 12.08.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser (Web App):

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

New Features IGEL UMS 12.08.110

Installer (Windows)

- Added: Additional information about new SSO functionality to the Windows installer.

UMS common

- Updated: Apache Tomcat from version 10.1.39 to 10.1.41

UMS Web App

Misc

- Added: Ability to add Redirect URIs to the installation, to be able to use these URIs for login.

Resolved Issues IGEL UMS 12.08.110

AD / LDAP integration

- Fixed: AD login could fail when an UPN suffix was used for an AD user and with that the logon with user@domain name was not possible.

Cloud IdP / SSO

- Fixed: UMS console login with hostname (without domain) no longer worked.
- Fixed: Allow FQDN with uppercases.
- Changed: Integrate umsstarter into `RMClient.exe` (updating installer and protocol registration) to eliminate the separate JAR.

Console Common

- Fixed: UMS Console only installations could run into a login/connect error if they were never connected to the UMS server.

Devices

- Fixed: Timeout issues while saving settings of a device.

Server Common

- Fixed: OS 11 devices could not download assigned CICs. (OS 11 devices connected via ICG and OS 12 devices were not affected)

WebDAV

- Fixed: In Distributed UMS or HA environments, the WebDAV file synchronization failed.

UMS Web App

Misc

- Fixed: Login to the UMS Web App failed if the UMS Server is not listening on the default port (8443)
- Fixed: Removed unused dependency org.apache.httcomponents.client5:httpclient5:5.4.2
- Fixed: Igel-rest-libs version 12.8.2 was removed from the build.
- Fixed: Several dialogs were wrongfully displayed in full width in Chromium-based browsers.

Users

- Fixed: When a user is reassigned to a different group while logged in, the UI did not consistently reflect the change.

Configuration

- Fixed: Additional timeout issues while saving settings of a device.

Search

- Fixed: Permissions for a device-record were not properly calculated if the device was in bin on server-start and restored afterwards.
- Fixed: Not all received changes were correctly flushed into the index.

Known Issues IGEL UMS 12.08.110

UMS Common

- AD logon will fail in an environment where the Domain Name System (DNS) cannot map to Key Distribution Centers (KDCs). This mapping is crucial for the UMS to locate the KDC responsible for a specific realm when authenticating.

Firmware Update of OS 11 versions

OS 11 devices with only a small amount of free space on the disc are using a multi-reboot workflow for an OS 11 firmware update. This workflow is broken if the UMS has version 12.08.xx. As a result, these devices will enter an infinite boot loop.
If you have devices with low disc space, either:

- update the devices before switching to UMS 12.08.xx if you have UMS 12.07.xx or lower installed.
- test with single devices before updating a larger number of devices. If your devices are affected, update to UMS 12.09.100 or higher before updating the device firmware.
- use an alternative source for firmware update instead of UMS (for example, external WebDAV or FTP).

Affected environments:

- UMS versions 12.08.100, 12.08.110, 12.08.120, 12.08.130
- Firmware update of any OS 11 version

Notes for Release IGEL UMS 12.08.100

Software:	Version 12.08.100
Release Date:	2025-05-27
Release Notes:	RN-1208100-2

Resolved Issues IGEL UMS 12.08.100

AD / LDAP integration

- Fixed: When editing global permissions for an LDAP user, the username was not displayed in the Edit dialog. When the Edit dialog was saved in this state, the username was changed to empty, and the user was broken.

Administrator application

- Fixed: Restoring a database backup of an embedded Derby database failed sometimes.

App Proxy

- Changed: Improved error handling for the Distributed App Repository.

Unified Protocol

- Fixed: In specific scenarios no UTC time was used when the TC connection state was set to offline.
- Fixed: If a big number of OS12 devices was connected to a single device-connector, the devices were shown as offline, but were still manageable.

Devices

- Fixed: Timeout-issues while saving settings of a device.

IGEL Management Interface (IMI)

- Fixed: Requesting all devices via IGEL Management Interface (IMI) was very slow when the database contained a large number of devices.

UMS common

- Changed: Usage of counters for id generation in file transfer use cases.
- Fixed: App status timestamp in App Information was not correctly displayed.
- Fixed: Automatic download of UMS license didn't work when proxy was configured.
- Fixed: Last boot time was not updated if "Adjust Internal Name if network name has changed" is selected.

UMS Web App

Configuration

- Changed: Added File ID to the details section for easier identification.
- Fixed: Keep displaying the selected tree section after object drag & drop.
- Fixed: Incorrect icons displayed for OS11 profiles in the Recycle Bin
- Fixed: Profile duplication failure.
- Fixed: The paginator’s memento was not working correctly for all tabs in item details.
- Fixed: Device tree layout glitched when folder names were too long, causing folder entity counts to move out of view.
- Fixed: Incorrect tooltip displayed for the Create Profile/Master Profile button when the user lacked permission.
- Fixed: Incorrect tooltips displayed on the expand/collapse tree.
- Fixed: Scroll to selected profile did not always work in the profile list.
- Fixed: The header of some empty directory lists was not displayed.
- Fixed: Performance issues with the Recycle Bin.
- Fixed: Incorrect icons shown for devices and CICs in the Recycle Bin.
- Fixed: Restoring a file from recycle bin in the web-app could not be done, if the user had no 'write' -permission on the target folder. UMS console was not affected.

Configuration Dialog

- Changed: The navigation tree in the Profile Configurator that contains only one app is now expanded by default.
- Fixed: An error was thrown in App Selector for a device exported as profile that contained non-configurable apps.

Devices

- Changed: The "Save Support Information" command (without logfiles & configuration from devices) is now accessible from the main sidebar.
- Changed: Device directory command buttons on the toolbar are now grouped into dropdowns.
- Changed: Device command buttons on the toolbar are now grouped into dropdowns.
- Changed: Asset Information Tracking is now also enabled for OS 12+ devices.
- Changed: Added Manage Igel Hypervisor commands: Restore, Backup
- Changed: Capability to execute commands for all VMs simultaneously.
- Changed: Button to execute data refresh for all VMs.
- Fixed: Randomly closing shadowing connections for OS12 devices and OS11 ICG connections.
- Fixed: Performance issues during shadowing sessions.
- Fixed: Timeout-issues while saving settings of a device.
- Fixed: The Device Attributes table now scrolls to the selected item if it is not visible.
- Fixed: Added German translations for filter dropdowns and table values.
- Fixed: Performance issues with the Recycle Bin.
- Fixed: The "Show Keys" tooltip did not display the correct message when the user lacked write permissions.

- Fixed: Device monitor information was not displayed correctly.
- Fixed: Incorrect icons were shown for devices and CICs in the Recycle Bin.
- Fixed: Sometimes the scroll bar was not displayed in the assigned object dialog.

Search

- Changed: Deleted devices are now removed from the index immediately.
- Changed: Added Keyboard navigation for the search tree.
- Changed: Added "Onboarding user" column.
- Changed: Added "Logged user" column filter.
- Changed: Search results now update automatically when filter values change.
- Changed: The "Share Option" button has been renamed to "Sharing" (English).
- Changed: Option to trigger a manual re-index moved to settings. (Search -> settings sidebar -> Index Configuration)
  The trigger is now shielded with a permission against mis-use. (Write permission for Node: Server Network Settings)
- Fixed: Missing translations for scheduler commands.
- Fixed: "Last Logged in User" did not show the correct data.
- Fixed: Reset and Save buttons overlapped with the dropdown menu for selecting the time when scheduling re-indexing.
- Fixed: Sorting by the "Last logged in user," "App on Device reports error," and "Onboarded by" columns could cause the app to break.
- Fixed: Columns selected in the table were not preselected in the export.
- Fixed: "Any fields" was not working for "Last logging user."
- Fixed: The reindex window appeared multiple times.
- Fixed: Criteria of a saved search were not displayed correctly if the criterion option was not present in the database.

Logging

- Fixed: Added missing tooltips to settings.
- Fixed: Missing translations for scheduler commands.
- Fixed: Log entries could be added to the table without a message parameter.

Network

- Changed: Tooltips are now available for settings.
- Fixed: Users without permission could close the settings sidebar.
- Fixed: The settings sidebar was closing before an option was chosen in the confirmation dialog.

Others

- Changed: The heap size for Elastic has been set back to 1 GB.

Supported Environment IGEL UMS 12.08.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Browser (Web App):

- Microsoft Edge 137.0.+
- Mozilla Firefox 139.0.+
- Google Chrome 137.0.+

Known Issues IGEL UMS 12.08.100

UMS Common

- Discovery of Cloud IdPs does not use the configured proxy.
- With a “console only” new installation, the login does not work because the `rmconsole.truststore` is not created in the user directory.

  Workaround: A full installation creates the `rmconsole.truststore`, copy this trust store to the user directory or keep it there.
- AD logon will fail in an environment where the Domain Name System (DNS) cannot map to Key Distribution Centers (KDCs). This mapping is crucial for the UMS to locate the KDC responsible for a specific realm when authenticating.

Installer (Linux)

- Due to a bug in the password authentication process, the installation can currently only be completed using the `root` user.

  This issue affects new installations only and does not impact update installations.

Firmware Update of OS 11 versions

OS 11 devices with only a small amount of free space on the disc are using a multi-reboot workflow for an OS 11 firmware update. This workflow is broken if the UMS has version 12.08.xx. As a result, these devices will enter an infinite boot loop.
If you have devices with low disc space, either:

- update the devices before switching to UMS 12.08.xx if you have UMS 12.07.xx or lower installed.
- test with single devices before updating a larger number of devices. If your devices are affected, update to UMS 12.09.100 or higher before updating the device firmware.
- use an alternative source for firmware update instead of UMS (for example, external WebDAV or FTP).

Affected environments:

- UMS versions 12.08.100, 12.08.110, 12.08.120, 12.08.130
- Firmware update of any OS 11 version

New Features IGEL UMS 12.08.100

App Proxy

- Added: Enabled proxy functionality for Distributed App Repository.

UMS Common

- Updated: Java JDK from version 17.0.13+11 to 17.0.15+6
- Updated: Apache Tomcat from version 10.1.34 to 10.1.39
- Added: Some indexes to improve performance.
- Added: Support of single sign on via Cloud Identity Provider (Entra ID, Ping Identity, Okta) incl. MFA.
- Changed: Unified and centralized login for UMS Web App and UMS Console incl. Single Sign-On within the different UMS applications.

Unified Protocol

- Added: Support for Asset Inventory Tracker (AIT) for OS12 devices (IGEL OS Base System 12.6.1 or higher needed).

UMS

- Added: Additional umsadmin-cli shell script, that provides the same functionality as `umsadmin-cli.bin` on Linux machines, but without the QT dependency. It can be used whenever QT dependencies are not available or not wished, like on headless Linux machines or containers.

UMS Web App

Devices

- Added: First-authentication keys can now be administrated in the UMS WebApp. (**Devices > settings sidebar > First Authentication Keys**)
- Added: Functionality to get Logfiles from a Device (OS12+ only) for Support via the Web App, including System Info (incl. ICG), Profiles and Apps. Command is now accessible from the command toolbar for devices and device directories.

Configuration

- Added: Quick Setup mode is now available for apps that support this feature.

- Added: **Explore Quick Start Configurations** button for users with completely empty Profiles, Priority-Profiles, or CIC trees.

Configuration Dialog

- Added: Additional parameters are available in the CIC configurator to enable screensaver with custom data partition for OS12 devices.

Search

- Added: Complete overhaul of the index functionality:
  Changes to devices are now reported to the index "on the fly" and will therefore be included in the search results "near live".
  A complete re-index of all devices and permissions will now occur "once a day" (default) as a fallback - interval and time can be configured.
  (**Search > settings sidebar > Index Configuration**)

Users

- Added: Local users and groups can now be managed in the UMS Web App.
- Added: Change password functionality is now available in the Web App.
- Added: Global permissions can now be managed in the UMS Web App.
- Added: Identity Provider (IdP) client configuration and IdP roles can now be managed in the UMS Web App.

Known Issues - Post-release - Fixed with UMS 12.08.110

AD / LDAP integration

- AD login could fail when an UPN suffix was used for an AD user and with that the logon with user@domain name was not possible.

Cloud IdP / SSO

- UMS console login with hostname (without domain) no longer worked.
- Allow FQDN with uppercases.
- Integrate umsstarter into `RMClient.exe` (updating installer and protocol registration) to eliminate the separate JAR.

Console, common

- UMS Console only installations could run into a login/connect error if they were never connected to the UMS server.
- The use of a hostname to connect to the console was not possible.

Devices

- Timeout issues while saving settings of a device.

Installer (Linux)

- Installer could not register mimetype for console login when package desktop-file-utils was missing on some Linux Systems.
- Linux installation took a very long time on some systems.
- On Ubuntu 22.04 and 24.04 when UMS was installed as a non-root service, the error "Wrong password" was always shown.

Server, common

- OS 11 devices could not download assigned CICs. (OS 11 devices connected via ICG and OS 12 devices were not affected)

UMS common

- Null pointer exception when reading a configuration file.

WebDAV

- In Distributed UMS or HA environments, the WebDAV file synchronization failed.

UMS Web App

Misc

- Login to the UMS Web App failed if the UMS Server is not listening on the default port (8443)
- Removed unused dependency org.apache.httcomponents.client5:httpclient5:5.4.2
- Igel-rest-libs version 12.8.2 was removed from the build.
- Several dialogs were wrongfully displayed in full width in Chromium-based browsers.

Users

- When a user is reassigned to a different group while logged in, the UI did not consistently reflect the change.

Configuration

- Additional timeout issues while saving settings of a device.

Search

- Permissions for a device-record were not properly calculated if the device was in bin on server-start and restored afterwards.
- Not all received changes were correctly flushed into the index.

Notes for Release IGEL UMS 12.07.110

Software:	Version 12.07.110
Release Date:	2025-04-24
Release Notes:	RN-1207110-1

Supported Environment IGEL UMS 12.07.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Resolved Issues IGEL UMS 12.07.110

UMS Common

- Fixed: **Wake up command** was not working properly in some cases.
- Fixed: **Messages between UMS Servers** were not processed.
- Fixed: In some cases, the **UMS license was not evaluated correctly**, which could result in issues such as being unable to log in to the UMS when using an external database.

App Proxy

- Fixed: **SSL configuration for Distributed App Repository** was not working out of the box.

Device Service

- Added: Additional **debug log output for TC Connection States**.

UMS Web App

Configuration

- Fixed: On the network page sometimes an error, related to duplicate keys, was displayed, rendering the page unusable.

Devices

- Fixed: A bug was found impacting the Shadow-functionality for servers in certain time zones. Secure Shadowing tokens — though properly generated and distributed — were consistently rejected during validation, as they appeared to fall outside their valid time window.

Logging

- Fixed: The internal counter for unified logging misused the global counter. This change is important for large installations.

Notes for Release IGEL UMS 12.07.100

Software:	Version 12.07.100
Release Date:	2025-03-06
Release Notes:	RN-1207100-1

Supported Environment IGEL UMS 12.07.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Microsoft Windows Server 2025	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

New Features in IGEL UMS 12.07.100

UMS common

- Added: Support for **Microsoft Windows Server 2025.**
- Updated: Java JDK from version 17.0.12+7 to 17.0.13+11
- Updated: Apache Tomcat from version 10.1.28 to 10.1.34

Administrator Application

- Added: Options for automatic download and manual registration of UMS license. (**Settings > UMS License)**
- Added: Option to UMS Administrator application to export UMS ID. (UMS Administrator application > **UMS ID Backup**)

Devices

- Added: **Support of IGEL Managed Hypervisor**. The administrator can see information about VMs running on an IGEL device and interact with them (start, stop, reimage and wipe).

