

IGEL Universal Management Suite v5

User Manual

UMS5

Universal Management Suite

Important Information

Please note some important information before reading this documentation.

Copyright

This publication is protected under international copyright laws. All rights reserved. With the exception of documentation kept by the purchaser for backup purposes, no part of this manual – including the products and software described in it – may be reproduced, manipulated, transmitted, transcribed, copied, stored in a data retrieval system or translated in any form or by any means without the express written permission of IGEL Technology GmbH.

Copyright © 2016 IGEL Technology GmbH. All rights reserved.

Trademarks

IGEL is a registered trademark of IGEL Technology GmbH.

Any other names or products mentioned in this manual may be registered trademarks of the associated companies or protected by copyright through these companies. They are mentioned solely for explanatory or identification purposes, and to the advantage of the owner.

Disclaimer

The specifications and information contained in this manual are intended for information use only, are subject to change at any time without notice and should not be construed as constituting a commitment or obligation on the part of IGEL Technology GmbH. IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including any pertaining to the products and software described in it. IGEL Technology GmbH makes no representations or warranties with respect to the contents thereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

IGEL Support and Knowledge Base

If you have any questions regarding an IGEL product and are already an IGEL customer, please contact your dedicated sales partner first. Er beantwortet gerne Ihre Fragen rund um alle IGEL-Produkte.

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 at the <http://www.igel.com/de/mitgliederbereich/anmelden-abmelden.html> .

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 also our notes regarding support and service information. Please visit our *IGEL Knowledge Base* <http://edocs.igel.com/> to find additional Best Practice and How To documentation as well as the *IGEL Support-FAQ* (<http://faq.igel.com>).

Contents

Important Information.....	2
1. Overview	7
1.1. Attributes of the IGEL UMS.....	7
1.2. IGEL UMS components.....	9
2. Installation.....	11
2.1. Installation requirements	11
2.2. Installing a UMS server	13
2.3. Updating UMS installation	15
3. First steps	19
3.1. Connecting the UMS console to the server	19
3.2. Registering thin clients on the UMS server.....	21
4. Working with the IGEL UMS	30
4.1. The console window	30
4.2. The IGEL UMS Administrator	44
5. Thin Clients	49
5.1. Managing thin clients.....	49
5.2. Configuring thin clients.....	56
5.3. Shadowing (VNC)	57
5.4. Firmware licenses	60
6. Profiles.....	63
6.1. Order of priority for settings.....	64
6.2. Order of priority for profiles	65
6.3. Using profiles	66
6.4. User profiles - IGEL Shared Workplace	74
6.5. Master profiles.....	80
6.6. Template profiles	85
7. Views	97
7.1. Creating a new view.....	98
7.2. Saving the view results list.....	102
7.3. Send view as mail.....	103
7.4. Assign profiles to a view	104
8. Tasks	105
8.1. Setting up a new task.....	105
8.2. Commands for Tasks	105
8.3. Details	106
8.4. Schedule.....	107
8.5. Assignment.....	109
8.6. Results.....	109

9.	Files	111
9.1.	Registering a file on the UMS server.....	111
9.2.	Transferring a file to a thin client.....	112
9.3.	Removing a file from a thin client.....	113
9.4.	Transferring a file to the UMS Server	113
10.	Universal Firmware Update.....	114
10.1.	Changing server settings.....	114
10.2.	Searching for and downloading updates	115
10.3.	Importing from a local source.....	115
10.4.	Importing from the UMS WebDAV	116
10.5.	Assigning an update to a thin client.....	116
11.	Search History	117
11.1.	Context Menu of a Search Query.....	117
12.	Recycle Bin	117
13.	Managing certificates	119
13.1.	Installing server certificates	119
13.2.	Removing a Certificate.....	119
13.3.	Saving a certificate	119
13.4.	Importing a console certificate	120
14.	Administration area	121
14.1.	UMS network	121
14.2.	UMS Server	122
14.3.	Global configuration	122
15.	Importing Active Directory users	143
15.1.	Explanation of symbols	144
15.2.	Searching in the Active Directory.....	145
15.3.	Import results list	146
16.	Administrator accounts and access rights.....	147
16.1.	Administrators and groups	147
16.2.	Access rights.....	148
17.	User logs.....	154
17.1.	Administration	154
17.2.	Logging dialog window.....	155
18.	Send log file to Support	158
18.1.	Support Wizard	158
19.	Optional add-ons	159
20.	Index	160

About this document

This document describes the procedure for installing and using the IGEL Universal Management Suite 5 (UMS 5) based on Version 5.02.100. The firmware parameters for the thin client are described in greater detail in the relevant IGEL Universal Desktop or IGEL Zero manual, even if these parameters can be configured via the UMS.

This document assumes that a fully functional installation of the IGEL UMS as well as at least one IGEL thin client which is to be managed are available.

Formatting and meanings

The following formatting is used in the document:

<i>Hyperlink</i>	Internal or external links
Proprietary names	Proprietary names of products, firms etc.
GUI text	Elements of text from the user interface
Menu > Path	Menu paths in systems and programs
Input	Program code or system inputs
<u>Keyboard</u>	Commands that are entered using the keyboard
<input checked="" type="checkbox"/>	Checked checkbox
<input type="checkbox"/>	Unchecked checkbox
Version 5.02.100	Firmware version

➔ Reference to other parts of the manual or other eDocs articles.



Note regarding operation



Warning: Important note which must be observed

What is new in 5.02.100?

You will find the release notes for the IGEL Universal Management Suite 5.02.100 both as a text file next to the installation programs on our *download server*

(http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7/) and in our *Knowledge Base* (<http://edocs.igel.com/>).

- A new *option in the context menu* (page 104) allows you to assign profiles directly to thin clients that were filtered via a **view** or **search**.
 - You can now configure global settings for the integrated *VNC viewer* (page 140) in a centralized manner.
 - For *files* (page 111) that are transferred via UMS, there is once again the Java certificate classification.
 - In the case of thin clients with IGEL Windows Embedded Standard 7, the content panel now shows a **description of the firmware**, provided that this was given when the snapshot was created.
- ➡ This description can be configured in the in the setup of IGEL Windows Embedded Standard 7.
- The *Help > Save support information...* (page 36) function now also saves profiles as well as the log for the IGEL Management Interface (IMI) extension.
 - The *Help > Save TC files for support* (page 36) function now also saves profiles assigned to the thin client as well as firmware information.
 - When *transferring files* (page 112) from the UMS to thin clients, the IP address of the UMS is now used instead of its name. This ensures that the transfer works even in the event of DNS problems.
 - From now on, it is possible to record the logon and logoff activities of users who log on via **Shared Workplace** or **Kerberos/Active Directory**.
 - The silent *installation* (page 13) of the UMS console under Windows can be configured beforehand.
 - If you change the vertical and horizontal limits in the *console window* (page 30) according to your needs, your changes will be retained after logging off.
 - You can *copy a session* (page 57) in the configuration dialog of a thin client.
 - With the help of an **administrative task**, you can *export view results via mail* (page 131).
 - You can export via mail the results of **administrative tasks**: *database backup* (page 123), *remove unused firmwares* (page 125), *refresh caches* (page 126), *delete logging information* (page 127), *delete task results* (page 128), *delete thin clients* (page 130) and *assign profiles to the thin clients of views* (page 132).
 - The *Support Wizard* (page 158) can collect the log files which are important for your support case and send them as a mail to IGEL Support.
 - With the help of an **administrative task**, you can *delete task execution data* (page 128).
 - For scenarios where the UMS is outside the thin clients' network, you can define one or more Linux thin clients as a *Wake-on-LAN* (page 137) proxy.

1. Overview

With the IGEL Universal Management Suite (UMS), you can remote configure and control IGEL thin clients even across WANs. With its open, network-friendly structure, you can incorporate the UMS into an existing company infrastructure.

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



Each IGEL thin client comes with a free version of the IGEL Universal Management Suite.

➔ An overview of devices supported by the IGEL Universal Management Suite can be found *in these FAQs* <http://edocs.igel.com/index.htm#10202898.htm>.

Typical areas of use

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

1.1. 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 thin client 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 thin client configuration in the most exceptional circumstances.

Asset management:

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

Commentary fields:

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

Support for numerous operating systems:

The UMS server can run on many common versions of Microsoft® Windows® Server and Linux, see *U_Installation Requirements* (page 11).

Access independent of the operating system:

The UMS console runs on any device with the Java Runtime Environment. You can also use the UMS console with Java Web Start without a local installation, see *Installation Requirements* (page 11).

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 thin client 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 thin clients.

Group and profile-based administration:

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

Trouble-free rollout:

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

Comprehensive support for all configuration parameters:

Most IGEL thin client 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 thin client screens, enabling them to rapidly identify problems and demonstrate solutions directly to users.

1.2. IGEL UMS components

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

- IGEL UMS *Server* (page 9)
- IGEL UMS *Administrator* (page 9)
- IGEL UMS *Console* (page 10)

1.2.1. UMS Server

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

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

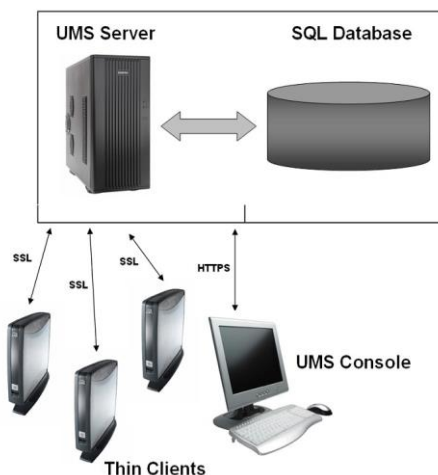


Figure 1: The backend

Typically, the UMS Console and UMS Server are installed on different computers. Data transmission between the UMS Server and thin clients as well as between the UMS Server and Console is encrypted. Further information regarding communication between the UMS Server, UMS Console, database and thin clients can be found in the Appendix.

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

1.2.2. UMS Administrator

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

The key parts of the UMS Administrator are as follows:

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

1.2.3. UMS Console

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

The key tasks of the UMS Console are as follows:

- Displaying the thin clients' configuration parameters
- Setting up profiles and planned tasks
- Administering firmware updates

2. Installation

This chapter describes the requirements for installing the UMS. The installation is explained with an example for *Windows* (page 13) and one for *Linux* (page 14) in each case. You are also told what you need to bear in mind when performing an update and where you can connect external database systems.

© Additionally see the training video "UMS Installation" on our TechChannel.

2.1. Installation requirements

You can run the IGEL UMS with Windows and Linux (x86 and x86_64). You will find information regarding installation of the UMS on 64-bit systems under FAQs for installing the UMS on 64-bit systems. You will find details of supported operating system versions in the UMS Data Sheet on the IGEL website.

Your hardware and software must meet the following minimum requirements:

UMS complete installation

- At least 1 GB of RAM (2 GB recommended)
- At least 1 GB of free HDD space (plus database system)

Individual console installation

- At least 512 MB of RAM (1 GB recommended)
- At least 250 MB of free HDD space



As an alternative to a local console installation, you can execute the UMS console as a Java Web Start application too. The console does not need to be installed here. If necessary, it can be downloaded from the UMS server and executed. Further information can be found under *UMS console via Java Web Start* (page 12).



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.

For details of the supported database systems, please see the UMS Data Sheet on the IGEL website. Details of the requirements when installing and operating the database can be found in the documentation for the particular DBMS.

The UMS Server and Load Balancer for high availability (HA) must be in the same IP network. NAT or proxies must not be between the UMS Server and Load Balancer because they can influence communication between the components.

The Embedded Database **cannot** be used for an HA network. You can use the Embedded Database for a dedicated test installation with only a single server for the UMS Server and Load Balancer.

2.1.1. UMS console via Java Web Start

Requirement: **Java 1.8.0_40** or newer.

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

1. In a web browser, open the address `http://[UMS-Server]:9080/start_rm.html`.
2. Click on the **Start IGEL Universal Management Console** link.

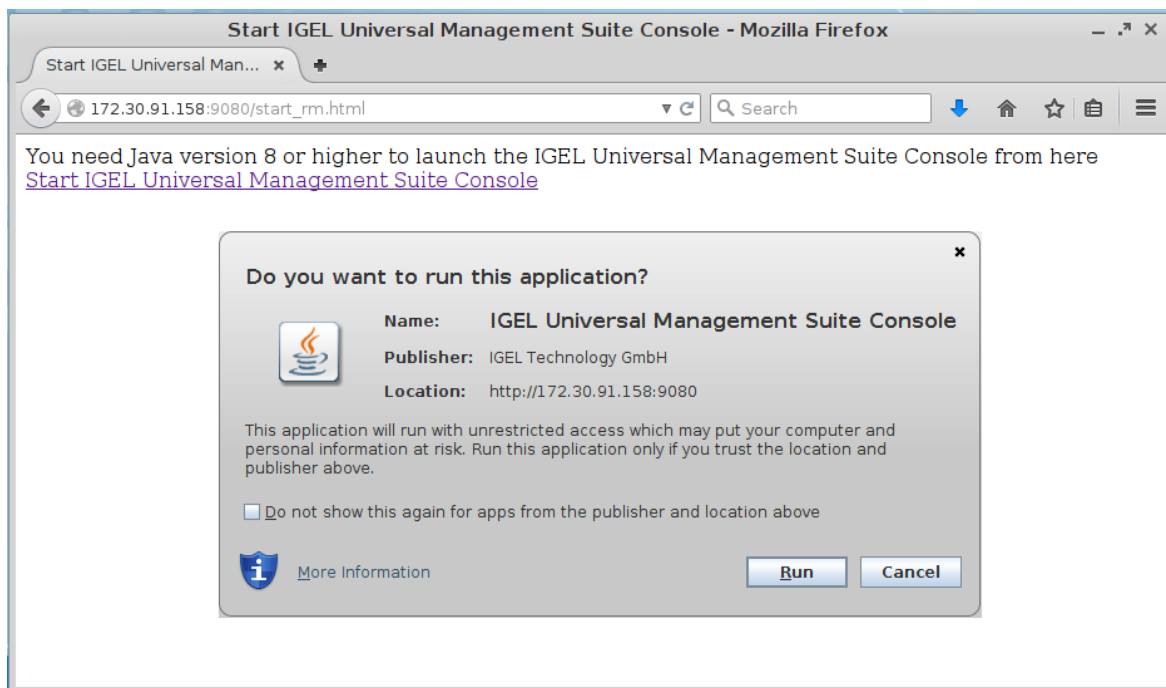


Figure 2: Java Web Start

3. Confirm that the downloaded JNLP file will be opened with the **Java Web Start Launcher**.
The application will be downloaded.
4. Allow the application signed by IGEL Technology GmbH to be executed.
The UMS console will start, and the *logon window* (page 19) will appear.



Starting the UMS console via Java Web Start ensures that the version of the console matches the version of the UMS server.

2.2. Installing a UMS server

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

➡ You will find instructions for installing the UMS HA (High Availability) Extension in the Appendix.

2.2.1. Installation under Windows

Standard installation

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

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



You will need administration rights for the computer in order to install the UMS.

3. Close all other applications and confirm that you have done so.
4. Read and confirm the license agreement.
5. Read the explanation of the installation process.
6. Select a path for the installation.
7. Select the type of installation.
8. Enter the user name and password for the database connection.
9. Choose a name for the entry in the Windows Start Menu.
10. Read the summary and start the installation process.

The Windows Installer will install the UMS, create entries in the Windows software directory and in the Start Menu and place a start icon on the desktop.

11. Close the program once installation is complete.

If you have chosen the standard installation, the UMS server will run with the Embedded Database.

12. Launch the UMS console.
13. Connect the UMS console to the server using the access data you entered during installation.

➡ You will find information regarding use of the UMS with external databases under *Connecting external databases* (page 17).

Silent installation of the UMS console

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



Silent installation is only possible for the UMS console. It is not possible for the UMS administrator and the UMS server.

➡ Further information can be found in the Unattended/silent installation of UMS console FAQs.

2.2.2. Installation under LINUX

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

1. Download the current version of the IGEL Universal Management Suite from the IGEL Download Server.
2. Log on as `root`.



You will need root privileges on the computer in order to install the UMS.

3. Open a terminal window, e. g. `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. You can make the installation file executable with the following command:

```
chmod u+x setup*.bin
```
5. Execute the installation file.
The installer will be unpacked to `/tmp`, will run its Java Engine and will remove itself again once the installation is complete.
6. Read and confirm the license agreement.
7. Read the explanation of the installation process.
8. Select the type of installation.
9. Select a path for the data directory.
10. Select the run level(s) for UMS.
11. Select the database system.

➡ You will find information regarding use of the UMS with external databases under *Connecting external databases* (page 17).

12. Enter the user name and password for the database connection.
13. Select whether you would like to set up program links for the UMS console and UMS administrator in the menu.
14. Read the summary and start the installation process.
15. Close the program once installation is complete.

If you have chosen the standard installation, the UMS server will run with the Embedded Database.

16. Launch the UMS console via the menu entry or with the command

```
/opt/IGEL/RemoteManager/RemoteManager.sh
```
17. Connect the UMS console to the server using the access data you entered during installation.

2.3. Updating UMS installation



Create a *backup of the database* (page 46) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.



If you use an older version of the IGEL Remote Manager with SAP DB, we recommend that you switch to the Embedded Database before updating the UMS. For a more detailed description of this switch, please contact IGEL Support.



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.

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.



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 server (`Unable to load tree` error message). In this case, you will need to update the installation of the UMS console.



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

2.3.1. Updating under WINDOWS



Create a *backup of the database* (page 46) 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.
2. Launch the installer.



You will need administration rights on the computer in order to install the IGEL UMS.

3. Close any other applications and confirm that you have done so.
4. Read and confirm the license agreement.
5. Read the explanation of the installation process.
6. Select a path for the installation.
7. Choose a name for the entry in the Windows Start Menu.

8. Read the summary and start the installation process.
9. Confirm that you have closed all other UMS applications.
10. Confirm the automatic updating of the database schema.

The Windows Installer will install the new version of the UMS, create entries in the Windows software directory and in the Start Menu and place a start icon on the desktop.

11. Close the program once installation is complete.

Once the update has been installed successfully, the UMS server will connect to the previously used database.

12. Launch the UMS console.
13. Connect the UMS console to the server using the access data you entered during installation.

2.3.2. Updating under LINUX



Create a *backup of the database* (page 46) before updating a previously installed version of the UMS. Otherwise, you risk losing all database content.

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.
2. Log on as `root`.



You will need root rights for the computer in order to install the UMS.

3. Open a terminal window, e. g. `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. You can make the installation file executable with the following command:

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

5. Execute the installation file.

The installer will be unpacked to `/tmp`, will run its Java Engine and will remove itself again once the installation is complete.

6. Confirm that any applications running will be closed.
7. Read and confirm the license agreement.
8. Read the explanation of the installation process.
9. Select a path for the installation.
10. Read the summary and start the installation process.
11. Confirm that you have closed all other UMS applications.
12. Confirm the automatic updating of the database schema.

13. Close the program once installation is complete.

Once the update has been installed successfully, the UMS server will connect to the previously used database.

14. Launch the UMS console via the menu entry or with the command
`/opt/IGEL/RemoteManager/RemoteManager.sh`

15. Connect the UMS console to the server using the access data you entered during installation.

Connecting external database systems

You will find details of the supported database systems and the HA add-on in the IGEL UMS Data Sheet and on the IGEL website respectively. Details of the requirements when installing and operating the database can be found in the administration manual for the particular DBMS.

- To configure the database, use the relevant DBMS management program.

The configuration for setting up the data source and connecting the UMS to the database should be carried out in the UMS Administrator.

All UMS Servers must work with the same database.

Oracle

To integrate Oracle, proceed as follows:

1. Set up a new database user with `Resource` authorization.
2. Set up a new Oracle type data source in the UMS Administrator.

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

Microsoft SQL Server

To connect the Microsoft SQL Server, proceed as follows:

1. Open the SQL Console of the SQL Server by selecting **New Query**.
2. Use the following script as a template, change it as necessary and then execute it.

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

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

3. Set up a new `SQL Server` type data source in the UMS Administrator.
4. Ensure that the **server port** of the SQL Server is configured correctly in the data source. The default value is `1433`.

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

PostgreSQL

IGEL UMS uses PostgreSQL functions (from Version 8.2). Older versions are not supported.

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>.

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

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

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

3. Launch the administration tool `pgAdmin`.
4. Create a new login role with the name `rmlogin`.
5. Create a new database with

```
name = rmdb
owner = rmlogin
encoding = UTF-8
```
6. Set up a new schema within the `rmdb` database with

```
name = rmlogin
```
7. Check whether the language `plpgsql` is available in the `rmdb` database.
If not, set it up.
8. In the **UMS Administrator**, create a new `PostgreSQL`-type data source with the host name of the PostgreSQL Server and the correct server port (default is `5432`), user `rmlogin` and database `rmdb`.

Apache Derby

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

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

1. For security purposes, enable **User Authentication** in the Derby DB.
2. Launch the ij Utility (in [derby-installation-dir]/bin).
3. To create the rmdb instance, execute the following command:

```
connect
'jdbc:derby:rmdb;user=dbm;password=dbmpw;create=true';
```

4. Define the UMS database user `rmlogin` with password `rmpassword`

```
CALL SYCS_UTIL.SYCS_SET_DATABASE_PROPERTY('derby.user.rmlogin',
'rmpassword');
```

5. Exit ij and launch the Derby Network Server.
6. In the **UMS Administrator**, create a new Derby-type data source with the host name of the Derby Server and the correct server port (default is 1527), user `rmlogin` and database `rmdb`.

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

3. First steps

In order to be able to work with the IGEL UMS, you will first need to install the UMS Server, Console and Database before registering at least one thin client or loading the UMS Demonstration Database Backup. This is available on the IGEL Download Server.

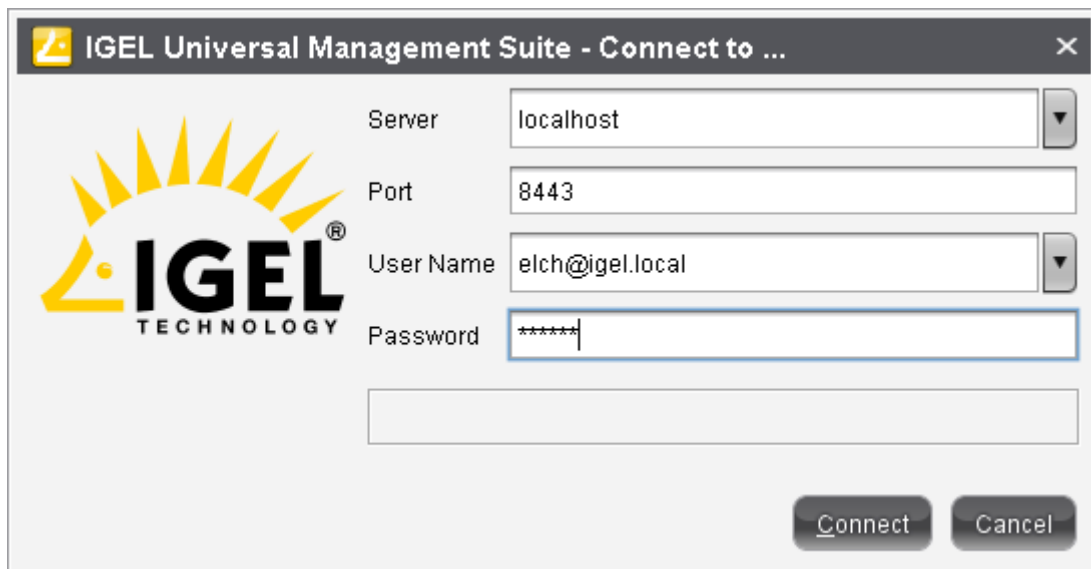
The procedure for connecting to the server and registering thin clients using the UMS Console is described below. You will find detailed information regarding the IGEL UMS functions in the chapter *Working with IGEL UMS* (page 29).

