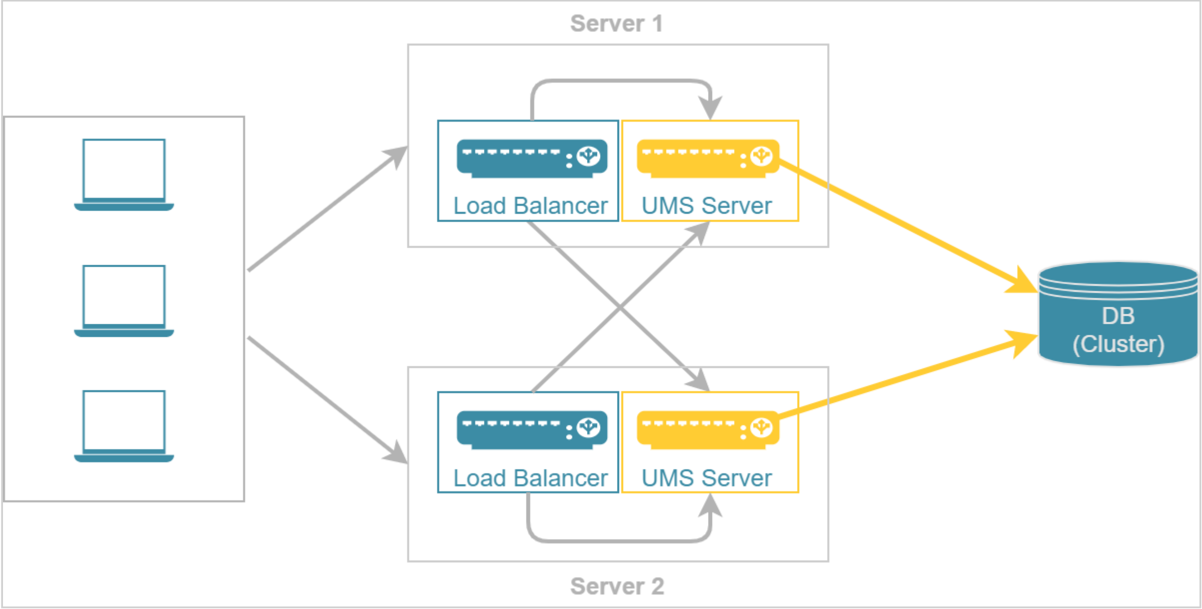
UMS Extensions

High Availability (HA)

The optional High Availability extension is part of the IGEL UMS. It is designed to address the needs of large environments in which new settings need to be rolled out at once, or in which the fail-safe rollout of new settings is mission-critical for the organization concerned. The technical implementation is based on a network of several UMS Servers.

An upstream UMS Load Balancer takes over the load distribution and thus ensures that each device can receive new settings at any time – even at the start of a working day when a large number of devices log in to the UMS Server simultaneously and request new configuration profiles or firmware updates. To ensure maximum process reliability and high availability, IGEL also recommends that the UMS Load Balancer and the database have a redundant design.

Example:



See also Configuration Options (see page 5).

Licensing with the IGEL OS 11 Licensing Model

The High Availability extension is included in the Workspace Edition, so that IGEL OS 11 devices can use a UMS High Availability network without an additional license.

See also the collection of articles High Availability.

Configuration Options

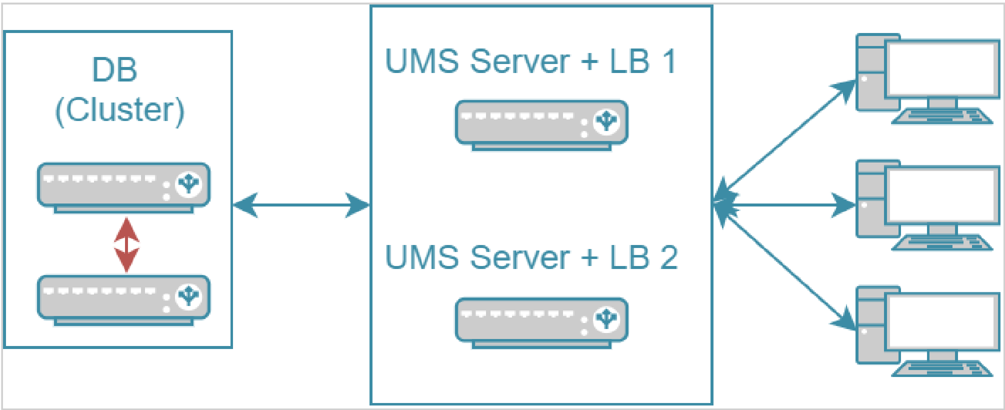
When planning the configuration of your High Availability (HA) network, you have to decide whether you want to install the UMS Server and UMS Load Balancer on the same host or on separate hosts. At the same time, there is a question how many UMS Servers and UMS Load Balancers are required. The following 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 Installation and Sizing Guidelines for IGEL UMS as well as IGEL UMS Sizing Guidelines & Architecture Diagrams 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 44) feature	2 UMS Servers 2 UMS Load Balancers

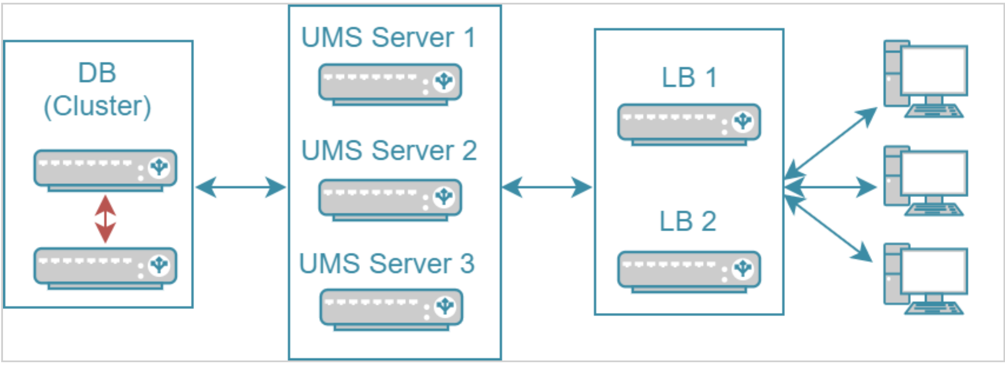


In this configuration, each of the two servers can also perform the tasks as a UMS Server alone. If both servers are active at the same time, this has a load-distributing effect. Note, however, that the load balancer generates extra load along with the actual UMS Server.

UMS Server & UMS Load Balancer are Installed on Separate Host Machines

If you need to manage a very large number of devices and/or do not want the server resources to be shared between the load balancer and the UMS Server, the installation on separate hosts should be considered.

Typical Use Cases	**#UMS Server Standalone & Load Balancer Standalone**
The installation of the load balancer on a separate host machine is • required if the number of devices > 50,000 • recommended if you do not want the load balancer to consume resources on the UMS Server host	Smallest typical configuration: 2-3 UMS Servers 2 UMS Load Balancers General sizing recommendations: • up to 6 UMS Servers • up to 3 UMS Load Balancers • 1 UMS Server per max. 50,000 devices • 1 LB per max. 3 UMS Servers

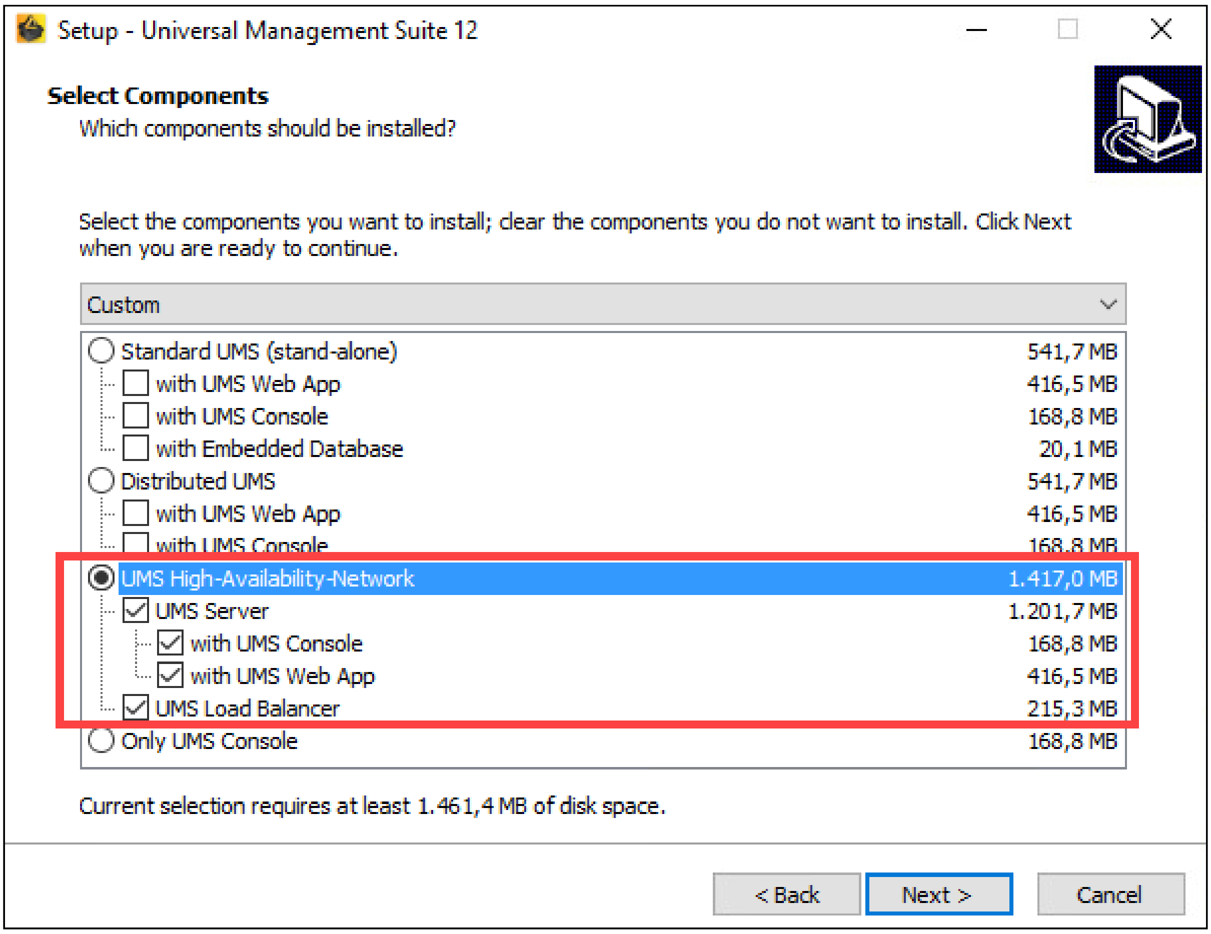


In the smallest typical configuration, queries from the devices are passed on to the UMS Servers by both load balancers. If one of the load balancers should fail, the other remains available and assumes responsibility for communications alone. A great number of UMS Servers could overload a single load 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.
Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the Distributed UMS) 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.