IGEL Cloud Gateway (ICG)

- Updated: End-user license agreement

Installer (Linux)

- Added: Option to select a user during a new installation to run the UMS Tomcat and other IGEL Services without root privileges.

Installer (Windows)

- Added: Option to select a user during a new installation to run the UMS Tomcat and other IGEL Services without system user privileges.

Unified Protocol

- Added: Possibility to use the UMS as Identity Broker for OS12 devices. The devices can login via UMS to the company AD even if they are outside of the company network. (IGEL OS 12.6.1 or higher needed)

UMS

- Added: **New licensing model for UMS with different levels of feature sets**. Please refer to the IGEL knowledge base for more information about the licensing levels and included features.

UMS Web App

UMS WebApp common

- Updated: Bundled Elasticsearch from version 7.17.7 to 7.17.27 and **increased the used heap space from 1GB to 2GB**

Apps

- Added: Distributed App Repositories available in the Web App.

Configuration

- Added: CIC import and export functionality.
- Added: Option to duplicate a Profile and a Priority Profile via a button in the profile details or with context menu directly on the profile card.
- Added: Notifications and messages about the final deletion process.
- Changed: Moved the button for CIC renaming to the action buttons toolbar.

Configuration Dialog

- Added: The file upload is now also possible in the CIC dialog.
- Changed: Progress spinners have been added to the profile, device, and CIC configuration dialogs to provide visual feedback during loading times.

Devices

- Added: Recycle Bin for Devices is now available in the Web App.
- Added: Support Information is now available in the Web App.
- Added: Option to follow Default Directory Rules in Device Scan Dialog.
- Added: Managed Hypervisor is now available in the Web App for OS12 devices.

Misc

- Added: The feature-based licensing model is now available in the Web App. It includes Priority Profiles, Template Keys and Custom Device Attributes

Others

- Added: Link to Quick Start Configurations in the Help menu.
- Added: License information in Info dialog.

Resolved Issues IGEL UMS 12.07.100

Configuration Dialog

- Fixed: When changing the "Authentication type" setting on the Citrix StoreFront Login page in the profile configuration dialog the settings below were not correctly disabled.

Console - Administration Section

- Changed: The permission “first authentication” is not required any more to restart, update or remove the ICG server. The permission ”WebDAV access” is required to install and update the ICG. READ permission of Proxy Server, Cloud Gateway is required to install. WRITE permission of Server is required to install the ICG.

Device Service

- Fixed: Some parameters were lost when an app was removed from an OS12 profile.
- Fixed: Parameters of deleted profiles were sent to the devices.

UMS Common

- Fixed: The error 'no provider jakarta.mail' has been fixed for UMS under Ubuntu 20.04 or 22.04.

Unified Protocol

- Fixed: Update of device system information resulted in an SQL error if the data was too long.

UMS

- Changed: Removed outdated certificate.
- Fixed: User logins in the UMS Console and WebApp did block database connections for a brief time, leading to long login times.

UMS Web App

Apps

- Added: Context menu for Apps list.
- Fixed: Version deletion was not possible.
- Fixed: When importing an App not via the App Portal, the "import by" field failed to display the user who performed the import.
- Changed: Apps details toolbar is responsive.

Configuration

- Fixed: Newly created CIC was not automatically selected after creation.
- Fixed: Wrong permissions were set in Profile/Priority Profile lists.
- Fixed: Context menu options were enabled if there was no read permission for CICs.
- Fixed: Sometimes files could not be loaded.
- Fixed: It was not possible to select Detach "Now" or "On reboot" options when detaching an assigned object from a CIC.
- Fixed: Wrong icon was shown for OS11 Profiles/Priority Profiles in "Move to recycle bin" dialog
- Fixed: Incorrect icon displayed when moving profiles to recycle bin.
- Fixed: Not assigned Profile incorrectly displayed the "Update Time" dialog when a file was assigned to it.
- Fixed: When importing a profile not via the App Portal, the "import by" did not show the user who imported it.
- Fixed: "Update time" dialog now appears when changing Apps in the App Selector or Use cases in the Use Case Selector dialogs.
- Fixed: Users with write permission on files but not on folders could delete files but could not restore them from the Recycle Bin.
- Changed: The Read-only label and icon in the "Edit configuration" dialog now have a warning color style.
- Changed: The "Edit Properties" button for Profiles has been repositioned to Action buttons.
- Changed: The Recycle Bin now sorts alphabetically, listing folders first, followed by devices.

Configuration Dialog

- Fixed: It was not possible to set Template Keys for instances in Registry.

Devices

- Added: Context menu for the Device list.
- Added: Toggle to hide empty device system information entries.
- Added: Delete license option to device deletion dialog.
- Added: Logging for bulk command to security log.
- Fixed: Device attribute list items could not be deleted.
- Fixed: The "Assigned Devices" section of the Webapp was not updating properly when switching between different files.
- Fixed: Wrong permission checked on Edit Configuration button. (UI only)
- Fixed: Scrollbar was missing for small window-sizes in device details.
- Fixed: In "Edit custom properties" dialog was wrong validation message for numeric input, visibility of focused element and width of input for comment.
- Fixed: Long loading time for Assign Object windows.
- Fixed: Device attribute sorting was not working correctly.
- Fixed: Screen fitting issue within visible area before shadowing.
- Fixed: Config_change flag for devices was sometimes not updated upon device changes.
- Fixed: Device selection was not retained when refreshing the page or navigating between sections.
- Fixed: Incorrect disabling of "Scan for devices" button.

- Fixed: Assign dialog could not load objects when user lacked read CIC permission but device had assigned CIC(s).
- Fixed: "Send settings", "Reboot" commands did not contain corresponding message in logging.
- Changed: Used Tyrus instead of Jetty as client for shadowing.
- Changed: The Read-only label and icon in the Edit configuration dialog now has a warning color style.
- Changed: Previous scan settings are saved.
- Changed: The "Rename" button for devices has been repositioned to the Action buttons.
- Changed: The "Edit Properties" button for Profiles has been repositioned to the Action buttons.
- Changed: The "Update Settings" dialog is now accessible via a button in the Action toolbar.

Settings

- Changed: EPR settings "Enable Priority Profile" update now takes effect immediately.

Search

- Added: New devices are now indexed immediately.

Notes for Release IGEL UMS 12.06.120

Software:	Version 12.06.120
Release Date:	2024-01-16
Release Notes:	RN-1206120-1

Supported Environment IGEL UMS 12.06.120

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)

Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Resolved Issues IGEL UMS 12.06.120

UMS Web App

Devices

Changed: **Improved logging for shadowing of devices**.

Configuration

Changed: **Accelerated check of profile compatibility**. This results in a faster assignment workflow.

Search

Fixed: **Devices missing in search result** if permissions were granted through UMS groups.

Notes for Release IGEL UMS 12.06.110

Software:	Version 12.06.110
Release Date:	2024-12-10
Release Notes:	RN-1206110-1

Supported Environment IGEL UMS 12.06.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)

Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

New Features IGEL UMS 12.06.110

App Proxy

- Added: Data is uploaded to App Binary Repositories immediately if the Repository configuration is changed or a new one is created.

UMS Common

- Added: OS11 devices get ICG addresses even if they are directly connected to the UMS.

Resolved Issues IGEL UMS 12.06.110

App Proxy

- Fixed: URL of load balancer for Distributed App Repository was not sent to the device.

Device Connector

- Fixed: Logging of OS12 commands didn't work if web port was changed.

Device Service

- Fixed: Some parameters were not fully copied when a profile was copied in the WebApp.
- Fixed: URL of load balancer for Distributed App Repository was not sent to the device.

IGEL Cloud Gateway (ICG)

- Fixed: SSH-Key input field does not grow outside the dialog window.

UMS common

- Fixed: Devices didn't receive the license with the latest expiration date when several licenses for the device including unlimited licenses were registered in UMS.

UMS Web App

Apps

- Fixed: Manual update check sometimes did not work.
- Fixed: **Search for updates** button was not always displayed.

Devices

- Fixed: Wrong permission checked for **Edit Configuration** button.
- Fixed: Files were not filtered by display name (quick assign control for **Profile contained files** tab).
- Fixed: Installed apps state was not correctly shown.

Configuration

- Fixed: User without rights could sometimes move profiles.
- Fixed: Users could sometimes see entities in the recycle bin they should not have seen.
- Fixed: **Delete** button on files was enabled for users that have denied Write permissions on the folder.
- Fixed: No logs when modifying profile / priority profile.

- Fixed: It was not possible to move some items to the recycle bin, regardless of permission.
- Fixed: It was possible to move directories to the recycle bin without Write permission.

Configuration Dialog

- Changed: The default printer parameter can now also be activated in a profile configuration and overwrite the device configuration.

Logging

- Fixed: No logs were generated when modifying a profile / priority profile.
- Fixed: Log message indexing was broken for some fields.

Network

- Fixed: Tree keyboard navigation did not work.

Search

- Fixed: Search was not working after update on some installations.
- Fixed: Issue with search permissions when updating to a newer version.
- Fixed: Wrong icon was used for **Edit Search** button.
- Fixed: No french translation for search input field.

Others

- Changed: Optimized usage of database connections and transactions.

Notes for Release IGEL UMS 12.06.100

Software:	Version 12.06.100
Release Date:	2024-10-24
Release Notes:	RN-1206100-1

Resolved Issues IGEL UMS 12.06.100

AD / LDAP integration

- Fixed: In special cases the **UMS Console did not respond** when the Test of an AD configuration was done.

Device Connector

- Fixed: **ICG connected devices could not communicate** with the UMS after a 30 day connection to the ICG without reconnect.
  Workaround: disconnect and connect the ICG

Device Service

- Fixed: **Import of profile sometimes resulted in wrong configuration**.

Files

- Fixed: **File upload via UMS Web App** did not support different data directory.

IGEL Cloud Gateway (ICG)

- Fixed: In some cases, the I**CG was not reconnected after UMS/ICG restart**.
- Fixed: **UMS console was frozen** if ICG was disconnected, and several UMS servers were offline.
- Fixed: **Devices were able to re-register via ICG** after deletion.

IGEL Management Interface (IMI)

- Fixed: Creation of **template keys and assignment of key values** to devices and device directories **via IGEL Management Interface (IMI) worked only for the superuser**.

UMS Common

- Fixed: **Wake up command was not working** properly in some cases.
- Fixed: **Security Logging Data was missing for LDAP/AD Users** (Information of user who performed action was missing).

UMS Web App

Login

- Changed: **Tooltips removed from Username and Password fields**.

- Fixed: **Remember me function did not save login data**.

Apps

- Changed: **Apps can be searched by Display name**.
- Fixed: The **app was not imported properly** if the app dependency version was empty.
- Fixed: The first **downloaded app did not appear** in the apps list.

Configuration

- Added: **Tooltips for Create New Profile** button **and Set Default Version button**.
- Fixed: The **tooltip remained displayed** on the "Clear All Filters" icon in Assigned Devices.
- Fixed: The **edit file dialog was broken** when opened from File details.
- Fixed: **Items in the file root directory were counted** even if the user had no Browse rights.
- Fixed: **Assign file permissions were not handled properly** in all cases.

Configuration Dialog

- Changed: **Removed the possibility to set template keys on special parameters with combined parameters** set as dependency because it resulted in confusing behavior (e.g. Wi-Fi Domain and Location).
  It is still possible to set template keys in Registry for such cases.

Devices

- Added: **Message if there are no assigned objects in Assigned Object tab**.
- Changed**: Shadowing works via Tyrus** instead of Jetty.
- Changed: **Previous scan settings are now saved**.
- Fixed: The **filter icons in the Assign Objects search** did not work properly.
- Fixed: The **"All selected" option in the Scan Dialog did not function** correctly.
- Fixed: The **number of devices handled was not correct** after multiple scans.

Logging

- Fixed: **Filtering for Logtime "Between"** did not work correctly.
- Fixed: **File and CIC actions** were logged even when logging was not enabled.

Search

- Changed: **The 'go to settings' button has been removed**.
- Changed: **The warning about stacking reindexing has been altered**.
- Fixed: **Value for broken comma was incorrect**.
- Fixed: **Case sensitivity** did not work for any field.
- Fixed: **Cost Center filter** did not work correctly.
- Fixed: Content of the dialog when the **"show terms" button** was clicked was not displayed.
- Fixed: Wrong data was shown for the **filter "within last"+"1"+"min"**.
- Fixed: **Combo box values** were **not sorted alphabetically**.
- Fixed: **Export of the search result included all elements**, not just the search results.

- Fixed: **Filter "Version" did not function** correctly.
- Fixed: **Two or more device attributes with multiple selected items returned incorrect values**.
- Fixed: **Device attribute of the date type did not work** correctly.
- Fixed: Issue with **search permissions** when **updating** to a newer version.
- Fixed: **Permission update in HA environments** could cause issues with database transactions.

Supported Environment IGEL UMS 12.06.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Red Hat Enterprise Linux (RHEL) 9	(64 bit)

Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
Oracle 21c	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

New Features IGEL UMS 12.06.100

Admin Tasks

- Added: **Administrative task for cleaning up expired licenses** and / or license duplicates. (**UMS Administration > Global Configuration > Administrative Tasks**)

IGEL Cloud Gateway (ICG)

- Added: Option to **authenticate to ICG Server with SSH key** for ICG install / uninstall / update / keystore update / restart.

Unified Protocol

- Added: Support for **OS 12 Wake on LAN Proxies**.

UMS Common

- Updated: **Apache Tomcat** to Version **10.1.28**
- Added: Now a **device license is only registered when it doesn't already exist**.
- Updated: **Spring Security** to version **6.3.1**
- Updated: **Spring** to version **6.1.10**
- Updated: **Spring Boot** to version **3.3.3**

UMS

- Added: Support of **Red Hat Linux version 9.**
- Added: Option to **specify the delimiter when the results of a view are saved**/sent by e-mail.
- Added: Support of **Oracle DB version 21**.

UMS Web App

Configuration

- Added: **Recycle Bin for Regular Profiles** is now available in the Web App.
- Added: **Recycle Bin for Priority Profiles** is now available in the Web App.
- Added: **Recycle Bin for CICs** is now available in the Web App.
- Added: **Recycle Bin for Files** is now available in the Web App.
- Changed: All selected **use cases** are now shown **in CIC details and cards**.
- Added: **Assigned CICs** tab is shown.
- Added: **Navigation to the assigned CIC from device** and file.

Configuration Dialog

- Added: **File size is now shown** in files properties in CIC dialog when available.

Devices

- Added: Option to manage **Device Attributes** is now available **in the Web App**.
- Added: New Device property **"Born on Date" (time of registration)**.

Search

- Added: **New filter** related to the **time of registration**.

Misc

- Added: Support for **French language.**
- Updated: **Angular to Version 18**.