3.1. Connecting the UMS console to the server

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

1. Launch the UMS console.
2. Click on **System > Connect to**.

3. Enter the access data in the logon window:



The screenshot shows a dialog box titled "IGEL Universal Management Suite - Connect to ...". On the left side of the dialog is the IGEL logo, which consists of a stylized yellow sunburst above the text "IGEL TECHNOLOGY". To the right of the logo are four input fields: "Server" with the value "localhost", "Port" with the value "8443", "User Name" with the value "elch@igel.local", and "Password" with masked characters "*****". Below the password field is an empty text box. At the bottom right of the dialog are two buttons: "Connect" and "Cancel".

Figure 3: Anmeldung an der Konsole

- **Server:** Use the host name `localhost` if you are logging on to the server's UMS console. Use the host name of the server if you are connecting from a remote UMS console.
 - **Port:** The port on which the GUI server receives the UMS connections is set to `8443` by default. You can change the port using the UMS administrator.
 - **User name:** User name for the connection between the UMS console and database. When setting up the UMS for the first time, this is the user name of the database user account which was created while the UMS server was being installed. If you belong to a domain configured in the UMS, enter `<User>@<Domain>`.
 - **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.
- 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 are stored in drop-down lists and can therefore be reused. You can delete this list of stored logon data under **Misc > Settings > General > Delete Logon History**.

3.2. Registering thin clients on the UMS server

You can register thin clients on the UMS server in the following ways:

- *Searching for thin clients within the network* (page 21)
- *Importing thin clients via CSV files* (page 23)
- *Registering manually on the thin client* (page 27)
- *Registering thin clients automatically* (page 28)
- *Setting up thin clients manually* (page 28)



If you would like to use your own server certificate on the thin clients, upload the certificate before you register the thin clients on the UMS. Further information can be found under *UMS network* (page 121). If you have not uploaded the certificate before registration, you will need to remove the old certificates from the thin clients manually after changing the certificate.

3.2.1. Searching for thin clients in the network

To search for thin clients in the network and select them for registration, proceed as follows:

1. Log in to the UMS Console.

The content panel of the console will be displayed.

2. Click on **Thin Clients>Scan Thin Clients** to access the window allowing you to search for thin clients in the network.

Alternatively, you can start a search by clicking on the button in the tool bar.

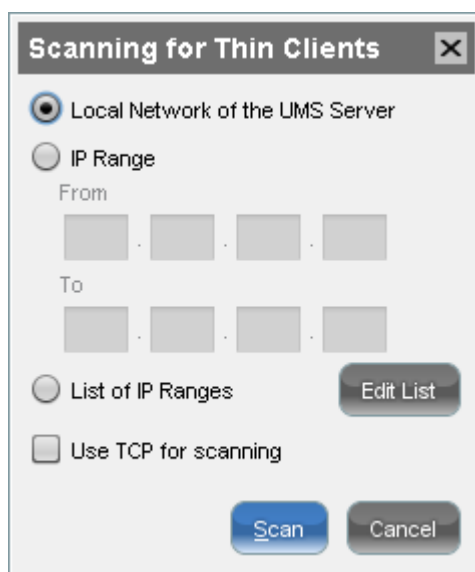


Figure 4: Scan for thin clients

1. You can search the entire network for thin clients that are switched on or restrict your search to specific IP address ranges.
2. Select the thin clients to be registered by checking the **Include** checkboxes.
3. Click **OK**.

3.2.2. Scan for Thin Clients

A thin client must be switched on and functioning if it is to be scanned. Furthermore, the thin client's firmware must support the IGEL UMS software. This is the case for all IGEL thin clients with original firmware as well as for devices from other manufacturers on which the IGEL Linux system was installed using the IGEL Universal Desktop Converter 2.

The following scan options are available:

Local network of the UMS server

With this option, a broadcast message is sent by the network containing the IGEL UMS server. The IGEL UMS server may be in a different network segment from the one that contains the IGEL UMS Console. If the server is installed on the IGEL UMS server and has various network interfaces, only the first interface will be used to send the broadcast message.

IP range

When a message is sent, each IP in the specified range will be contacted, even if routers suppress broadcast messages.

List of IP ranges

If a number of network segments need to be scanned, you can create a list of the IP ranges. To do this, click on **Edit List** and **Add** to add ranges.

Use TCP for searching

Select this option if you would like to use TCP instead of UDP for scanning. In certain networks, scanning with TCP is more reliable, although it does take longer.

Once the scanning procedure is complete, the thin clients that have been detected will be displayed in a sortable list in the scan results window.

In the **Certificate Stored** column, you can see whether a thin client already has a certificate from a UMS Server. Thin client certificates can now be registered on the Server.

In the **Filter** field, you can enter a search string, e.g. parts of the device name, IP address or MAC address, which will be searched for in all visible fields.

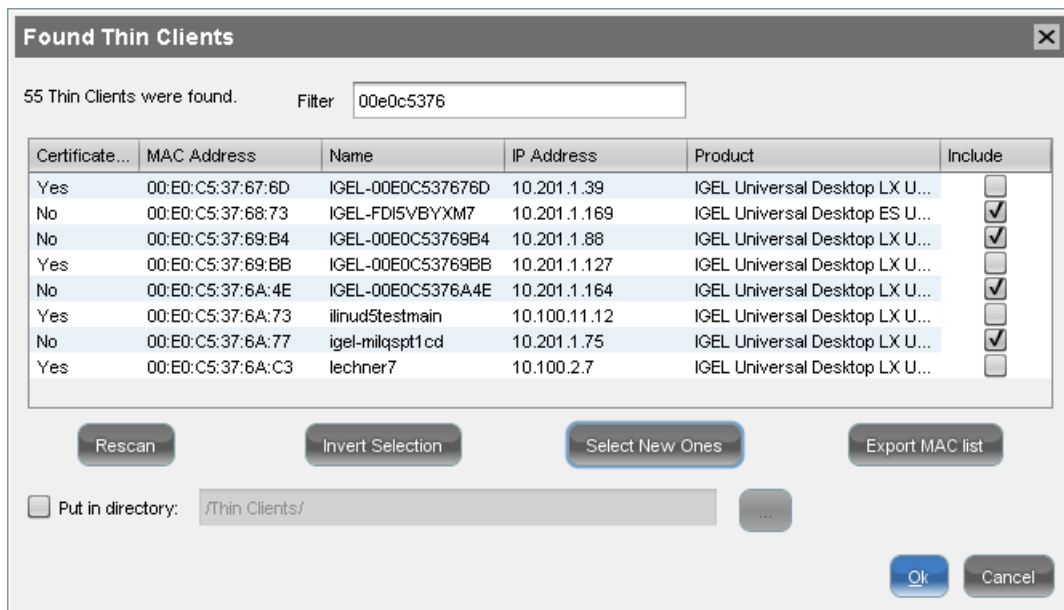


Figure 5: Results of the scan process

3.2.3. Registering thin clients

To register new thin clients, proceed as follows:

1. In the **Include** column, highlight the thin clients that you would like to register in your IGEL UMS Database.
2. Click **Select New Devices** to select all thin clients without a certificate.
3. Confirm your selection by clicking on **OK**.

The thin clients will now be registered in your database. This may take some time depending on the performance of the IGEL UMS Server.

If a thin client is registered in the IGEL UMS Database, the server certificate will be saved on the thin client. Further access to the thin client will now be validated on the basis of this certificate. Only the owner of the other private part of the certificate can manage the thin client.

4. Store the thin clients in a selected **directory** within the navigation tree immediately after registering them. This will save you having to sort them manually.

The result of the procedure and any error messages will be displayed in a new window.

5. Close this window in order to return to the main screen.

3.2.4. Importing thin clients

You can register thin clients before they are actually installed within the network. To do this, you will need a CSV file with the following thin client data:

- MAC address
- Name
- Firmware ID



This method is not always appropriate when setting up the UMS for the first time because the thin client firmware must already be in the database.

To import thin clients, proceed as follows:

1. Select **System > Import > Import Thin Clients**.

Thin clients that have been imported successfully will be highlighted in green.

Erroneous entries, e. g. an invalid firmware ID or an error during the import process will be highlighted in red.

2. Click on **Clear** to delete all messages from the window.
3. Click on **Import TCs** to launch the import procedure.

To correct erroneous entries, proceed as follows:

- Change the entries highlighted in red with the following editing functions:

- **Ctrl-C** and **Ctrl-V** for copying and pasting a highlighted row
- **Del/Ctrl-X** for deleting a highlighted row
- **Return/Enter** inserts an additional row under a field.

Import with short format

The short format provides the information required for the import and assignment to a profile: **MAC address, device name, firmware ID, profile ID**.

The ID of a firmware version already registered can be found via **Misc>Firmware Statistics**.

The ID of a profile is shown in the **description data** and in the **tool tip** for the profile.

Example:

```
00E0C5540B8B; IGEL-00E0C5540B8B; 1; 26
```

```
00E0C5540B8C; IGEL-00E0C5540B8C; 1; 26
```

```
00E0C5540B8D; IGEL-00E0C5540B8D; 1; 26
```


Import Thin Clients

Short Format
 Long Format
 IGEL Serial Numbers Format

TC-Import Data: (fields marked with * are mandatory)

MAC-Adresse *	Name *	Firmware-ID *	Profilzuordnungen
00-E0-C5-54-0B-8B	IGEL-00E0C5540B8B	3	26
00-E0-C5-54-0B-8C	IGEL-00E0C5540B8C	3	26
00-E0-C5-54-0B-8D	IGEL-00E0C5540B8D	3	26

Figure 6: Import with short format

Import with long format

Unlike the short format, the long format also allows further data, e.g. the storage directory in the UMS navigation tree, serial number, location etc. to be imported. You will see what information can be imported after selecting the long format in the import dialog.

The short format provides the information required for the import, assignment to a profile and further data:

- **Directory:** Storage directory in the UMS navigation tree
- **MAC address:** MAC address of the thin client
- **Version:** Firmware version of the thin client
- **Name:** Device name of the thin client
- **Location:** Location of the thin client
- **Department:** Department to which the thin client is assigned
- **Comment:** Comment regarding the thin client
- **Inventory number:** Inventory number of the thin client
- **Commissioning:** Date on which the thin client was commissioned
- **Serial number:** Serial number of the thin client
- **Profile assignment:** ID of the assigned profile
- **Cost center:** Cost center to which the thin client is assigned

Example:

```

/Import;00E0C5540B9A;IGEL Universal Desktop
LX;5.03.100.01;IGEL-1;Büro1;EDV;Meier;0815;01.06.2014;F44
M;26;01

/Import;00E0C5540B9B;IGEL Universal Desktop
LX;5.03.100.01;IGEL-2;Büro2;EDV;Müller;4711;01.06.2014;F45
M;26;01

/Import;00E0C5540B9C;IGEL Universal Desktop
LX;5.03.100.01;IGEL-2;Büro3;EDV;Schulz;42;01.06.2014;F46M;
26;01
  
```

Import Thin Clients

Short Format
 Long Format
 IGEL Serial Numbers Format

TC-Import Data: (fields marked with * are mandatory)

Directory	MAC Adresse...	Version *	Name *	Site	Department	Comment	Asset ID	In-Service D...	Serial Num...	Profile Assi...	Cost Center

Figure 7: Import with long format



The **Firmware** column in the preview is made up of two values from the import file (system and firmware version).

The ID of a profile is shown in the **description data** and in the **tool tip** for the profile.

Import with IGEL serial number

When ordering your IGEL thin clients, you can request an import file in serial number format. With the import file in serial number format, you can integrate the devices into the UMS and configure them before they have even been delivered.

The short format provides the following information:

- **MAC address:** MAC address of the thin client
- **Name:** Device name of the thin client
- **Version:** Firmware version of the thin client
- **Serial number:** Serial number of the thin client

Example:

```
08154711;14D3B8C01B14110EBE;00E0C56133E4
47110815;14D3B8C01B14110EC6;00E0C56133EC
42007ABC;14D3B8C01B14110ED7;00E0C56133FD
007ABC42;14D3B8C01B14110EF9;00E0C561341F
```

Figure 8: Import with serial number format



The thin client firmware is not imported from the file. As a rule, the firmware with the highest ID will be assigned to the thin client. The IDs for firmware versions already registered can be found via **Misc > Firmware Statistics**.

In the import file, the serial number constitutes the first part of each row. In the preview, it is listed as the last column.

3.2.5. Registering thin clients manually

You can also register a thin client on the UMS Server on the client itself:

1. Enter the name and the address of your UMS Server and the server port (standard setting 30001) under **System>Remote Management** in the thin client setup.
2. Carry out the registration procedure, entering the login data for the UMS Server.
3. Reboot the thin client.

On thin clients with the UDLX firmware, you will find a dedicated program for registering on the UMS Server under **System** in the **Application Launcher**. As a result, you can determine from the client itself the sub-directory in the navigation tree to which the client will be added.

There are two ways to pass on the IP address of the UMS Server to the thin client:

- If you register a thin client on the UMS Server, the IP address of the server will be saved on the thin client. The registry key is: `system.remotemanager.server0.ip`.

The thin client connects to this IP address in order to retrieve its settings each time it boots.

Alternatively, you can configure your DHCP server in such a way that it provides the IP address via Option 224.

- The second way is to create an alias with the name `igelrmserver` for the UMS Server in your DNS.

If you would like to add thin clients to your UMS Database manually, you must use one of these options. Otherwise, the thin client will not be able to connect to the server.

3.2.6. Registering thin clients automatically

The IGEL UMS Server can be configured in such a way that all thin clients without a certificate which boot in the server's network are automatically registered.

1. To do this, enable the **Automatic Registration** parameter under **Settings>Further Settings** in the **IGEL UMS Administrator** program.
2. You can register an IGEL thin client on the UMS Server automatically by setting the DNS entry `igelrserver` (Record Type A) or a DHCP option (224).
3. Set the DHCP option 224 as a string - not as DWORD - to the IP address of the server by adding the following to the `dhcpd.conf` file in the appropriate section, e.g. in the global area:

```
option igelrserver code 224 = text
option igelrserver "<IP of the UMS Server>"
```

4. You should also set the DNS entry `igelrserver` to the IP address of the UMS Server.

Warning: If this option is enabled, each thin client without a certificate in the network will be added to the UMS Database. If you reset a client to the factory settings and reboot it, it will immediately be registered on the server again. We recommend automatic registration if new clients are to be registered during a network rollout. Once the clients have been registered, disable the automatic registration option on the UMS Server.

3.2.7. Setting up thin clients manually

To create an entry for a thin client in the database manually, proceed as follows:

1. Select **New Thin Client** either in the context menu of a thin client directory or in the menu under **System>New**.
2. Give the MAC address, the name and the firmware of the thin client and, optionally, select a directory for the client.

The firmware for the thin clients must be available in the database for the manual set-up. To ensure that this is the case, it can be imported along with the firmware or provided by thin clients that have already been registered. This method is therefore not always appropriate when setting up the IGEL UMS for the first time.

4. Working with the IGEL UMS

The IGEL Universal Management Suite provides extensive tools for managing your thin client infrastructure. The majority of administrative tasks can be found in the UMS Console, while the UMS Administrator provides a number of tools for server configuration.

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

4.1. The console window

The UMS console contains the following areas:

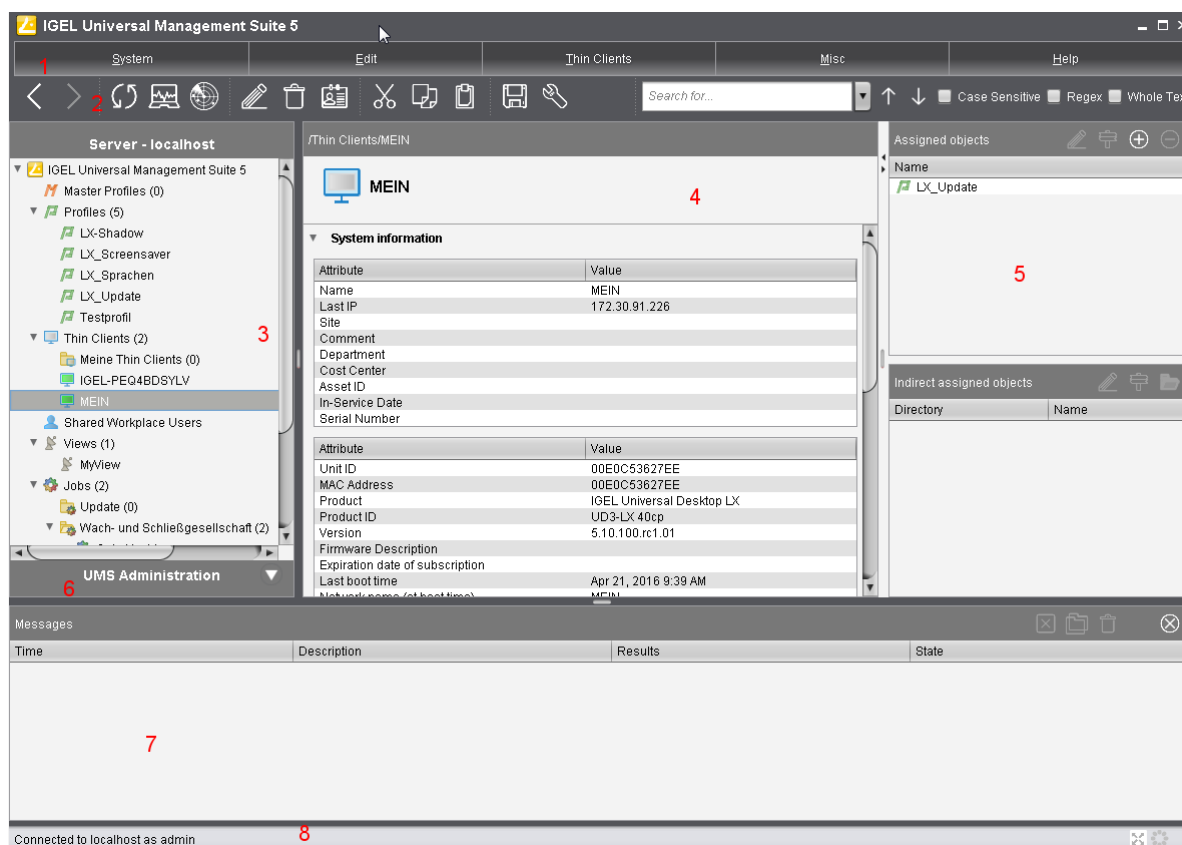


Figure 9: The UMS console window

- 1 *Menu bar* (page 31) All commands and actions can be executed from the menu. You can use shortcuts (**Alt** + underlined character in the menu element) to access the menu bar via the keyboard.
- 2 *Symbol bar* Frequently used commands relating to objects in the navigation tree.
- 3 *Navigation tree* Provides access to all UMS objects such as thin clients registered on the UMS server, directories, profiles, views, scheduled tasks etc.
- 4 *Content panel* (page 39) Information regarding the selected object. Many entry fields can be edited directly.
- 5 *Assigned objects* (page 40) Objects assigned to the thin clients or folders.
- 6 *UMS Administration* (page 39) Administrative tasks, e. g. configuring domains, Universal Firmware updates and the scheduled backup of the UMS Database (only Embedded DB)
- 7 *Messages* (page 39) Messages regarding actions launched in the UMS console. Messages regarding successful procedures will be shown in green. Messages regarding problems when executing procedures will be shown in red.
- 8 *Status row* (page 40) Status messages from the console, e. g. the server currently connected and the user name.



You can change the vertical and horizontal limits between the navigation tree/UMS administration, content panel and messages in order to adjust the size of the areas to suit your needs. From UMS **Version 5.02.100**, the changes are saved so that they will be available again the next time that you log on.

4.1.1. Menu bar

The menu bar comprises the following menus:

- **System**
- **Edit**
- **Thin clients**
- **Misc**
- **Help**

System

Menu path: **Menu Bar > System**

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

- **Connect to:** Allows you to establish the UMS server connection
 - **Server:** IP or host name of the UMS server
 - **Port:** Port number, default: 8443
 - **User name:** User name, "<username>@<domain>" 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, thin clients
- **Export:** Allows you to export objects such as firmware, profiles, thin clients
- **Administrator accounts:** Allows you to set up and manage UMS user accounts and user groups
- **Logging:** Allows you to display and export recordings of messages, events and VNC log entries.
- **License management:** Allows you to create and assign firmware licenses to thin clients
- **VNC Viewer:** Allows you to shadow a thin client
- **Open Customization Builder:** If licensed: Allows you to launch the Universal Customization Builder (UCB), for more details see the UCB appendix
- **Exit:** Allows you to close the UMS console application

Edit

Menu path: **Menu bar > Edit**

In this menu, you will find options for editing highlighted objects:

- **Save description:** Allows you to save changes to the data in the content panel
- **Edit Configuration:** Allows you to edit configuration parameters for the selected thin client or profile
- **Rename:** Allows you to rename an object in the navigation tree
- **Delete:** Allows you to delete an object in the navigation tree
- **Access control:** Allows you to manage user and group rights for the selected object
- **Cut:** Allows you to cut a data object and copy it to the clipboard.
- **Copy:** Allows you to copy data objects to the clipboard.
- **Paste:** Allows you to paste data objects from the clipboard.

Thin Clients

Menu path: **Menu Bar > Thin Clients**

In this menu, you will find all commands that can be sent to selected thin clients at the top.

- **Suspend:** Puts highlighted thin clients into suspend mode.
- **Shutdown:** Shuts down highlighted thin clients.
- **Wake up:** Starts highlighted thin clients via the network (Wake-on-LAN)
- **Restart:** Restarts highlighted thin clients.

- **Update:** Updates the firmware for the highlighted Linux clients.
- **Update on Shutdown:** Updates the firmware when the highlighted Linux clients are shut down.
- **Download Firmware Snapshot:** Downloads the firmware snapshot for the highlighted Windows client.
- **Partial Update:** Carries out a partial update on highlighted Windows clients.
- **Create Firmware Snapshot:** Creates a firmware snapshot of a highlighted Windows client.
- **Reset to Factory Defaults:** Resets highlighted thin clients to factory defaults.
- **Other thin client commands:**
 - **Send Message:** Sends a message to highlighted thin clients.
 - **Reset to Factory Defaults:** Resets highlighted thin clients to factory defaults.
 - **UMS Settings->TC:** Sends the configuration of the UMS to the highlighted thin clients.
 - **TC Settings->UMS:** Reads the local configuration of the highlighted thin clients to the UMS.
 - **Update Desktop Customization:** Updates the set desktop background and the boot logo on highlighted Linux clients.
 - **UMS File->TC:** Defines a file which is sent to highlighted thin clients.
 - **TC File->UMS:** Defines a file which is sent from highlighted thin clients to the UMS.
 - **Delete File from TC:** Defines a file which is deleted from highlighted thin clients.
 - **Download MPlayer Codecs:** Downloads codecs for the MPlayer to highlighted Linux clients.