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom

○ Standard UMS (stand-alone)	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
□ with Embedded Database	20,1 MB
○ Distributed UMS	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
● UMS High-Availability-Network	1.417,0 MB
☑ UMS Server	1.201,7 MB
☑ with UMS Console	168,8 MB
☑ with UMS Web App	416,5 MB
☑ UMS Load Balancer	215,3 MB
○ Only UMS Console	168,8 MB

Current selection requires at least 1.461,4 MB of disk space.

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 8)
- Installing the First Server in an HA Network (see page 10)
- Adding Further Servers to the HA Network (see page 17)

For information on how to update the HA installation, see Updating the Installation of an HA Network (see page 24).

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.[1]			

> - 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**.

[1] http://www.igel.com/igel-ums-universal-management-suite/

For High Availability (UMS HA) with IGEL UMS Load Balancers, network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see IGEL UMS Communication Ports.
Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the Distributed UMS) 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.

Database Systems (DBMS)

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

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.
- A database system supported by the UMS; see the "Supported Environment" section of the release notes.
- All installation requirements described under HA: Installation Requirements (see page 8) are fulfilled.
- The current version of the UMS is downloaded from the IGEL Download Server[2].

> ⓘ 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 10)
2. Preparing the Servers (see page 10)
3. Starting the Installation (see page 11)
4. Defining the Database Connection (see page 14)
5. Checking the Installation (see page 15)
6. Saving the IGEL Network Token (see page 16)

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.

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

[2] https://www.igel.com/software-downloads/

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.

   > ⓘ 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.

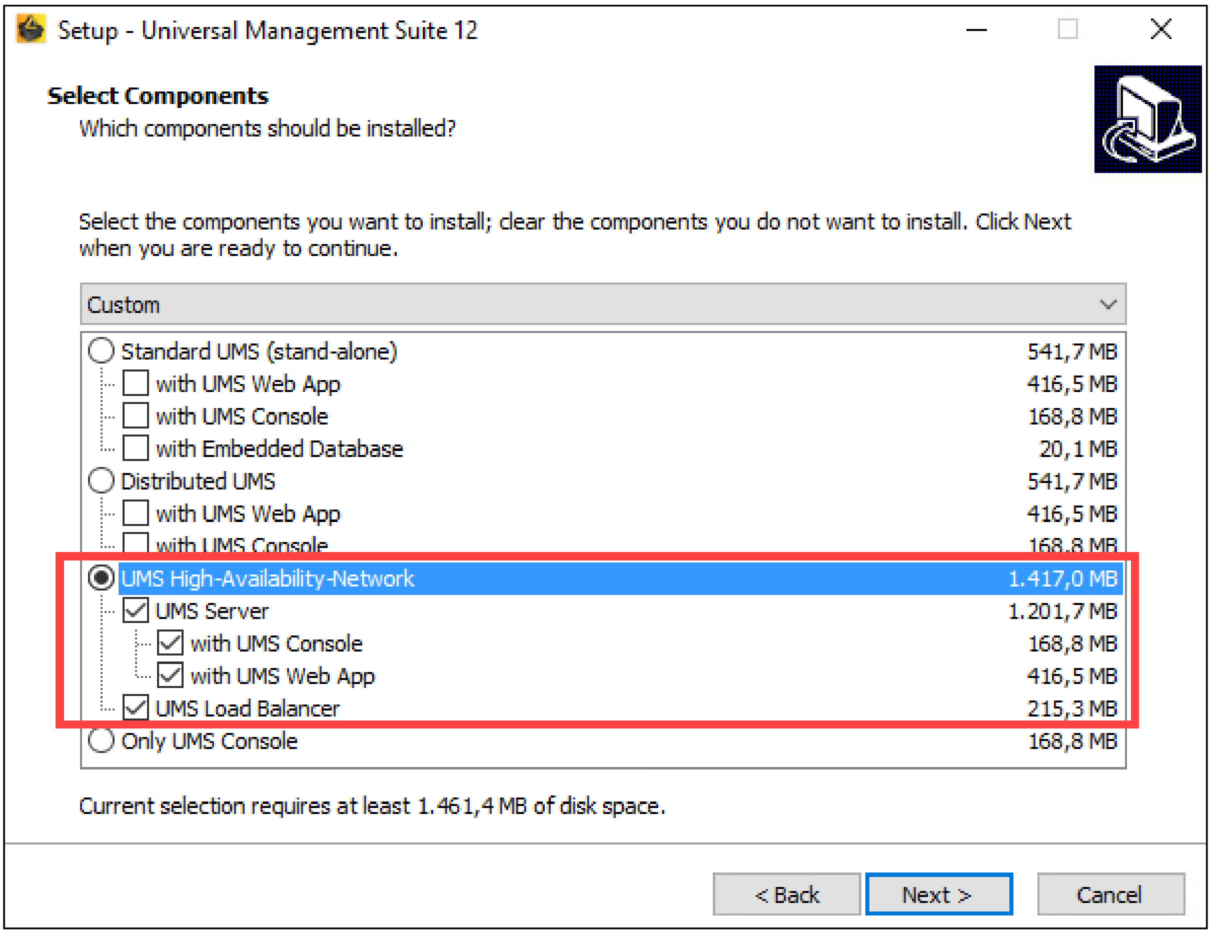
5. Depending on your desired HA network configuration (see page 5), select the components to be installed: **UMS Server + UMS Load Balancer** or **UMS Server**.

   > ⚠ **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.

   > ⓘ
   > - For the management of the UMS installation, you require the UMS Console. In multi-instance installations, the UMS Console does not necessarily have to be installed on every UMS Server.
   >   **Note**: For security, performance, or other reasons, the UMS Console is often additionally installed on a separate host.
   > - You cannot manage IGEL OS 12 devices without the UMS Web App. Thus, the UMS Web App must be selected during the installation of the UMS. In multi-instance installations, the UMS Web App does not necessarily have to be installed on every UMS Server, see Important Information for the IGEL UMS Web App.

- The UMS Administrator application, which is necessary for the management of the UMS installation, will be automatically installed during the installation of the UMS Server.

For information on the UMS components, see Overview of the IGEL UMS.



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

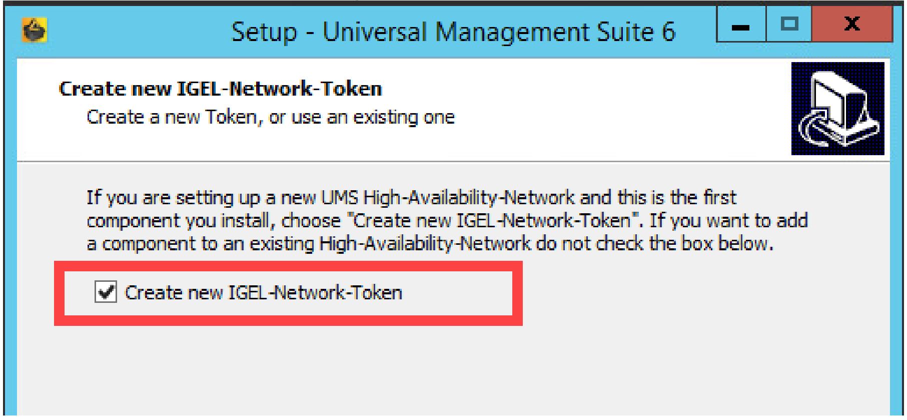
Custom

○ Standard UMS (stand-alone)	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
□ with Embedded Database	20,1 MB
○ Distributed UMS	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
● UMS High-Availability-Network	1.417,0 MB
☑ UMS Server	1.201,7 MB
☑ with UMS Console	168,8 MB
☑ with UMS Web App	416,5 MB
☑ UMS Load Balancer	215,3 MB
○ Only UMS Console	168,8 MB

Current selection requires at least 1.461,4 MB of disk space.

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.



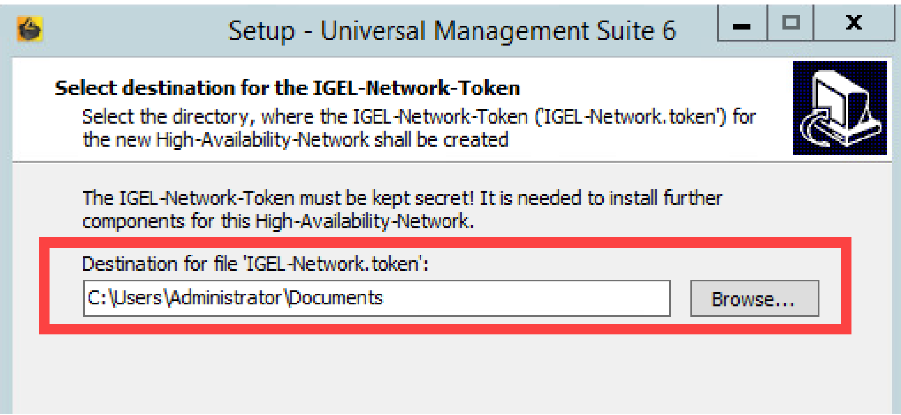
Create new IGEL-Network-Token
Create a new Token, or use an existing one

If you are setting up a new UMS High-Availability-Network and this is the first component you install, choose "Create new IGEL-Network-Token". If you want to add a component to an existing High-Availability-Network do not check the box below.