Notes for Release IGEL UMS 12.05.130

Software:	Version 12.05.130
Release Date:	2024-08-27
Release Notes:	RN-1205130-1

Readme 12.05.130_UMS.txt

Supported Environment IGEL UMS 12.05.130

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

New Features IGEL UMS 12.05.130

UMS

- Updated: **Java JDK from version 17.0.11+9 to 17.0.12+7**

Resolved Issues IGEL UMS 12.05.130

UMS

- Fixed: **View results** that were **exported with an administrative task didn't contain any monitor information.**

UMS Web App

WebApp

- Fixed: **Some App-Versions were not importable** due to a mismatch of expected and provided values of dependent apps. (Full fix will be provided with UMS 12.06.100)

Notes for Release IGEL UMS 12.05.120

Software:	Version 12.05.120
Release Date:	2024-07-31
Release Notes:	RN-1205120-1

Readme 12.05.120.txt

Supported Environment IGEL UMS 12.05.120

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

New Features IGEL UMS 12.05.120

Server, common

- Updated: **Apache Tomcat from version 10.1.24 to 10.1.26**

Resolved Issues IGEL UMS 12.05.120

UMS Web App

Config Dialog

- Fixed: **Navigation to "apps.cups_printing.print.cups"** in Registry caused the browser window to freeze due to a large instance number.
- Fixed: Parameters based on **combo box component** (e.g. post-session command option) were not shown in the Configuration Dialog.
- Fixed: **Select file button** was disabled on CIC creation.

WebApp

- Fixed: Entries for **generic commands** were missing in security log due to a NPE.
- Fixed: Automatic **update of Default Version** sometimes did not take place when triggered manually.
- Fixed: **Case sensitive checkbox** in the search was broken, in some cases checkbox could not be checked.

Notes for Release IGEL UMS 12.05.110

Software:	Version 12.05.110
Release Date:	2024-07-22
Release Notes:	RN-1205110-1

Readme 12.05.110.txt

Supported Environment IGEL UMS 12.05.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Resolved Issues IGEL UMS 12.05.110

WebApp

- Fixed: A bug where commands on a folder were send to a different folder. For details, see UMS Web App Sends Commands to the Wrong Devices (see page 560) .
- Fixed: "0 System Error", which occurs randomly
- Fixed: An unused package was delivered with the elastic search installation to customers. (Package was deactivated and inactive.)

Notes for Release IGEL UMS 12.05.100

Software:	Version 12.05.100
Release Date:	2024-07-15
Release Notes:	RN-1205100-1

Readme 12.05.100.txt

New Features IGEL UMS 12.05.100

Due to changes in certificate handling you must restart your ICGs after completing UMS installation.

Console, administration section

- Added: **Additional checks for web certificate import**; a warning message is shown when a subject alternative name has the wrong type.

Default Directory Rules

- Added: **Views and default directory rules for onboarding** user name / user role and user mail domain.

IGEL Cloud Gateway (ICG)

- Added: **“Restart ICG Service” button** to ICG overview panel toolbar to restart an ICG service.

IGEL Management Interface (IMI)

- Added: **IMI extension to manage template keys**.
  There are 5 new Rest calls:
  - reading template keys and values,
  - creating new template key
  - assigning values to a key
  - device and directory

Installer (Linux)

- Added: Information that the customer has to **restart any existing ICG after an update installation** of the UMS from version 12.4 (or lower) to 12.5 (or higher).

Installer (windows)

- Added: Information that the customer has to **restart any existing ICG after an update installation** of the UMS from version 12.4 (or lower) to 12.5 (or higher).

Template keys and groups

- Added: **Additional static template key: SERIALNUMBER** (for the serial number of the device)

UMS

- Updated: **Java JDK from version 17.0.10+7 to 17.0.11+9**
- Updated: **Apache Tomcat from version 10.1.18 to 10.1.24**
- Added: **Support for Ubuntu 24.04**

UMS Web App

Configuration

- Added: **Corporate Identity Customizations (former Firmware Customizations)** are now available in the Web App for OS11 and OS12 devices. Existing Firmware Customizations are now also available as Corporate Identity Customizations in the UMS Web App.
- Added: It is now possible to **add multiple use cases to one Corporate Identity Customization in the Web App**.

Network

- Added: **Additional information to network page.**

Search

- Added: It is now **possible to mark a Search as "public"** and therefore share it with all other users within the UMS cluster.
- Added: **Time Relative Searches: Filters that work on timestamps** can now be used to do "relative" searches (before, after, ...).
- Added: The Search section now shows **both types of saved Searches: The own ones (private) and public ones.**

Supported Environment IGEL UMS 12.05.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Ubuntu 24.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)
Azure	SQL Managed Instance

Resolved Issues IGEL UMS 12.05.100

Configuration Dialog

- Fixed: **Local User password was not saved when set in profile** (page Security / Logon / Local User).

Console, administration section

- **Fixed: If a mass license was registered several licenses with the same content were shown** at **Device Licenses** (**UMS Administration > Global Configuration > Licenses > Device Licenses**).

Device Connector

- Fixed: **Reconnecting the ICG management connection** to an ICG could end up in an endless loop, blocking an attempt to manually connect.
- Fixed: In installations with multiple load balanced ICGs or UMSs on different ports, **shadowing sometimes did not select the correct port.**
- Fixed: In some cases, the ICG was not fully connected, ICG was shown as online but **device commands were not processed**.

Devices

- Fixed: **Issue with export of device settings** in case of several configured network cards.

Files

- Changed: **File-Service checks the source directory for WRITE permission**. If the source directory has no WRITE permission, a file cannot be moved.
- Changed: **Upload of a file with an already existing filename is now allowed.** Filename will be changed to filename(x).

IGEL Cloud Gateway (ICG)

- Fixed: **Improved ICG connect/disconnect overview** calculation for offline UMS Servers.
- Fixed: In the **upgrade process from OS11 to OS12 an Endpoint is called to get Configuration Settings. This request failed.**
- Changed: The **ICG connection state is now divided into OS11 and OS12 connection states.**
- Fixed: **Device got a NOTALLOWED error message when the ICG was disconnected and connected again to the UMS.**

Installer (windows)

- Changed: To avoid subsequent errors, we will **no longer allow spaces in passwords. This also corresponds to the generally used convention in the IT environment.**

UMS common

- Fixed: **Logfiles were sometimes not archived every day.**

Unified Protocol

- Fixed: **The device registration with UMS one-time keys and newer OS12 devices did not work**. The usage count of the one-time key was increased by one, but the device could not be registered. The registration with mass-deployment keys worked, but the usage count was two instead of the expected one.
- Fixed: In case the **Device Network adapter was changed the MAC address and Hardware Information was not updated correctly.**

UMS

- Changed: Consent text of Insight Service. Now the Insight Service is enabled by default if the Insight Service has not been configured yet. **The Insight Service can be enabled/disabled at UMS Administration > Global Configuration > UMS Features.**

UMS Web App

Apps

- Changed: **Renamed "App Proxy" to "Update Proxy".**
- Changed: **UMS as an Update Proxy tooltips and label** for checkbox.
- Fixed: **Esc closing did not work for settings**.

Configuration

- Changed: **Introduced tabs for Configuration Section (Profiles, [Priority Profiles,] CICs, Files).**
- Changed: **If a file has no thumbnail, a proper message is shown in the content file section.**
- Changed: **Close config dialog via ESC and close button on top right corner.**
- Changed: If a **new directory is created it appears at the top of the list** until it is renamed/saved.
- Changed: **Unified representation of "Number of contained profiles/files/..."** for all objects.
- Fixed: Profile tree **performance issues.**
- Fixed: **Drop down menu for Assign object** to directory/device was shown shortly in the wrong place.
- Fixed: **Display of file size** when information is not available.
- Fixed: **Detach assigned directory from profile,** priority profile, file is possible for users without bulk permission.

- Fixed: After creating a **new profile, icon in list card was wrong.**
- Fixed: **Changing the name of a profile** did not update the name in the card.
- Fixed: **Long filenames broke the layout** of the upload-dialog (Files, Profiles, Priority Profiles & Apps).
- Fixed: **Logging action for files** was carried out regardless of settings.
- Fixed: S**ave-Button was not activated** on file name change for some types of classifications.
- Fixed: It was not possible to go to the **profile's details clicking on its name** in the list of assigned objects of a device.
- Fixed: Now the f**ile name is used in case the file display name is an empty string.**
- Fixed: **Wrong view was shown in Content tab** after file selection.
- Fixed: **Tooltip for deleting icon for Files**.
- Fixed: **Priority profiles options did pop up** and disappear on creating folder for regular profiles.

Config Dialog

- Changed: **More user-friendly save workflow** was implemented **for Template Keys.**
- Fixed: **Parameters on Appliance Mode page** were shown for OS 11 in the Configuration Dialog in the Web App.
- Fixed: The option to **include Registry in the search is now shown without the switch**.
- Fixed: Change **highlight was not shown** for some parameters.
- Fixed: Change **highlight was not removed** on reverting changes for some parameters.

Devices

- Changed: **Close config dialog via ESC** and **close button** on top right corner.
- Changed: **New directory created appear at the top of his parent** children until is renamed/ saved.
- Fixed: **Installed Apps date format.**
- Fixed: **Registration for multiple devices.**
- Fixed: Edit Custom Properties dialog has **missing "Date Input" property.**
- Fixed: **Assign object button for folders** was active when permission Device Bulk Action was not set for the user.
- Fixed: **German translation** was missing in the Scan device table column.
- Fixed: **Dialog "apply now/on next boot"** was not shown properly when devices were moved from one folder to another.
- Fixed: Wrong **format of date/time for "Installed App" tab**.
- Fixed: **Filtering in devices.**
- Fixed: **Sorting for Installed apps on devices.**
- Fixed: Move **device directory dialog** did not display correctly.
- Fixed: Error on trying to **assign an app to a device** by selecting the default version.

Logging

- Changed: **Paging dropdown** is opened **on top**, instead of below.
- Fixed: Some **commands were logged twice.**
- Fixed: Added **missing translations.**
- Fixed: **Datetime control was not visible.**

- Fixed: **Filters** in logging **did not work.**
- Fixed: **Category column was not sorted** properly.

Misc

- Changed: **Updated to hibernate-search 7.1.0**

Network

- Changed: **Order of labels** in Network Information page.
- Fixed: **Added "Not set" flag** in case specified fields have no data in database.

Search

- Changed: **Added option to copy public searches** into private ones.
- Changed: The **list filters** shown for a new search ("Default Filters") was changed to: [All Fields], App Installed, Last Boot Time, Name.
- Changed: **Export button is disabled while export is in progress.**
- Changed: **Wait indicator** was added for the list of saved Searches.
- Changed: **Search is now disabled while mass indexing** is happening.
- Changed: **Validation for IP address.**
- Changed: **Animation for opening advanced search is faster**.
- Fixed: **Search for device attributes** was not working.
- Fixed: **Jump functionality** did not work.
- Fixed: **Scrollbar in active filter** was not displayed properly.
- Fixed: **Data filter is not disabled** when query is complex.
- Fixed**: "Last IP"-dropdown filter did not work.**
- Fixed: **Case sensitive was disabled when query is complex.**
- Fixed: **Search** was sometimes no longer working when **using a Linux based UMS**.
- Fixed: **Filter for the last know IP-Adress was misbehaving** when used in query language.
- Fixed: **Case sensitive checkbox** was not toggled properly.
- Fixed: **Autocompletion** was not working properly.
- Fixed: **Case sensitive for index-only** search did not work.
- Fixed: **Column for last logged in user** sometimes did not show any values.
- Fixed: **Indexing failed if Db contained more than one onboarding token** for a device.
- Fixed: **Scrollbar for filters did not move** to the bottom automatically.
- Fixed: **Select column disappeared** when there was an error in search.

Known Issues IGEL UMS 12.05.100

UMS Web App

Configuration

- Using the same image for multiple use cases in single Corporate Identity Customization (CIC) might result in only one of the use cases applied correctly. **To avoid it, please either upload the image again or use single use case CICs in such situations.**

Notes for Release IGEL UMS 12.04.120

Software:	Version 12.04.120
Release Date:	2024-05-21
Release Notes:	RN-1204120-1

Readme 12.04.120.txt

Supported Environment IGEL UMS 12.04.120

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

Known Issues IGEL UMS 12.04.120

UMS Web App

Search

- The **Contains Text** search field (**UMS WebApp > Search**) currently excludes all hardware information fields.
  Hardware information (e.g. bios-vendor, boot-mode, CPU type) need to be filtered for by their respected filter-fields.

Devices

- Shadowing via the UMS Web App sometimes does not work if:
  - the UMS is installed on a Linux server and
  - the browser is installed on the same machine

Workaround:

1. Use a browser that is installed on a different machine.
   - Substitute “localhost” in the URL with the IP of the machine.

New Features IGEL UMS 12.04.120

UMS

- Added: **Option to force setting the network name** of a device from UMS-internal name.

UMS Web App

Apps

- Added: The administrator can now **see for each App Version if only the Metadata is present**, or if the complete binaries are also stored in the UMS.
- Added: Option to **block devices from using public App Portal as download source**. (For "Air-gapped-Systems")
- Added: Option to **block the cleanup-job that runs inside the Update Proxy**. (If the job is activated, the binaries of unused app versions are regularly deleted. Manually imported apps are never deleted by the clean-up job.)

Resolved Issues IGEL UMS 12.04.120

Console, Common

- Fixed: **Delete action in context menu** and toolbar didn't consider if recycle bin was active.

Device Service

- Fixed: **Partition password for OS11 partitions** was stored encrypted by the WebApp configuration.

Profiles

- Fixed: Some **profile settings** were lost if the underlying version of the apps was changed.

Unified Protocol

- Fixed: In some cases, a **duplicate key error** occurred when a license request event was written.
- Changed: **Type of device-connector (UMS or ICG) is transferred to device with settings.**

UMS

- Changed: The **heartbeat signal offset is configurable** now and for the heartbeat interval greater values can be specified.

UMS Web App

Apps

- Changed: If the **Update Proxy is enabled, newly imported Metadata will automatically trigger the download of the corresponding binaries.**
- Changed: The u**pload-buttons inside the app-section are now unified:** Users can upload **both ipgk-files and iam-files** via the same workflow, and the system will respond accordingly.

Configuration

- Fixed: **Long filenames** broke the layout of the upload-dialog. (Files, Profiles, Priority Profiles & Apps)
- Changed: **Upload-Button in files has now the same icon as the other upload-buttons in UMS Web App.**

Configuration Dialog

- Fixed: **Profile and Device Configuration Dialogs** could not be closed by hitting ESC key or using the X button.
- Fixed: It was possible to save an **invalid configuration** in some cases.

Devices

- Fixed: **Shadowing via the UMS WebApp** didn´t work when Security Logging was enabled.
- Changed: **Disabled constant connection check for shadowing via the Web UMS**.
  This will lead to a more stable shadowing experience but will result in a timeout after some minutes after the connection is idle.

Search

- Fixed: **Search for AD-Group-Users** was broken.

Notes for Release IGEL UMS 12.04.110

Software:	Version 12.04.110
Release Date:	2024-04-23
Release Notes:	RN-1204110-1

Readme 12.04.110.txt

Supported Environment IGEL UMS 12.04.110

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

Resolved Issues IGEL UMS 12.04.110

Installer (Linux)

- Fixed: Error **importing Certificate Private Keys**.

UMS Common

- Fixed: **MS SQL Server database connection** with DB type ‘SQL Server AD Native’ or ‘SQL Server Cluster AD Native’. For more information, see Known Issue: UMS Cannot Connect to the MS SQL Database (see page 1557).

Notes for Release IGEL UMS 12.04.100

Software:	Version 12.04.100
Release Date:	2024-04-09
Release Notes:	RN-1204100-1

Readme 12.04.100.txt

Known Issue: UMS Cannot Connect to the MS SQL Database

The problem applies to windows environments only. UMS Console only installations are not affected.

Problem

The UMS cannot connect to the database after the update to UMS 12.04.100. This applies to UMS Server service igelRMGUIServer and UMS Administrator application.