The command is only relevant to IGEL Linux Version 3.x or lower.

- **Remove codecs:** Removes MPlayer codecs on highlighted Linux clients.



The command is only relevant to IGEL Linux Version 3.x or lower.

- **Download Flash Player:** Downloads the Flash Player plugin for Firefox on highlighted Linux clients.
- **Remove Flash Player:** Removes the Flash Player plugin for Firefox on highlighted Linux clients.
- **Store UMS Certificate:** Stores the UMS certificate on highlighted thin clients.
- **Remove UMS Certificate:** Removes the UMS certificate on highlighted thin clients.
- **Refresh License Information:** License information will be refreshed.
- **Refresh System Information:** System information will be refreshed.
- **Take over settings from...:** Sends profile settings to the thin client on a one-off basis.
- **Clear 'Configuration Change Status' Flag:** Resets configuration change flags (blue dot next to the icons for the thin clients).
- **Check Template Definitions:** Checks the assignment of template values.
- **Scan for Thin Clients:** Searches for thin clients in the network of the UMS server.

Misc

Menu path: **Menu Bar > Misc**

- **Default directories:** Allows you to automatically assign thin clients to directories according to rules
- **Search:** Allows you to search for objects - the search is listed in the navigation tree under **Search History** and can be changed again there.
- **Scheduled Jobs:** Allows you to manage public holiday lists and assign tasks to hosts

Host Assignment: Allows you to assign virtual hosts to selected thin clients

- **Universal Management Suite Host:** Host name of the UMS
- **Last Scheduler Run:** Date and time when the Scheduler last ran
- **Available Thin Clients:** Restricts the available thin clients displayed
- **Assigned Thin Clients:** Tree or list view of the available clients on the selected host

Manage Public Holidays: Allows you to establish public holiday lists which you can use when creating new tasks.

- **Date lists:** Allows you to set up lists for public holidays
- **Days:** Allows you to specify the date of the public holidays in a public holiday list
- **Change Password** Allows the password of a logged-on 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:** Allows you to delete from the database firmware versions which are not used by any thin client or profile
- **Cache Management:** Allows you to view, refresh and empty the UMS server cache
- **Settings:** Configuration parameters such as console language and appearance, timeout values for online checks or Universal Firmware Update search etc.

General:

- **Language:** Language selection for the graphical user interface
- **External VNC viewer:** Allows you to select an external VNC viewer
- **Always apply settings on next boot:**
 - Apply
 - Do not apply
- **Always confirm move actions:**
 - Confirm
 - Do not confirm
- **Always confirm unassign actions:**
 - Confirm
 - Do not confirm
- **Always confirm overwriting of elements in search history:**
 - Confirm
 - Do not confirm
- **Elements in search history (max):** Maximum number of elements that the search history will show.
- **Clear the user and server list of the login dialog:** Allows you to clear the logon history

Appearance:

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

The following are available to choose from: Smart contrast, pewter, cinder gray, ocean and the legacy appearance from UMS 4.

- **TC commands always in the background:**
 - In the background
 - Not in the background
- **Open message area automatically on new messages:**
 - The message area in the lower part of the UMS console window will open automatically when incoming messages are received.
 - Will not open automatically
- **Show content amount of directories:**
 - Will be shown
 - Will not be shown
- **Load collapsed/uncollapsed tree status at login:**
 - The navigation tree will be restored to how it was at the last logon.
 - Will not be restored
- **Show category root icon:**
 - Show icons as symbols for the main categories in the navigation tree.
 - Show folder symbols for the main categories in the navigation tree.
- **Directory tool tip contains directory tree path:**
 - Will be shown
 - Will not be shown
- **Directory tool tip contains directory and content amount:**
 - The number of directories and the objects in the directory will be shown in the tool tip.
 - They will not be shown.

Online check:

- Allows you to check whether the thin clients are online:
 - Allways:** Interval in milliseconds
 - Never:** No check
 - Check now:** Check once

Configuration dialog: Allows you to select the number of graphic effects in the configuration dialog

- **Low:** Recommended for slow devices
- **Medium:** Recommended for devices with average graphics power
- **High:** Recommended for devices with high graphics power

Universal Firmware update:

- **Activate automatic status refresh:** The registration status of the firmware update will be refreshed in the background.
 - Will be refreshed automatically
- **Automatic status refresh interval:** Interval in seconds

UMS HAE: Allows you to configure the High Availability Extension status update



You will see the status in the content panel if you click on a server or load balancer under **UMS Administrator > Server**.

Activate automatic process status refresh: The process status will be refreshed in the background.

Will be refreshed automatically

Automatic process status refresh interval: Interval in seconds

Help

Menu path: **Menu Bar > Help**

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

- **User Manual:** Link to the manual on edocs.igel.com
- **User Manual (offline):** Open the user manual in PDF format.
- **IGEL Knowledge Base:** Link to further online documentation on edocs.igel.com
- **Save Support Information...:** Saves log files from the UMS server and UMS console as well as profiles and associated firmware information for the selected thin clients in a ZIP file. If the IGEL Management Interface (IMI) extension is being used, its API log file will be saved too. Further information can be found under *Support Wizard* (page 158).
- **Save TC Files for Support:** Saves log and configuration files for a thin client, for example `setup.ini` and `group.ini`, in a ZIP file.
- **Third Party Licenses:** A list of licenses for third-party software and libraries used in the UMS.
- **Info:** Shows details of the current version of the UMS console and Java environment as well as the logged-on user

4.1.2. Navigation tree

You can highlight or select objects in the navigation tree by clicking on them. Multiple selections are possible using the **Shift** or **Ctrl** key.

From UMS 5.01.100, you can specify whether the UMS console should remember the open areas in the navigation 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 logon** under **Misc > Settings > Appearance**.

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 navigation tree is subdivided into the following areas:

- **Master profiles (page 80):** Allows you to create and organize master profiles.
- **Profiles (page 63):** Allows you to create and organize standard profiles.
- **Template Keys and Groups (page 85):** Keys and values for use in template profiles.
- **Thin Clients (page 32):** Allows you to organize managed thin clients.
- **Shared Workplace Users (page 75):** Allows you to assign specific profiles to AD users.
- **Views (page 97):** Allows you to create configurable list views for thin clients.
- **Job (page 105):** Allows you to define scheduled tasks, e.g. firmware updates.
- **Files (page 111):** Allows you to register files for transferral to thin clients.
- **Universal Firmware Update (page 114):** Allows you to download the current firmware versions for distribution to thin clients.
- **Search History (page 41):** Saved search queries.
- **Recycle Bin (page 43):** Deleted and restorable objects.

4.1.3. Symbol bar

In the **symbol bar**, you will find buttons for frequently used commands:



Figure 10: The symbol bar

The symbols are as follows (in the correct order):



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 thin clients



Online check of the thin clients



Search for thin clients within the network



Change object names in the navigation tree



Delete objects in the navigation tree



Specify access rights for selected objects



Cut an object



Copy an object



Paste an object



Save the edited description data for thin clients or profiles



Edit configuration parameters for thin clients or profiles



Search for names, MAC addresses, IP addresses or IDs
The user's last 20 search queries are saved.

Quick Search

Finds objects in the navigation tree using a name, MAC, IP, 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.

4.1.4. Content panel

The **content panel** shows the properties of the particular object highlighted in the tree. This can be the contents of a directory, e.g. the profiles, thin clients, sub-folders, tasks etc. contained therein, or detailed information relating to an object such as a thin client's system information, the basic data for a profile, the hit list for a view etc.

These details are shown in the content panel for the following objects:

- **Directory:** Elements subordinate to the directory
- **Profiles:** Name, Description, Based on, Profile ID, Overwrite Session checkbox
- **Thin Clients:** System information, Template Definition Check Results, Monitor information, Features, Installed updates and hotfixes (WES), User login history
- **View:** Name, Description, Rule, Matching Thin Clients
- **File:** Source URL, Classification, Thin Client file location, Access rights
- **Job:** Details, Options, Job info, Schedule, Execution Results
- **Search History:** Name, Rule, Search type, Matching Thin Clients
- **Server:** Information regarding the service executed, requests, failed and waiting requests
- **Active Directory / LDAP:** Active Directory / LDAP domains
- **Administrative tasks:** List with tasks, execution history
- **Licenses:** License summary, registered licenses
- **Automatic UDC license deployment:** License server, status information, deployed licenses
- **Universal Firmware update:** Settings for the Universal Firmware Update, settings for the FTP servers to which the files are copied (optional)
- **Logging:** Message log setting, logging event settings
- **Task protocol:** Task protocol settings
- **Cache:** Cache configuration
- **Wake-on-LAN:** Wake-on-LAN configuration
- **Mail settings:** Mail settings, recipient for administrative task result and service mails
- **Thin client attributes:** Thin client attributes
- **VNC:** Secure VNC connection, graphics settings
- **Misc settings:** Recycle bin, secure VNC connection, template profiles, master profiles

4.1.5. UMS Administration

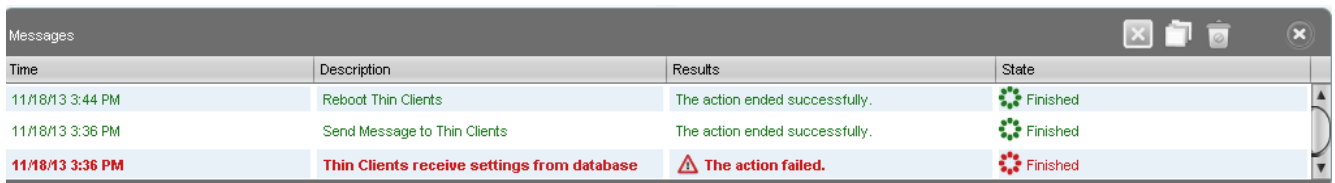
With Version 3.09 of the IGEL Universal Management Suite, a number of UMS Administrator settings options have been moved to the administration area of the UMS Console. The console now features a new **UMS Administration** area.

Configuration of the Active Directory and the server settings for Universal Firmware Updates have been moved from the UMS Administrator to the administration area of the UMS Console. In the UMS Administrator, a corresponding note is shown on the previously used tabs. You will also find new functions such as the alternative LDAP configuration or scheduled backups.

4.1.6. Messages

The **Messages** window area contains information regarding the successful or unsuccessful execution of commands. If a command could not be executed successfully, a message written in red appears in the list. A warning symbol will also flash in the status bar of the UMS Console until the user selects the message.

- Click **Show Result** or double-click the message in order to view the relevant details.
- You can 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.



Time	Description	Results	State
11/18/13 3:44 PM	Reboot Thin Clients	The action ended successfully.	Finished
11/18/13 3:36 PM	Send Message to Thin Clients	The action ended successfully.	Finished
11/18/13 3:36 PM	Thin Clients receive settings from database	The action failed.	Finished

Figure 11: The Messages window

4.1.7. Status bar

The **status bar** shows the name of the UMS Server currently connected and the user who is logged in to the 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.

4.1.8. Assigned objects

To ensure that you can quickly tell directly and indirectly assigned objects apart, the **assigned objects** area is subdivided into two parts.

Directly assigned objects have been assigned to an individual thin client, folder or profile, whereas indirect objects have been "inherited" via the file structure.

- Double-click an object in the assignment area in order to directly edit the profile assigned to a thin client.

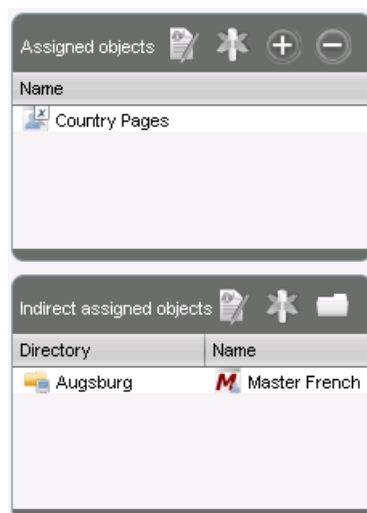


Figure 12: Directly and indirectly assigned objects

4.1.9. Context menu

You will be given an object-dependent **context menu** by right-clicking on the corresponding object. Depending on your selection, actions for folders, thin clients, 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 TC > UMS** can only be executed for an individual thin client. In contrast, the command **File UMS > TC** can be executed for all thin clients in a directory.

4.1.10. Search for objects in the UMS

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

- Quick Search
- Search function
- View

Quick Search in the symbol bar 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: object name, object ID, MAC address, IP address. These data are buffered locally when the 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.

Create new Search [X]

Select criterion

<input type="radio"/> Last known IP address	<input type="radio"/> Name	<input type="radio"/> Network Name
<input type="radio"/> Product name	<input type="radio"/> Product ID	<input type="radio"/> Firmware version
<input type="radio"/> Online	<input type="radio"/> Directory	<input type="radio"/> Asset ID
<input type="radio"/> Comment	<input type="radio"/> Department	<input type="radio"/> Cost center
<input type="radio"/> In service date	<input type="radio"/> Mac address	<input type="radio"/> Serial number
<input type="radio"/> Site	<input checked="" type="radio"/> Boottime (Absolute)	<input type="radio"/> Boottime (Relative)
<input type="radio"/> Firmware Update (Relative)	<input type="radio"/> Partial Update (Relative)	<input type="radio"/> Total operating time
<input type="radio"/> Profile Assignment	<input type="radio"/> Monitor1 serial number	<input type="radio"/> Monitor1 vendor
<input type="radio"/> Monitor1 model	<input type="radio"/> Monitor1 size	<input type="radio"/> Monitor2 serial number
<input type="radio"/> Monitor2 vendor	<input type="radio"/> Monitor2 model	<input type="radio"/> Monitor2 size
<input type="radio"/> Flashplayer	<input type="radio"/> Device serial number	<input type="radio"/> Network speed

Figure 13: Search Parameters for Thin Clients

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 thin client, 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** in the navigation tree and can therefore be processed or reused easily.

Views (page 97) function very similarly to search queries. Here too, various criteria can be linked and the query saved. Unlike with search queries, however, **views** are available to all UMS administrators together – depending on their authorizations. **Views** can also be taken into account when defining *planned tasks* (page 105).

4.1.11. Deleting objects in the UMS / recycle bin

With the IGEL Universal Management Suite from Version 4.07.100 onwards, you can also move objects to the **recycle bin** instead of permanently deleting them straight away. The recycle bin is enabled or disabled globally for all UMS users.

- Enable the recycle bin in the administration area under **Additional Settings>Enable Recycle Bin**.

If an object in the structure tree is deleted (**Delete** function in the symbol bar, in the context menu or the **Del** key), it will be moved to the recycle bin following confirmation.

If the recycle bin is active, objects can also be deleted directly and permanently by pressing **Shift-Del**.

Directories are moved to the recycle bin along with their sub-folders and all items and can therefore be restored again as a complete structure. You will find the UMS recycle bin as the lowest node in the UMS console structure tree. Items in the recycle bin can be permanently deleted there or restored. To do this, bring up the context menu for an item in the recycle bin.

If you cannot bring up the context menu for items in the recycle bin, the recycle bin is probably inactive. Check the status of the recycle bin as described above.

Virtually all items from the UMS structure tree can be moved to the recycle bin: thin clients, profiles, views, tasks, files and their directories. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history items can only be deleted permanently (with **Shift-Del**). The highest nodes in the structure tree cannot be deleted either. However, this procedure will affect all deletable items beneath this node!

- Objects in the recycle bin cannot be found via the search function or views and cannot be addressed by planned tasks.
- Thin clients 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 along with all assigned profiles from the recycle bin.
- The fact that profiles in the recycle bin are no longer effective means that the settings for thin clients may change. Profiles previously assigned to thin clients 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.

4.2. The IGEL UMS Administrator

The IGEL UMS Administrator application is only available on one UMS Server as this makes it possible to intervene directly in communications between the services. It allows basic data such as the ports used or data sources connected to be edited. These functions are not available in the administration area of the console.

The Administrator's server configuration can be exported and imported again for backups via **File**. You can change the language of the Administrator tool under **File>Settings>Language**.

The authorizations for changing settings depend on whether a person is authorized to change IGEL UMS files on the server system. When using the IGEL UMS Administrator, you should therefore use the same user account as you did when you installed the UMS.

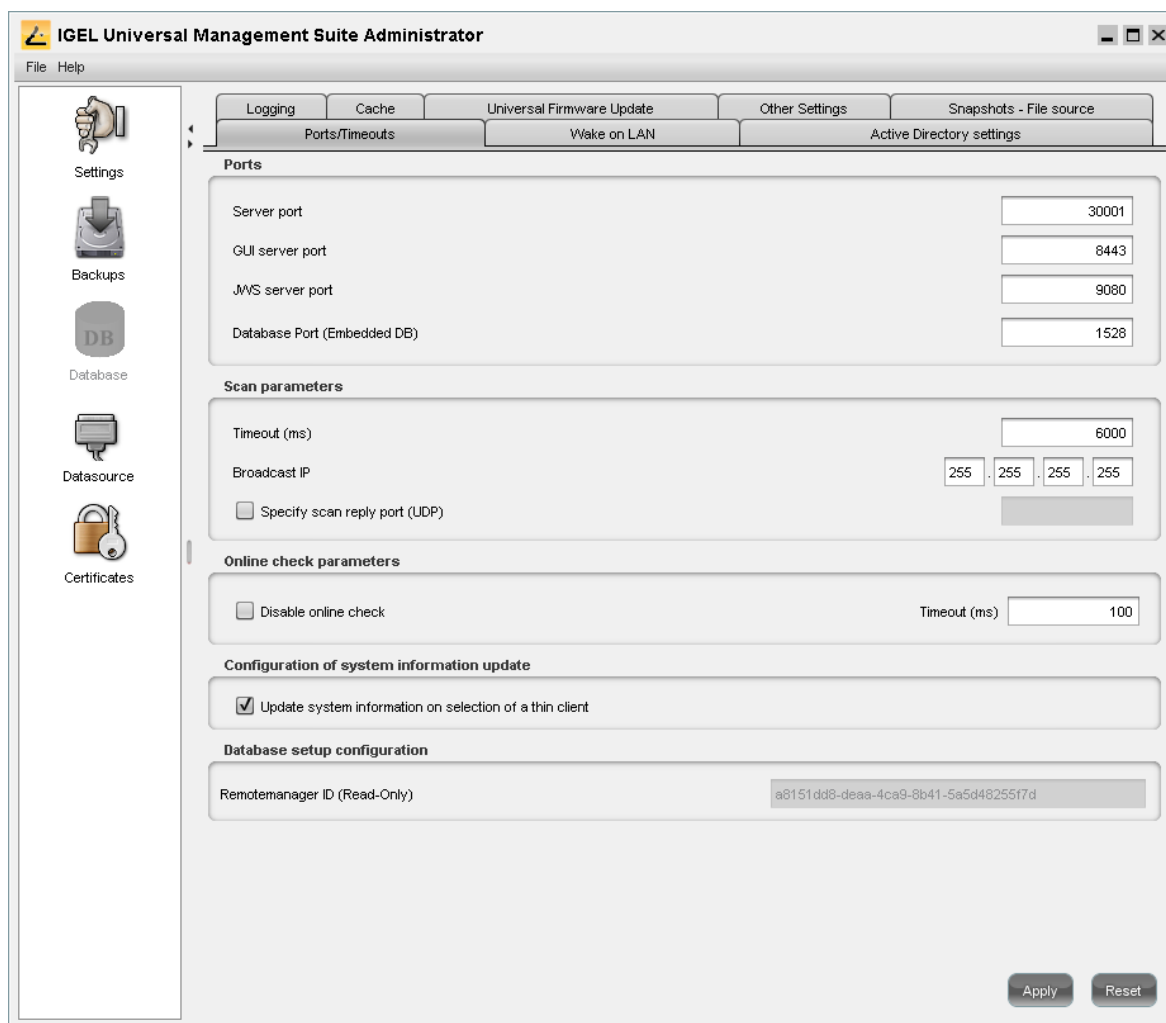


Figure 14: UMS Administrator

4.2.1. Server settings

Using the UMS Administrator, you can change various server settings.

Ports/time limits

When the application is launched, the **Settings** window of the UMS Administrator will be displayed. Here, you can specify the ports to be used by the UMS and other related settings such as the time limit etc.

The IGEL UMS server uses these open ports for incoming queries:

Port name	used by	Task
Server port	TC server	The thin clients connect to this port. The default port is 30001. It can be changed here.
GUI server port	IGEL UMS Console	Establishes the connection to the server. You must enter this port in the logon window of the IGEL UMS Console, the default number is 8443.
HTTP port	Java Web Start interface	If you would like to use Java Web Start, you must specify this port in the connection URL, e.g. <code>http://hostname:9080/start_rm.html</code> . The default port for the UMS TC web server is 9080.
DB port		Communication with the Embedded DB takes place via port 1528, for external databases you can set the port under Data Sources .

- Activate **Allow SSL Connections only** in order to encrypt network traffic to and from IGEL UMS. If you do, Java Web Start will only work with the GUI Server port (default 8443).

Do not activate **Allow SSL Connections only** if you have thin clients with Windows Embedded 7 before version 3.08.100 running and want to use Universal Firmware Update. Those older Windows firmwares do not support updates via HTTPS.

In the **Scan Parameters** area, the following values can be configured:

Time out	This parameter specifies how long the IGEL UMS will wait for a response to scan packets that were sent to the network. The value is given in milliseconds and is set to 6000 by default.
Broadcast IP	Broadcast address that is used for scan packets. 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. The default setting here is 255.255.255.255. Under normal circumstances, this does not need to be changed.
Specify scan reply port (UDP)	Allows you to specify a set port via which the thin clients respond if you use UDP for scanning. If TCP is used, this port is not needed because the response is given via a configured socket. If you leave the default setting and do not specify a port, the application will select any free port.

In the **Online Status Check Parameters** area, **Time Out** specifies how long the system will wait for a response to an online status query message. The IGEL UMS Console attempts to contact all thin clients that are currently visible in the console. Each thin client in this area must respond to the status query in the specified time or will otherwise be flagged as offline. The default value is 100 ms.

To disable the online status check, proceed as follows:

- Select **Disable Online Status Check**.

You can also disable the online check on the UMS Console. The difference in this case is that the function is only disabled for this one console installation.

Further settings

Various other general parameters can be configured here:

Query thin clients	You can restrict the maximum number of simultaneous queries (such as <code>get_settings_on_boot</code>) accepted if for example there are problems with a large number of clients booting at once. In this case, however, it would be better to use a UMS High Availability network in order to distribute client queries across a number of UMS Servers.
Planned tasks	Allows you to define the maximum time allowed for planned tasks.
Change thin client names	In the UMS Console, you can give thin clients a device name. The thin clients have a name within the network – by default, this is <code>IGEL-<MAC address></code> . You can now synchronize both of these: <ul style="list-style-type: none">• Select Change UMS-Internal Name to use the network name of the TC in the UMS.• Select Change Network Name to use the name in the UMS as the device name too.
Automatic registration	Allows you to automatically register IGEL thin clients which boot within the network.

4.2.2. Backups

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. For external database systems, please use the backup and recovery procedures recommended by the DBMS manufacturer. In this case, certificates must be backed up separately.