☑ Create new IGEL-Network-Token

9. Specify a directory for saving the IGEL network token. The directory must be writeable for the administrator.

> Be sure to keep the IGEL network token in a safe place! It will be needed for all subsequent server installations. If the IGEL network token is lost, the complete installation must be started again.



Select destination for the IGEL-Network-Token
Select the directory, where the IGEL-Network-Token ('IGEL-Network.token') for the new High-Availability-Network shall be created

The IGEL-Network-Token must be kept secret! It is needed to install further components for this High-Availability-Network.

Destination for file 'IGEL-Network.token':
C:\Users\Administrator\Documents

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.

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

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

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

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 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.

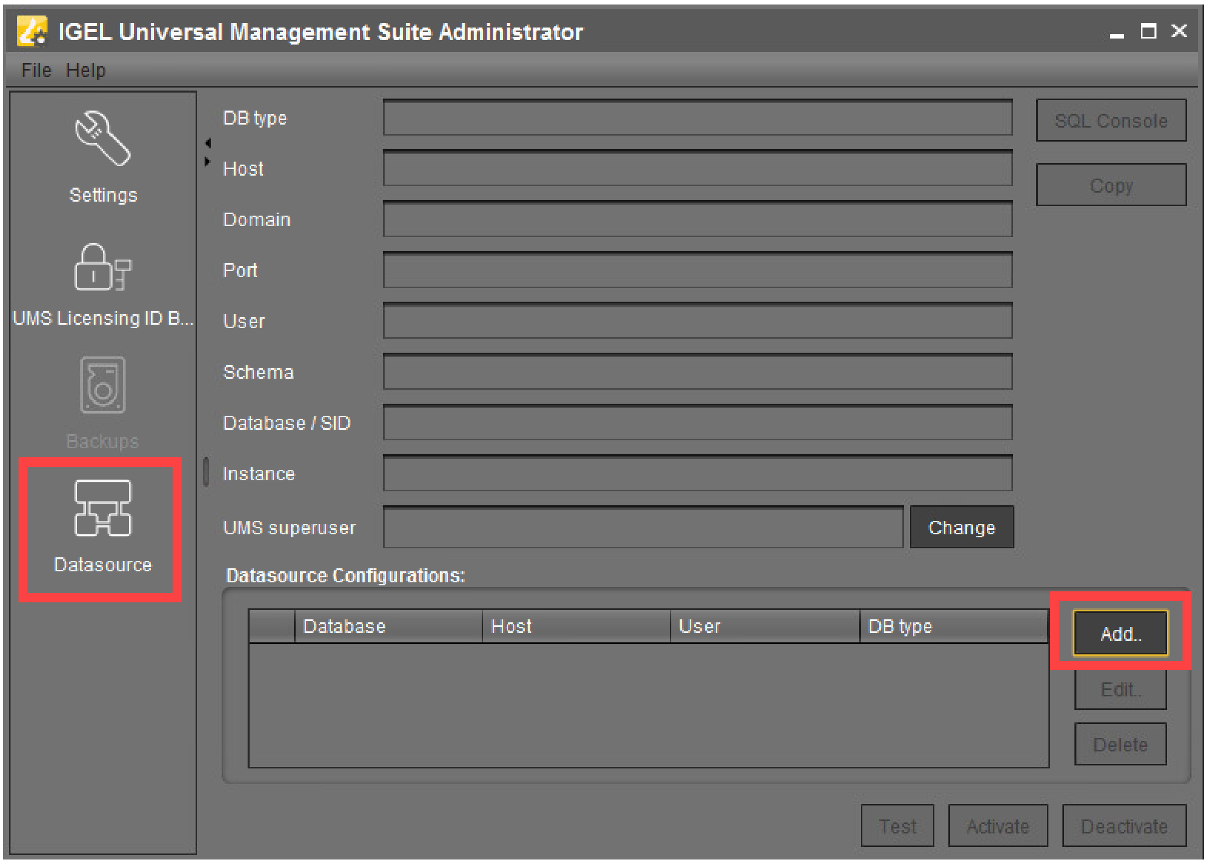
    ⓘ If SQL Server AD Native (see page 10) is used, you must also set the correct startup type and logon settings for the "IGEL RMGUIServer" service and restart the service. For details, see "Configuring the UMS Server Windows Service" under "Setting Up the UMS for SQL Server AD Native" (see page 10).

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**.



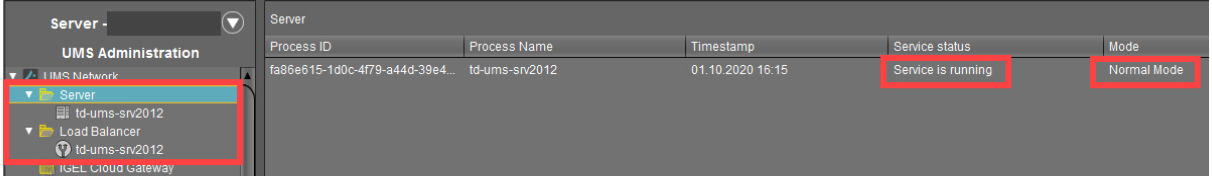
3. Enter the connection properties of the prepared database schema. See also How to Set Up a Data Source in the IGEL UMS Administrator.

4. Click **Activate** to enable the data source. See also Activating a Data Source.

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 42).

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.



Server

Process ID	Process Name	Timestamp	Service status	Mode
fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

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 17).

Adding Further Servers to the HA Network

Introduction

Further HA servers – with UMS Server, UMS Load Balancer, or both – can be installed in the same way as the first one. However, you do not need to create a new IGEL network token. Instead, you must select the network token created previously during the installation of the first server in an HA network.

In addition, a connection with the same database that is used by the first server must be established. The UMS HA network only works if all servers are connected to the same database.

Prerequisites

- A High Availability (HA) installation with a configured database, see Installing the First Server in an HA Network (see page 10).

  > ⚠ 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 11).
- A server with the operating system supported by the UMS; see the "Supported Environment" section of the release notes.
- All installation requirements described under HA: Installation Requirements (see page 8) are fulfilled.
- The same version of the UMS as for the first HA server is downloaded from the IGEL Download Server[3].

Instructions

To add a new server to the UMS HA installation, follow the instructions in the order given:

1. Preparing the Server (see page 17)
2. Preparing the IGEL Network Token (see page 18)
3. Starting the Installation (see page 18)
4. Checking the Installation (see page 21)

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**.

[3] https://www.igel.com/software-downloads/

For High Availability (UMS HA) with IGEL UMS Load Balancers, network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see IGEL UMS Communication Ports.
Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the Distributed UMS) 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.

ⓘ 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 42)) and use in this case the network token created upon the UMS Server startup from the directory:
Windows: `C:\Windows\System32\config\systemprofile\IGEL-Network.token`
Linux: `/root/IGEL-Network.token`

Starting the Installation

1. Launch the UMS installer.

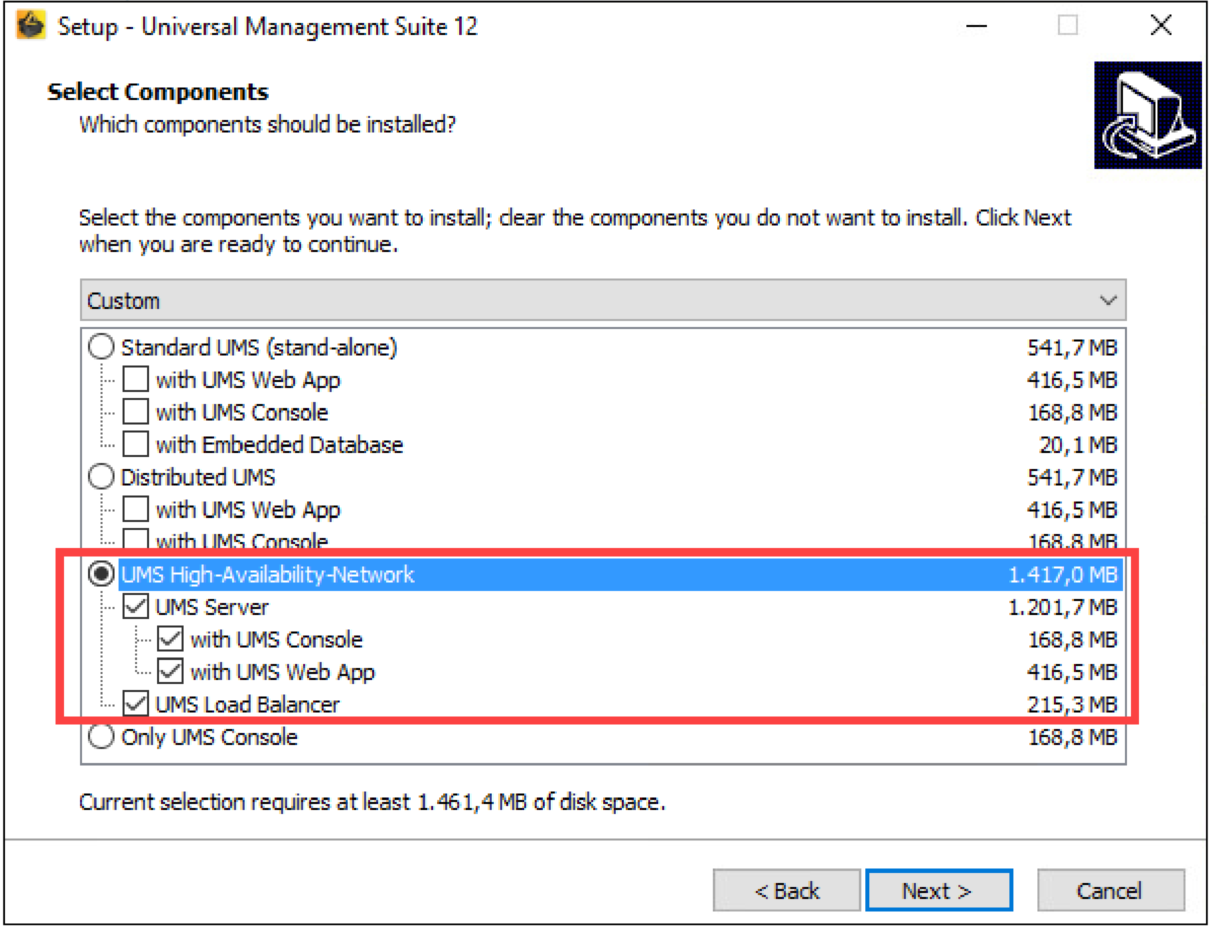
   ⓘ You need administration rights to install the IGEL UMS HA.