Environment

- UMS 12.04.100
- Windows Server
- Microsoft SQL Server database using AD native authentication
- DB Type:
  - SQL Server AD native
  - SQL Server Cluster AD native

Solution

The reason for this issue is a windows library shipped in the wrong version (`mssql-jdbc_auth-12.4.0.x64.dll`).

A possible work-around is to manually replace the library at two locations in UMS installation:

- `[UMS installation directory]/rmguiserver/bin/ mssql-jdbc_auth-12.4.0.x64`
- `[UMS installation directory]/rmadmin/mssql-jdbc_auth-12.4.0.x64`

Replace the two files with version 12.4.2 of the library: `mssql-jdbc_auth-12.4.2.x64` . This can be found in Maven Central repository[231]:

https://repo1.maven.org/maven2/com/microsoft/sqlserver/mssql-jdbc_auth/12.4.2.x64/mssql-jdbc_auth-12.4.2.x64.dll

231. https://mvnrepository.com/artifact/com.microsoft.sqlserver/mssql-jdbc_auth/12.4.2.x64

Supported Environment IGEL UMS 12.04.100

UMS Server:

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

UMS Client:

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

Backend Database (DBMS):

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

New Features IGEL UMS 12.04.100

Administrator Application

- Added: **Commands to the IGEL UMS Administrator Command-Line Interface** to manage Web certificates. The following actions are supported:
  - Creation of root of signed certificates.
  - Renewal of certificates.
  - Import of root certificates, signed certificates, decrypted private keys and certificate chains.
  - Export of certificates and certificate chains.
  - Deletion of certificates.
  - Assigning a certificate to current server or to all UMS servers.
  - Listing existing certificates, details of a certificate or assigned server of a certificate.

Console, Administration Section

- Added: **Advanced Searches** (created in UMS Web App) **are assignable to Administrative Tasks**.

Jobs

- Added: **Advanced Searches** (created in UMS Web App) **are assignable to Jobs**.

Security

- Added: **Notification** is created when a device communication certificate uses a **weak signature algorithm**.

UMS Common

- Added: **App Signing Certificate** as **new file class** to be able to roll out certificates specifically used for custom app signing.
- Updated: **Azul Zulu JRE from version 17.0.8.1+1 to 17.0.10+7**
- Updated: **Apache Tomcat from version 10.1.15 to 10.1.18**

Unified Protocol

- Added: Possibility to **export the "Client certificate chain"**.
- Added: **Compatibility for F5 BigIP to manage OS12 devices** (IGEL OS with version 12.3.2 or higher required).

UMS

- Added: **Improved import of Web Certificates and Web Certificate Chains**:

    - When a signed certificate is imported, which is signed by a public certificate, such public CA certificates can be additionally imported automatically.
    - When a keystore is imported, the certificate chain can be built automatically.
    - It is no longer possible to import a certificate when a certificate with the same fingerprint is already present.
    - Additional checks referring to validity, signature verification, subject alternative names and private keys have been added.
- Added: **Support for Azure SQL Managed Instance** via SQL login.

UMS Web App

Apps

- Added: **Dependencies of Apps**: A **new tab** will show the dependencies for each version. Old versions will sync over time.

Configuration

- Added: **Support for dynamic file classificatio**n.
- Added: It is now possible to **drag and drop files from one directory to another**.

Configuration Dialog

- Added: **Pages** that show the selected parameter **are listed in Registry**.
- Added: **Indicator** for Sessions **configured via a Profile** is added in Device Configuration.
- Added: **Input validation** for the **Template Key Directory name**.
- Added: **Input validation** for the **Template Key name**.
- Added: It is now possible to **add all available values** for the selected parameter **to the Template Key values**.
- Changed: More **UI elements** are **redesigned** for the new light and dark modes.

Search

- Added: **Case sensitive searches**: To give the user more control over search terms it is now possible to mark a search as case-sensitive or insensitive.
- Added: The user can now **switch from the apps view to the search view** on a new tab to see on which devices the app (or app version) is installed.
- Added: **Custom Device Attributes** are now available as columns.
- Added: **Added filter** "firmware id".
- Added: **Added filter** "app version id".
- Added: **Added filter** for devices with app version directly assigned.
- Added: **Warning message when you leave the unsaved search**.
- Added: **Security logging for deleting views**.

Misc

- Added: **Security logging for user action** (profile, master profile, devices, etc.)

Resolved Issues IGEL UMS 12.04.100

Files

- Fixed: **File cache for OS11 devices** is now updated if a file was changed in UMS Web App.
- Fixed: A **folder** with `NOT-SET` of `BROWSE` right was **not visible in the file tree**, although the subfolder had an `ALLOW` of `BROWSE` right and although the folder contained a file with an `ALLOW` of `READ` right.
- Fixed: In a **distributed UMS new files were not synchronized** to the WebDAV directory of each UMS server.

Installer (Windows)

- Changed: It is **no longer allowed to define only blank characters as a password**.
- Changed: The wizard-pages for **memory allocations are swapped: first UMS Server** (Tomcat), **second UMS Console** and added additional text info on the wizard-pages how and where the user can change the memory allocation later on.

UMS Common

- Fixed: The **SQL Console could not handle multi-line statements**.
- Fixed: The function to send an **e-mail works again** with UMS running on Ubuntu 20.04 or 22.04.

Unified Protocol

- Fixed: **App installation state time** is only changed when the state has changed.
- Changed: **Improved error handling** for the management WebSocket connection between UMS and ICG.
- Changed: When a **shadowing/secure terminal action** is triggered but the forwarding of the device port forwarding event fails, the UMS closes the port forwarding WebSocket to the device.
- Fixed: Device **Last Boot Time was not updated** with every reconnect.
- Fixed: **Devices** did **reconnect every 30 minutes**.

UMS Web App

Apps

- Fixed: **Wrong label in German** for Automatic Updates.
- Fixed: **App version state badge** behaves properly without the text protruding from the badge.
- Fixed: **Assigned objects tab** content in app details in **not scrollable**.
- Fixed: **Issue creating the** `pxe-config.json` with non-base-system apps.

Configuration

- Fixed: Files - **assigned objects list does not update** after new assign or detach.
- Fixed: **File tree was not reloaded** after the file was uploaded.
- Fixed: **File edit dialog opens correctly** from toolbar as well from settings accordion.
- Fixed: **Certificate content starts with space**.
- Fixed: **Lower part of letters is chopped** in profile names.
- Fixed: Template keys and activated settings **filter and pagination not working**.
- Changed: **Tooltip is added to create directory button for files tree**.
- Changed: Enabled **keyboard navigation for files-list**.
- Changed: **Redesign Update Time dialog** after saving changes in Configuration Dialog.
- Changed: The **file classification** display is now **more user-friendly**.
- Changed: Minor **performance update**.

Configuration Dialog

- Fixed: **Search input overlay** broke layout in some cases.
- Fixed: Wrong behavior of showing **dependent parameters on the Network / Proxy page**.
- Fixed: **Template Key button was shown** when the Template Key feature was not enabled.

Devices

- Fixed: **Login History** did not display correctly **in Dark mode**.
- Fixed: **Commands** on the toolbar of the device-details are **executed on the correct device** after selecting a different one on the list.
- Fixed: **Filter could result in an endless loop**.
- Fixed: Removed **strange characters in comment of device**.
- Fixed: The **Default Version now is correctly shown and saved when it is assigned to a device**.
- Fixed: The **current folder is now always pre-selected** as the value in the dropdown of the Scan-dialog.
- Changed: **Properties for devices and device-folders are now collapsible**.
- Changed: **Assign-Dialog** got more height.
- Changed: The **assign dialog version field now shows first the Default Version**.
- Changed: Minor **performance update.**

Network

- Changed: To create a better onboarding experience the **Communication Token** is now a separate field on the server and ICG page.
- Changed: **Network page** was **redesigned** according to our Unified Design System.
- Changed: Add **copy option** on each row in fingerprints accordion.

Logging

- Fixed: **Search filter cannot be reset** in certain situations.
- Fixed: **Parameter is cut off at special char**.

- Changed: It is **no longer necessary to deploy the UMS Web App to use** the feature "**Unified Logging**".

Search

- Fixed: UMS users could see devices in the search that they should not see - **AD Group permission issue**.
- Fixed: **Search button** now aligned properly **on Firefox browser**.
- Fixed: **Bug** that **didn’t allow search** with filter for device attributes **with whitespace**.
- Fixed: **Paginator** now opens in right position.
- Changed: **Autocomplete** is now also **available in Dark Mode**.
- Changed: **Improved stability for indexing**.
- Changed: **Filters** in autocomplete are **sorted alphabetically**.
- Changed: **Saved searches** are now **shown in alphabetical order**.
- Changed: **Removed unnecessary log-entries**.
- Changed: **Button for reindexing disabled until response from backend arrives**, info message is shown.

Misc

- Fixed: **Error on UMS WebApp-login** when web certificate is FQDN only.
- Fixed: **Various labels and colors**.
- Changed: **Various dialogs** are now moved to the Unified Design System.
- Changed: **Font size** in 'About' dialog is increased.
- Changed: **Collapse functionality** for tree area is now easier to use and state is remembered by the browser.

Notes for Release IGEL UMS 12.03.110

Software:	Version 12.03.110
Release Date:	2024-02-05
Release Notes:	RN-1203110-1

Readme 12.03.110.txt

Supported Environment IGEL UMS 12.03.110

- **UMS Server:**

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **UMS Client:**

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **Backend Database (DBMS):**

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)

Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

New Features IGEL UMS 12.03.110

UMS Web App

Configuration

- Added: **Change Indicator** is now **added to the Registry tree and Adjustments.**
- Added: **Pages** that show the selected parameter are **listed in Registry**.
- Added: The **current parameter** is shown above variable expression in the **Template Key sidebar**.

- Changed: **More** User Interface elements of the **Configuration Dialog** are now using the new unified design.

Resolved Issues IGEL UMS 12.03.110

UMS, Common

- Fixed: **View performance in UMS Console improved**.

Console, Administration

- Fixed: **Export of Web certificates chain** failed when private key of end certificate **was not known**.

Device Service

- Fixed: Some **passwords could not be reset** in the WebApp config dialog.

Automatic License Deployment (ALD)

- Fixed: **Error** occurred in `ums-server.log` when and **OEM license was deployed**.

Misc

- Changed: **New IGEL logos**.

UMS WebApp

Configuration

- Fixed: **Group-Permission** were not respected when calculating permissions for files.
- Fixed: **Error message was incorrectly shown** when assigning a file to a profile.
- Fixed: **Permission Calculation** for editing and vreating a profile were not correct. (Help-Desk Use case)

Devices

- Changed: **Properties for devices** and device-folders are now collapsible.
- Changed: **Assigned objects tab content** in app details is now scrollable.
- Fixed: In the **assigned object tab the wrong version of an app** was sometimes shown.
- Fixed: **Parts of the device details** were loaded and calculated **twice**.
- Fixed: **Minor performance improvement:** Refactored database-calls for calculating the content of a device folder.

Network

- Fixed: **Malformed entries in the Browser-Cache** could lead to unreadable entries in the Network-Section.

Search

- Changed: The **"app with error"-filter will no longer be shown** on installations with embedded Databases, since the database does not currently support this feature.
- Fixed: **A bug** was present that showed **complex queries** in the simple UI-state.
- Fixed: **A bug** was present where **Device Attributes filter froze** the frontend in some cases.
- Fixed: **Device attributes with names with whitespaces** work now.
- Fixed: **Malformed saved searches** could lead to a state where no saved search was loaded.
- Fixed: **The query-string was not readable in Dark Mode.**

Misc

- Changed: New IGEL logos.
- Fixed: **Layout-Bug** causing errors in console
- Fixed: For most **objects the content of the parent folder was additionally calculated.**
- Fixed: Incorrect **labels.**
- Fixed: **Lower part of labels** was cut off.
- Fixed: **Pagination on filters** not working correctly.
- Fixed: Bug where **streams** were unintentionally closed.
- Fixed: A bug was present where l**og messages were saved twice**.

Configuration Dialog

- Fixed: **Password value** of the `custom_partition.sourc%.password` parameter was stored as plain text in the database and on profile export.
- Fixed: **Wrong Change Indicator** was shown in some cases.
- Fixed: **Change Indicator** was shown in some cases.
- Fixed: **Empty container** was shown for some tree nodes in Registry
- Fixed: **Template parameters** were not found when searching in Registry.
- Fixed: Some parameters on the **Default Wi-Fi network** page could not be edited.
- Fixed: **Citrix StoreFront** Sessions could not be added to autostart.

Notes for Release IGEL UMS 12.03.100

Software:	Version 12.03.100
Release Date:	2023-12-13
Release Notes:	RN-1203100-1

Readme 12.03.100.txt

Supported Environment IGEL UMS 12.03.100

- **UMS Server:**

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **UMS Client:**

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **Backend Database (DBMS):**

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)

Microsoft SQL Server 2019	(with Cluster Support)
Microsoft SQL Server 2022	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

New Features IGEL UMS 12.03.100

UMS Common

- Added: **UMS-Console and ICG log security relevant events** in a separate log file.
- Changed: Updated spring boot to version 3.1.4 in all services.
- Changed: Updated spring to version 6.0.10
- Updated: **Microsoft SQL** driver version to **11.2.1** to support MS SQL Server 2022
- Updated: **Azul Zulu JRE** from version 17.0.7 to **17.0.8**
- Updated: **Apache Tomcat** from version 8.5.89 to **10.1.15**

Console, Common

- Changed: The **user name of a UMS administrator is modifiable** now.

Jobs

- Added: The **OS12 Specific Device Commands** can also be executed **via jobs** in the UMS Console. See UMS WebApp [Apps] for more information about Specific Device Commands.

Permissions

- Added: **New service to unify permission calculation**.

Unified Protocol

- Added: Management of **Device Attributes for OS 12** devices (base_system 12.3.0 or higher needed).
- Added: Support of **User Login History for OS12** devices.
- Added: Support of **Specific Device Commands for OS12** devices (base_system 12.3.0 or higher needed).

Installer (Windows)

- Added: Now it is **possible to manually edit the maximum memory consumption of the UMS-Console and Tomcat during installation** with the installer wizard.
- Updated: **Apache Tomcat** from version 8.5.89 to **10.1.15**

Installer (Linux)

- Updated: **Apache Tomcat** from version 8.5.89 to **10.1.15**

Custom Device Attributes

- Added: **Device attributes**, which are **used in a default directory rule** and therefore cannot be deleted, **are marked with a hook** (**UMS Administration > Global Configuration > Device Attributes**).

Administrator Application

- Added: Option for **automatic cipher adjustment on update**. (New secure ciphers are activated, weak ciphers are removed) (**IGEL UMS Administrator > Settings > Cipher (Server-side)**).

UMS Web App

Apps

- Added: **Base Systems** (OS12) as well as **other apps can now register Specific Device Commands**, that this specific app or Base System understands, to the UMS.
- Added: **Profiles from Version Tab**. It is now possible to **create a profile specifically based on the selected version from the app version tab**.

Configuration

- Added: **Files**: It is now possible to **manage, add and configure files via the WebApp**. For **images and certificates** a **preview** will be shown.

Network

- Added: **UMS Features**: It is now possible to manage specific "UMS Features" from the WebApp: **Priority Profiles and Parametrization (Support for Template Keys) can be activated** here. (**Network > Settings > UMS Features**)

Devices

- Added: **Specific Device Commands**. It is now possible to send Specific Device Commands **via the WebApp**, both **for a single Device as well as for all devices within a folder**. (OS12 only)

Search

- Added: Device Attributes. It is now possible to **search for** (user generated) **Device Attributes**.
- Added: **30+ Filters**, including 'Last logged on user', Devices where (at least) one **App reports an error**, Devices with **App installed**, Devices with **directly assigned App**.
- Added: **30+ Columns**
- Added: **Manual Reindex**. It is now possible for the user to start the re-index-process manually.