Creating a Backup

To create a backup, proceed as follows:

1. Click on **Change** next to the **Directory** entry field to change the destination directory.
The file selection window will appear.
2. Specify the storage location for your backups.
3. Click on **Create**.
4. Enter a name for this backup in the pop-up window.

The data will be saved in the directory you have selected.

The certificate files `server.pem` and `server.crt` will also be included in the backup.

Restoring a Backup

Your current database will be overwritten. It is strongly recommended that you create a backup of the current data before another backup is restored.

To restore a saved backup, proceed as follows:

1. Select the desired backup from the backup list.
2. Click on **Restore**.
3. Once your data have been restored, the login data for the database will be displayed.

Deleting a Backup

To delete a saved backup, proceed as follows:

1. Select the desired backup from the backup list.
2. Click **Delete** to remove backups that you no longer need.

Both the entry in the UMS Administrator and the backup file on the hard disk will be deleted!

Backup on the command line

A command line program for creating a backup with batch file scripts is also available. The program is called `embackup.exe` and it can be found in the `rmadmin` directory in the UMS installation directory.

You can launch the program with the following options:

<code>b path/filename:</code>	the path and the name of the backup file that is created
<code>r path/filename:</code>	the backup file with the specified path will be restored in the database
<code>u username:</code>	UMS user name
<code>p password:</code>	Password of the UMS user

Tipp & Trick

See *Planned backup (Embedded DB)* (page 123)

4.2.3. Data sources

The connection to a database system is provided via data sources which you can manage in the UMS Administrator. 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* (page 17)

Setting up a Data Source

1. Click on **Add** to add a first data source or an additional one.

A dialog window will open.

2. Select the DBMS type, the host / port for establishing the connection and the user set up on the DBMS.

More detailed information regarding the supported DBMS can be found in the UMS Data Sheet on the IGEL website and in the UMS HA appendix.

Provided that a data source has not been enabled, these settings can still be changed by selecting **Edit**. The active data source is protected against changes to its configuration. By selecting **Change Password**, you can set a new password for the database user. This is also possible when a data source is active.

3. Click on **Test** to test the connection to the database.

This is also possible when a data source is inactive.

Activating a data source

You can set up a number of data sources. However, only one can be actively used by the server.

To activate this data source, proceed as follows:

1. Select a data source from the list of sources that have been set up.
2. Click **Activate**.
3. Enter the password for the data source that you have selected.

While the data source is being activated, the application checks whether a valid database schema can be found. If no schema is found, a new schema will be created. An out-of-date schema will be updated, and, if the schema contains unfamiliar data, these will be overwritten.

4. Confirm each of these actions.

Warning: Overwriting existing data means that the entire database schema will be deleted and not just the out-of-date tables used by the IGEL UMS.

Copying a data source

To switch from the standard installation with an Embedded DB to an external database system, e.g. an Oracle RAC cluster, proceed as follows:

1. Prepare the new database in accordance with the installation instructions for the UMS.
2. Set up a suitable new data source for this DBMS.
3. Select the Embedded DB data source which is still active.
4. Click **Copy**.
5. Select the destination data source.
6. Start the process after entering the destination login data.
7. Activate the new data source.

Optimizing the active Embedded DB

- Click **Optimize Database** to optimize an active Embedded Database.

The contents of the database will be restructured.

The database index will be renewed in order to speed up database operations.

A message window will appear once the procedure has been successfully completed.

4.2.4. Certificates

Via the **Certificates** window area, you can not only save and restore certificates but also convert them, e.g. from the Remote Manager 2.x format into the current format in each case.

You can also import an exported KeyStore file when reinstalling the IGEL UMS.

5. Thin Clients

The **Thin Clients** node is a key part of the navigation tree. Here, you can organize and manage all devices registered on the UMS Server. This includes IGEL thin clients and external devices installed with UDC.

5.1. Managing thin clients

In the IGEL UMS, you can sort thin clients 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 thin clients in keeping with your company structure.

© Additionally see the training video "Managing Thin Clients" on our TechChannel.

5.1.1. Creating a directory

You can create as many directories and sub-directories as you want in order to group the thin clients together. When you create sub-directories, the thin clients organized in it form sub-groups of a group.

A thin client 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.

To create a directory or sub-directory, proceed as follows:

1. Select a directory, e.g. **Thin Clients**.
2. Click **System>New >New Directory** in the main menu bar
or select the option **New Directory** from the context menu of the selected directory.
3. Enter a name for the new directory.

4. Click **OK**.

The new directory will be displayed directly below the selected directory in the structure tree.

You can now move thin clients to this new directory.

5.1.2. Importing a directory

If you are planning a complex directory structure, you do not need to set it up in a step-by-step manner in the UMS Console. Instead, you can create a `csv` file (e.g. with a spreadsheet program) in which you determine the directory structure and then import the structure from this list.

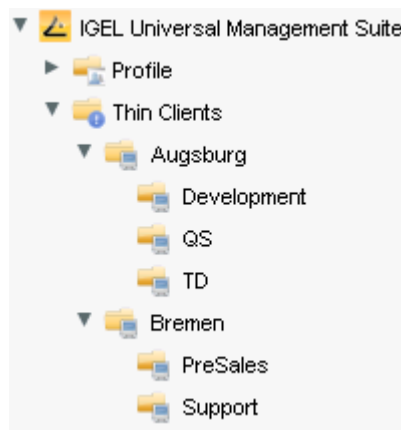


Figure 15: UMS structure tree

The tree structure shown above is based on the following file:

```
Thin Clients; Augsburg; TS
Thin Clients; Augsburg; QA
Thin Clients; Augsburg; Development
Thin Clients; Bremen; Support
Thin Clients; Bremen; PreSales
```

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.

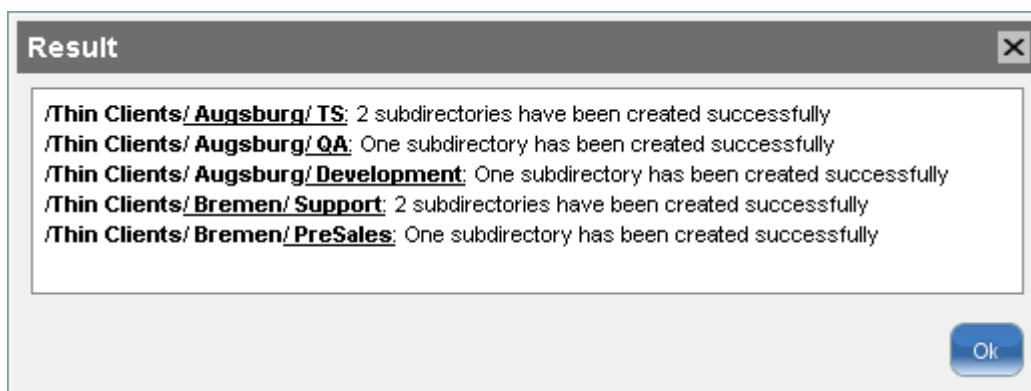


Figure 16: Result of import

5.1.3. Deleting a directory

To delete a directory, proceed as follows:

1. Select the directory that is to be deleted.

Be sure to delete the directory in the structure tree rather than in the content panel of the console window, otherwise the entire directory path will be deleted at the same time.

2. Click **Delete** in the context menu of the directory

or click **Delete** in the tool bar

or press the **Del** button.

A list of all objects that are to be deleted will appear.

If a directory is deleted, all sub-directories and objects such as thin clients, profiles or views contained in it will be deleted too.

3. Confirm that you wish to delete the relevant objects by clicking on **OK**.

5.1.4. Moving thin clients

Drag and drop is the easiest way of moving thin clients from one directory to another:

1. Press and hold down the **Ctrl** key if you would like to select a number of thin clients.
2. Use the **Shift** key to select a row of thin clients.
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 thin client or revoked as a result of the thin client being moved to a different directory, its configuration too will change. The new configuration can take effect either immediately or when the thin client 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**.

5.1.5. Defining rules for stipulated directories

You can define rules for default directories. During the registration process, the thin clients will automatically be allocated to specific directories in the tree on the basis of these rules. They are given the settings of the profiles for these directories. As a result, all you need to do is register the thin clients in order to ensure that they are automatically assigned previously created profiles.

To define rules for default directories, proceed as follows:

1. Select **Misc>Default Directories**.

The list of pre-defined rules will be shown in the pop-up dialog.

2. Click **Add**, **Edit** and **Remove** to add a new rule or edit or delete an existing one.
3. Click the up and down buttons to change the order of the rules.

The order of the rules is important because the first rule satisfied by a thin client determines the directory in which the thin client will be stored.

Creating/editing a directory rule

1. Click **Add** under **Misc>Default Directories** to create a new rule.
Click **Edit** under **Misc>Default Directories** to change an existing rule.
2. Select the directory where the thin clients are to be stored if they satisfy the rule.
3. Enable the option **Overwrites Existing Directory Allocation** in order to re-register in the destination directory a previously registered thin client.
4. Enable the option **Apply Rule When the TC is Booted** in order to move a previously registered thin client to the associated directory in accordance with the directory rule each time its reboots. In this case, there is no need to re-register it

Establishing conditions

With the help of the assistant dialog, you can establish in three steps the conditions which must be met in order to use the rule.

1. Select a search parameter or a selection criterion.

The available criteria are:

- IP address
- Name of the thin client
- Network name
- Product name
- Product ID
- Firmware version
- Network mask

2. Specify the reference value for the criterion.

The possible entry ranges will vary depending on the chosen criterion. Further information on the various entry areas can be found under **Search**.

3. Click **Continue** to proceed.

You will be given an overview of the defined default directory.

4. Enable the option **Further Narrow Down Search** or **Set Further Selection Criterion** in order to define the rule more precisely.

The assistant will once again open the **Select Search Parameter** window.

5. Repeat steps 1 to 3.

6. Click **Finished**.

The new rule will be set up and will be shown in the list.

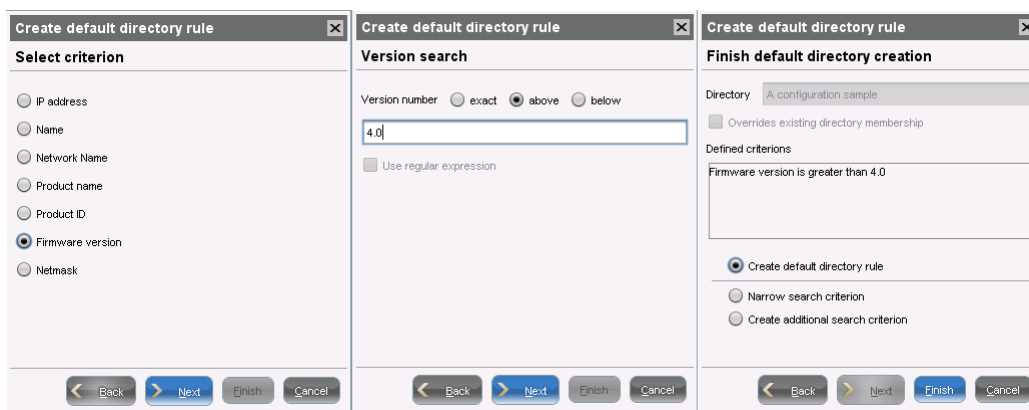


Figure 17: Create default directory rules

Using a directory rule

The rules can be used regardless of new clients being imported or existing clients booting:

- Click **Use** in the directory rule overview.

You can also define how thin clients which do not satisfy any of the rules are to be handled. You can leave them in the current directory or collect them in a specific other folder.

Examples

First example:

Assigning a thin client to a directory on the basis of device data

A thin client satisfies this rule if it is a UD3 device with a firmware version higher than 4.0 and the IP address comes from the 10.201.0.x range.

Modify Default Directory Rule

Select a Directory

- Thin Clients
 - Augsburg
 - Bremen
 - A configuration sample
 - CE Devices
 - ES Devices
 - LX Devices
 - IGEL-00E0C54EE5CE

AND

Criterion	Operator	Value
Product ID	like	UD3.*
Firmware version	greater t...	4.0
IP address	like	10.201.0.*

OR

Overrides existing directory membership

Apply rule when TC is booting

Ok Cancel

Figure 18: Change default directory rule

Second example:

Assigning a thin client to a directory on the basis of network masks

If a thin client is registered in the IGEL UMS, it is moved to a folder which is determined on the basis of the **Network Mask** criterion. If the relevant folder does not exist, it will be created. Because this rule always applies, it is not a good idea to define a further rule. Only the first rule will be effective. If the network mask rule sorts all thin clients into directories, no further rule is active. The relevant folder is determined through this operation:

Folder = IP address AND network mask

IP address	Network 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

Special case – structure tag

The **structure tag** is a special selection criterion for directory rules. A flag of this type can be allocated locally on the thin client or assigned to each thin client via DHCP. If a thin client is registered and returns such a structure tag, it can be stored in the designated directory on the basis of a directory rule. Unlike with "normal" directory rules, the rule with structure tags covers several directories at a time – this makes this solution more flexible and straightforward and provides optimum support when rolling out thin clients automatically.

A Best Practice document regarding the use of the structure tags can be found *here* (<http://edocs.igel.com/index.htm#10202089.htm>).

Requirements:

The following requirements must be met if a thin client is to supply the information regarding storage in a specific directory.

- IGEL UMS 4.08.100 or newer
- Client with IGEL Linux 5.05.100 or newer or with Microsoft Windows Embedded Standard 7 3.11.100 or newer
- Structure tag is assigned to the client manually or via DHCP

Assigning a structure tag to the thin client:

- Automatically via DHCP: Use Option 226 of your DHCP server in order to supply the thin clients in the network with the desired structure tags. The client then passes on the tag to the UMS Server upon registration.
- Manually on the thin client: You can also allocate the structure tag during manual registration from the thin client. See IGEL Linux remote administration.

5.2. Configuring thin clients

You can configure a thin client via the UMS in the following ways:

1. Via **Navigation Tree > [Thin Client Context Menu] > Edit Configuration**: Here, you can edit the client setup as you would if you were working at the device itself.
2. Via a *profile* (page 63): You assign part-configurations to the client via a profile.
3. Via shadowing with *VNC* (page 57): By shadowing the client, you can work in the setup on the device itself.

You can edit the thin client configuration locally in the client setup or directly for this client in the IGEL UMS:

- Double-click on the thin client in the navigation tree
 - or select **Edit configuration** from the menu / context menu
 - or select the corresponding symbol from the symbol bar.

The thin client setup dialog in the UMS and the profile configuration procedure are structured in the same way as the local setup application. Details of this are set out in the relevant system manual.

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 thin client will automatically retrieve its settings each time it boots.
 - **Immediately**: The settings will be transferred to the thin client immediately.

If the thin client is not switched on, this operation cannot be performed and the thin client 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`.

5.2.1. Copy session

You can copy a session in the configuration dialog of a thin client. This creates a duplicate with all properties of the original session.

To copy a session, proceed as follows:

1. Open the configuration dialog via **Navigation Tree > Thin Clients > [Directory]** by double-clicking on the thin client.
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 on .

A duplicate of the original session will be created.

5.3. Shadowing (VNC)

The IGEL UMS Console allows you to observe the desktop of a thin client on your local PC via shadowing with VNC. In order to enable shadowing, you must allow remote access in the security options for the thin client.

➡ See also the Best Practice document *Secure Shadowing* (page 59).

🕒 Additionally see the training video "Shadowing" on our TechChannel.

5.3.1. Launching a VNC session

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 **thin client** from the structure tree.

5.3.2. 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 thin client to your PC. The coding option Tight is particularly useful in a network with a low bandwidth. It contains two additional parameters: <ul style="list-style-type: none"> • Compression level: The higher the compression, the longer the computing operation takes! • JPEG quality: If you select Off, no JPEG data will be sent.
Use Draw Rectangle Method	This option improves performance. However, artifacts may be encountered.
Color Depth	8 or 24 bits per pixel
Update Period	Time period between two updates. A longer time period reduces network traffic, but the update may not be seamless. Please note: An update query will be sent as soon as you move the mouse or enter a key in the VNC Viewer. This event will be passed on to the remote host.
Save Properties as Standard Values	Saves the current settings as standard values for future VNC sessions.

You can specify an external VNC viewer program from another provider in the UMS Console:

- Click **Misc>Settings>General**.

To pass on the IP address of the thin client to an external application, add the parameter `<hostname>`.
Example:

External VNC viewer: `C:\Program Files\TightVNC\vncviewer.exe <hostname>`

5.3.3. External VNC viewer

You can specify an external VNC viewer program from another provider in the UMS Console:

- Click on **Misc>Settings>General**.

To pass on the IP address of the thin client to an external application, add the parameters `<host name>` and `<port>` in **External VNC Viewer**.

Examples:

- **TightVNC:** `"C:\Program Files\TightVNC\tnvviewer.exe" <host name>:<port>`
- **UltraVNC:** `"C:\Program Files\uvnc\UltraVNC\vncviewer.exe" -connect <host name>:<port>`
- **RealVNC:** `"C:\Program Files\RealVNC\VNC Viewer\vncviewer.exe" <host name>:<port>`
- **TigerVNC:** `"C:\Program Files\TigerVNC\vncviewer.exe" <host name>:<port>`

Place the program path in double quotation marks as shown above to ensure that the call works even if there are spaces in the path.

5.3.4. Secure Shadowing (VNC with SSL/TLS)

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

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 authorizations) can shadow clients.

Direct shadowing without logging on 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.

➔ Further information regarding secure shadowing can be found in the best practice document.

5.4. Firmware licenses

IGEL thin clients from the Universal Desktop product range (e.g. UD5) are supplied with an installed license. This license enables you to use various firmware functions and is linked to the MAC address of the thin client. Manually created thin clients or hardware from other manufacturers "converted" using the UDC may not have a license. The license must therefore be added to the firmware later on. Upgrade licenses too can be rolled out later on using the UMS license management system.

5.4.1. License management

Under **System > License Management**, you manage your licenses and the hardware associated with the licenses.

Under **IGEL Licenses**, you can filter based on licenses. The selection criteria are:

- Show all licenses
- Show valid subscriptions
- Show expired subscriptions
- Show subscriptions which will expire in the next
- Show all licenses of thin client
- Show test licenses

If you select **Show subscriptions which will expire in the next**, input fields for months or days are shown:



The screenshot shows a user interface for filtering licenses. It features two input fields: the first is labeled "month(s)" and the second is labeled "day(s)". To the right of these fields is a grey button labeled "Apply".

Under **Hardware**, you can search for thin clients according to defined criteria:

- Click **Export MAC list** to export the MAC addresses of all thin clients, all unlicensed thin clients, or all thin clients selected via a view to a CSV file. You can send this file to IGEL Technology GmbH in order to request a license file for these devices.

You can add the received license file by clicking **Add (+)** in the license management. The license is distributed to the previously selected thin clients at the next start process.

The thin client must be able to contact the UMS server with its fully qualified domain name, e. g. `mytcserver.mydomain.tld`.

5.4.2. UDC2 test licenses

If you are testing the IGEL Universal Desktop Converter 2 (UDC2), please use the normal licensing mechanism. UDC2 test licenses are already linked to your hardware, which is represented by its MAC address.

5.4.3. Distributing UDC2 licenses

The IGEL Universal Desktop Converter 2 includes a USB token with the IGEL Universal Desktop OS as well as a SIM card with the licenses you will need to run this firmware on an intended system.

Install the IGEL Universal Desktop OS 2 on the intended system (see IGEL UDC2 installation manual) and license the software

- by creating a license during installation, or
- by distributing licenses to previously installed systems using the UMS license management feature.

Important: The IGEL Universal Desktop OS 2 must be installed on the intended devices and the devices must be registered on the UMS Server.

To create a UDC2 license, proceed as follows:

1. Insert the SIM card with the licenses into the USB token's card slot.
2. Insert the USB token into the PC on which the UMS Console is installed.

This only applies to the Windows version.

3. If necessary, install the driver for the smartcard reader. You will find a driver on the USB token.
4. Launch the UMS Console application and navigate to **System>Manage Licenses**.

The new window shows license information.

5. Click **Display Licenses from the Smartcard** and confirm that you wish to begin the procedure.

The number and type of available licenses will be shown.

6. Select the unlicensed devices for which a license is to be created.

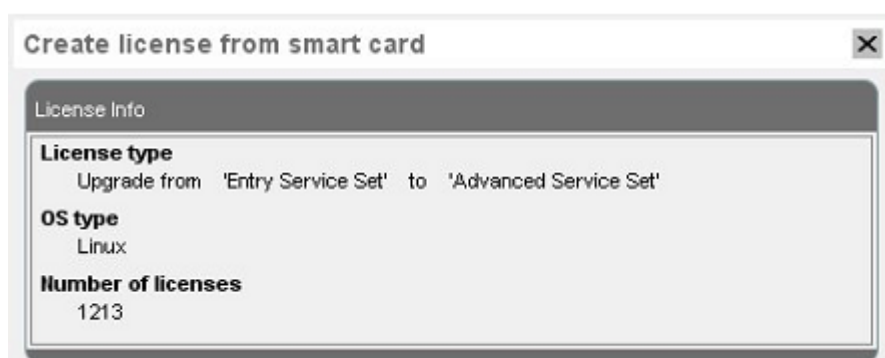


Figure 19: Create licenses from IGEL smart card

A license will be created from the license pool on the stick. After rebooting twice, the device will have the functions provided by the license.

As an alternative, you can send UMS settings to UDC2 devices in order to transfer licenses. Reboot the devices in order to activate the new licenses.

/Thin Clients/IGEL-00E0C560108F		/Thin Clients/IGEL-00E0C560108F	
MAC Address	00-E0-C5-60-10-8F	MAC Address	00-E0-C5-60-10-8F
Product	IGEL Universal Desktop OS	Product	IGEL Universal Desktop OS
Product ID	UC2-X20 LX	Product ID	UC2-120 LX
Firmware	4.01.300.01	Firmware	4.01.300.01
		Last boot time	10/2/09 3:51 PM

Figure 20: License management

- Check whether the device has used the license correctly. The product ID should have changed from X20 to 120, 520 or 720. This depends on the license type (Entry, Standard or Advanced).

In addition, the IGEL thin clients and UDC devices licensed with the IGEL UMS will now be shown in the license management dialog.

Licenses created from the license pool are saved on the token so that you can reuse them if you need to reinstall the IGEL firmware on the device.

5.4.4. Upgrading licenses

When upgrading the license of a UD device, you should use the same mechanism with a USB token and SIM card as you do for UDC licenses.

Upgrade licenses available on a SIM card are displayed along with their license type, e.g. **IGEL Shared Workplace**. The device selection only shows suitable devices, e.g. IGEL thin clients without **Shared Workplace** license.

6. Profiles

Profiles are predefined configurations which can be assigned globally to directories, groups, users or thin clients via the Universal Management Suite. The following types exist:

Standard profiles ...can be assigned to objects (thin clients or users) directly or indirectly via directories. An object 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 thin client.

Master profiles (page 80) ...allow more flexible access rights within the IGEL UMS as they can override the settings for standard profiles and have their own authorizations.

These various profile types can be combined with each other.

Special profile types

User profiles (page 74) Standard and master profiles can be assigned to Active Directory users and thus allow:

- Shared Workplace: Changing users at a workstation
- Roaming Doctors: Changing workstations for a user

Template profiles (page 85) Standard and master profiles can be used even more flexibly and combined with the help of values determined dynamically.