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

3. Read the **Information** regarding the installation process.

4. Select a path for the installation.

5. Select the components to be installed depending on your desired HA network configuration. See also Configuration Options (see page 5).



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom

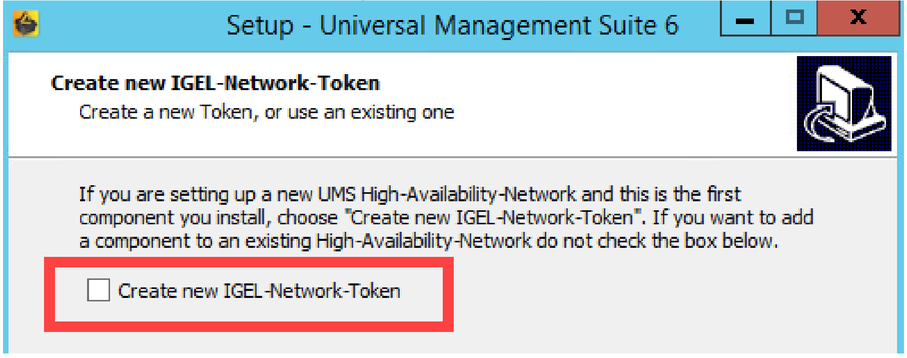
○ Standard UMS (stand-alone)	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
□ with Embedded Database	20,1 MB
○ Distributed UMS	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
● UMS High-Availability-Network	1.417,0 MB
☑ UMS Server	1.201,7 MB
☑ with UMS Console	168,8 MB
☑ with UMS Web App	416,5 MB
☑ UMS Load Balancer	215,3 MB
○ Only UMS Console	168,8 MB

Current selection requires at least 1.461,4 MB of disk space.

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.



Setup - Universal Management Suite 6

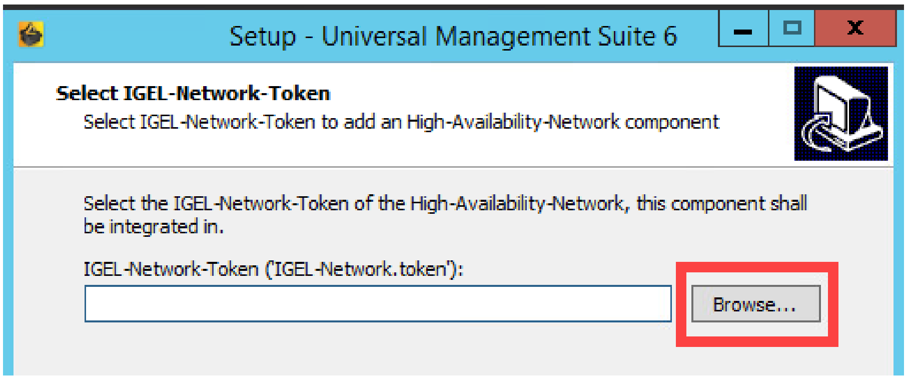
Create new IGEL-Network-Token

Create a new Token, or use an existing one

If you are setting up a new UMS High-Availability-Network and this is the first component you install, choose "Create new IGEL-Network-Token". If you want to add a component to an existing High-Availability-Network do not check the box below.

□ Create new IGEL-Network-Token

9. Select the IGEL network token to be used.



Setup - Universal Management Suite 6

Select IGEL-Network-Token

Select IGEL-Network-Token to add an High-Availability-Network component

Select the IGEL-Network-Token of the High-Availability-Network, this component shall be integrated in.

IGEL-Network-Token ('IGEL-Network.token'):

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

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

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 (see page 17) 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 details, see "Configuring the UMS Server Windows Service" under "Setting Up the UMS for SQL Server AD Native" (see page 17).

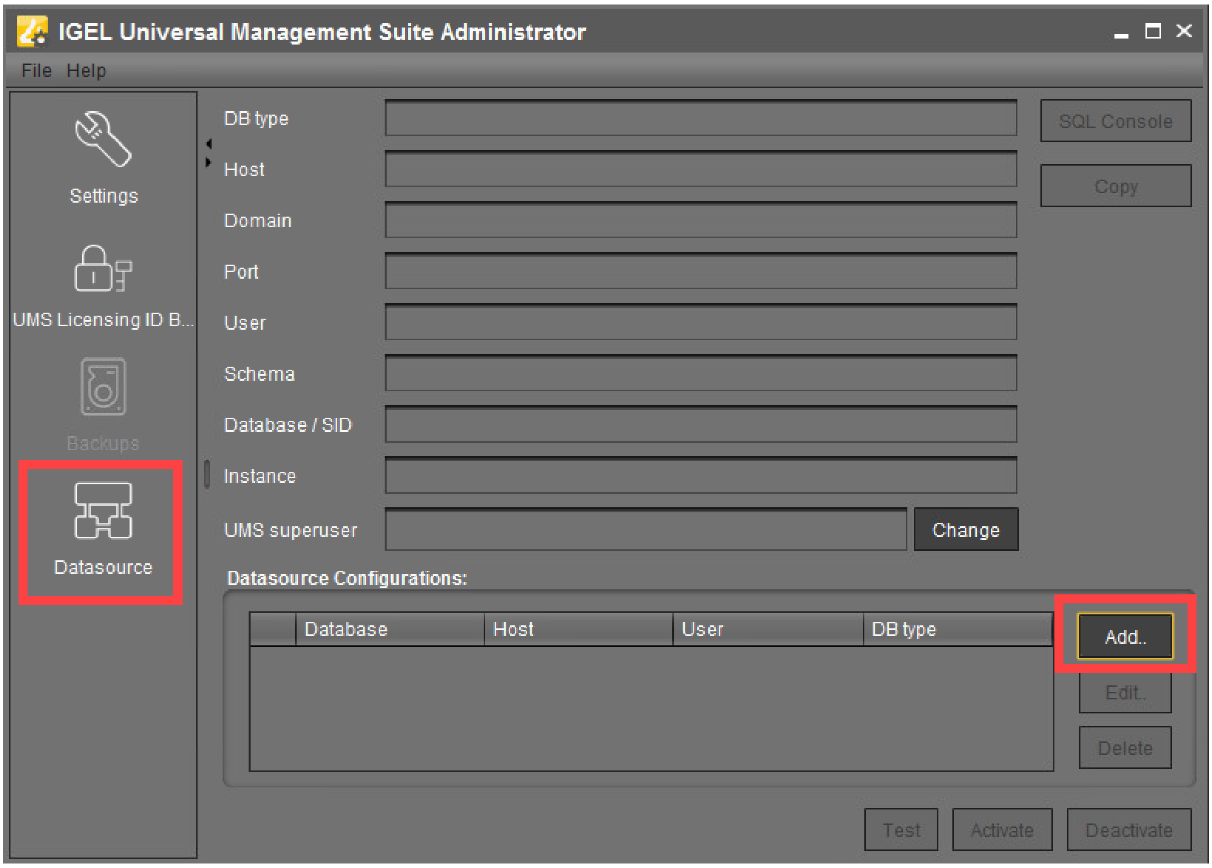
Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 42).

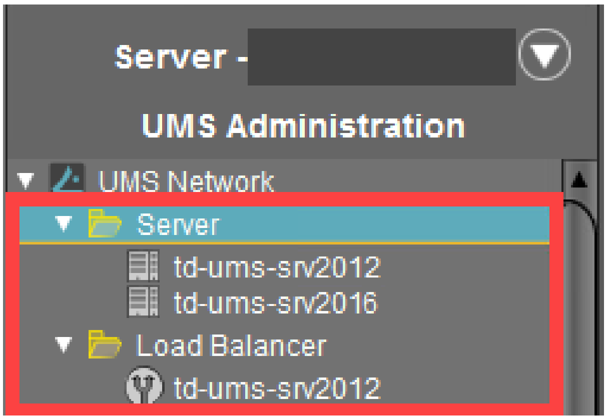
2. If you have included a UMS Server in the installation, open **UMS Administrator > Datasource** and verify that the database connection has been successfully transferred from the already running UMS Server.

   > ⓘ 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 14) 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 37).

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

For the future, you may also find it useful to read: Creating a Backup of the IGEL UMS and Which Files Are Automatically Synchronized between the IGEL UMS Servers?.

Updating the Installation of an HA Network

Use Case

You have a UMS High Availability (HA) (see page 3) installation and need to update it.