Misc.

- Added: **New lightweight and modern UI design** to optimize the usability and user experience of the UMS WebApp.
- Added: **Light & Dark Mode**: It is now possible to switch between a light and a dark mode.

Configuration Dialog

- Added: Support for **Light & Dark Mode** in the new unified design.
- Added: **Change Indicator in the navigation tabs and in the navigation tree**.
- Added: The **path of the parameter** is shown **on the Registry page**.
- Added: The **activation toggle** is implemented **for parameters on the Registry page**.
- Added: **Switch to show only enabled parameters in Registry for Profile Configuration** is implemented.
- Added: The **Template Key** functionality is provided **for parameters on the Registry page**.
- Added: **Registry** can now be included **in the Search**.
- Added: It is now possible to **edit an item with a double click of the table row**.
- Changed: Boolean values are now displayed as read-only checkboxes in tables in Config dialog.

Resolved Issues IGEL UMS 12.03.100

UMS, Common

- Fixed: **Network adapter information of the device** was only **updated** on boot, but not **during settings transfer**.
- Fixed: **Stdout and stderr log files** are now **cleared upon restart of UMS Server on Linux**.
- Fixed: **Error log messages** were not written **to device authentication log** in some cases.

Security

- Updated: **ActiveMQ** to version **5.18.3 to fix** critical security **vulnerability ISN-2023-27**.

Console, Administration

- Fixed: The edit **dialog** of an **Active Directory Service** that is using the LDAPS connection, always showed the default port (**UMS Administration > Active Directory/LDAP**).

Firmware

- Fixed: Some firmwares were not deleted when the **Remove unused firmwares action** was performed.

Unified Protocol

- Fixed: **Errors after OS12 upgrade of an OS11** device which is **managed via ICG**.
- Fixed: **Error log messages** were **not written to device authentication log** in some cases.

Device Service

- Fixed: **Group permissions for Template Keys** were not considered.
- Fixed: **Password reset in ConfigDialog for Devices** was not possible.

Device Connector

- Fixed: The **OS12 management connection logged entries with "ICG connected"** even if it was not connected.

IGEL Cloud Gateway (ICG)

- Fixed: If no public port was configured for an ICG and the **internal port was not set to the default (8443)** the wrong port was sent to OS12 devices.

Views

- Fixed: Result of **views with last boot time criterion** (absolute and relative) **did not contain OS12 devices**.

Console, web start

- Changed: **Removed Java Web Start support**.

UMS Web App

Configuration

- Fixed: **Priority Profiles** now **show included Apps**.
- Fixed: **AD group members** are now able to **see their template keys**.

Apps

- Changed: **Increased the maximum file size for apps** to be prepared for bigger OS 12 Versions
- Fixed: **Error in calculation of usage**: The number "how often a base system version is used" was sometimes too low. Devices that had the OS-Version installed but had not fully registered were not considered.
- Fixed: The **version info of** some **apps** showed contradictory information (the list vs. the details section).

Devices

- Fixed: It was possible to **assign multiple values of a (Boolean) Template Key**.

Search

- Changed: **Additional WQL autocompletion support**: Customers will now get autocompletion support if they edit the **middle of a WQL-query string**.
- Changed: Additional WQL autocompletion support: The autocompletion feature for the query language now has a **better handling for whitespaces during autocomplete**.
- Changed: Add Renderer: "**Runtime since last Boot**" & "**Total Uptime**" - values in column is now **human readable**.
- Fixed: For embedded Databases numeric-only **values** were n**ot found using the "any-field"**.
- Fixed: **Last Boot Time was not shown for OS12 Devices**.
- Fixed: For embedded Databases **pre-registered devices were not searchable**.
- Fixed: **Users** could be present **in the database twice**.
- Fixed: **Installations using "SQL Server AD Native"** were not able to use the search function in the WebApp.

Misc.

- Fixed: **Various typos**

Configuration Dialog

- Fixed: Some **parameters could not be configured** in the dialog.
- Fixed: The **translated values are now shown** in tables for range parameters.

Known Issues IGEL UMS 12.03.100

UMS Web App

- **Password value** of the **"custom_partition.source%.password"** parameter is **stored as plain text in the database and on profile export**.

Notes for Release IGEL UMS 12.02.130

Software:	Version 12.02.130
Release Date:	2023-11-10
Release Notes:	RN-1202130-1

Readme 12.02.130.txt

Notes for Release IGEL UMS 12.02.120

Software:	Version 12.02.120
Release Date:	2023-09-19
Release Notes:	RN-1202120-1

Readme 12.02.120.txt

Notes for Release IGEL UMS 12.02.110

Software:	Version 12.02.110
Release Date:	2023-08-16
Release Notes:	RN-1202110-1

Readme 12.02.110.txt

Notes for Release IGEL UMS 12.02.100

Software:	Version 12.02.100
Release Date:	2023-07-31
Release Notes:	RN-1202100-1

Supported Environment IGEL UMS 12.02.100

- **UMS Server:**

Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **UMS Client:**

Microsoft Windows 10	(64 bit)
Microsoft Windows 11	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Microsoft Windows Server 2019	(64 bit)
Microsoft Windows Server 2022	(64 bit)
Ubuntu 20.04	(64 bit)
Ubuntu 22.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 8	(64 bit)
Amazon Linux 2	

- **Backend Database (DBMS):**

Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)

Microsoft SQL Server 2019	(with Cluster Support)
PostgreSQL	11 - 15
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 11 - 15)

Removed Support in IGEL UMS 12.02.100

UMS Server

- Microsoft Windows Server 2012 (64 bit)
- Microsoft Windows Server 2012 R2 (64 bit and with Update 2919355)
- Ubuntu 16.04 (64 bit)
- Ubuntu 18.04 (64 bit)

UMS Client

- Microsoft Windows Server 2012 (64 bit)
- Microsoft Windows Server 2012 R2 (64 bit and with Update 2919355)
- Microsoft Windows 8.1 (64 bit and with Update 2919355)
- Ubuntu 16.04 (64 bit)
- Ubuntu 18.04 (64 bit)

Backend Database (DBMS)

- PostgreSQL 9.6, 10.12
- Oracle 12c

Added Support in IGEL UMS 12.02.100

Backend Database (DBMS)

- PostgreSQL 14, 15
- Amazon Aurora PostgreSQL (Compatible with PostgreSQL 14, 15)

Known Issues IGEL UMS 12.02.100

Unified Protocol

- If the command logging for OS12 devices is activated, the UMS Web App needs to be installed on each UMS Server.
- In an HA environment with an installed UMS Load Balancer, the scan and register command for OS 12 Thin Clients might not be successful. This problem occurs with OS 12 versions previous to 12.2.100.

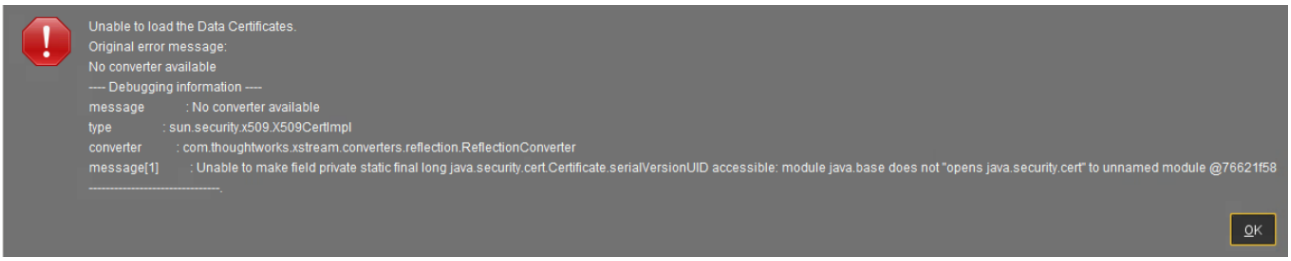
UMS Web App

- The **Search** in the UMS Web App **will not work if UD Pockets** are used in the UMS.
  Customers who use UD Pockets need to either use Views/Searches in the UMS Console or should not update before the issue has been fixed.

Errors Occur after the Update to UMS 12.02.100

Symptom

After updating to UMS 12.02.100, errors like `'....module java.base does not "opens java.security.cert"'` or errors with the same pattern occur, especially when you work with certificates.



Environment

- IGEL UMS 12.02.100 on Windows (update installation)

Problem

In UMS 12.02.100, Java was updated from version 8 to 17. For the migration, we had to add additional Java options for UMS Console, UMS Administrator and IGELRMGUIServer. These options look like this:

```
vmparam --add-opens=java.base/java.security.cert=ALL-UNNAMED
```

During the update, the files `RMClient.config` and `RMAdmin.config` are updated and for the IGELRMGUIServer service additional Java options are added.

- The additional entries for the UMS Console:

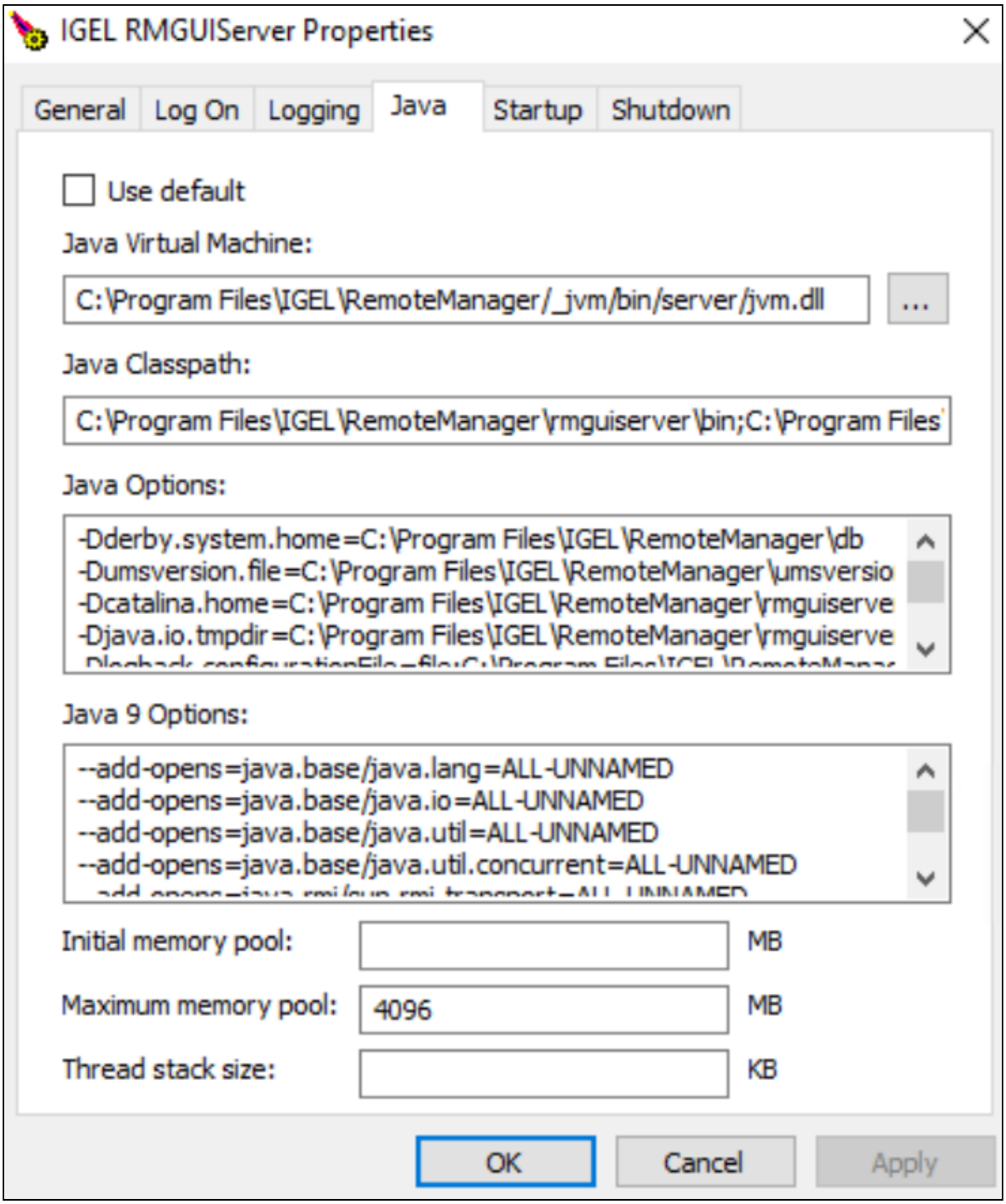
```
vmparam --add-opens=java.desktop/javax.swing=ALL-UNNAMED
vmparam --add-opens=java.desktop/javax.swing.table=ALL-UNNAMED
vmparam --add-opens=java.base/java.security.cert=ALL-UNNAMED
vmparam --add-opens=java.desktop/javax.swing.event=ALL-UNNAMED
vmparam --add-opens=java.base/java.security=ALL-UNNAMED
vmparam --add-opens=java.base/java.util=ALL-UNNAMED
vmparam --add-opens=java.base/java.lang=ALL-UNNAMED
vmparam --add-opens=java.base/sun.security.provider=ALL-UNNAMED
vmparam --add-opens=java.base/sun.security.util=ALL-UNNAMED
vmparam --add-opens=java.base/sun.security.x509=ALL-UNNAMED
vmparam --add-opens=java.base/java.io=ALL-UNNAMED
vmparam --add-opens=java.base/java.util.concurrent=ALL-UNNAMED
vmparam --add-opens=java.base/sun.security.pkcs=ALL-UNNAMED
vmparam --add-opens=java.base/sun.util.calendar=ALL-UNNAMED
vmparam --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
vmparam --add-opens=java.desktop/sun.swing.plaf.synth=ALL-UNNAMED
```

- The additional entries for the UMS Administrator:

```
vmparam --add-opens=java.desktop/sun.swing.plaf.synth=ALL-UNNAMED
```

- The additional entries for the UMS Server (open `.../rmguiserver/bin/editTomcatService`):

```
--add-opens=java.base/java.lang=ALL-UNNAMED
--add-opens=java.base/java.io=ALL-UNNAMED
--add-opens=java.base/java.util=ALL-UNNAMED
--add-opens=java.base/java.util.concurrent=ALL-UNNAMED
--add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
--add-opens=java.desktop/javax.swing.table=ALL-UNNAMED
--add-opens=java.base/java.security.cert=ALL-UNNAMED
--add-opens=java.base/sun.security.x509=ALL-UNNAMED
--add-opens=java.base/sun.security.pkcs=ALL-UNNAMED
--add-opens=java.base/sun.security.provider=ALL-UNNAMED
--add-opens=java.base/sun.security.util=ALL-UNNAMED
--add-opens=java.base/sun.util.calendar=ALL-UNNAMED
--add-opens=java.base/java.security=ALL-UNNAMED
```



When the update of the Java options fails, you get the mentioned errors. In this case, you can't work properly with the UMS. Errors will occur at several sections, especially when you work with certificates.