© Additionally see the training video "Managing Profiles" on our TechChannel.

6.1. Order of priority for settings

Parameters set via a profile are blocked in the configuration dialog and indicated by a lock symbol.

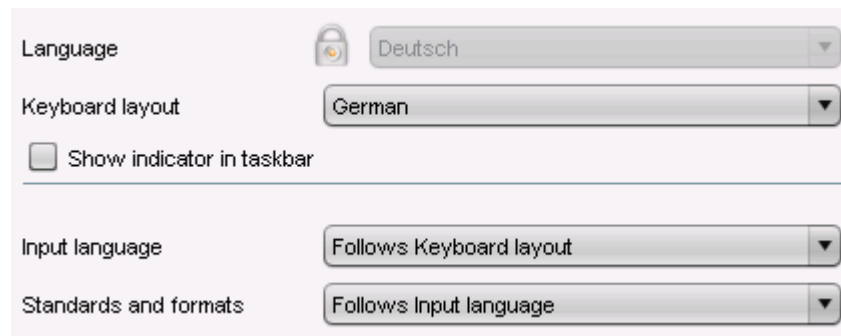


Figure 21: Setting with lock symbol

They can only be edited in the profile. The name of the profile responsible for the locked status will be shown if you move the mouse pointer over the lock symbol.

Each parameter has two value types:

- values determined by the thin client 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 thin client, the value of the parameter will be changed back to its previous thin client value. The profile value will not be copied to the thin client settings.

6.2. Order of priority for profiles

If you have assigned several profiles to a thin client and enabled a specific setting in all profiles, you may like to know which profile provides the valid value for this setting or, in other words, which profile has priority over the others.

Try to avoid enabling the same settings in a number of profiles by setting up separate groups of active parameters for different profiles. Otherwise, the following symbolic rule applies:

The closer an object to which the profile was assigned is to the thin client, the higher the position of the profile is in the hierarchy.

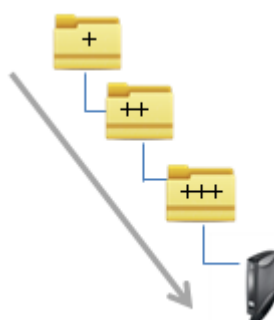


Figure 22: The priority of the standard profiles increases from one level to the next.

Higher priority	than...
closer to the thin client	further away from the thin client
Sub-directory	Higher-level directory

If a number of profiles are assigned to a directory or a number of profiles are assigned directly, the newer profile with the higher profile ID will overwrite the settings.

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 tool tip with the profile ID will be shown.

The lists of assigned profiles and indirectly assigned profiles are sorted according to the order of priority. As far as direct profiles or indirect profiles on a directory level are concerned, profiles higher in the list have higher priority.

6.3. Using profiles

In this chapter, you can learn about the procedure for

- *Creating profiles* (page 66)
- *Allocating profiles* (page 71)
- *Checking profiles* (page 71)
- *Removing assigned profiles from a thin client* (page 72)
- *Overwriting sessions* (page 70)
- *Exporting and importing profiles* (page 67)
- *Configuring profile settings* (page 69)
- *Deleting profiles* (page 72)

6.3.1. Creating profiles

You can create a sub-directory hierarchy in order to organize your profiles:

- Select the Profile node or a sub-directory in the UMS tree structure.

The Profile Directory area contained in it is shown at the right.

To create a new profile, proceed as follows:

1. Select Profile from the menu **System>New**,
or select the corresponding option from the context menu
or import a previously created profile.
The **New Profile** dialog window will appear.

The new profile will be stored in the selected profile directory. If no profile directory was selected, it will be stored in the **Profiles** node itself.

2. Enter a name and a **description** for the profile.
3. Specify whether the new profile should use the settings for an existing profile or thin client.

If you need an "empty" profile that will not use any existing settings, you must select a firmware version for the new profile. In this case, do not select an object from the tree structure.

4. Select the firmware the profile shall be based on.
5. Select one of the possible options:
 - **Activate no settings**
 - **Activate all settings**



Attention! This option blocks all settings in the local setup!

- **Overwrite Sessions**

6. Click **Create** to set up and save the profile.
7. Set your settings.
8. Click **Apply** to save the settings without quitting the profile.
9. Click **Save** to save the settings and quit the profile.

New profile - options

The options in the **New Profile** window have the following meanings:

Activate no Settings	No settings are initially active. You have to enable the desired settings when editing the profile configuration.
Activate all Settings	All available parameters for the profile are enabled. A thin client that receives settings from this profile cannot be configured directly. This option makes sense only if you would like to have all settings for a thin client managed on the basis of this profile.
Overwrite Sessions	Overwrites the sessions defined for the thin client with sessions defined for the profile. If the checkbox is empty, the sessions defined in the profile are added to the sessions which were previously defined for the thin client.

In many cases, profiles which contain all parameters for an item of firmware take up space in databases and backup files unnecessarily. You should therefore use this option only if it seems necessary. In the majority of cases, it is advisable to configure a thin client on the basis of several profiles with specific configuration parts. If firmware has not yet been registered in the database, profiles cannot be created because information regarding the settings which are then assigned to the profile is needed. You can create profiles only with a firmware version which is already registered in the UMS Database.

6.3.2. Exporting and importing profiles

In the IGEL UMS, you can export profile configurations from the database to the file system. This can be helpful for backup purposes or when importing the profile data from one UMS installation to another.

If you have an XML file with profile data or a ZIP archive with several profiles, you can import these to your UMS installation or to an installation other than the original one.

Exporting a profile and firmware

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!

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.

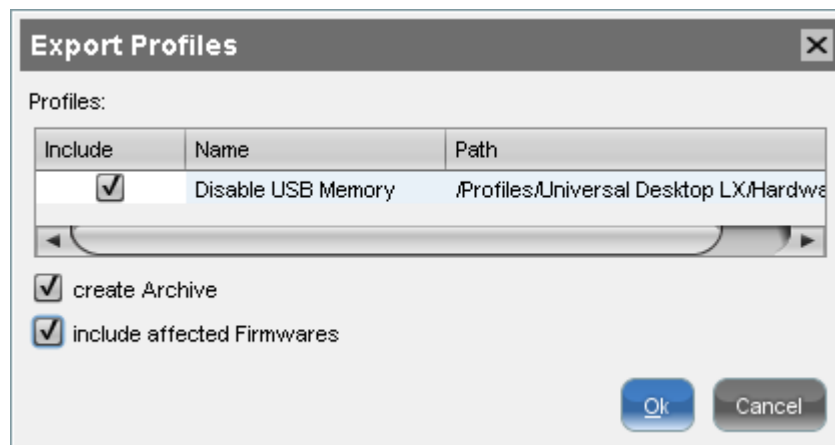


Figure 23: Export profile

3. Select the destination file.

Please note that existing files will be overwritten with the new profile data.

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.

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

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.

6.3.3. Configuring profile settings

The properties of a profile consist of so-called description data and the profile configuration.

Description data consist of the name of the profile, a description text, the firmware version and the overwrite flag for sessions. Example:

The screenshot shows a dialog box titled '/Profiles/Universal Desktop LX/Hardware/Disable USB Memory'. It contains the following fields:

Name	Disable USB Memory
Description	No USB drive available
Based on	IGEL Universal Desktop LX-FTC 4.06.500.01
Overwrite Sessions	<input type="checkbox"/>

Figure 24: Description data of profile

- Edit these data and update them in the database via **Edit>Save Description Data**.

Please note that settings that are not supported in the new firmware will be lost in the profile if you update the firmware of thin clients and you would also like to update the profile assigned to the clients.

To edit the settings for the profile, proceed as follows:

- Double-click a profile
or select a profile in the tree structure and click **Edit>Edit Configuration**.

Paths highlighted in blue in the configuration menu lead to parameters that have already been set via the profile. These are shown with a lock in the thin client configuration.

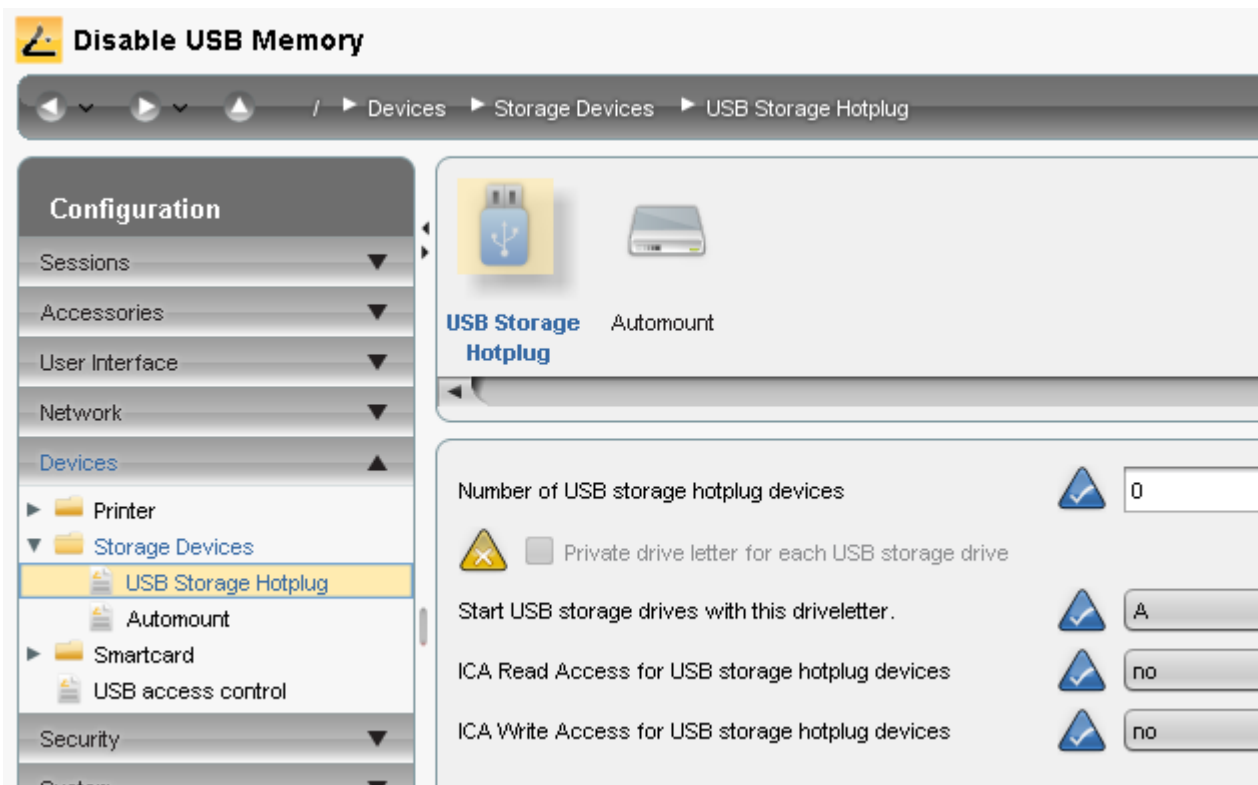


Figure 25: Profile settings

To determine when your changes are to take effect, proceed as follows:

1. Make the required changes.
2. Click **Save**.
3. Decide whether the new settings are to take effect immediately or when the relevant thin clients next boot.

This corresponds to the way the system behaves when the thin client configuration is changed directly.

6.3.4. Overwriting sessions

The **Overwrite Sessions** profile option ensures that only the sessions for this profile are created on the thin client. Sessions created in other profiles or directly in the thin client configuration are disabled.

If a number of profiles with the **Overwrite Sessions** option enabled are assigned (directly or indirectly) to a thin client (or Shared Workplace user), the profile with the highest priority "wins", i.e. only the sessions for this profile are available on the thin client.

Exception: If the highest-priority profile with the option enabled is a standard profile and if *master profiles* (page 80) with sessions are assigned to the thin client or user, the thin client will receive all sessions of the overwriting standard profile and the master profiles – sessions in master profiles can only be overwritten by a master profile.

6.3.5. Allocating profiles

If you have created a profile and changed its settings, you can assign it to the thin clients. You can assign an unlimited number of profiles to each thin client.

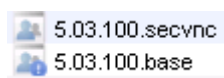
Fundamentally speaking, there are two modes of assignment: **direct** or **indirect**.

Indirect means that you assign the profile not to an individual thin client but to a thin client directory and all thin clients in this directory take on the settings for this profile (see *Order of profiles* (page 64)).

Please note the following rules:

- If you assign a profile to a directory, it is **indirectly** assigned to each thin client in this directory including the sub-directories.
- If you subsequently move a thin client to this directory, the directory profiles will affect this thin client too.
- If you remove a thin client from this directory, the profile will no longer influence this client.

Assigned profiles with configuration changes not yet transferred to the thin client are flagged with an exclamation mark in the list of assigned objects:



6.3.6. Checking profiles

If you have assigned a profile to a thin client, check the results:

1. Select a thin client and click **Edit>Edit Configuration**.

The current configuration for the thin client will be displayed.

A lock symbol will be shown in front of each overwritten setting, i.e. in front of an active setting for an assigned profile. The value that you have specified in the profile will be shown. You cannot change the setting here.

2. Move the mouse over the lock symbol.

A tool tip will show the profile from which the parameter value was taken. This is useful if you have assigned more than one profile to the thin client. 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 thin client, profile or assigned file, or edit the configuration.

- Select an object.
- Click the **Edit** symbol to edit the object.
- Click the **Navigate** symbol to navigate to this object in the tree structure.
- Double-click an assigned object to jump straight to it.

6.3.7. Removing assigned profiles from a thin client

You can remove assigned profiles from a thin client or a thin client directory:

1. Select a thin client or a thin client directory in the **Profiles** window area.
2. Click the **Remove** symbol.
or
3. Select an assigned profile from the list in the window area for a thin client or a directory in the **Assigned Objects** area.
4. Click the **Remove** symbol.

This profile will now no longer affect the individual thin client(s) in the directory. The overwritten value for the settings is reset to the value which was valid before the profile was assigned.

6.3.8. Deleting profiles

If you would like to delete a profile, you have the following options:

1. Select the profile in the UMS navigation tree.
2. In the symbol bar, click on the **Delete** symbol
or press the **Del** button on your keyboard
or 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 thin client or every thin client directory to which it was assigned. The profile values no longer affect the thin client settings. In addition, all settings for the profile from the database will be deleted.

6.3.9. Compare profiles

IGEL Universal Management Suite 5 introduces a new feature that enables you to compare two profiles side by side.

Follow these steps to compare two profiles:

1. Select two profiles, holding down the **Ctrl** key.
2. Right-click one of these profiles.
3. Choose **Compare Profile Settings ...** from the context menu.

The Compare Profile Settings view opens.

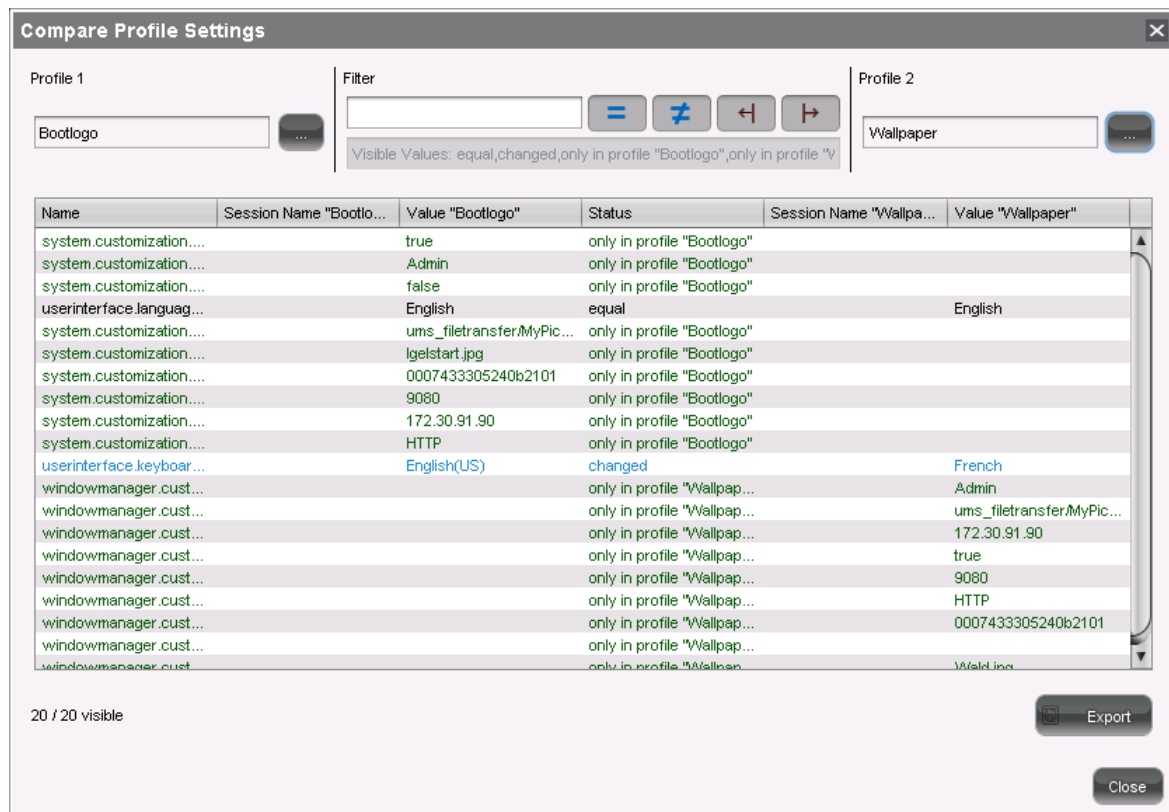


Figure 26: Comparing profiles

The default view lists all settings from both profiles. Use the following buttons to filter the view:



Toggle visibility of settings that are equal in the profiles.



Toggle visibility of settings that are not equal in the profiles.



Toggle visibility of settings that are only present in profile 1.



Toggle visibility of settings that are only present in profile 1.

- Click these buttons to deactivate a filter.
- Click these buttons to activate a filter again.



inactive active

- Activate or deactivate several filters at once.
- Click **Export** to save the comparison view as a CSV, HTML or XML file to your local disk.

6.4. User profiles – IGEL Shared Workplace

IGEL Shared Workplace is an optional feature of the IGEL Universal Desktop firmware which must be licensed separately. It allows user-dependent configuration based on settings profiles created in the IGEL Universal Management Suite and linked to the user accounts in the Active Directory. In the process, user-specific profile settings are passed on to the thin client along with the device-dependent parameters. You will find an overview of the parameters which can be individually configured for a user further on in this document.

Typical applications for Shared Workplace are workstations used for shift work or in call centers, where different staff members use the same device and thus need their own individual settings, such as for session types or mouse-button configuration for right/left-handed operation.

Another possible application is in roaming environments where users frequently switch IT workstations, e.g. in hospitals and at service/ticket counters, checkouts and reception areas. After a user has logged in, the thin client 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 in 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 new UMS High Availability Extension. The high level of UMS Server availability achieved ensures that users receive their own personalized profile at all times.

The IGEL Shared Workplace feature is included in the IGEL thin client firmware from version 4.08.100 (UD-LX) and 2.09.500 (UD-ES) and can be used in conjunction with the new version 4 of the IGEL UMS.

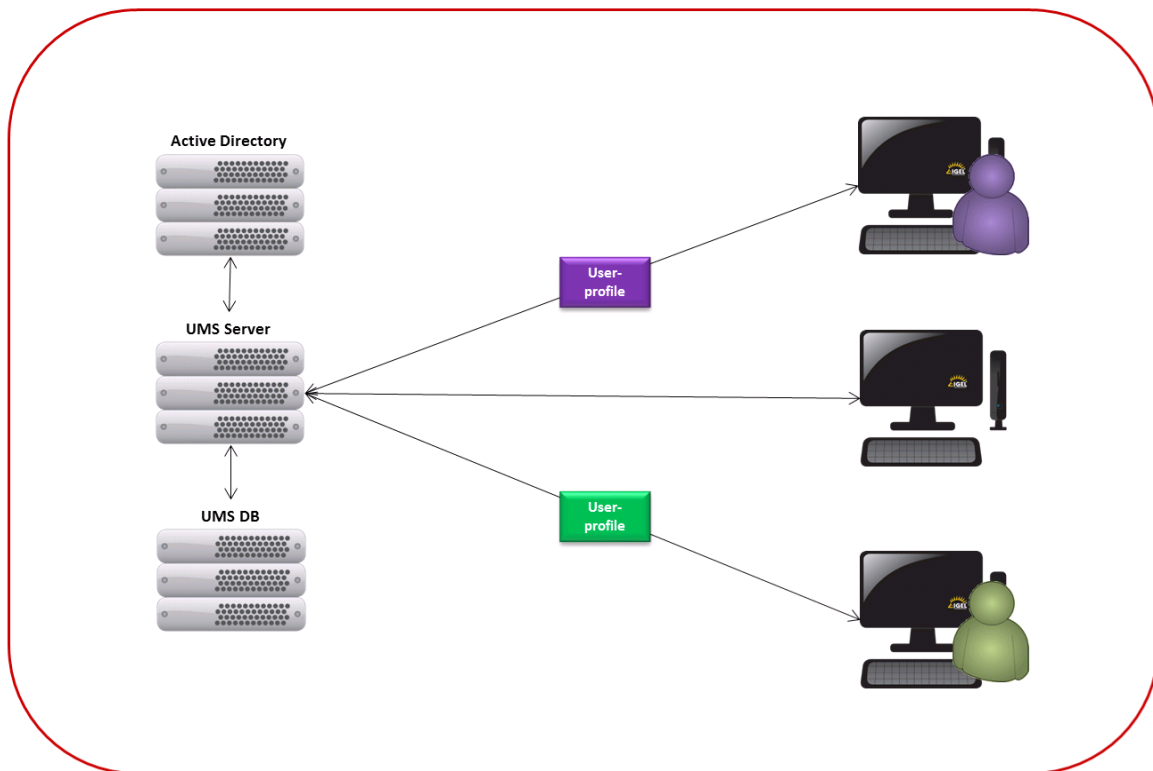


Figure 27: IGEL SHARED WORKPLACE scenario

© Additionally see the training video "Shared Workplace" on our TechChannel.

6.4.1. Setting up and using the feature

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 an Active Directory.
- Thin clients which are to allow user logins must have a license for the IGEL Shared Workplace function. This can be transferred to the thin clients via the IGEL UMS license management system.

If a thin client has been given a license for IGEL Shared Workplace, this cannot simply be canceled. The function itself can be disabled via the list of available services in the thin client configuration, or the facility to log in via IGEL Shared Workplace remains disabled.

- Although not absolutely necessary, the use of the High Availability Extension 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 ES, bear in mind that the default password **user** must be set for the standard user **user**, otherwise it will not be possible to log in.

See also our best practice Display Configuration for Shared Workplace (SWP).

Configuration in the UMS Console

In this chapter, you will find out how to link an Active Directory, assign user profiles, enable the IGEL Shared Workplace, set up the user login/logout and assign priorities.