General Overview

There are two possible HA update procedures:

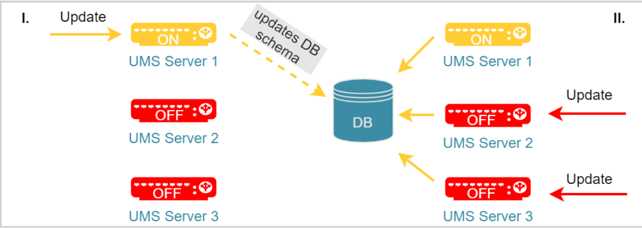
- With short downtime of the servers (see page 24)(recommended)
- Without downtime of the servers, but with automatic copying the productive database to a temporary database (see page 25), which generally results in longer update time

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 Updating HA Installation: With Downtime of the Servers (see page 26).



IGEL recommends using this HA update method due to a number of advantages:

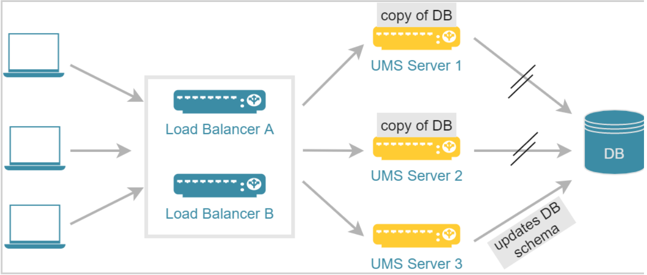
- The update procedure is much faster.
- No database inconsistencies since no other servers and processes use the database during the update.

- 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 Updating HA Installation: Without Downtime of the Servers (see page 31).

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.

- Updating HA Installation: With Downtime of the Servers (see page 26)
- Updating HA Installation: Without Downtime of the Servers (see page 31)

Updating 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 24).

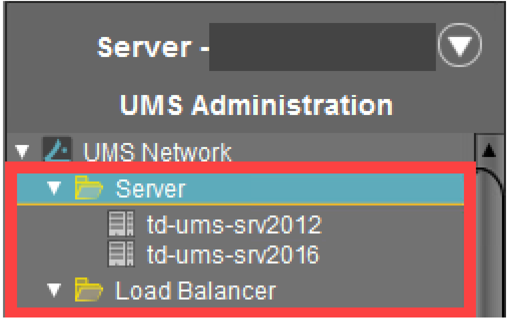
To update the HA installation, follow these instructions in the order given.

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[4]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.

> **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.

[4] 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

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 42).
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.

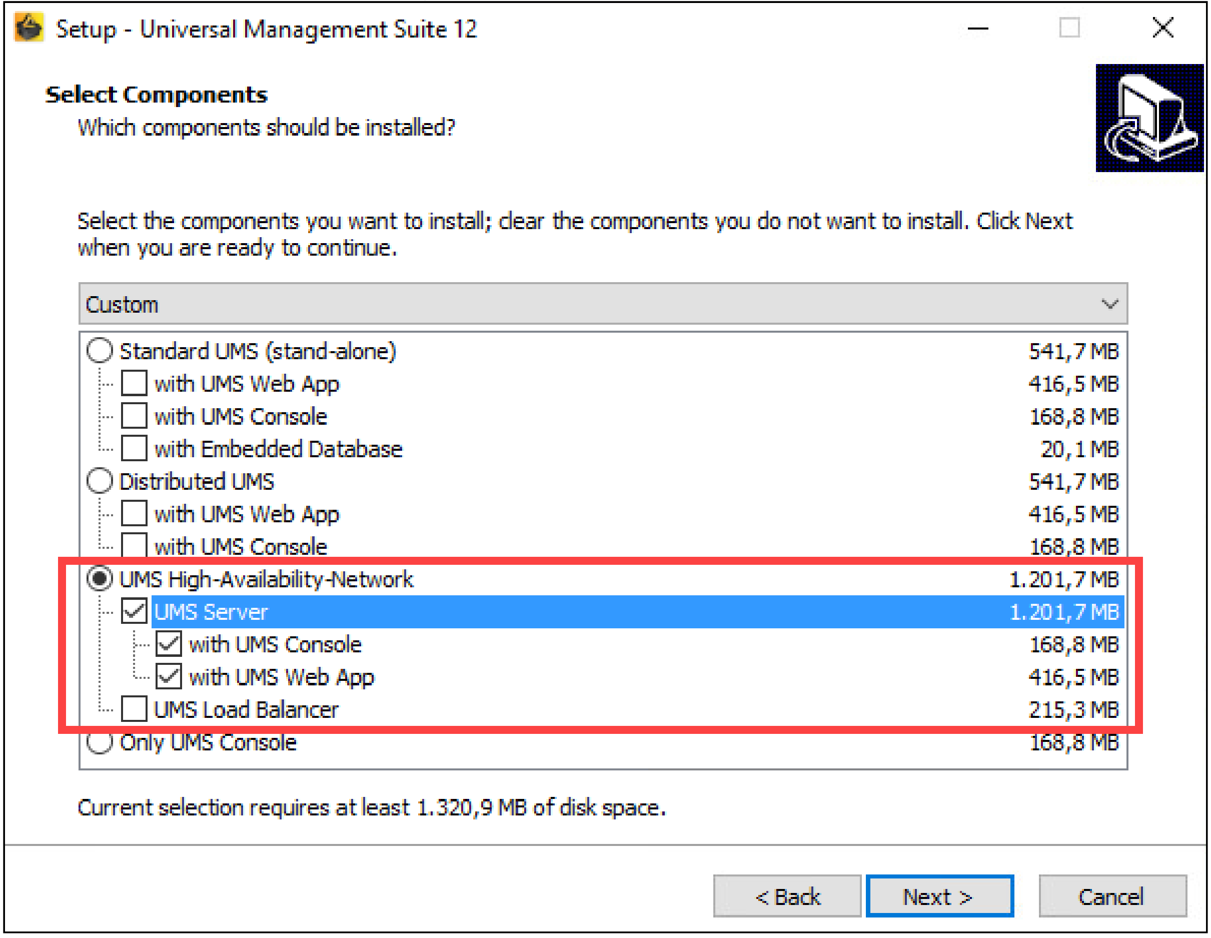
> ⓘ You need administration rights to update the IGEL UMS HA.

> ⚠ 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)



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom

○ Standard UMS (stand-alone)	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
□ with Embedded Database	20,1 MB
○ Distributed UMS	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
● UMS High-Availability-Network	1.201,7 MB
☑ UMS Server	1.201,7 MB
☑ with UMS Console	168,8 MB
☑ with UMS Web App	416,5 MB
□ UMS Load Balancer	215,3 MB
○ Only UMS Console	168,8 MB

Current selection requires at least 1.320,9 MB of disk space.

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.

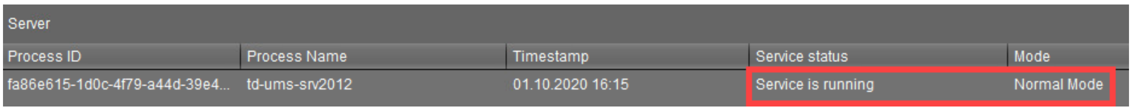
   > ⓘ **UMS 12 Communication Ports**
   > If you are going to make network changes, consider the following ports and paths:
   > - For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
   >   SSL can be terminated at the reverse proxy / external load balancer (see IGEL UMS Configuration for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

10. Read the summary and start the installation process.

11. Close the UMS installer once the installation is complete.
    The UMS Server will start and update the database.

    > ⓘ If SQL Server AD Native (see page 26) 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 details, see "Configuring the UMS Server Windows Service" under "Setting Up the UMS for SQL Server AD Native" (see page 26).

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



Server

Process ID	Process Name	Timestamp	Service status	Mode
fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	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.

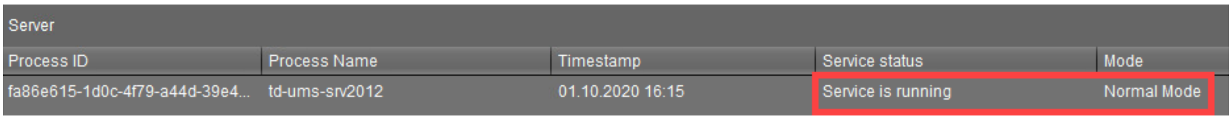
> Load balancers are able to interoperate with UMS Servers of newer versions, but they should have the same version as the UMS Servers for optimal performance.

See also Load Balancer Is Not Stopping during the Update of the HA Installation.

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 42).

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



Server

Process ID	Process Name	Timestamp	Service status	Mode
fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

Updating HA Installation: Without Downtime of the Servers

Before the update, see Updating the Installation of an HA Network (see page 24).

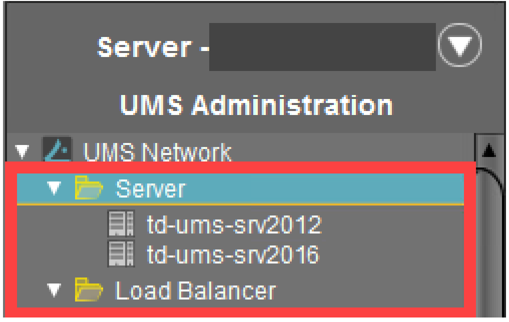
To update the HA installation, follow these instructions in the order given.

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[5]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.

> **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.