Solution

The Java 9 options need to be added to fix your environment:

1. Open editTomcatService (.../rmguiserver/bin/editTomcatService).
2. Copy the following entries and paste them to the Java 9 options (not Java options) section. (If this section already contains entries, overwrite them.):

   --add-opens=java.base/java.lang=ALL-UNNAMED
   --add-opens=java.base/java.io=ALL-UNNAMED
   --add-opens=java.base/java.util=ALL-UNNAMED
   --add-opens=java.base/java.util.concurrent=ALL-UNNAMED
   --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
   --add-opens=java.desktop/javax.swing.table=ALL-UNNAMED
   --add-opens=java.base/java.security.cert=ALL-UNNAMED
   --add-opens=java.base/sun.security.x509=ALL-UNNAMED
   --add-opens=java.base/sun.security.pkcs=ALL-UNNAMED
   --add-opens=java.base/sun.security.provider=ALL-UNNAMED
   --add-opens=java.base/sun.security.util=ALL-UNNAMED
   --add-opens=java.base/sun.util.calendar=ALL-UNNAMED
   --add-opens=java.base/java.security=ALL-UNNAMED

3. Restart the IGEL RMGUIServer service and test again.

Limitations IGEL UMS 12.02.100

Check also the "Feature Matrix: UMS Web App vs. UMS Console" under Overview (see page 1593).

UMS Web App - Apps

- Quick assign (app section) is not working.
- If the App Portal window is opened from the UMS Web App, close it regularly, respectively if there was an “idle” time between app imports.
- When creating a profile, it is possible to select apps that do not have configurable parameters (e.g. Chromium Multimedia Codec, Citrix Multimedia Codec, etc.).

UMS / UMS Web App - Core Functionality and Extensions

- Shared Workplace is currently not supported for IGEL OS 12 devices.

UMS / UMS Web App - Device Management

- (Un)Installation of apps requires a reboot.
- **Update** command:
  - 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 (see page 1593).
  - The update or rollout of OS 12 apps and the OS 12 base system cannot be scheduled by jobs. Only the activation of already deployed OS 12 apps and the OS 12 base systems can be scheduled by jobs.
- The secure terminal is available only via the UMS Console.
- The Asset Inventory Tracker is currently not supported for IGEL OS 12 devices.
- The UMS Console can only be used for:
  - Deleting profiles and clients; to open, edit, or create profiles for IGEL OS 12, the UMS Web App must be used.
  - Default directory rules
  - Admin account administration
  - Setting permissions on tree nodes
  - SQL console usage (also possible at UMS Administrator)
  - Starting the UMS Web App
- Copying of OS 12 profiles is not possible. Instead, you can currently use the export / import of profiles; see Exporting and Importing Profiles in the IGEL UMS Web App (see page 1593).

UMS Profiles

- OS 11 and OS 12 profiles are not compatible: Direct assignment of OS 12 profiles to OS 11 devices is not allowed (and vice versa).

New Features IGEL UMS 12.02.100

UMS Common

- Added: **Direct assignment of OS12 profiles to OS11 devices** is **not allowed** (and vice versa).
- Changed: The **proxy server usage for "Deployment (ALD)"** has been **renamed to "IGEL Cloud Services (ICS)"**. A **proxy** set under **Global Configuration > Licenses > Deployment > Edit Proxy Configuration** is now used for **all IGEL Cloud Services**.
- Added: **MS SQL Server** option '**trustServerCertificate**' (default is false, on upgrade set to true).
- Changed: '**Allow SSL connection only**' setting (**IGEL UMS Administrator > Settings**) is now **checked by default**.
- Updated: **Azul Zulu JRE** from version 8u352 to **17.0.7**.
- Updated: **Apache Tomcat** from version 8.5.84 to **8.5.89**.

Console, Administration Section

- **Removed**: UDC2 Deployment. (**UMS Administration > Global Configuration > Licenses > UDC2 Deployment**).

Admin Tasks

- Added: Administrative **task for detaching objects from view results**.

Unified Protocol

- Added: **Log messages for commands sent by a device** are now displayed **in the UMS Web App logging section**.
- Added: **Proxies for management of OS 12 devices via ICG** are now supported.

Server, Common

Changed: For each service, **only the registered license with the latest expiration date is transferred to a device**.

Administrator Application

- Added: Admin **CLI commands** to show, set and delete **UMS cluster FQDN**.

Universal Customization Builder (UCB)

- **Removed**: the "**Universal Customization Builder**" feature from the UMS.

Installer (Windows)

- Added: **During the installation process**, the user can now create a **desktop icon for the UMS Administrator**.
- Changed: Now it is possible to **upgrade from an "UMS Standard Server (stand-alone)" installation to a "Distributed UMS"**.

Installer (Linux)

- Updated: Added **Distributed UMS as an additional install option** into Linux Installer.

Device Service

- Added: **Export and import of OS12 profiles**.
- Added: **Export and import of OS12 app metadata**.

Device Connector

- Added: **Support for SSL offloading on reverse proxy** with optional mTLS.

UMS Web App

Apps

- Added: **Export of all/some/one version of an app (metadata)**: App versions can be exported as '`*.iam`'.
  This file contains all necessary data to be imported into another UMS.
  The artifacts needed for the device are not included and need to be retrieved by the device via the App Portal.
  (The UMS does not handle these artifacts unless the 'use UMS as Update Proxy'-mode is activated. If this update-proxy mode is enabled please use the `*.ipkg` data and workflow instead.)

- Added: **Import of apps (metadata)** via `*.iam` packages as well as via `*.ipkg` packages.

Configuration

- Added: Export of OS12 profile: It is now **possible to export an OS12 profile as well as priority profiles** (`*.ipm`).
  All apps (-versions) configured in this profile are **automatically included**.

- Added: Export of OS12 profiles: It is now **possible to export all/some OS12 profiles (or priority profiles) within a folder (including all subfolders)**. (`*.ipm`)

- Added: Import of OS12 profiles: It is now **possible to import OS12 profiles** as `*.ipm` packages. The user can decide to **import the profile in the selected folder or recreate the original folder structure**.
  Profiles can be imported as priority profiles and vice versa. **If the folder structure needs to be recreated**, **the path will begin with the new selected object root**. (profile/priority profile)

- Added: Added a **new tab to the profiles** where the user can see **which apps are configured within a profile** (including the version of the used app).

- Added: Added functionality to **open the configuration dialog by double-clicking on a profile** (or priority profile).

- Added: **Template Key functionality** is now provided **for Profile Configuration**.

Devices

- Added: **Scan & Register**: It is now possible to scan for devices within the network (or certain IP ranges) and register selected devices.
- Added: Additional information to Installed Apps Tab: It is now **possible to see the state of all registered/downloaded/activated apps as reported by the device**. (State and message)
- Added: **Export OS12 device settings as profile**. It is now possible to export an OS12 device "as a profile". **All activated settings will be saved as a profile**. (`*.ipm`)
- Added: Added functionality to **open the device settings by double-clicking on the device**.

Search

- Added: A completely **new search functionality** was **added.**
  - Searches **can be saved, edited, and reused**.
  - **Complex searches** can be used utilizing a **SQL-like query language**. (Activatable under "Advanced search")
  - **Simple searches** will be **translated into the query language** to give the user insight into the structure. (**If Advanced search is activated**)
  - Please note: **Time-based searches are currently not available on installation using a Derby database**.

- Added: **First implementation of autocompletion for the query language**.

Settings

- Added: Logging settings to the Logging section: It is **now possible to activate/deactivate the logging from within the UMS Web App**. This includes the option to activate the logging via the Unified Protocol.

Misc.

- Added: **Context menu** for **Devices**.
- Added: User can now see **how many objects (devices, profiles, ...) are inside a folder, and combined with its subfolders separately** (x from y).

Resolved Issues IGEL UMS 12.02.100

Console, Common

- Changed: The following **characters** are **no longer allowed when a new administrator account is created**: `"/ \ [ ] : ; | = , + * ? < >`

Views

- Fixed: In the **csv export of 'Send view result as mail...'** (**View context menu > Send view result as mail...**) entries with special characters were not correctly formatted.
- Fixed: **View export** via mail (**view context menu > Send view result as mail...)** was missing all monitor information.
- Removed: View criterion '**Has Web certificate with SHA256 fingerprint**' from list of selectable view criteria.
- Removed: View criterion '**Unified Protocol Device**' from list of selectable view criteria.

Admin Tasks

- Changed: **Improvements in Administrative Tasks wizard dialog**s.

AD / LDAP integration

- Fixed: **Shared Workplace via ICG** change Password problem.

Firmware

- Fixed: It was not possible to **assign IGEL OS Honeywell's firmware updates**.

Unified Protocol

- Fixed: **Rolling of Unified Protocol logs (OS12)**. Details can be found in `<installation directory>/rmguiserver/logs/README.md`.
- Fixed: **Proxy support for validation of Onboarding Service token**.
- Fixed: In case an **ECS certificate** was used as UMS Web or ICG certificate, **OS 12 devices can't be registered**.

High Availability Feature

- Updated: **HA Health check** handles Distributed UMS correctly.

Device Service

- Fixed: **Session order in the device configuration dialog** was different in UMS Web App and Device.

Installer (Linux)

- Fixed: For a **'client only' installation on Linux**, the **shortcut icons** are now placed in the correct folder so that they can be displayed correctly.

UMS Web App

Common

- Fixed: **Removed** unnecessary **certificate check for the subject alternative name on "localhost" for inter-service communication**.
- Fixed: **UMS Web App login fails** when **password contains paragraph character**.
- Changed: Upgraded **Node** to **version 18** and **Angular** to **version 15**.
- Changed: Closed an endpoint for unauthenticated users **exposing the UMS Web App version**.

Apps

- Fixed: **For communication with the App Portal** (e.g. for downloading apps), the **Proxy configuration** is **now taken into account**.
- Fixed: Changing the **Default Version of apps** will now **trigger the update on the device**.
- Fixed: A bug was present that caused **database issues if the categories delivered by the app portal only differed in terms of case-sensitivity**.
- Fixed: Apps will now use the **image from the latest version in the database**.
- Fixed: The **automatic update of the standard version** was not done after the **automatic app import** (if configured).
- Fixed**: App version usages** are now calculated correctly.
- Fixed: **Available versions showed wrong information** if the version is not standard conform.
- Changed: The **Installed Apps** will now show the **display version instead of the technical version**.

Configuration

- Fixed: **Not all base system versions** were **shown in the "Assign Object" dialog**.

Devices

- Fixed: **Devices with non-transferred changes will now be marked with an exclamation mark again**.
- Fixed: **Last Boot Time** was **not shown for OS12 devices**.

Misc.

- Changed: the **root directory is now expanded by default**.
- Added: **More tooltips**.
- **Changed**: Various **translations and labels for better understanding**.

Notes for Release IGEL UMS 12.01.110

Software:	Version 12.01.110
Release Date:	2023-04-18
Release Notes:	RN-1201110-1

Supported Environment UMS 12.01.110

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	
Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows 11	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Microsoft Windows Server 2022	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Ubuntu 20.04	(64 bit)	

Ubuntu 22.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	
Amazon Linux 2		

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 12c	(with Cluster Support)
PostgreSQL	9.6 and 10 - 13
Apache Derby	10.9 - 10.14
Amazon Aurora	Aurora PostgreSQL (compatible with PostgreSQL 10 - 13)

New Features UMS 12.01.110

Release 12.01.110

Unified Protocol

- Added: Additional field in **Advanced System Information** showing for **OS 12 devices to which device connector it is connected to**.
- Added: **OS 12 devices** are now **listed in the ICG connected devices** list.

Installer (Windows)

- Added: In **HA** server installations, the **UMS Console installation** is **optional**.

UMS Web App

Configuration

- Added: **Apps from external developers** can now be added to **profiles** and will be shown as **implicit assignments**.
- Changed: **Profiles for OS11 and OS12** will now be better distinguishable from each other **using different icons**.
- Changed: **Priority profiles for OS11 and OS12** will now be better distinguishable from each other **using different icons**.

Devices

- Added: For **OS12 devices**, a new **property** called "**Connected to**" was added, where the user now can see by which **device connector** the device reaches the UMS.

Misc

- Added: It is now possible to **generate a configuration for PXE-Boot** via the UMS Web App.

Release 12.01.100

UMS common

- Added: By default, **OS11 profiles are not regarded for OS12 devices and vice versa**.
- Added: **UMS cluster public address** for load distribution of specific device calls.
- Changed: The **logging file names** now follow a common schema. See `README.md` in the logs folder of the UMS Server.
- Updated: **Azul Zulu JRE** from version 8u345 to **8u352**.
- Updated: **Apache Tomcat** from version 8.5.82 to **8.5.84**.
- Changed: Updated **Spring Framework library** to the latest LTS version.

High Availability Feature

- Added: A message dialog is shown if an **HA installation** is recognized during an **upgrade installation**.

Profiles

- Changed: **Renamed "Master profiles" to "Priority profiles"**.
- Added: **Profiles based on the OS12 firmware** can only be created and changed in the UMS Web App. The **assignment** is still **possible in the UMS Console**.

Automatic License Deployment (ALD)

- Added: Now an **automatic license renewal, incl. product pack switch** if necessary, can be configured for **expiring device licenses** (**UMS Administration > Global Configuration > Licenses > Deployment**).
- Added: For Automatic License Deployment, **global distribution conditions** can be configured (**UMS Administration > Global Configuration > Licenses > Deployment**)
- Added: **Pack comments created on the IGEL License Portal** are shown at the registered packs overview and the details of a pack (**UMS Administration > Global Configuration > Licenses > Deployment**).
- Changed: **Hardware removal actions** are now also **logged** and are **shown in the 'Executed actions'** area like license deployment actions (**UMS Administration > Global Configuration > Licenses > Deployment**).
- Changed: **Automatic License Deployment can now deploy evaluation licenses to OS11 and OS12 devices.**

Configuration Dialog

- Removed: **Obsolete Log4j** version 1.2.17 from TCSetup.

Console, common

- Added: New **installer page** informing the user about the **removal of the MDM feature** during an update installation if devices are managed via MDM.
- Added: **Installed app** information section in device detail information area.
- Removed: **IGEL Mobile Device Management Essentials**.

Server, common

- Added: **Propagate change of UMS Server port** on next server start.

Console, administration section

- Changed: **Renamed "UMS Licensing ID" to "UMS ID"**, and the **node** was **moved** to **Global Configuration > UMS Administration > Global Configuration > UMS ID**.
- Changed: Item **'Cloud Gateway Options**' in the administration tree was **renamed to 'First-authentication keys'** and received a new icon (**UMS Administration > Global Configuration > First-authentication keys**).

Console, web start

- Added: **Warnings about Webstart no longer being supported** are displayed when starting UMS Console via Java Webstart and on the `start_rm.html` page.

Unified Protocol

- **Introduced new scalable, stateless, websocket-based communication protocol for OS12 devices**

    - Works with any enterprise load balancers (SSL passthrough and websocket support required)
    - Secured by client certificates
    - Communication over UMS Web Port
- Added: **Devices** are **now informed about new root certificates** to support the exchange of the web certificate chain.
- Added: **Payload compression** to reduce bandwidth in customer environment.
- Added: New **log file to log communication of device and the UMS**. Can be activated in `logback.xml`.
- Added: **UMS firmware customizations** can now **also** be **deployed to OS12 devices**.
- Added: Support for **unified protocol via IGEL Cloud Gateway** (ICG 12.01.100 or higher needed).

IGEL Cloud Gateway (ICG)

- Added: **ICG support for Debian 11** environment.

Administrator application

- Added: **Warning message** is shown when **OS12 devices would no longer be manageable after the change of web server port**.
- Added: New subcommand "`umsadmin-cli db show`" to **show all details of a data sourc**e.
- Added: **Admin CLI** prints more details upon unexpected errors.