Linking an Active Directory

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

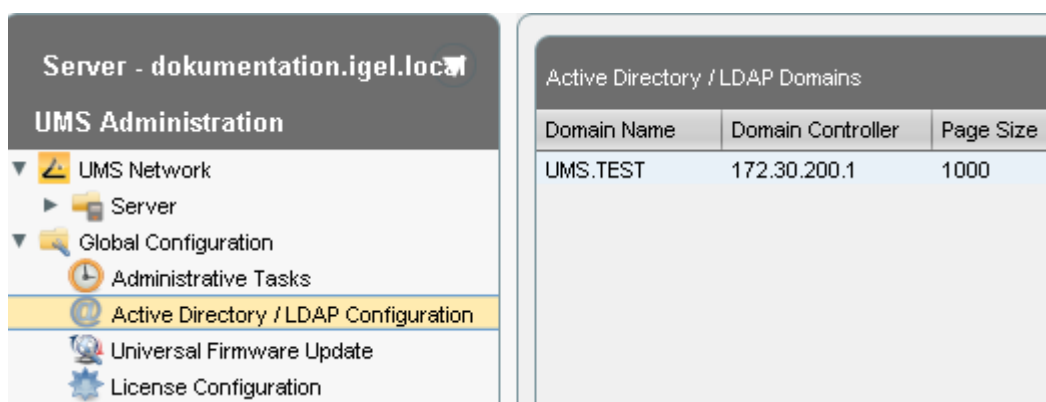


Figure 28: Connect Active Directory

Assigning a user profile

- 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]

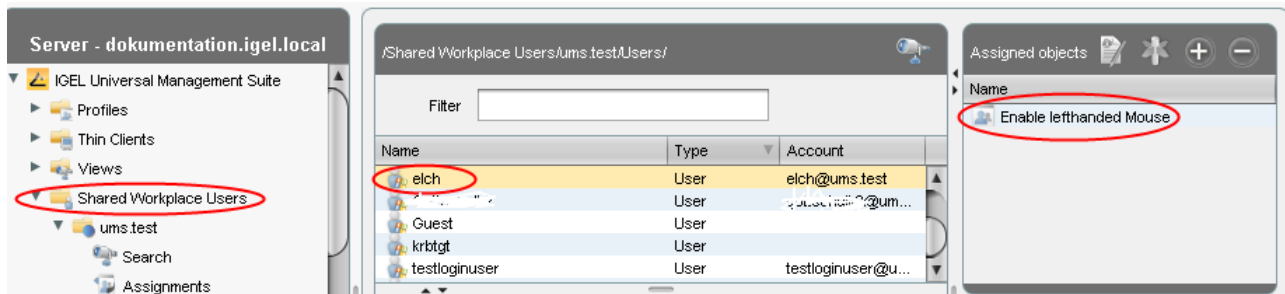


Figure 29: Assign user profile

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

Activating IGEL Shared Workplace

- Activate the IGEL Shared Workplace function for one or more thin clients and define the links for logging out of the system (Linux).
- You can do this by assigning an appropriate profile to the thin client or in the setup for the individual thin client:

Setup/Configuration>Security>Login>IGEL Shared Workplace

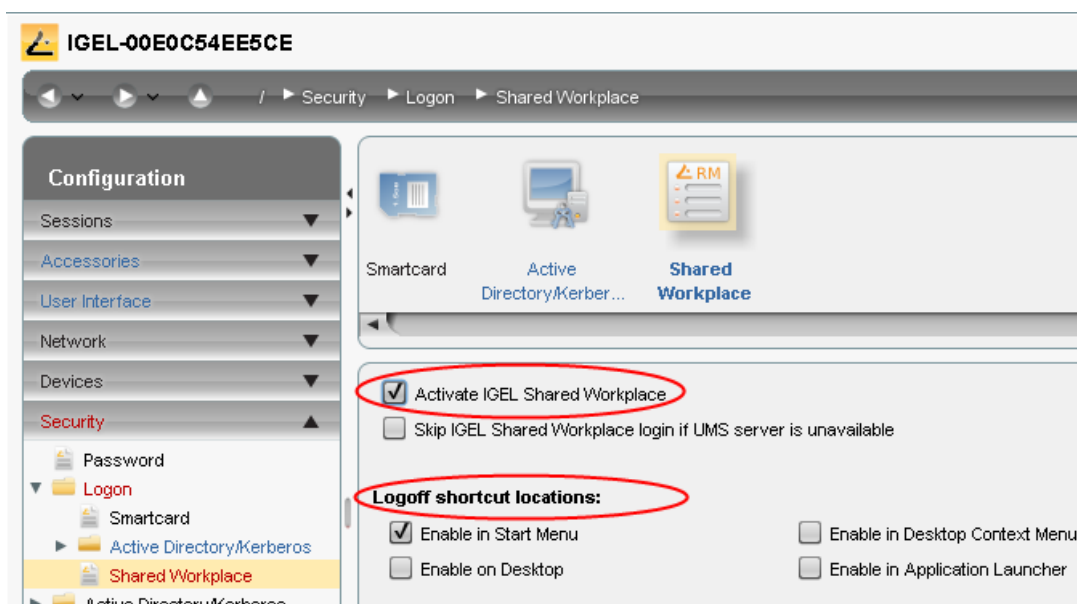


Figure 30: Activate IGEL Shared Workplace

User login

After the next reboot, the thin clients set up for IGEL Shared Workplace will show a login window (provided that they are licensed for this function). A user can then log in at the thin client using their AD login data and will receive the profiles saved for them from the UMS.

The thin client configuration which is actually active for the user logged in is the result of cumulating all profiles which have been assigned either directly or indirectly to the thin client or the user.

Order of priority for profiles

If you allocate a number of profiles, it may be that specific user or client settings are made a number of times. A certain order of priority must be defined for these settings.

The priority of the profiles is as follows:

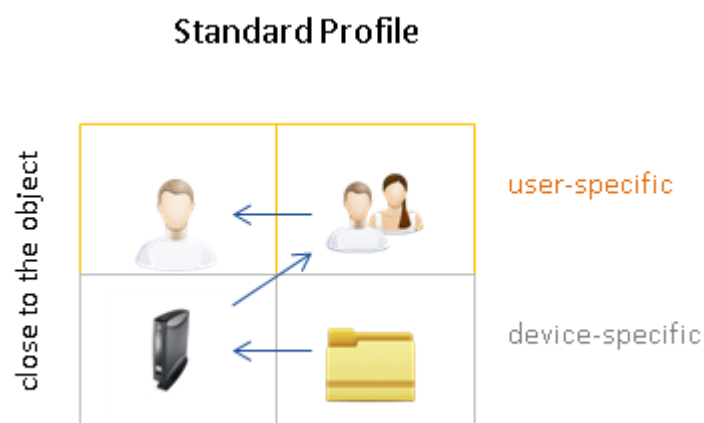


Figure 31: Hierarchy of standard profiles

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

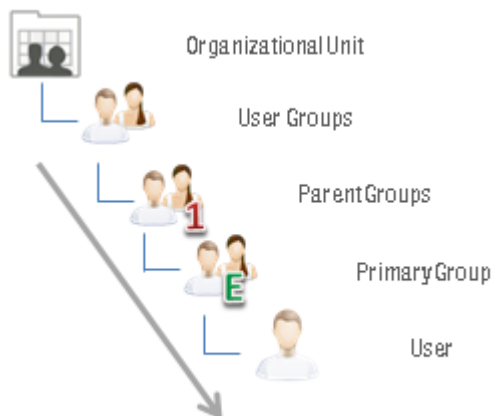


Figure 32: The priority of the standard profiles increases from one level to the next.

Higher priority	than...
primary groups	other groups
other groups	organizational unit

Rules within same levels

- Profiles which are assigned to the user's primary group are prioritized in descending order according to profile ID (highest ID = highest priority).
- Groups within a level are prioritized in alphabetical order.
- Profiles assigned directly to the user/device are prioritized in descending order according to profile ID.

Logout and change of user

As a user, you log out of a thin client with the Windows Embedded Standard system via the start menu.

For IGEL Universal Desktop Linux, you can place buttons for logging out in the **Application Launcher**, on the desktop and in the IGEL Menu.

A hotkey for logging out can also be configured. You will also find these settings under **Setup/Configuration>Security>Login>IGEL Shared Workplace**.

6.4.2. Parameters configurable in the user profile

Not all parameters available in an item of firmware can be configured on a user-specific basis. Whilst, in a number of cases, this is due to technical reasons, there are also instances where it makes sense to configure a parameter only for the device rather than for the user.

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 (page 79)

Universal Desktop Windows Embedded Standard (page 79)

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.

- Touchscreen configuration
- Update settings
- Security settings
- Remote management
- Customer-specific partition
- Server for background images
- Customer-specific boot splash
- 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)

6.5. Master profiles

The aim of introducing master profiles is to be able to reproduce the more complex system of rights management for UMS administrators in very large or distributed environments. Important profile configurations can now be assigned to all registered thin clients on a priority basis without having to revoke the rights of other administrators to manage other settings or profiles.

Master profiles have their own section in the IGEL UMS navigation tree. In terms of their effects, they are identical to standard profiles, but are prioritized differently. Master profiles are profiles whose settings override all standard profiles.



Figure 33: Master profiles in the tree

© Additionally see the training video "Masterprofiles" on our TechChannel.

6.5.1. Enabling master profiles

You can specify yourself whether or not you would like to use master profiles. They are enabled as standard.

To disable the **master profiles** function, proceed as follows:

1. Select **Additional Settings** in the **UMS Administration**.
2. Disable **master profiles**.

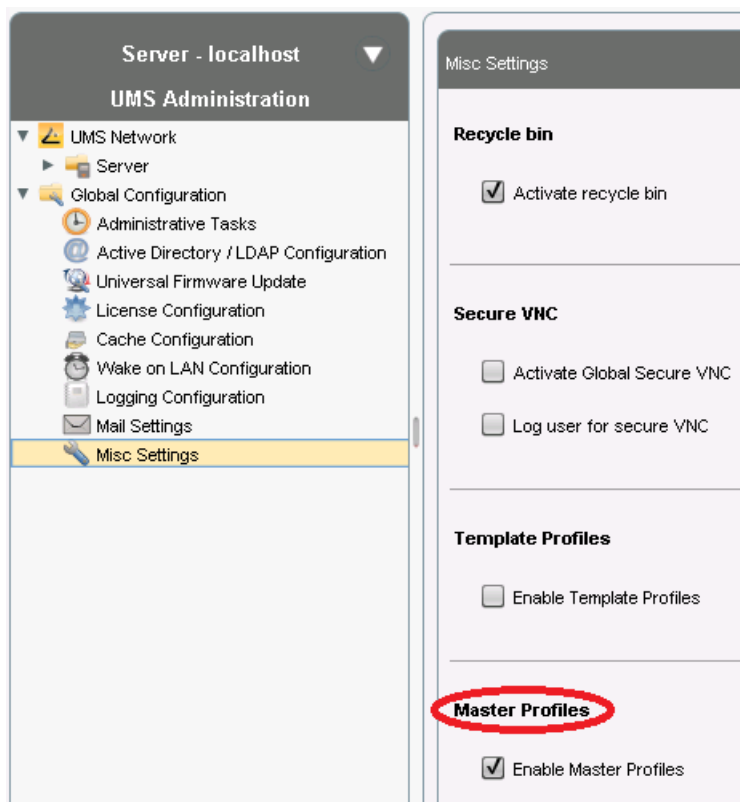


Figure 34: Disabling master profiles

6.5.2. Order of priority for profiles

Master profiles override all standard profiles.

Master profiles are prioritized the other way around compared to the standard profiles. This means that a competing profile setting is prioritized higher the higher up in the hierarchy the profile is assigned, i.e. the further away from the object it is.

The priority of the master profiles is as follows:

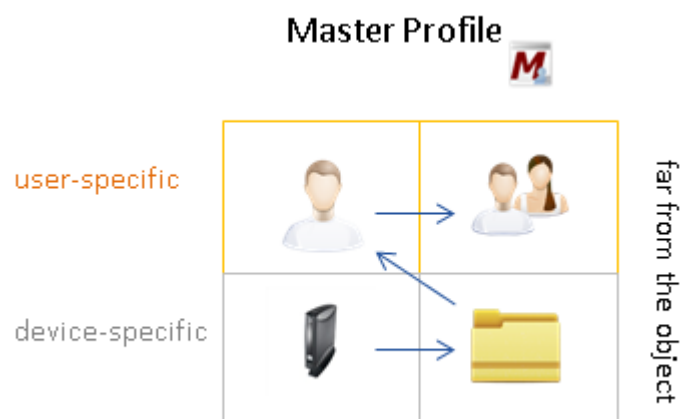


Figure 35: Hierarchy of master profiles

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

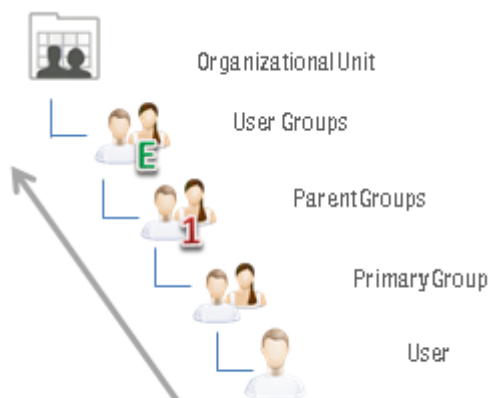


Figure 36: The priority of the master profiles decreases from one level to the next.

Higher priority	than...
organizational unit	other groups
other groups	primary groups

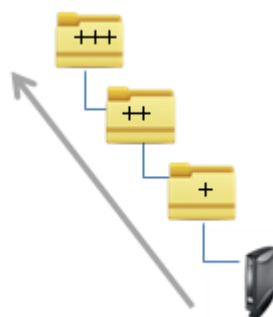


Figure 37: The priority of the master profiles decreases from one level to the next.

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

Summary of priorities in descending order

1. User-specific master profiles ("closer" to the user means lower priority)
2. Device-specific master profiles ("closer" to the device means lower priority)
3. User-specific standard profiles ("closer" to the user means higher priority)

4. Device-specific standard profiles ("closer" to the device means higher priority)

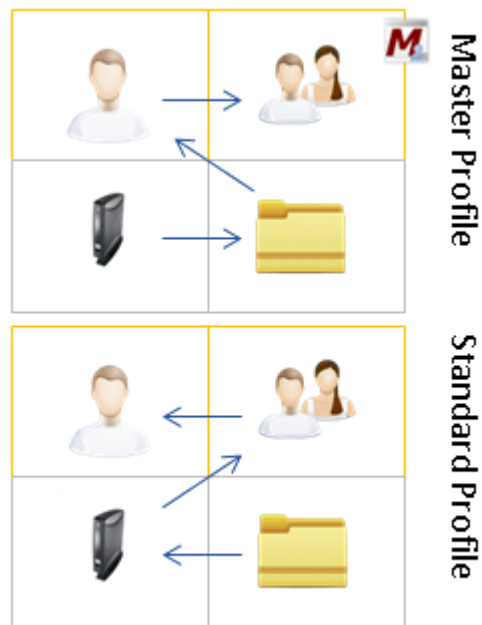


Figure 38: Summary of priorities

Rules within same levels

- Master profiles which are assigned to the user's primary group are prioritized in descending order according to profile ID.
- Groups within a level are prioritized in alphabetical order.
- Master profiles assigned directly to the user/device are prioritized in descending order according to profile ID.

6.6. Template profiles

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



Standard profiles AND master profiles can become template profiles through the use of variables.

Example



A company's thin clients are spread across a number of sites. All clients 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

Up until now, a dedicated profile with global settings and session data would be created for each site. Sometimes, the desired combination of settings can be achieved by passing on various profiles.

Problem

In many cases, the desired settings cannot be combined via various profiles, e.g. for configuring a session. 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 thin clients as well as placeholders, so-called **template keys**. The template keys contain parameters which are to receive divergent values for different clients at different sites.

The template profile is then assigned to the clients directly or indirectly. The site-relevant template values are assigned to the particular clients that are to receive this value.

The thin client thus receives a profile whose settings are made up of fixed data updated in the profile and the template values assigned to it that are referenced by template keys in the profile.

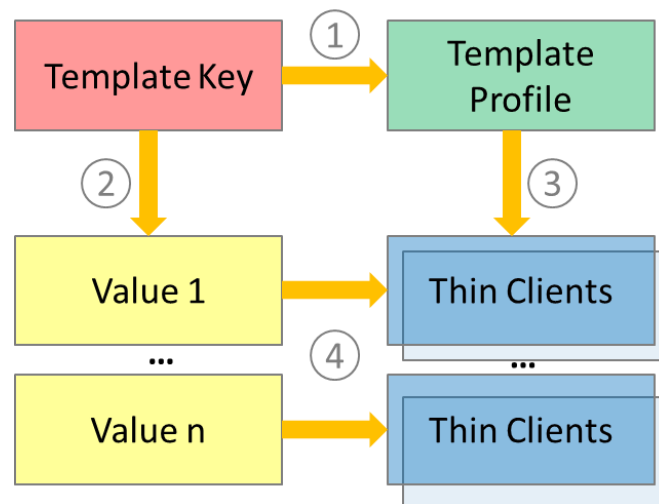


Figure 39: Template profiles functional diagram

1. Template keys are used in one or more profiles.
2. A template key has a number of values.
3. The template profile is assigned directly or indirectly to a number of thin clients.
4. A value from the key can be assigned to one or more thin clients.

A thin client thus receives not only general profile settings but also the template value assigned to it instead of the configuration which is represented in the profile by the associated template key as a placeholder.

© Additionally see the training video "Templateprofiles" on our TechChannel.

6.6.1. Activate template profiles

If you would like to use the **template profiles** function, you must enable it first.

- Enable template profiles in the UMS Console under **UMS Administration>Global Configuration>Misc Settings**

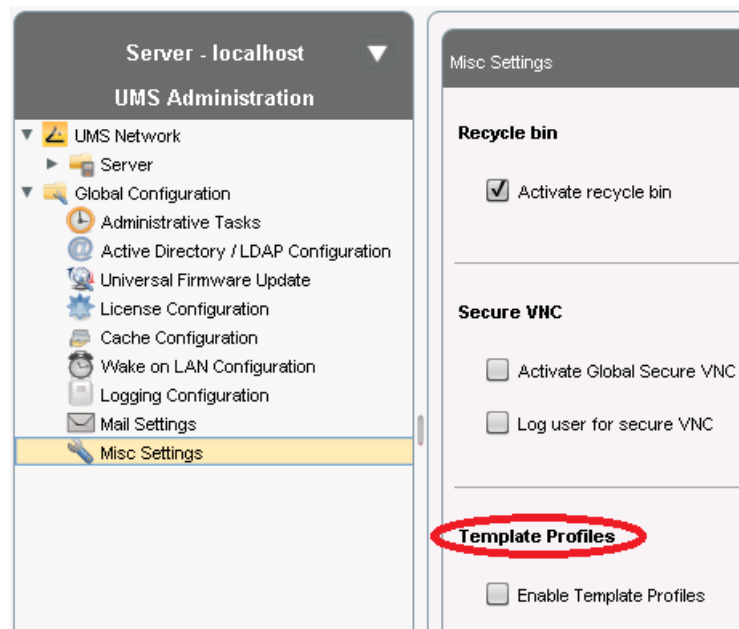


Figure 40: Activate template profiles

The **Template Keys and Groups** node will open in the navigation tree:

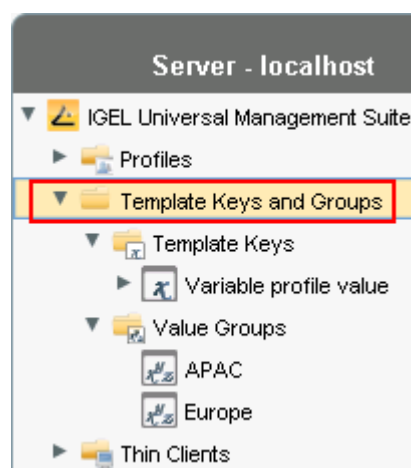


Figure 41: Template Keys and Value Groups

6.6.2. 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 on **New Template Key**.

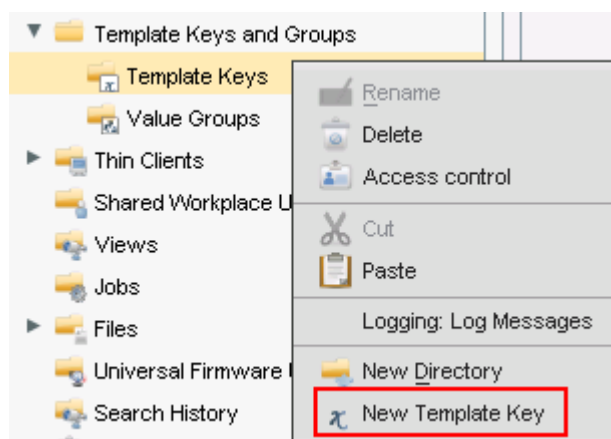


Figure 42: Create new template key

Alternatively, this function is also accessible via the menu **System>New>New Template Key**, the focus must be on the **Template Keys** node.

An assistant will guide you through the steps for creating a new template key:

3. Define a **name** for the key.
4. Select a **value type** for the key (String, Checkbox, Integer or Floating point number).
5. Optionally, give a **description** of the key.
6. Click on **Next**.

Figure 43: Basic data for a template key

To specify the first value of the key, proceed as follows:

1. Enter the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

Figure 44: Create value for the key

To specify further values for the key, proceed as follows:

1. Change the entries under **Value** and **Description**.
2. Click again on **Create Value**.
3. Click on **Finish** to save the key with its values once you have created all desired values.

The screenshot shows a window titled "New Template Key" with a sub-header "Create Values". The "Template Key Name" field contains "Variable Profile Value". Below this is a table titled "Specified Values" with two columns: "Value" and "Description". The table contains three rows: "Value-1" (First value of the key), "Value-2" (Second value of the key), and "Value-3" (Third value of the key). Below the table is a "New Value" section with two input fields: "Value" (containing "Value-3") and "Description" (containing "Third value of the key"). A "Create Value" button is to the right of the "Description" field. At the bottom are four buttons: "Back", "Next", "Finish", and "Cancel".

Value	Description
Value-1	First value of the key
Value-2	Second value of the key
Value-3	Third value of the key

New Value

Value: Value-3

Description: Third value of the key

Buttons: Back, Next, Finish, Cancel

Figure 45: New template keys

The key with its values will be shown in the tree:

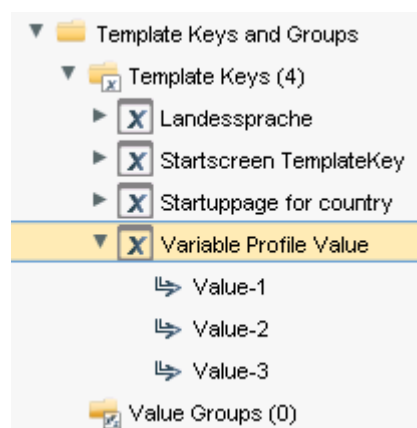


Figure 46: Template key and its values

The recommended workflow is to create template keys and values from the *profile configuration* (page 91).

Create keys and values in the profile

In profiles, specific parameters with a template key can be configured. To do this, combine the following steps to form a workflow:

- *Create template keys and values* (page 88)
- *Use template keys in profiles* (page 93)

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. Configure in the familiar manner the **parameter values** which are to apply to all thin clients with this profile.
4. Select a parameter which is to obtain a client-specific value from a **template key**.
5. Click the activation symbol in front of the parameter until the desired function is active (here: Template key 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.