[5] 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

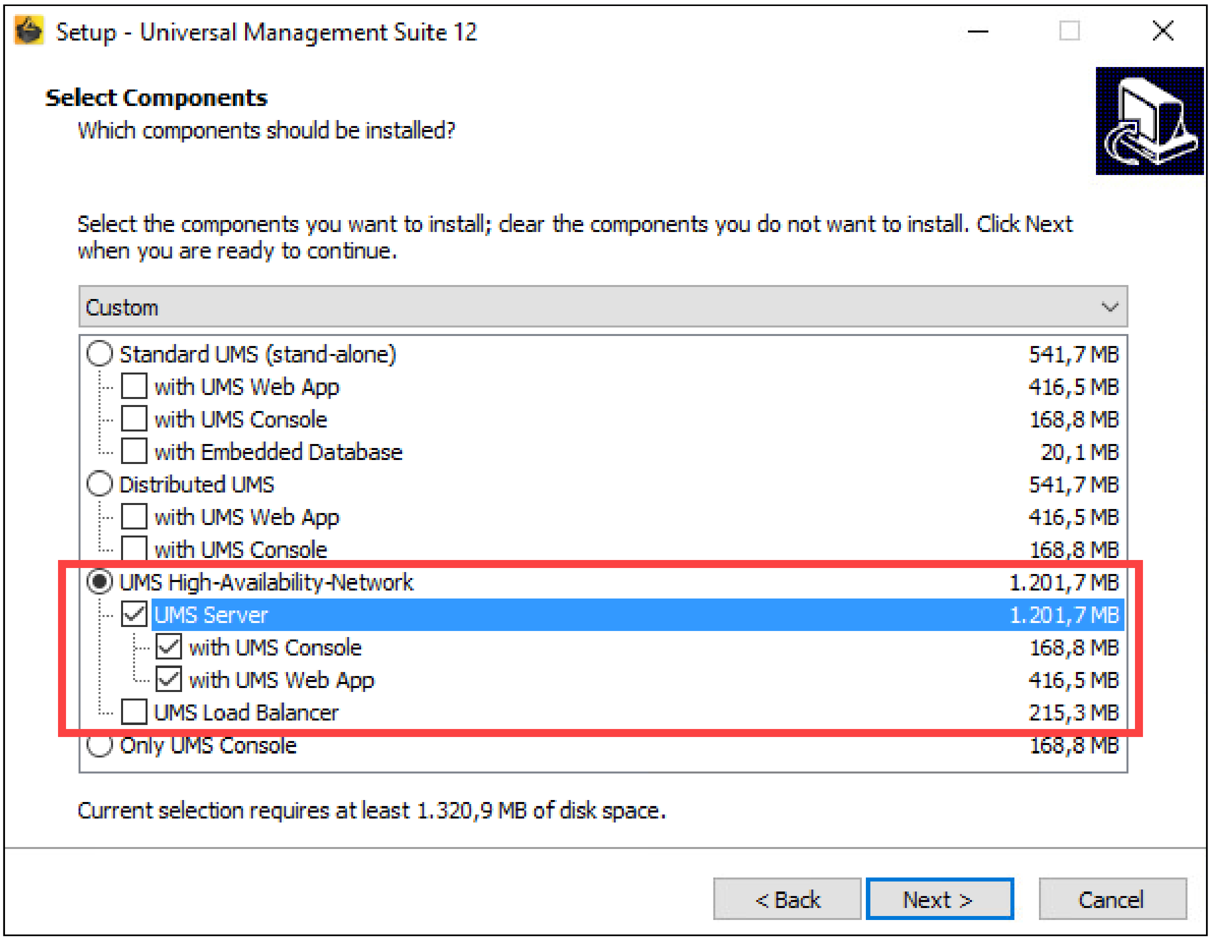
You can select any UMS Server within the HA network to start the update procedure.

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)



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Custom

○ Standard UMS (stand-alone)	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
□ with Embedded Database	20,1 MB
○ Distributed UMS	541,7 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	168,8 MB
● UMS High-Availability-Network	1.201,7 MB
☑ UMS Server	1.201,7 MB
☑ with UMS Console	168,8 MB
☑ with UMS Web App	416,5 MB
□ UMS Load Balancer	215,3 MB
○ Only UMS Console	168,8 MB

Current selection requires at least 1.320,9 MB of disk space.

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:

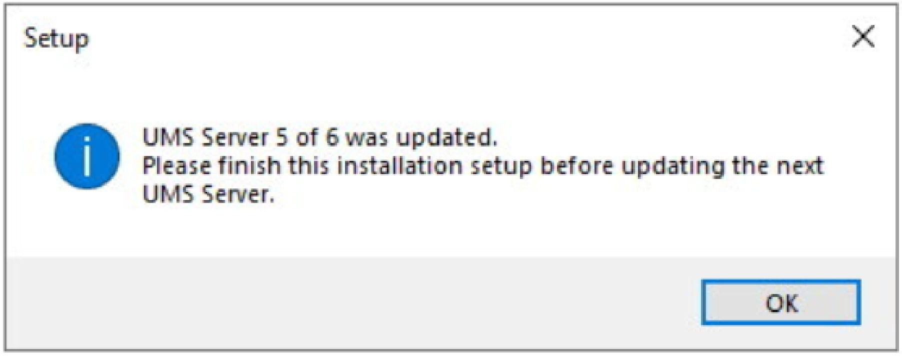
- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
  SSL can be terminated at the reverse proxy / external load balancer (see IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) or at the UMS Server.
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL https://app.igel.com/ (TCP 443) is required.

- For the UMS Web App, TCP 8443 `/webapp/*` and `/wums-app/*` are required.
- For the UMS Console, the root is required, i.e. TCP 8443 `/*`
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

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

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:



Setup

UMS Server 5 of 6 was updated.
Please finish this installation setup before updating the next UMS Server.

10. Close the UMS installer once the installation is complete.

> ⓘ If SQL Server AD Native (see page 31) 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 details, see "Configuring the UMS Server Windows Service" under "Setting Up the UMS for SQL Server AD Native" (see page 31).

11. Continue with the update of the next UMS Server.

Updating the Last UMS Server

▶ Repeat steps 1-9 (see page 32) 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 Load Balancer Is Not Stopping during the Update of the HA Installation.

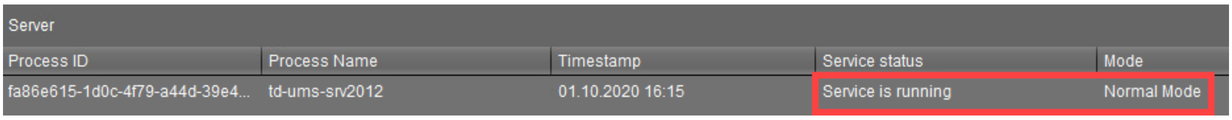
Checking the Installation

1. Check if all processes are running. For the list of UMS HA processes, see IGEL UMS HA Services and Processes (see page 42).

2. In the UMS Administrator, 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 31), 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**.
   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



Server

Process ID	Process Name	Timestamp	Service status	Mode
fa86e615-1d0c-4f79-a44d-39e4...	td-ums-srv2012	01.10.2020 16:15	Service is running	Normal Mode

Licensing the High Availability Extension

IGEL OS 11 and Higher

The IGEL UMS High Availability Extension no longer requires an additional license.

Before IGEL OS 11

The High Availability Extension comes in packages of 50 licenses. These licenses are installed in the UMS. The UMS checks if the number of licenses is at least as high as the number of devices connected to the UMS.

Each version of the IGEL UMS contains five test licenses allowing you to evaluate the function free of charge and without having to register.

▶ Register the license file you receive in the UMS Console under **UMS Administration > Global Configuration > Licenses > UMS Licenses**.

> ⓘ An HA network only works with a license covering all managed devices registered in the UMS. A mixed mode (devices with HA support and devices without HA support) is not possible.

UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems

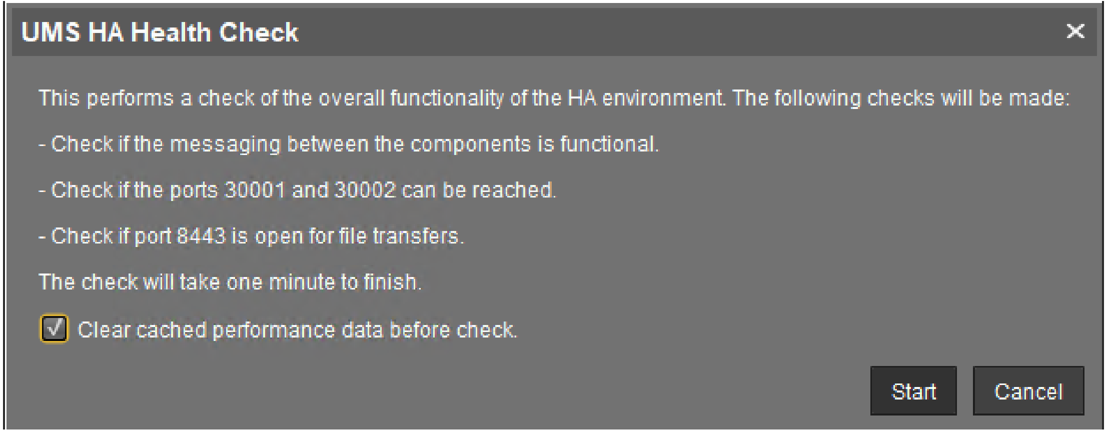
With the **UMS HA Health Check**, you can perform an overall check of your multi-instance IGEL Universal Management Suite (UMS) installations. It checks whether the interaction between the components of the High Availability (HA) system or the Distributed UMS is working properly, in particular, whether 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.

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.



UMS HA Health Check

This performs a check of the overall functionality of the HA environment. The following checks will be made:

- Check if the messaging between the components is functional.

- Check if the ports 30001 and 30002 can be reached.