Devices

- Added: If an **OS12 device is removed from the UMS**, it **can be specified whether the licenses should be deleted** on the device. In this case, also all registered licenses of the device are removed from the UMS and the Unit ID is removed from all registered product packs in the ILP.
- Added: Two options for the **device settings export**, to either **include all passwords or replace them with a placeholder**.

Views

- Added: New **view criterion for installed apps**.

AD / LDAP integration

- Added: It is not possible to display the **settings of OS12 devices for Shared Workplace users**.

Installer (Windows)

- Added: New **precondition check during update installation** will identify running UMS Servers in a **distributed environment** and warn about the possibility of data loss.
- Updated: Updated text of **End User License Agreement (EULA)**.

Installer (Linux)

- Added: New **precondition check during update installation** will identify running UMS Servers in a **distributed environment** and warn about the possibility of data loss.
- Updated: Updated text of **End User License Agreement (EULA)**.
- Added: New **configuration dialog for entering or confirming UMS Server IP address** in Linux installer.

UMS Web App

Configuration

- Added: **Profiles (and priority profiles) can** now **be opened and edited in the UMS Web App via** the **new configuration dialog**.
- Added: **Profiles (and priority profiles) can** now **be created within the UMS Web App**.
- Added: OS12 Support: **Profiles (and priority profiles) based on OS12** are now **fully supported within the UMS Web App**.
- Added: It is now **possible to change the "scope of an OS12 profile" (or priority profiles)** after its creation. (Apps can be added or removed).

Apps

- Added: Global **permission "App Management" (System > Administrator accounts > (select the administrator) > Edit > General - WebApp)**. Without this permission, an admin cannot import new apps, new versions of an app or configure the update stream.
- **Added: App section**: New section to import and manage apps, based on the needs of the customer.
- Added: **Default Version for apps**: It is now possible to set a certain version of an app as "Default Version", to mark it as production-ready.
- Added: Automatic Update Stream: It is now **possible to mark an app** in a way **that all upcoming versions are automatically imported into the UMS Web App**.
- Added: Automatic Update Stream: It is now **possible to mark an app** in a way **that all upcoming versions are automatically used as "Default Version"**.
- Added: It is now **possible to create a profile based on the "Default Version" of an app**. The profile will automatically follow the "Default Version", if updated.
- Added: It is now **possible to import apps, or new versions of an app** via cross-tab-communication with the App Portal.
- Added: The **EULA of an app** can now be **accepted via the UMS Web App**.
- Added: **UMS as an Update Proxy**: It is now possible to configure your **UMS network as a download source**, where your devices can download apps, including the new OS base system. (Defined as default)
- Added: **UMS as an Update Proxy**: It is now **possible to upload "private" apps into your UMS** system for distribution. This is currently meant for private builds or use cases where the UMS has no internet connection but will be expanded to company-specific apps.
- Added: Apps. It is now **possible to configure the capabilities of a device separately from the Base System** (firmware).

Devices

- Added: The **device configuration can** now be **opened and edited in the UMS Web App via the configuration dialog**.
- Added: **Apps can** now **be assigned** to a folder or a device **explicitly**. This is possible as "Default Version" or as a specific version of an app.
- Added: **If a profile is assigned** to a device (or a device folder) **that contains an app**, **the app will also be implicitly assigned to the device/folder**. This can be overwritten by an explicit assignment.
- Added: It is now possible to send **simple messages (plain text) to OS12 devices**.

- Added: **Demo state of a license** is shown in the license information.

Network

- Added: You can add an **"Alias" (or nickname) to your installation**. This will be shown in the header and in the browser tab. **The permission for "Server Network Settings" is needed** to change the value.

Settings

- Added: A new **overlay for NETWORK and APPS where settings, specific for each section, can be retrieved and edited.** This is planned for all sections.
- Added: **Apps > Settings > UMS as an Update Proxy** (see above). The **permission for "UMS Features" is needed**.
- Added: **Apps > Settings > App Portal** - It is now possible to specify the URL of the App Portal. **The permission for "Server Network Settings" is needed.**
- Added: **Apps > Settings > Automatic Updates** - It is now possible to tell the UMS network when to check for new updates of apps/base systems. **The permission for "Server Network Settings" is needed.**
- Added: **Network > Settings > IGEL OS Onboarding** - Routing information for onboarding (calculated – read-only)
- Added: **Network > Settings > IGEL OS Onboarding** - Download certificate chain of selected server as *.crt-file for onboarding. (PEM-format)

Misc

- Added: Icons got an overhaul to be able to improve the separation for "colors with meaning" (e.g. "Warning", "Error", "Offline", etc.) from "design".
- Added: First improvements for visually impaired users.
- Added: **Support for the IGEL Insight Service**.

Resolved Issues UMS 12.01.110

Release 12.01.110

Devices

- Fixed: Improved **performance** of **Advanced Health Status update**.

Universal Firmware Update

- Fixed: DB error **importing Honeywell OS Firmware Update** zip file in the UMS.

Console, common

- Changed: The behavior to **display a service license name** from always updating the name whenever a new device is registered to only updating the name when a device with newer firmware is registered.

Views

- Fixed: In the creation dialog of a view with the **criterion 'Installed Apps'**, **not all available app states** were shown.

Default Directory Rules

- Fixed: In the creation dialog of a **Default Directory Rule with the criterion 'Installed Apps', not all available app states** were shown.

Unified Protocol

- Fixed: **Pre-imported devices can** now also **be registered**.
- Changed: **Communication within the UMS Server** will now always **use 'localhost' instead of the configured UMS address**.

UMS Web App

Configuration

- Fixed: Deleting of a selected profile (in the UMS Console) could lead to an **endless spinner** in the **UMS Web App > Configuration**.

Apps

- Fixed: **Apps that do not have an EULA** will no longer show the "**warning icon**" for an unaccepted EULA.
- Fixed: **Versions of apps** will now always **correctly** be **compared (from oldest to newest)**.
- Changed: The **App Portal will be notified about all imported versions** – not only the ones with an accepted EULA.
- Changed: **Apps with malformed icons** will no longer lead to **broken user interfaces**.

Devices

- Fixed: Different **custom properties** with the same value will now be displayed correctly and are editable again.
- Fixed: **Commands sent to an OS12 endpoint** will now be logged via **unified logging**.

- Fixed: If **Elastic Search** was temporarily **unavailable**, the **list of devices** could **not** be **loaded**.
- Fixed: If **Elastic Search** was temporarily **unavailable**, the **list of assigned objects** could **not** be **loaded**.

Network

- Fixed: The sum of all connected devices of an **IGEL Cloud Gateway** will now correctly include OS12 devices.

Misc

- Changed: The page default (**how many objects are loaded**) was **changed to "100"**.

Release 12.01.100

UMS common

- Changed: Updated **driver for MS SQL Server datasources**.
- Fixed: **Failed device requests** were **not** always **counted** in the request statistics of the process.
- Fixed: The **automatic registration of devices** was not working.
- Changed: **Fallback for HTTPS requests** to the UMS Server is now the **last known IP**. Formerly, it was the host.
- Fixed: '**On-the-fly' changes of logging** during runtime works for all UMS components.
- Fixed: **Last boot-time** in GUI now shows the last boot-time stored in the database table of the device.
- Fixed: **Last boot-time** in the database table of device now contains correct boot-time.
- Fixed: Server **performance** dropped if **scanning for devices** ran into an error.
- Fixed: **Device import from CSV file via command line** didn't work anymore.

Console, common

- Fixed: **Save** icon was not enabled for devices if the user has the **access right to 'Edit System Information'**
- Fixed: The **number of deployed licenses** was **not shown correctly** when devices were licensed manually.
- Fixed: '**Save support information..' (Help -> Save support information...)** failed if ICG certificates in the used certificate chain have the same display name.
- Fixed: When the `shift` key was held while clicking 'Delete' in a devices context menu, the **device was not deleted directly but moved in the bin**.
- Fixed: Collection of the **console log files via 'Save Support Information...'** did not take the selected 'days back' into account **(Help -> Save Support Information...**).

Console, administration section

- Changed: **UMS Licensing ID** certificate files are now **exported with the ".crt" extension**.
- Changed: It is **no longer possible to create more than one first authentication key with the same password** (**UMS Administration > Global Configuration > First-authentication keys**).

IGEL Cloud Gateway (ICG)

- Fixed: **Primary key violation** occurred while processing connection status information of ICG-managed devices.

- Fixed: **ICG Gateways are not removed from the UMS** when installed on the same host with different ports

Server, common

- Fixed: **A device which is connected via ICG to the UMS** no longer receives settings and other messages once the TC Key has changed or is lost.
- Fixed: **Secure Terminal / Secure shadowing failed for devices connected over ICG** when the devices were configured to send **periodic heartbeat signal**.

Devices

- Fixed: Under certain circumstances, the **result dialog** was not shown **when a device was removed offline**.

Profiles

- Fixed: The **profile setting 'OpenVPN - Set Auto'** did not persist after copying or importing a profile, where the setting was enabled.

Device Service

- Fixed: The **configuration dialog of the UMS Web App** for profiles showed predefined firmware settings for OS11 devices in some cases.

Views

- Fixed: It was not possible to go back to the panel of the '**Installed Apps' criterion** after it was combined with another criterion in the view creation dialog.
- Fixed: The **auto-completion popup** was not displayed when 'in' was typed as the beginning of a criterion.
- Fixed: **Criteria** in views are **not** always **properly converted from Text Mode to Graphical Mode**.
- Fixed: **Syntax error visualization** (red squiggly underline) in View Queries were always displayed at unrelated text in the first line when entering multi-line queries.
- Fixed: **Error** occurred for views consisting of **several device license criteria combined with AND and OR**.

Installer (Windows)

- Fixed: **UMS Server now starts only if the DB exists**.
- Fixed: A **High Availability token file** was not created on the first HA installation when a path was provided for this file but did not exist.
- Fixed: The **version number in the Windows start menu program group is never updated on update installations** and has been stripped to conform to Windows guidelines.

Installer (Linux)

- Fixed: UMS Console and Administrator applications did not show **proper application name in Gnome Shell taskbar**
- Fixed: **UMS Server now starts only if the DB exists**.

Administrator application

- Fixed: **Enabling and disabling SSL-only connections via 'umsadmin-cli'** showed '-1' for the Java Webstart port when ports are listed afterwards.

- Fixed: **Copying an embedded database to any external type** (e.g. SQL, Postgre) **via Administrator CLI** was broken.

UMS Web App

Configuration

- Fixed: A bug was present that **showed values in profiles, which consist of an URL, incorrectly**.

Network

- Fixed: The **fingerprint of the certificate of a server** will now be shown correctly.
- Added: The **fingerprint of the root certificate of a server** will also be **shown, if known to the system**.

Devices

- Changed: The **area for command buttons** is now better used.
- Fixed: **Public address (if defined)** will now be used for **shadowing via the unified protocol**.
- Fixed: The **tooltip** for the disabled edit button for **custom properties** was not shown.
- Fixed: If the **certificate** is missing for a **shadow** session, the **UMS Web App will now be able to retrieve it automatically**.

Logging

- Fixed: Commands **"Reboot", "Shutdown" and "Suspend"** resulted in **missleading log message**s.

Misc

- Fixed: Certain errors resulted in **Stacktrace** being **shown to the end use**r.
- Fixed: **Name of devices/profiles/folders was not fully visible in the header** even if there was enough space.
- Changed: A **filter term with space in the beginning or end** produces the same result as without spaces.
- Changed: To give cleaner optics the **splitter is no longer visible, but will keep its function**.
- Changed: The **design of dialogs** was improved.
- Changed: **Some dialogs** can now be c**losed with the "X" icon and by hitting "Esc"**.

Limitations UMS 12.01.110

Check also the "Feature Matrix: UMS Web App vs. UMS Console" under Overview (see page 1614).

UMS Web App - Apps

- Quick assign (app section) is not working.
- If the App Portal window is opened from the UMS Web App, close it regularly, respectively if there was an “idle” time between app imports.
- When creating a profile, it is possible to select apps that do not have configurable parameters (e.g. Chromium Multimedia Codec, Citrix Multimedia Codec, etc.).

UMS / UMS Web App - Core Functionality and Extensions

- Shared Workplace is currently not supported for IGEL OS 12 devices.

UMS / UMS Web App - Device Management

- (Un)Installation of apps requires a reboot.
- Only the following commands are possible in the UMS Web App. You can send these commands to a device also via the UMS Console (also as a scheduled job):
  - Reboot
  - Shutdown
  - Suspend
  - Send settings
  - Receive settings
  - Refresh system information
  - Send Message (plain text only)
  - Reset to factory defaults
  - Update
    - 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 (see page 1614).
    - The update or rollout of OS 12 apps and the OS 12 base system cannot be scheduled by jobs. Only the activation of already deployed OS 12 apps and the OS 12 base systems can be scheduled by jobs.
- The secure terminal is available only via the UMS Console.
- The Asset Inventory Tracker is currently not supported for IGEL OS 12 devices.
- The UMS Console can only be used for:
  - Deleting profiles and clients; to open, edit, or create profiles for IGEL OS 12, the UMS Web App must be used.
  - Default directory rules
  - Admin account administration

    - Setting permissions on tree nodes
    - SQL console usage (also possible at UMS Administrator)
    - Starting the UMS Web App
- Import/export of OS 12 profiles is not possible.
- Copying of OS 12 profiles is not possible.

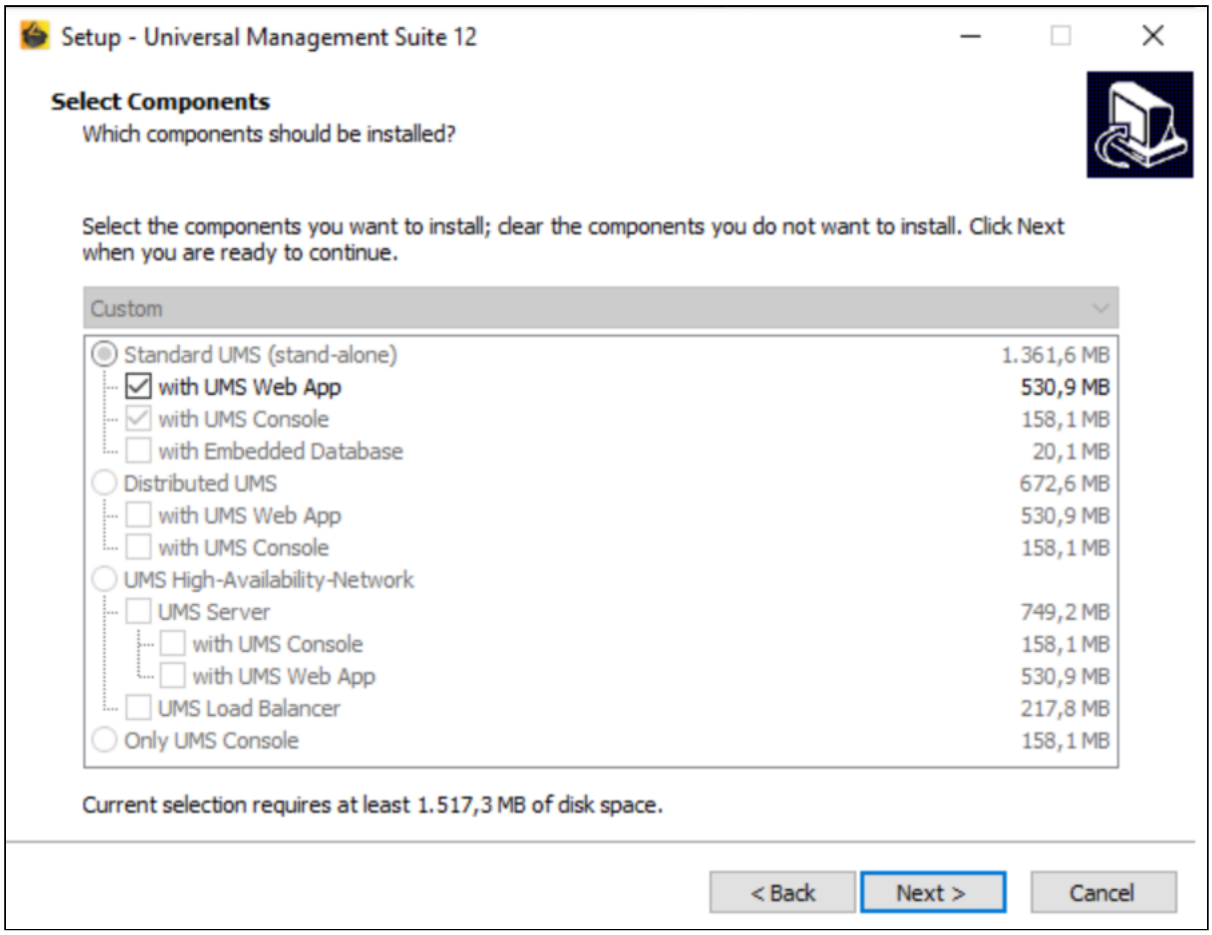
UMS Profiles

- OS 11 and OS 12 profiles are not compatible: OS 11 profiles should not be used for devices with OS 12, and OS 12 profiles should not be used for devices with OS 11.