6. Click on the **selection symbol**  in order to select a template key.
7. Click on **Add**  to create a new template key.

An assistant will guide you through the steps for creating a new template key:

8. Give a **name** for the key.

The **value type** for the key is stipulated by the parameter.

9. Optionally, give a **description** of the key.

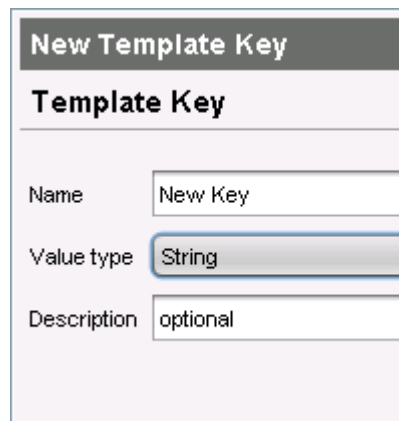


Figure 47: Creating a template key

10. Click on **Next**.

To enter the first value of the key, proceed as follows:

1. Define the desired parameter value in the **Value** field.
2. Optionally, add a **description** of the value.
3. Click on **Create Value**.

In the case of parameters with a fixed value range such as selection menu or checkbox, the available options will be provided for selection. Click on **Add all** to create values for each entry in the value range or **Create Value** to add selected entries only.



Figure 48: Defining a value for the template key

4. Click on **Finish** to save the key with its values.
5. Click on **OK** to return to the profile.

The key will be shown in the profile parameter:

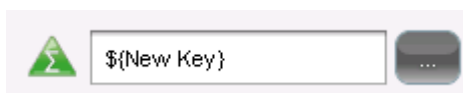



Figure 49: New template key

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: .

6.6.3. Use template keys in profiles

Template keys are listed in the **Template Keys and Groups / Template Keys** node in the navigation tree. They can be moved to their own sub-folders.

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. Configure in the familiar manner the parameter values which are to be shared by all thin clients with this profile.
4. Now select a parameter which is to be supplied with client-specific values from a **template key**.
5. Click the **activation symbol** in front of the parameter until the desired function is active (here: Template key 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.

6. Click on the selection symbol  to choose a template key.
7. Double-click on the desired **template key**.

Alternatively, you can create a new key, see *Create template keys and values in the profile* (page 91).

8. Click on **OK**.
9. **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: .

6.6.4. Assign template profiles and values to the thin clients

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 thin client.

To assign to a thin client 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 thin clients or a thin client directory.
2. Select a **value** for each **template key** used in the profile.
3. Assign the relevant values to the corresponding thin clients.

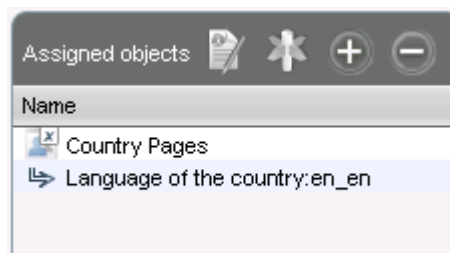


Figure 50: Example of template profile and value assignment



4. Assign further key values to further thin clients. Several values for various keys can also be assigned collectively (**Shift** and **Ctrl** keys).

Each thin client must then have an assigned value for each key in the assigned profiles.

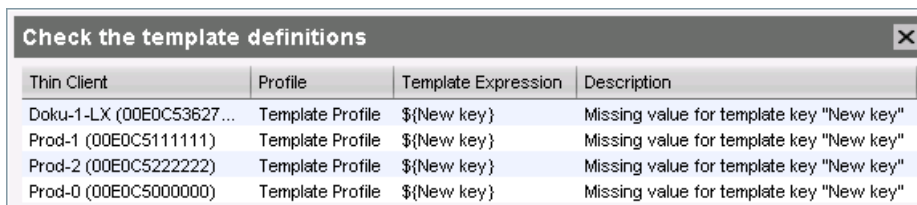
To check that template profiles and values have been assigned correctly, proceed as follows:

1. Click on **Thin Clients** in the top menu bar.
2. Select **Check the Template Definitions**.

The selected and checked thin clients are flagged according to the result:

-  all template keys are defined
-  missing template keys

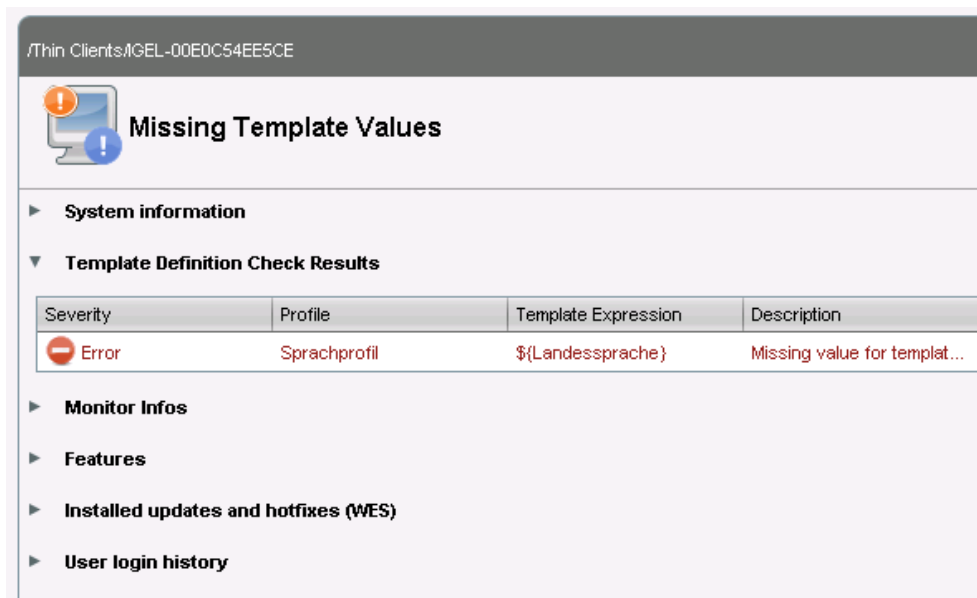
3. Double-click on the message in the message window to open the error log for the check function:



Thin Client	Profile	Template Expression	Description
Doku-1-LX (00E0C53627 ...)	Template Profile	\${New key}	Missing value for template key "New key"
Prod-1 (00E0C51111111)	Template Profile	\${New key}	Missing value for template key "New key"
Prod-2 (00E0C52222222)	Template Profile	\${New key}	Missing value for template key "New key"
Prod-0 (00E0C50000000)	Template Profile	\${New key}	Missing value for template key "New key"

Figure 51: Check log

Or click on a thin client and the results of the check will be shown immediately:



Severity	Profile	Template Expression	Description
Error	Sprachprofil	\${Landessprache}	Missing value for templat...

Figure 52: Results of check on the thin client

As soon as the thin clients receive their updated profile settings (e.g. automatically after restarting the clients), the keys contained in the profile for each thin client will be replaced by the corresponding value from their assignment to the thin client and then transferred to the thin client. The local thin client setup thus receives only the usual parameter values and no more keys.

6.6.5. Value groups

In value groups, logically associated values from various template keys can be brought together and assigned together to thin clients.

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 thin client 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 valid values from each key, multiple selections are possible.

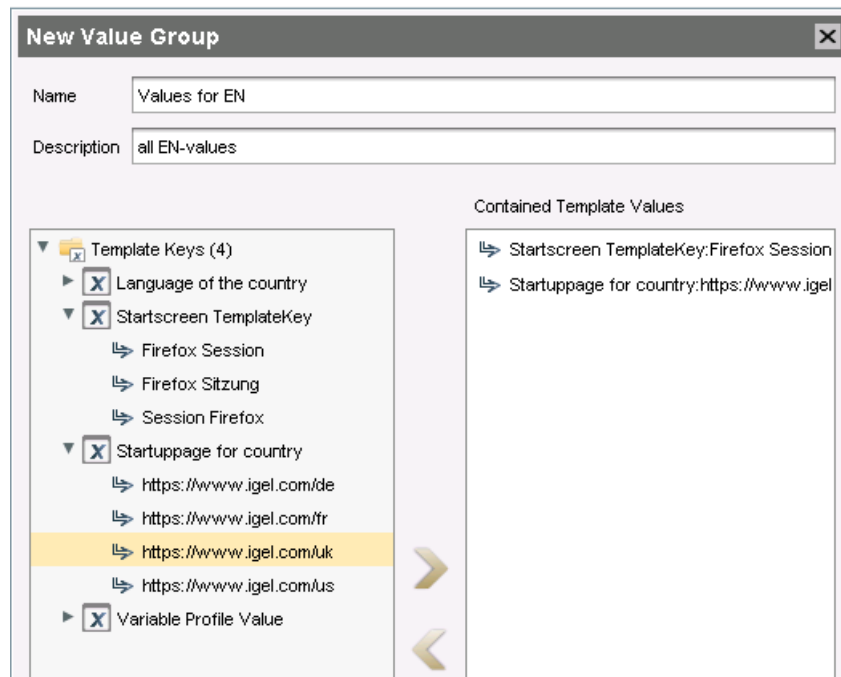


Figure 53: Selecting key values

5. Confirm your settings by clicking on **OK**.
6. Create further groups.

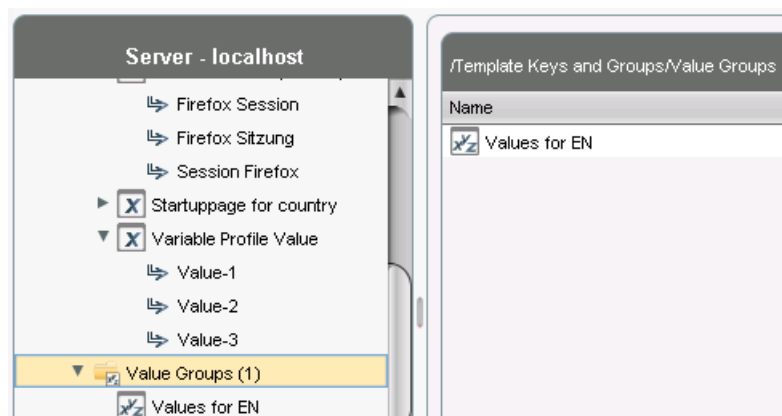


Figure 54: One value group per country

7. Assign the template profile to all thin clients.
8. Assign the appropriate group in each case to the devices.
9. Highlight the **Thin Clients** tree node.
10. Click on **Thin Clients>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 thin clients 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 thin clients. In addition, a better overview is possible if there are a large number of template keys and values.

7. Views

A thin client view is a selection of the thin clients available in the database which is created on the basis of definable rules. All thin clients which satisfy this rule are shown in the **View**.

Example:

You would like to view a list of the thin clients which have an IP address in a specific address range. In order to generate this list, you can create a view whose rule is determined by the IP address range. The views are shown in the UMS tree structure and you can configure access rights for this purpose.

Views not only provide information regarding the database content but can also be used for example to define planned tasks (such as a firmware update) for a specific selection of thin clients. As a result, you do not need to assign the task to individual thin clients that are to be updated. Instead, the devices are determined on the basis of the view, e.g. using the firmware already installed, for the duration of the task.



A view does not make changes to thin client settings or the directory structure of the UMS tree. It merely offers a specific view of the thin clients registered in the UMS.

If you click a **View**, it will be shown as a table in the content panel. You can individually define the type and number of columns.

Defining columns for your **View**:

1. Click the choice button in the edge right above of the window.



2. Choose the column types you want to be shown in the table.

➡ Additionally see the training video **Working with Views** on our TechChannel.

7.1. Creating a new view

To create a new view, proceed as follows:

1. Move the mouse over the **Views** tree node.
2. In the context menu, select **New View**
or select **System>New>New View** in the menu.
The **Create New View** window will open.
3. Give the view a name and a more detailed description.
4. Click **Continue**.
The **Select Search Parameter** window will open.
5. Gradually link together several criteria in a logical fashion.
6. Define the view parameters, e.g. for the firmware under 4.09.100 if you would like to distribute this update and all clients with older firmware are to be updated.
Equal to, **Higher than** and **Lower than** are available as comparative operators. You can also define a regular expression for the search.
7. Click **Continue**.
The **Create New View** window will open.
8. Click **Create View** to finish creating the view
or specify your search in more detail.

In the chosen example, we add a further restriction in the form of the product ID. This makes it possible to narrow down the selection to UD LX devices for which the new firmware is suitable. To do this, select the regular expression `UD.*LX`. This will capture all Universal Desktop Linux-type devices.

7.1.1. Example of how to create a view

The example shows the following individual steps:

1. We give the view a name and a description: Update UDLX, update to 4.09.100 and select a first search parameter: **Firmware version**

Figure 55: Define search parameters

2. We define a first search criterion: below 4.09.100 and select further restrictions: **Next>Narrow search criterion**

Figure 56: Create new view

- As a further search parameter, we select **Product ID** and as a search criterion we define `UD.*LX` and enable **Use Regular Expression**.

The figure shows two screenshots of the 'Create new view' dialog box. The left screenshot is titled 'Select criterion' and displays a list of search criteria with radio buttons. 'Product ID' is selected. The right screenshot is titled 'Text search' and shows a text input field containing 'UD.*LX'. Below the input field are three checkboxes: 'Consider case' (unchecked), 'Compare whole text' (unchecked), and 'Use regular expression' (checked). Both screenshots have 'Back', 'Next', 'Finish', and 'Cancel' buttons at the bottom.

Figure 57: Text search

- We check the **Create View** checkbox and click **Finished**. The result is shown in the content panel.

The figure shows the 'Create new view' dialog box in the 'Finish view creation' stage. It includes fields for 'Name' (Update UDLX) and 'Description' (Update to 4.09.100). Below these is a 'View criteria' section with a text area containing 'Firmware version is less than 4.9.100 AND Product ID is like UD.*LX'. At the bottom, there are three radio buttons: 'Create view' (checked), 'Narrow search criterion', and 'Create additional search criterion'. The 'Finish' button is highlighted in blue.

Figure 58: Finish view creation

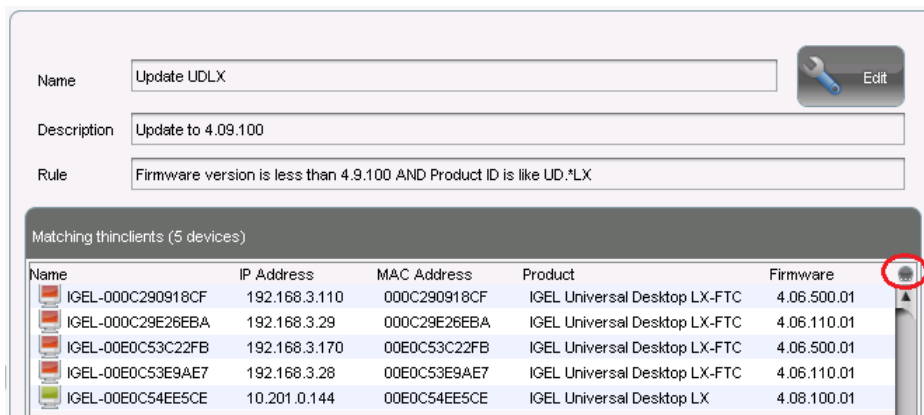


Figure 59: Matching thin clients

- In the results view, we click **Edit** in order to configure the data shown.
The **Edit View** window opens.

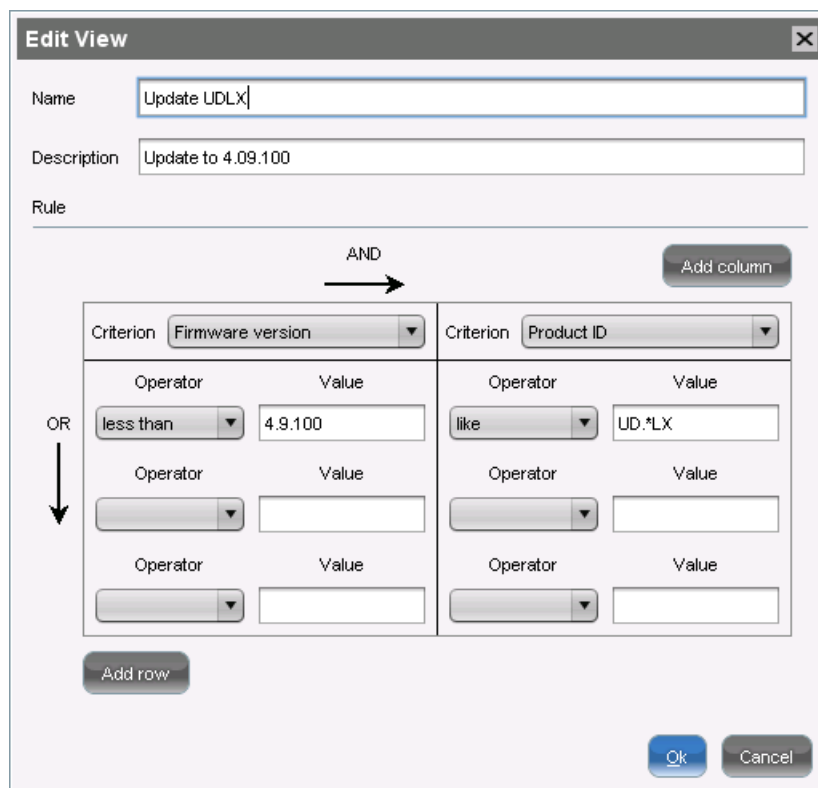


Figure 60: View expert mode

If you would like to enter a number of filter criteria, you can also switch to the expert mode at the start of the creation process. This view allows the quick logical linking (AND/OR) of several criteria and values.

7.2. Saving the view results list

- Select **Save Under**, e.g. in the context menu of a view, in order to save the current view results list in file form. Four file formats are available for the export: XML, HTML, XSL-FO and CSV.

This is an example of an XML file for the above view:

```

<?xml version="1.0" encoding="UTF-8" ?>
- <table>
  <creation-date>2. März 2012</creation-date>
  <caption>Update UDLX</caption>
  <description>Update auf Version 4.09.100</description>
  <columnheader>Name</columnheader>
  <columnheader>IP Adresse</columnheader>
  <columnheader>MAC Adresse</columnheader>
  <columnheader>Produkt</columnheader>
  <columnheader>Firmware</columnheader>
- <row>
  <cell>IGEL-00E0C54EE5CE</cell>
  <cell>10.201.0.144</cell>
  <cell>00E0C54EE5CE</cell>
  <cell>IGEL Universal Desktop LX</cell>
  <cell>4.08.500.01</cell>
</row>
</table>

```

Figure 61: XML export of results

7.3. Send view as mail



Mails can only be sent if you have configured appropriate *mail settings* (page 138) under **UMS Administration > Configuration > Mail Settings**.

To send a view as mail, proceed as follows:

1. Right-click on a **view**.
2. Select **Send View Result as Mail...** in the context menu.

The **Send View Result as Mail...** window opens.

3. Enter the recipient address in the **Mail recipient** field. A number of recipient addresses can be entered, separate them with a ";" (semicolon).
4. Under **Result format**, select the format in which the view is to be sent.
5. Check the **Create archive** box to send the view as a zip file.

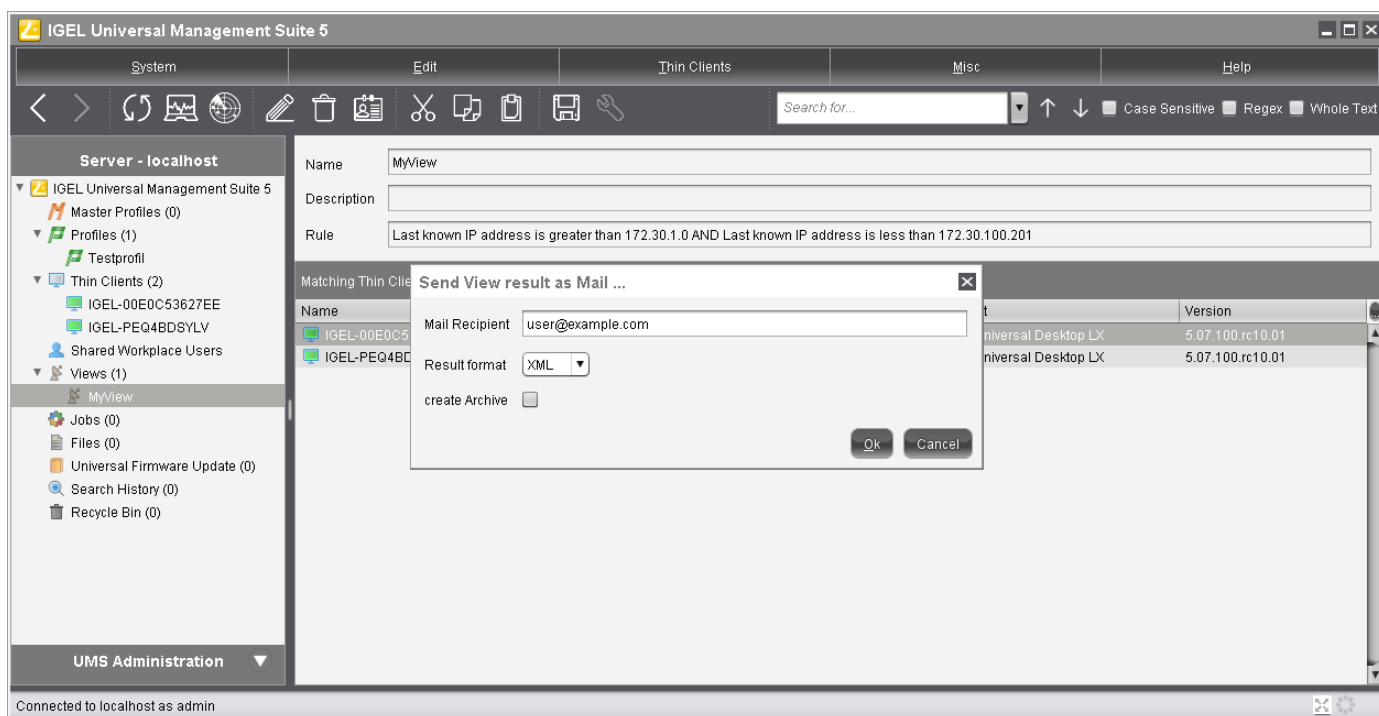


Figure 62: Sending view results via e-mail



You can also send views automatically and regularly as an *administrative task* (page 131).


7.4. Assign profiles to a view

Via the context menu of a view, you can assign on a one-off basis profiles to thin clients that you have filtered via the view. If you want to be certain that the profile is assigned even to newly recorded thin clients that fulfill the view criterion, you can do this using an *administrative task* (page 132).



Using the same principle, you can assign profiles to thin clients that you have filtered via a search.

To assign a profile 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 profiles to the thin clients of the view...** .
The **Assign profiles** window will open.
4. Select the desired profile from the left-hand column and move it to **Selected objects** on the right by clicking on  .
5. Click on **OK**.
The **Time changed** window will open.
6. Select whether the changes should take effect on **Next reboot** or **Now** and confirm this by clicking on **OK**.



Via **Remove profiles from the thin clients of the view...**, you can undo the assignment of profiles.

8. Tasks

Menu path: **Navigation Tree > Jobs**

You can define jobs for the UMS. A job consists in sending a command for specific thin clients automatically at a defined time. Jobs can be repeated at intervals or on specific days of the week.