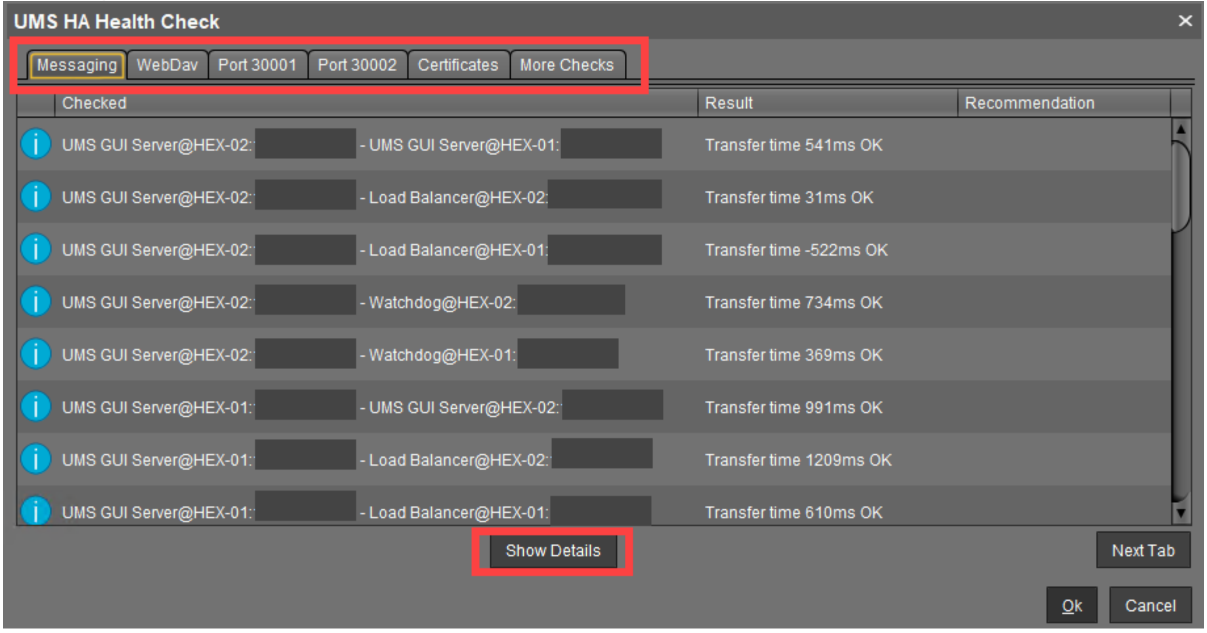
- Check if port 8443 is open for file transfers.

The check will take one minute to finish.

☑ Clear cached performance data before check.

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.



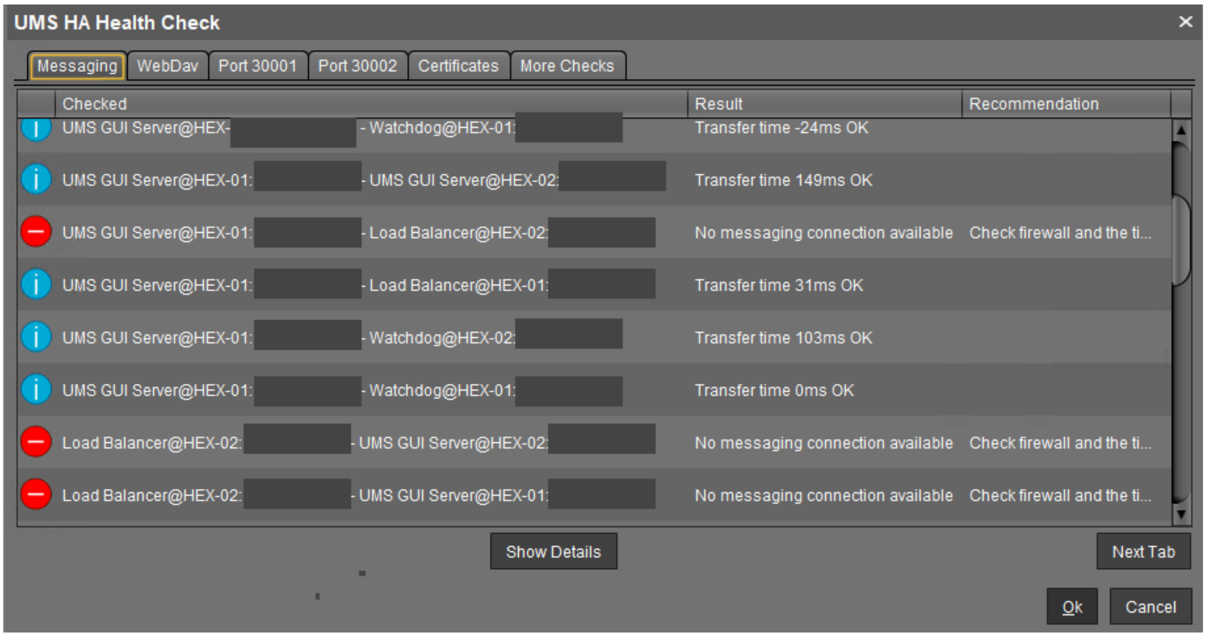
Checked	Result	Recommendation
UMS GUI Server@HEX-02:[redacted] - UMS GUI Server@HEX-01:[redacted]	Transfer time 541ms OK	
UMS GUI Server@HEX-02:[redacted] - Load Balancer@HEX-02:[redacted]	Transfer time 31ms OK	
UMS GUI Server@HEX-02:[redacted] - Load Balancer@HEX-01:[redacted]	Transfer time -522ms OK	
UMS GUI Server@HEX-02:[redacted] - Watchdog@HEX-02:[redacted]	Transfer time 734ms OK	
UMS GUI Server@HEX-02:[redacted] - Watchdog@HEX-01:[redacted]	Transfer time 369ms OK	
UMS GUI Server@HEX-01:[redacted] - UMS GUI Server@HEX-02:[redacted]	Transfer time 991ms OK	
UMS GUI Server@HEX-01:[redacted] - Load Balancer@HEX-02:[redacted]	Transfer time 1209ms OK	
UMS GUI Server@HEX-01:[redacted] - Load Balancer@HEX-01:[redacted]	Transfer time 610ms OK	

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



Checked	Result	Recommendation
ⓘ UMS GUI Server@HEX- [redacted] - Watchdog@HEX-01: [redacted]	Transfer time -24ms OK	
ⓘ UMS GUI Server@HEX-01: [redacted] - UMS GUI Server@HEX-02: [redacted]	Transfer time 149ms OK	
⛔ UMS GUI Server@HEX-01: [redacted] - Load Balancer@HEX-02: [redacted]	No messaging connection available	Check firewall and the ti...
ⓘ UMS GUI Server@HEX-01: [redacted] - Load Balancer@HEX-01: [redacted]	Transfer time 31ms OK	
ⓘ UMS GUI Server@HEX-01: [redacted] - Watchdog@HEX-02: [redacted]	Transfer time 103ms OK	
ⓘ UMS GUI Server@HEX-01: [redacted] - Watchdog@HEX-01: [redacted]	Transfer time 0ms OK	
⛔ Load Balancer@HEX-02: [redacted] - UMS GUI Server@HEX-02: [redacted]	No messaging connection available	Check firewall and the ti...
⛔ Load Balancer@HEX-02: [redacted] - UMS GUI Server@HEX-01: [redacted]	No messaging connection available	Check firewall and the ti...

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.
- 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?.

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 39)".

More Checks

If other problems are detected, the corresponding results and recommendations are displayed here.

Detailed Report

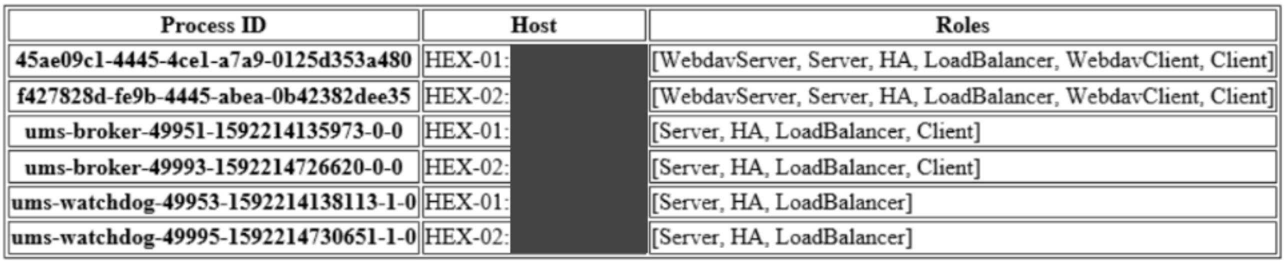
A detailed report generated in HTML format upon the click on the **Show Details** button provides some additional information.

✓ **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:[redacted]	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
f427828d-fe9b-4445-abea-0b42382dee35	HEX-02:[redacted]	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
ums-broker-49951-1592214135973-0-0	HEX-01:[redacted]	[Server, HA, LoadBalancer, Client]
ums-broker-49993-1592214726620-0-0	HEX-02:[redacted]	[Server, HA, LoadBalancer, Client]
ums-watchdog-49953-1592214138113-1-0	HEX-01:[redacted]	[Server, HA, LoadBalancer]
ums-watchdog-49995-1592214730651-1-0	HEX-02:[redacted]	[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 Configuration Options (see page 5). In addition, the UMS Watchdog always runs on each node.

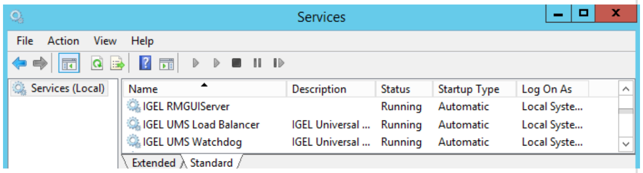
UMS Server	• Handles all requests from the devices and the UMS Console. • Talks to the devices. • Executes jobs. • Acts as a message broker for internal messages.
UMS Load Balancer	• Forwards incoming requests from the devices to one of the UMS Servers with load balancing. The UMS Load Balancer has a 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.

The following table shows how you can find out which processes are running and how/where you can stop or start them.