Known Issues UMS 12.01.110

Upgrade of the Distributed UMS from 6.10 to 12.01.110: Distributed UMS mode deactivated (Windows only)

An upgrade installation from UMS 6.10 on Windows with the Distributed UMS feature enabled does not allow the user to select Distributed UMS during the upgrade procedure.



After the installation, the UMS is no longer configured as Distributed UMS.

Enabling Distributed UMS in the UMS Console (see page 1616) again will help, but a more permanent solution is as follows.

After the upgrade from 6.10 to 12.01.110, the Distributed UMS flag in the database will be lost and the file `rmguiserver/conf/dbsetup_options.properties` contains the lines:

```
configsettings.HA_DISTRIBUTED_MODE=false
already_read.HA_DISTRIBUTED_MODE=true
```

1. Stop the UMS Server.
2. Edit the file `rmguiserver/conf/dbsetup_options.properties` to contain the line

   ```
   configsettings.HA_DISTRIBUTED_MODE=true
   ```
3. Delete the line

   ```
   already_read.HA_DISTRIBUTED_MODE=true
   ```
4. Save the settings.
5. Start the UMS Server again.
   After the UMS Server finished its startup sequence, the file `rmguiserver/conf/dbsetup_options.properties` should now contain the lines:

   ```
   configsettings.HA_DISTRIBUTED_MODE=true
   already_read.HA_DISTRIBUTED_MODE=true
   ```
6. Repeat the above steps for each Distributed UMS Server.

UMS Proxy

- If you manage IGEL OS 12 devices, please do not use currently UMS proxys (**UMS Console > UMS Administration > Global Configuration > Proxy Server**) due to several issues. The fix is planned for the next UMS release.
  If you manage IGEL OS 11 devices only, UMS proxys can further be used without any limitations.

UMS as a Service

FAQ - IGEL Universal Management Suite as a Service (UMSaaS)

Introduction

This FAQ addresses key questions about the IGEL Universal Management Suite as a Service (UMSaaS), a cloud-hosted service of the IGEL UMS. UMSaaS enables scalable and secure endpoint management without requiring customer-owned infrastructure.

System Environment

- UMS Version**:** Configured, managed and maintained by IGEL (latest version provided)
- IGEL OS Version**:** 12 or higher recommended

- Devices can only connect to one UMS instance (either on-prem or cloud)
- Ideal for distributed environments or cloud-first IT strategies.

Eligibility & Availability

When Will UMSaaS Be Generally Available?

1st April 2025

What Are the Differences Between UMS On-Prem and UMSaaS?

With UMSaaS, IGEL hosts the UMS in the Cloud and controls configuration, updates, and maintenance. Customers concentrate on device and user management. See the table below that outlines responsibilities:

	UMS On-prem	UMS as a Service
Installation	Customer	IGEL
Hosting	Customer	IGEL
Configuration	Customer	IGEL
Maintenance	Customer	IGEL
UMS Releases Updates	Customer	IGEL
UMS Management	Customer	IGEL

	UMS On-prem	UMS as a Service
UMS User Management	Customer	Customer
User Profile Management	Customer	Customer
IGEL OS Endpoint Management	Customer	Customer

Who Is Eligible to Purchase UMSaaS?

At the start of the new service offering, IGEL offers UMSaaS to customers with 5000 seats or above, but also customers with fewer seats can buy the new service.

Security & Compliance

Is My Data Secure in the Cloud?

IGEL doesn't store any specific personal identifiable information (PII) customer data, just OS configuration data residing in the UMS database.

What Encryption Is Used?

Communications between UMSaaS and OS are encrypted with mTLS (TLS1.3).

Where Is the Data Stored? (Which Country/Region?)

IGEL partners with hyperscalers, like AWS and Microsoft. The data is stored in your chosen region. IGEL offers the ability to have multi region infrastructure.

Who Has Access to the Data?

All details can be found under https://www.igel.com/privacy-policy/

How Does the Cloud Security Compare to On-Premises?

UMSaaS is a generic installation of UMS, the only difference is the UMS version that will be in the cloud.

How Is Access Controlled?

Access to UMSaaS is managed and controlled by IGEL Cloud Specialists. Customers control access to UMSaaS through the IGEL UMS Web App, the IGEL UMS browser-based interface.

What About GDPR, HIPAA, SOC 2, ISO 27001?

IGEL is ISO 27001 certified. This includes UMSaaS.

Can You Provide Compliance Certifications?

IGEL is ISO/IEC 27001 certified; for further information, seehttps://www.igel.com/about-us/press-releases/igel-achieves-iso-iec-27001-certification-sets-new-standard-for-information-security/

What Happens If There Is a Breach?

The customers will receive an IGEL Security Notification (ISN).

Is the Data Backed Up?

All data is backed up in the Cloud daily. The ability to restore or retire data is available to customers, if required.

Cost & Pricing

How Much Will This Cost Compared to On-Prem?

IGEL will support you in evaluating your total cost of ownership. Please contact your IGEL sales representative for more information.

How Is Pricing Structured? (Subscription-Based, per User, per Device?)

UMSaaS SKUs are generally based on the number of seats.

Will I Save Money in the Long Run?

UMSaaS allows you to cut or reduce the costs of your own server hardware and software, as well as the corresponding IT maintenance.

What Are the Total Cost Savings (Hardware, Maintenance, Staffing)?

IGEL will support you in evaluating your total cost of ownership.

Are There Discounts for Volume or Long-Term Contracts?

Absolutely. All details and options are included in the IGEL pricebook.

Performance & Reliability

What Is Your Uptime Guarantee?

IGEL offers a 98.5 % uptime to all of its customers.

Is There a Service Level Agreement (SLA)?

Yes, an SLA is available. Please contact your IGEL sales representative for details.

How Do You Handle Outages?

The handling of outages follows a well-established major incident policy and process within IGEL. Our first priority is to restore services as quickly as possible. IGEL communicates any outages via the IGEL Cloud Serviceshttps://support.igel.com/csm and can provide root cause analysis reports per request.

How Fast Is the Cloud Service Compared to On-Prem?

Predicting the performance of cloud services versus on-premises infrastructure is difficult, as it depends on factors like use case, network latency, hardware, configuration, and workload type.

Are There Latency Issues?

IGEL has designed UMSaaS to be resilient using failover options (kept within the same regions) in order to offer little to no latency.

How Does Scaling Work?

IGEL administrators can adapt the service provision according to changing customer needs (i. e. additional seats).

Can I Easily Add/Remove Users?

You can add or remove users on your UMS Web App.

What Happens During High Traffic Loads?

On rare occasions, high traffic loads (high volume device connection to UMSaaS) will only impact the time needed for the endpoint to receive the configuration.

Integration & Migration

Will UMSaaS Integrate with My On-Prem Active Directory?

Yes.

Do You Offer APIs?

Yes, the IGEL Management Interface (IMI)[232] can be used to connect to UMSaaS.

232. https://kb.igel.com/en/igel-management-interface/current/imi-manual

Is Migration of Existing IGEL On-Prem Installations to UMSaaS Possible?

Yes, an automatic migration process is in development. For the time being, IGEL Customer Success specialists can support you in migrating from on-prem to the cloud environment.

How Long Does the Migration Take?

Configurations and profiles can easily be migrated with the help of IGEL Cloud Specialists, and only device re-registration is expected to take time.

Will There be Downtime?

On UMSaaS upgrades to newer versions and patching, usually expected to take between 15 - 20 minutes. Any administration downtime will be announced at least one week in advance. During downtimes, configuration changes cannot be done, but devices will continue to run with their latest configuration.

Is There Support for the Migration?

A QuickStart Package is part of the UMSaaS subscription, see IGEL-AS Standard QuickStart[233]

Is There a Cost for Migration Services?

Yes. Please contact your IGEL sales representative for more information.

Are There Different Editions of the UMSaaS?

At this point, no.

Will UMSaaS offer 2FA?

Yes.

Will UMSaaS offer SSO?

Yes.

Will UMSaaS Integrate with Third Party IdPs (like EntraID, Okta, Ping etc.)?

Yes, this is already offered as part of the IGEL OS 12 package and fully extends to UMSaaS.

233. https://www.igel.com/wp-content/uploads/2020/06/IGEL-AS_Standard_QuickStart.pdf

Data Ownerhip & Exit Strategy

Who Owns My Data Once It Is in the Cloud?

All details can be found under Privacy Policy | IGEL[234]

Can I Export My Data If I Decide to Leave?

Yes. Your data will be deleted 30 days after you quit the service. Details can be found in the UMSaaS customer agreement, see UMSaaS agreement[235].

What Happens If IGEL Shuts Down?

That is not likely to happen, but details on how such cases are governed can be found in the UMSaaS customer agreement, see UMSaaS agreement[236].

Does IGEL Have a Disaster Recovery Plan?

IGEL uses failover as a disaster recovery plan. Failovers switch to other regions when an issue is encountered in the existing hosting region. Failovers are automatic in the event that a region is unavailable. Failovers remain in specified regions/continents and do not failover outside of existing regions/continents.

Support & Maintenance

What Kind of Customer Support Do You Offer?

Available support packages can be found in the IGEL pricebook. Please contact your IGEL sales representative for more information.

Is 24/7 Support Available?

A 24/7 support option is available.

Is Support via Phone, Chat, Email Available?

Yes.

Who Handles Maintenance and Updates?

IGEL handles maintenance, updates, and configuration of the UMS as a Service.

234. https://www.igel.com/privacy-policy/
235. https://www.igel.com/wp-content/uploads/IGEL-UMSAAS-LICENSE-AGREEMENT.pdf
236. https://www.igel.com/wp-content/uploads/IGEL-UMSAAS-LICENSE-AGREEMENT.pdf

Is the Maintenance Automatic or Do I Need to Do Anything?

Maintenance is fully coordinated from IGEL.

Can Updates Break Our Integrations?

Cloud Specialists in close contact with our customers are ensuring compatibility to any specific requirements, before updates are rolled out.

Can I test the cloud service before fully migrating?

Yes.

Does IGEL Offer a Free Trial?

Proofs of concept can be arranged with IGEL.

Can I Run a Hybrid Model First (On-Prem + Cloud)?

If you want to operate an on-prem + cloud UMS environment: the devices can only be attached to one UMS, but a split of license between the on-prem and cloud UMS is possible.

Datasheet - IGEL Universal Management Suite as a Service (UMSaaS)

Cloud-hosted modern endpoint management. Always up to date. Always secure. Without the Overhead.

IGEL UMSaaS delivers the full power of the IGEL Universal Management Suite (UMS) as a cloud-hosted, fully managed service.
Hosted and operated by IGEL on leading hyperscalers, UMSaaS enables organizations to manage, configure, and secure IGEL OS endpoints—without maintaining on-prem infrastructure.

Ideal for cloud-first or distributed IT strategies, UMSaaS simplifies operations, ensures continuous updates, and provides enterprise-grade reliability and compliance.

Key Highlights

- Fully managed by IGEL: hosting, maintenance, patching, and updates included.
- Always current: latest UMS version automatically delivered.
- Secure by design: mTLS (TLS 1.3) for the communication between IGEL OS devices; HTTPS (TLS 1.2 & 1.3) for customers accessing the UMS Web App.
- Regional control: data hosted in your chosen region
- High reliability: 98.5 % uptime SLA with daily backups and automatic failover.
- Scalable: grow from pilot to tens of thousands of devices effortlessly.
- Compliance-ready: ISO 27001 certified hosting.

UMS On-Prem vs UMSaaS – At a Glance

Capability	**UMS (On-Prem)**	**UMSaaS (IGEL-Managed)**
Hosting & Infrastructure	Customer	IGEL
Configuration & Updates	Customer	IGEL
Maintenance & Patching	Customer	IGEL
User & Profile Management	Customer	Customer
Endpoint Management	Customer	Customer
Security & Backups	Customer	IGEL
Uptime SLA	N/A	9898.5% Uptime SLA. Availability typically exceeds 99.9% based on continuous performance monitoring across all hosting regions.
Licensing Model	Perpetual / Subscription	Subscription (per seat)

Is UMSaaS right for you?

UMSaaS is ideal for organizations that want to:

- Reduce infrastructure and operational costs.
- Manage remote or globally distributed endpoints.
- Move toward a secure, cloud-managed environment.
- Focus IT resources on users—not servers.

Architecture & Scalability

- Each customer operates in a dedicated, isolated tenant, ensuring full separation and data protection.
- Hosted on leading hyperscalers, with multi-region deployment options.
- Built-in failover within each region for business continuity.
- Designed to manage tens of thousands of endpoints with minimal latency.
- Access via the UMS Web App, offering the same management capabilities as on-prem UMS.

Integration & Migration

- Active Directory & SSO integration (supports Entra ID, Okta, Ping and others).
- APIs available via the IGEL Management Interface (IMI).
- Migration support:
    - IGEL Cloud Specialists assist with onboarding and migration.
    - Automated migration tooling under development.
    - Proof-of-concept environments available.

Data Security & Ownership

- Customers retain full ownership of all configuration and device data.
- Daily cloud backups with optional restore or data retirement.
- Data deleted 30 days after service termination.
- ISO/IEC 27001 certified hosting and processes.

Included IGEL Services

UMSaaS is delivered together with:

- Enterprise Plus TRM Service – dedicated Technical Relationship Manager (TRM) for proactive support and lifecycle guidance.
- QuickStart Enterprise Plus – expert-led onboarding ensuring a smooth deployment.

Getting Started

1. Contact IGEL Sales to assess your environment and subscription sizing.

2. QuickStart onboarding with IGEL Cloud Specialists.
3. Go live with your fully managed UMSaaS environment.

Learn More

- https://www.igel.com/blog/cloud-powered-endpoint-management-for-the-modern-enterprise/
- https://kb.igel.com/en/universal-management-suite/current/faq-igel-universal-management-suite-as-a-service-u?_gl=1*5lpck5*_gcl_au*MTczODg1ODIyOC4xNzU3NTAxMDI2&_ga=2.33004798.1718239713.1761043151-696533073.1741081745