<table>
<tr><th>Windows</th><th>Linux</th></tr>
<tr><td>

Services:



Services

<table>
<tr><th>Name</th><th>Description</th><th>Status</th><th>Startup Type</th><th>Log On As</th></tr>
<tr><td>IGEL RMGUIServer</td><td></td><td>Running</td><td>Automatic</td><td>Local Syste...</td></tr>
<tr><td>IGEL UMS Load Balancer</td><td>IGEL Universal ...</td><td>Running</td><td>Automatic</td><td>Local Syste...</td></tr>
<tr><td>IGEL UMS Watchdog</td><td>IGEL Universal ...</td><td>Running</td><td>Automatic</td><td>Local Syste...</td></tr>
</table>

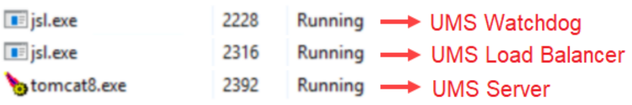
The processes are normally stopped here.

</td><td rowspan="3">

- 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`

</td></tr>
<tr><td>

Task Manager:



<table>
<tr><td>jsl.exe</td><td>2228</td><td>Running</td><td>→ UMS Watchdog</td></tr>
<tr><td>jsl.exe</td><td>2316</td><td>Running</td><td>→ UMS Load Balancer</td></tr>
<tr><td>tomcat8.exe</td><td>2392</td><td>Running</td><td>→ UMS Server</td></tr>
</table>

Emergency stop if the process cannot be stopped in the **Services**.

</td></tr>
<tr><td>

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”`

</td></tr>
<tr><td colspan="2">

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.

</td></tr>
</table>

Shared Workplace (SWP)

IGEL Shared Workplace (SWP) allows user-dependent configuration using profiles created in the IGEL Universal Management Suite and linked to the AD user accounts. In the process, user-specific profile settings are passed on to the device along with the device-dependent parameters. You will find an overview of the parameters that can be individually configured for a user u (see page 52)nder Parameters Configurable in the User Profile (see page 52).

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 3). 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 46)
- Parameters Configurable in the User Profile (see page 52)
- Display Configuration for Shared Workplace (SWP) (see page 55)

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 3) 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 55).

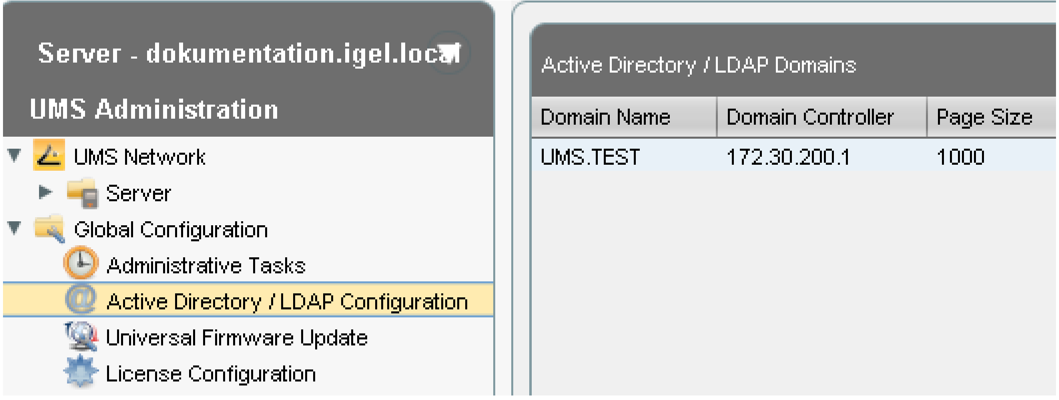
In this chapter, you can learn about:

The priority of user-specific profiles is dealt with in Order of Effectiveness of Profiles in IGEL Shared Workplace. See also Order of Effectiveness of Profiles.

Linking an Active Directory

To link an Active Directory in the UMS, proceed as follows:

1. Click on **Active Directory** in the **UMS Administration** area.
2. Click on **Add**.
   The **Add Active Directory / LDAP Service** mask will open.
3. Enter the **domain name** and the access data.
4. Confirm your settings by clicking on **OK**.
   Your Active Directory will now feature in the list.


Server - dokumentation.igel.local
UMS Administration
UMS Network
Server
Global Configuration
Administrative Tasks
Active Directory / LDAP Configuration
Universal Firmware Update
License Configuration
Active Directory / LDAP Domains

Domain Name	Domain Controller	Page Size
UMS.TEST	172.30.200.1	1000

> ⓘ Other LDAP servers (*Novell eDirectory*, *OpenLDAP* etc.) cannot be used for *IGEL Shared Workplace* user authentication purposes.

Assigning a User Profile

Go to your Active Directory in the UMS navigation tree under **Server > Shared Workplace User**.

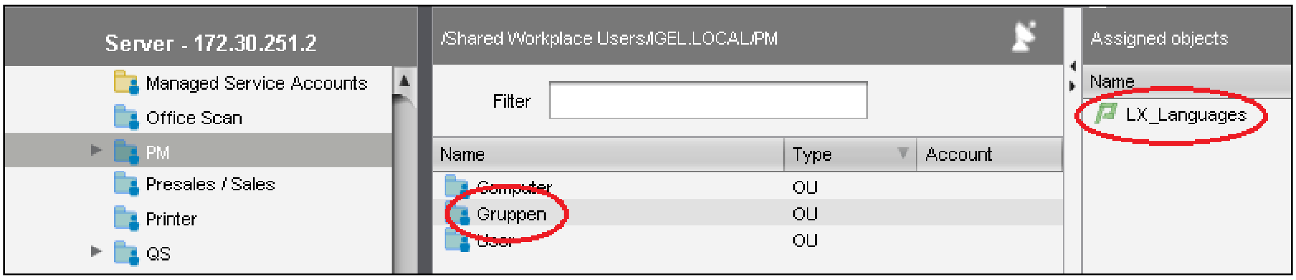
You can browse it or search for it by using this symbol: 🔭 .

- Select an object within the AD structure.

You will need to authenticate yourself vis-à-vis the Active Directory in order to do so.

- Assign the desired user profile to this object:

Server > Shared Workplace User > [Active Directory] > [Object]



Name	Type	Account
Computer	OU	
Gruppen	OU	
User	OU	

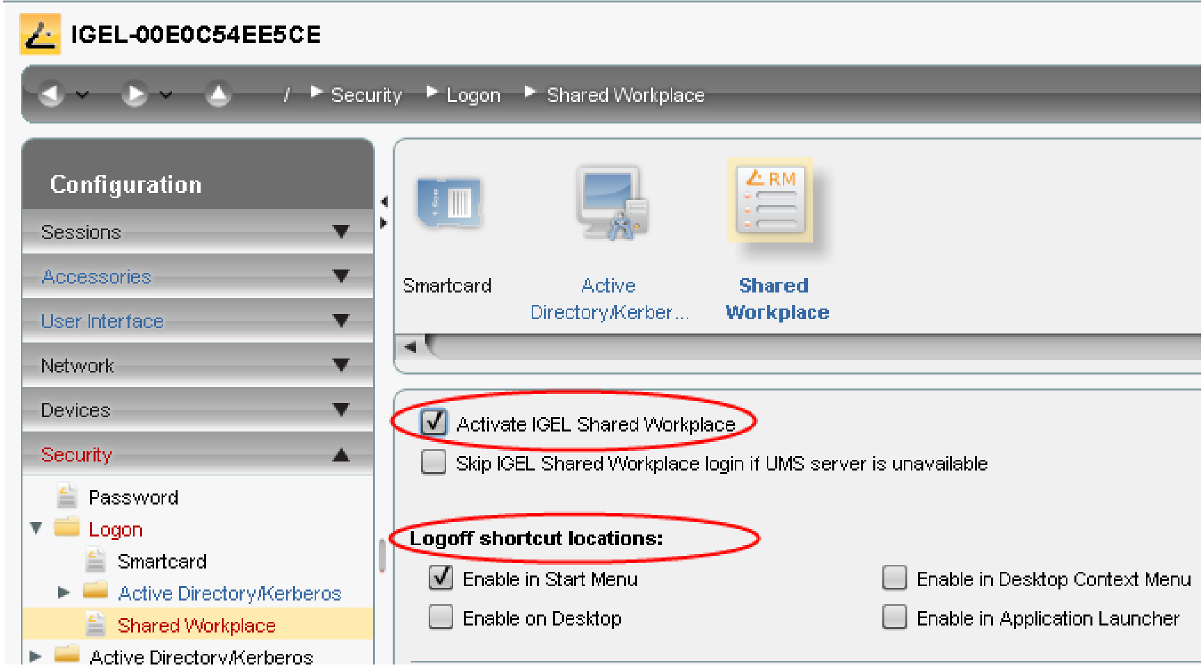
As with devices, a number of profiles can be assigned. In this case, indirectly as well as directly assigned profiles will be taken into account.

ⓘ Right-click the name of a user account, to see the profile settings of the device.

Enabling 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).



☑ Activate IGEL Shared Workplace

□ Skip IGEL Shared Workplace login if UMS server is unavailable

Logoff shortcut locations:

☑ Enable in Start Menu

□ Enable in Desktop Context Menu

□ Enable on Desktop

□ Enable in Application Launcher

User login

If you have a license, you can easily log in to a endpoint device with IGEL Shared Workplace:

1. Boot the device.
   A login window will appear.
2. Log in with your AD login data.
   You will receive the profile settings that are stored for you in the UMS.

> ⓘ The device configuration which is active for the user logged in is the result of cumulating all profiles which have been assigned either directly or indirectly to the device or the user. See also Prioritization of Profiles in the IGEL UMS.

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 53)
- Universal Desktop Windows Embedded Standard (see page 54)

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 55).

- 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.

IGEL Management Interface (IMI)

See the documentation on this page: IGEL Management Interface (IMI)