You have the following options in the context menu for a job:

- **Edit Job:** Opens the **Edit Job** dialog with which you can change settings for the job.
- **Rename:** Opens the **Input** dialog in which you can give the job a new name.
- **Delete:** Removes the job.
- **Clear outdated results:** Removes outdated results.
- **Access control:** Opens the **Access control** dialog with which you can change the rights for the job. Further information can be found under *Object-related access rights* (page 150).
- **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: Log Messages:** Opens the **Log Messages** dialog. Further information can be found under *Logging dialog window* (page 155).
- **Execute Job:** Executes the job immediately.

8.1. Setting up a new task

➤ Select **New Scheduled test jobJob** from the **Context** menu or **System**.

The configuration window contains three tabs:

- **Details**
- **Schedule**
- **Assignment**

8.2. Commands for Tasks

Menu path: **UMS Administration > Navigation Tree > Jobs**

You can define one of the following commands for a job:

- **Update:** Executes the firmware update with the existing settings (Linux).
- **Shutdown:** Shuts down the thin client.
- **Reboot:** Reboots the thin client.
- **Suspend:** Puts the thin client into suspend mode.
- **Update on Boot:** Executes the firmware update when the thin client starts (Linux).
- **Update on Shutdown:** Executes the firmware update when the thin client shuts down (Linux).
- **Wake up:** Starts the thin client via the network (Wake-on-LAN).

- **Settings TC->UMS:** Reads the local thin client settings to the UMS.
- **Settings UMS->TC:** Sends the UMS local settings to the thin client.
- **Download MPlayer Codecs:** Loads codecs for the MPlayer (Linux).



This command is only relevant to IGEL Linux Version 3.x or lower.

- **Remove MPlayer Codecs:** Removes codecs for the MPlayer (Linux).



This command is only relevant to IGEL Linux Version 3.x or lower.

- **Download Flash Player:** Downloads the Flash player plug-in for Firefox (Linux)
- **Remove Flash Player:** Removes the Flash player plug-in for Firefox (Linux).
- **Download Firmware Snapshot:** Executes the firmware update with the existing settings (WES).
- **Partial Update:** Executes the partial update with the existing settings (WES).
- **Update desktop customization:** Updates the desktop background and the boot logo (Linux).

8.3. Details

Name	Name of the task
Command	Command which is executed for all assigned thin clients.
Start date/execution time	Time of first execution.
Active	Tasks can be enabled or skipped as necessary.
Comment	Further information regarding the task.
Back up results	Loggable results are collected in the database. This is not possible with the <code>Wake-on LAN</code> command.
Max. processes	Maximum number of processes executed simultaneously, these processes may thus be executed in block fashion.
Time-out	The maximum waiting time before the UMS sends the command to the next thin client.
Delay	The minimum waiting time before the UMS sends the command to the next thin client.
Retry when booting	Parameter for the update command - clients that are switched off perform the update when they next boot.
Job ID	Internal task number which cannot be changed. This field is empty if a task is new.
User	Name of the UMS user executing the command.

Figure 63: Job details

8.4. Schedule

Start date/execution time	Time of first execution.
Expiry data/time	After this point, no further commands will be executed.
Repeat job	A task 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>Planned Tasks>Public Holiday Lists .
Abort execution	When tasks are executed repeatedly, incomplete tasks can be aborted. No further commands will then be sent to thin clients.

The **Max. processes**, **delay** and **time-out** 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 thin clients 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).

New Job [X]

Details | **Schedule** | Assignment

Execution time: 15:59 Start date: 3/1/12

Expiration date: 3/4/12 Time: 15:59

Repeat Job

Never

Every: 0 day 0 hour

Weekdays: Mon Tue Wed Thu Fri Sat Sun

Exclude Public Holidays: [] [...]

Date	Comment

Cancel job execution

Never

Time: 00:00

Max. duration: 00:00

Ok Cancel

Figure 64: Job schedule

8.5. Assignment

By selecting **Add (+)**, you can assign a task to specific thin clients.

You can also select a thin client directory. The task will then be assigned to all devices located in this directory at the point of execution.

The most flexible assignment can be achieved by selecting devices dynamically with the help of a selected view. At the point of execution, the devices will first be ascertained on the basis of the selection conditions for the view. The tasks will then be assigned to them.

Write authorization for the relevant objects is required in order to set up static thin client 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 task must have write authorization for the relevant thin client. This must be taken into account, even if other users have write authorization for a task and especially if the database user has set up a task.

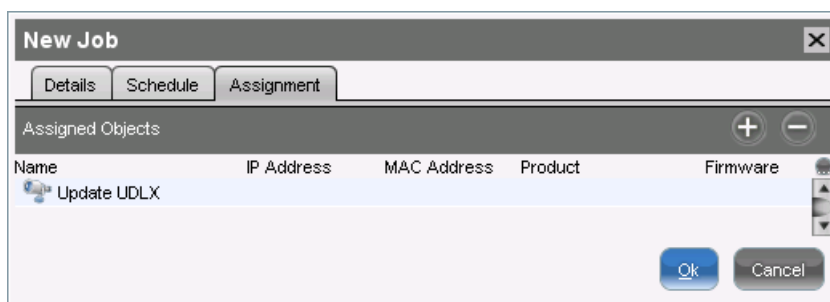


Figure 65: Job assignment by view

8.6. Results

A fourth tab appears in the view for a completed task: **Results**. Here, you are given an overview of the status for the execution of a task. You can select items from the overview using a drop-down list. This results view can be deleted and updated using two buttons. The following status reports are issued by the task message system for the assigned thin clients:

Being executed	The task is currently being executed.
OK	The task is complete, all assigned thin clients have been dealt with.
Out of time	The task was aborted before all assigned thin clients could be dealt with because the abort time or the maximum duration has been reached.
Aborted	The task was stopped for an unknown reason (e.g. server failure).

Thin clients too are given a status for task execution:

Running	The command is currently being executed. The server is waiting for a reply.
Waiting	The task is running, the command will be executed when the next process is available.
Transferred	The command was successfully executed or transferred to the thin client.
Aborted	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 task was reached.

Name	MAC Address	Execution time	Status	Message
Direct assigned configuration	462946923649	Nov 20, 2007 11:27	run next boot	
Factory Workplace 1	432423432432	Nov 20, 2007 11:27	run next boot	
Factory Workplace 2	324320470932	Nov 20, 2007 11:27	run next boot	
Indirect assigned configurati...	003123091023	Nov 20, 2007 11:27	run next boot	
London 1	553453453455	Nov 20, 2007 11:27	run next boot	
London 2	309128308120	Nov 20, 2007 11:27	run next boot	
Manchester 1	0E0490329309	Nov 20, 2007 11:27	run next boot	

Figure 66: Job status list

9. Files

Through a **file transfer**, you can save files in the thin client's local file system. A file must be registered on a UMS Server before it can be sent to the thin client. Examples include virus scanner signatures required locally on the thin client, browser certificates, license information etc.

9.1. Registering a file on the UMS server

A file must be registered on the UMS server before it can be loaded onto a thin client.

To register a file on the UMS server, proceed as follows:

1. In the UMS console, select **System > New > New File** from the menu bar or go to **Files** in the navigation tree and select **New File** from the context menu.
2. Under **File Source**, select a local file or one already on the server.
3. Select the upload location (URL). From UMS 5.01.100, you can only use the directory `ums_filetransfer` or sub-directories created in it.
4. Under **Classification**, select the type of file. This serves to automatically establish suitable storage locations and file authorizations. Choose between:
 - **Undefined**
 - **Web Browser Certificate**
 - **SSL Certificate**
 - **Java Certificate**
 - **Common Certificate (all purpose)**
5. For the **Undefined** classification, specify the path in the client's local file system under **Thin Client Storage Path**.
6. For the **Undefined** classification, allocate **access rights** and the owner.


These will be attached to the file when it is transferred to the client and will be used on the destination system.
7. Confirm the settings by clicking on **OK**.

The file will now be copied to the web resource and will be registered on the UMS server.

Figure 67: Registering new file

9.2. Transferring a file to a thin client

In order to upload a file to a thin client, it must be assigned to the thin client either directly or indirectly via a thin client directory or profile.

- Via drag and drop, move the file to the thin client directory or integrate the file on the thin client itself in the **Assigned objects** window via the  symbol as you would when assigning profiles.

If a file has been assigned to a profile, it will be transferred to the assigned clients along with the profile settings.

When the UMS settings are transferred, a file assigned in this way will be copied to the thin client, e.g. while the thin client is booting. As long as the file is assigned to the thin client, 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 thin client is compared to the registered file. If the checksums differ from each other, the file will be transferred again.



Up until UMS **Version 5.02.100**, the thin client must be able to contact the UMS server with its fully qualified domain name (e.g. `mytcserver.mydomain.tld`). From UMS **Version 5.02.100**, the IP address of the UMS will be used when transferring the file. This ensures that the transfer works even in the event of DNS problems.

If a file was directly replaced in the file system in the `ums_filetransfer` directory, it must be updated in the UMS console using the command **Update file version** from the file's context menu. The UMS server will otherwise not recognize the change in the file version.

9.2.1. Transferring a file without assignment

A file registered on the UMS Server can also be transferred to the thin client without preparation. To do this, use the command **Transfer File to the Thin Client** from the thin client's context menu or the thin client menu in the menu bar. The file does not need to be assigned to the thin client.

This is a straightforward file copying operation. The file is not updated if the file version on the UMS Server changes.

9.3. Removing a file from a thin client

To remove a file from a thin client, proceed as follows:

- Delete the file assignment
or
- remove the file directly with the help of the command **Delete File from TC** from the thin client's context menu.

If you delete a file from the tree structure, this file will be removed from all devices to which it was assigned.

9.4. Transferring a file to the UMS Server

To download a file on a thin client to the web resources, proceed as follows:

- Click **Files>File TC>UMS** in the context menu of a thin client.

The UMS cannot search through the thin client's local file system. You therefore have to know the location and name of the file you would like to download to the web resource.

A file transferred from a thin client 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 files later on via **New File**.

To read out the current local configuration of the thin client, you will need to copy the two local files `setup.ini` and `group.ini` via the IGEL Universal Management Suite.

1. Select **Files> File TC>UMS** from the thin client's context menu in the UMS Console. Specify `/wfs/<file name>` as the source (thin client save path).
2. Select the destination on the UMS server, e.g.
`http://umsserver.domain:9080/ums_filetransfer/<filename>`.
3. Begin the file transfer by selecting **File TC>UMS**.

10. Universal Firmware Update

Firmware updates for all IGEL thin clients and Universal Desktop OS (Universal Firmware Converter UDC) are available on the public IGEL server <http://myigel.biz>. Within the UMS, you can check for newly available updates, download them and easily distribute them to thin clients.

10.1. Changing server settings

IGEL's public update server is pre-configured. If you would like to use your own FTP server for distributing updates, you can change the server settings accordingly:

1. In the **Administration** area of the UMS Console, switch to **Global Configuration>Universal Firmware Update**.
2. Click **Edit**.

The Edit FTP Server Configuration window will open.

Figure 68: IGEL Universal Firmware update

3. Change the settings for your server.
4. Click **Test Server Connection** in order to check communication with the IGEL Server and, optionally, with your own FTP server.

Problem

You want to use a proxy server to access the IGEL update server via HTTP.

Solution

Configure the proxy settings for Universal Firmware Update:

1. Start the UMS console.
2. Go to **Administration > Global Configuration > Universal Firmware Update**.

3. Click **Edit Proxy Configuration**.
4. Enable the HTTP proxy and define a connection.

Click **Save** to activate your changes.

10.2. Searching for and downloading updates

To search the public IGEL server for updates, proceed as follows:

1. In the console navigation tree, right-click **Universal Firmware Updates**.
2. Select **Search for New Updates** from the context menu.

A window containing a list of all updates which match the firmware versions registered in the UMS Database will open.



Figure 69: Available updates on server

3. Click **Information** in order to view the release notes for each update.
4. Check the **Include** checkbox to download the relevant firmware.

The update will be added to the navigation tree and the current processing status will be shown.



Figure 70: Status of firmware download

10.3. Importing from a local source

You can also load updates from a local source, e.g. from a USB stick.

An item of firmware from a local source does not have the meta-information stored on the IGEL Server.

1. Select **Firmware Archive** from the firmware updates context menu.
2. Select a compressed Linux update (ZIP file) or a Windows snapshot (SNP) file.

3. Specify a directory for storing the update before it is distributed to thin clients later on.
4. Click **OK** to start the import.

Figure 71: Import from ZIP or SNP file

10.4. Importing from the UMS WebDAV

You can also register as a Universal Firmware Update a snapshot of a Windows Embedded Standard thin client that was created earlier and stored in a web resource:

1. Select **Snapshot** from the **Universal Firmware Updates** context menu.
2. Specify the update to be imported.

10.5. Assigning an update to a thin client

There are two ways to assign a registered firmware update to a thin client:

- Directly:
 - by drag and drop
 - via **Assigned objects** in the thin client window
- Indirectly:
 - via a directory



Assigning an update does not start the update process as such. The information needed for the update is merely transferred to the thin client.

You have two options for starting the update process:

- Manually: Right-click the thin client and select **Update & snapshot commands > Update** or **Update on Shutdown** from the context menu.
- As a scheduled job:
 - a) Right-click **Jobs** in the navigation tree.
 - b) Select **New Scheduled Job**.

- c) Enter a Name.
- d) Select **Update**, **Update on Boot** or **Update on Shutdown** as the Command.
- e) Complete the configuration of the task, see *Details* (page 106).
- f) *Assign* (page 108) the task to thin clients or directories.

11. Search History

Menu path: **Navigation Tree > Search History**

Here, all search queries are saved as individual objects and can be edited further via the context menu.

11.1. Context Menu of a Search Query

Menu path: **Navigation Tree > Search History**

The following options are available to you in the context menu of a search query:

- **Delete:** Deletes the search result from the list.
- **Edit Search:** Allows you to change the search query.

The following options are only active if you have searched for **thin clients**:

- **Assign profiles to the thin clients from the search...:** Assigns profiles to the thin clients that you searched for.

➔ For details of the procedure, see the chapter *Assign profiles to a view* (page 104).

- **Detach profiles from the thin clients from the search...:** Removes the assigned profiles.

12. Recycle Bin

Menu path: **Navigation Tree > Recycle Bin**

In the IGEL Universal Management Suite, you can move objects to the **recycle bin** instead of permanently deleting them straight away. The recycle bin is enabled or disabled globally for all UMS users.

➤ Enable the recycle bin in the administration area under **Misc > Settings > Enable Recycle Bin**.

If an object in the navigation tree is deleted (**Delete** function in the symbol bar, in the context menu or the **Del** key), it will be moved to the recycle bin following confirmation.



If the recycle bin is active, objects can also be deleted directly and permanently by pressing **Shift-Del**.

Directories are moved to the recycle bin along with their sub-folders and all elements and can therefore be restored again as a complete structure. You will find the UMS recycle bin as the lowest node in the UMS console navigation tree. Elements in the recycle bin can be permanently deleted there or restored. To do this, bring up the context menu for an element in the recycle bin.



If you cannot bring up the context menu for elements in the recycle bin, the recycle bin is probably inactive. Check the status of the recycle bin as described above.

Virtually all elements from the UMS navigation tree can be moved to the recycle bin: **Thin clients, profiles, views, tasks, files** and their **directories**. Shared Workplace users cannot be deleted, while administrator accounts (in account management) and search history elements can only be deleted permanently (with **Shift-Del**). The highest nodes in the navigation 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.
- Thin clients 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 thin clients may change. Profiles previously assigned to thin clients will be reactivated if they are restored again.
- Scheduled 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.

13. Managing certificates

Manage your UMS certificates for server, client and console application.

13.1. Installing server certificates

The IGEL UMS saves a certificate on each thin client it controls. This certificate prevents unauthorized access to the thin client configuration. During the installation, a distinct pair of keys (one public and one private) is generated for each IGEL UMS Server. When registering a thin client in the UMS, the public part is automatically transferred to the thin client and saved there. From this point onwards, a comparison with the server's private key will be made each time that the thin client is accessed. If other IGEL UMS installations try to access the thin client, access will be denied.

You can also upload a certificate of your own to the UMS, for more information read the instructions in *UMS Network* (page 121).

13.2. Removing a Certificate

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

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

To remove the certificate, proceed as follows:

- Select **Remove UMS Certificate** under **Thin Clients>Commands>Other Thin Client commands**.

Each IGEL UMS Server can now access the thin client configuration until one of the servers registers the client.

13.3. Saving a certificate

You can also save the certificate on a thin client which is already registered in the database. This can be particularly helpful if the certificate has been deleted from the thin client manually.

To save a certificate on a thin client, proceed as follows:

1. Select a group or an individual thin client.
2. Select **Save Certificate** under **Thin Clients>Commands>Other**.

As an alternative, you can also re-register the thin client.

13.4. Importing a console certificate

If you install the IGEL UMS Console on another computer, you will need to import the `<INSTALLDIR>\rmclient\cacherts` certificate.

- Copy this file onto a diskette
or
- Save this file in an approved folder which can be accessed from the destination computer.

14. Administration area

The UMS Administration area brings together a number of configuration options which, in the past, were only available via the UMS Administrator on the UMS Server itself. These include linking **Active Directories** and setting up **Universal Firmware Updates**.

New tools such as **Administrative Tasks** or the **Server Services Status View** are also available here.

14.1. UMS network

The **UMS Network** node shows information regarding the SSL certificate currently used.

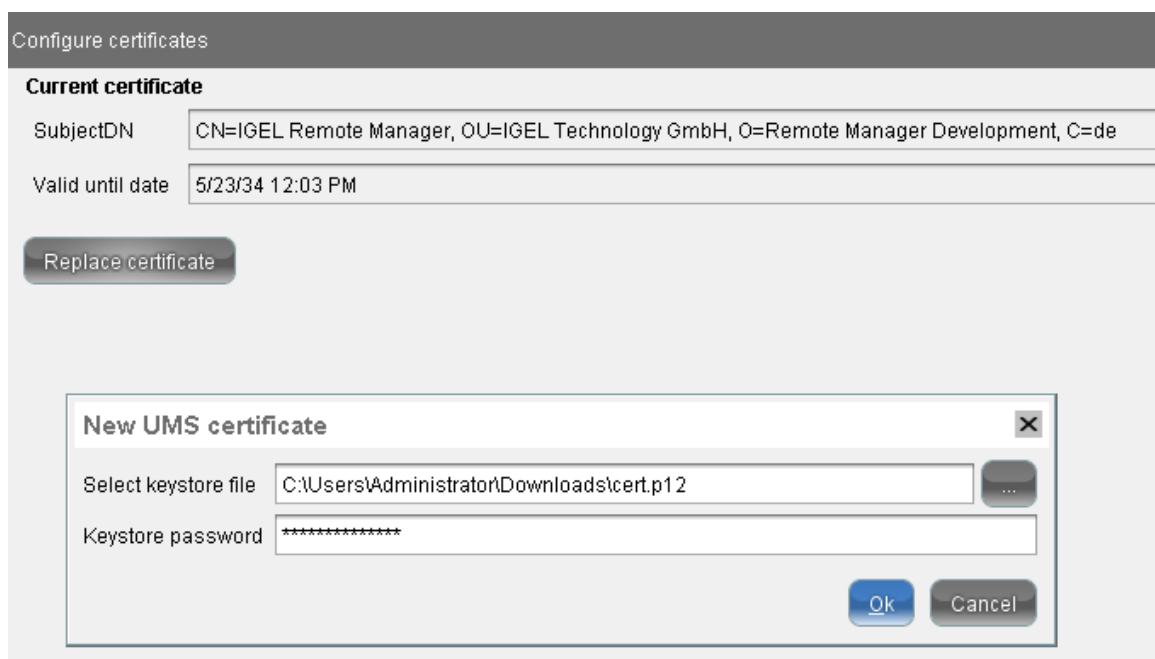
You can also replace the certificate (self-signed) which is generated during installation with your own SSL certificate here. This must be in the PKCS 12 format.

If you replace certificates, do this before registering thin clients on the UMS. Otherwise, you will need to *remove the old certificates from the thin clients* (page 119) manually after changing the certificate.

To install your own SSL certificate, proceed as follows:

1. Click on the **Replace Certificate** button.
2. Select your certificate file under **Select Keystore File**.
3. In the **Keystore Password** field, enter the password for your certificate file.
4. Confirm your settings by clicking on **OK**.

The UMS Console will then prompt you to restart the UMS Server in order to complete installation of the certificate.



14.2. UMS Server

The **Server** sub-node lists all servers and Load Balancers belonging to the UMS installation.

With a standard installation, only one available server normally appears here – in a HA network, all installed servers and Load Balancers are shown.

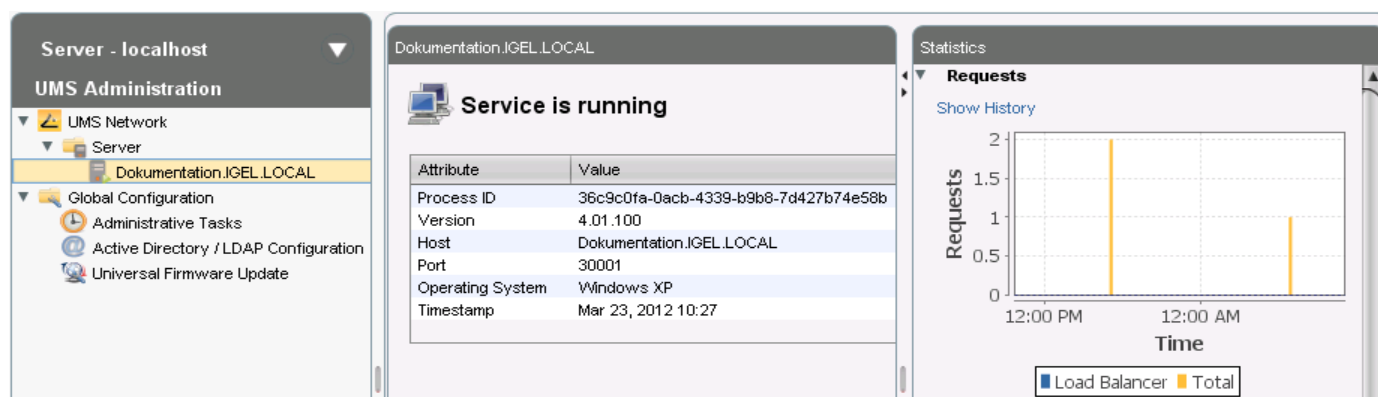


Figure 72: Status of UMS server

An overview of **queries** as well as **queries that are waiting or have been rejected** by thin clients makes it possible to estimate the server load across the relevant time period.

- Click **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.

14.3. Global configuration

Under **Global Configuration**, you can regulate *Administrative Tasks* (page 123), integrate user data from the *Active Directory* (page 122), set up *Universal Firmware Updates* (page 135) and manage *licenses* (page 134).

14.3.1. Linking an Active Directory / LDAP

It can make sense to link the UMS Server to an existing Active Directory for two reasons:

- You would like to import users from the AD as UMS administrator accounts.
- You would like to use user profiles via IGEL Shared Workplace.

For both purposes, you first need to link the relevant Active Directories in the administration area under **Global Configuration > Active Directory / LDAP Configuration**.

1. Add a new entry to the list of linked Active Directories by selecting **Add (+)**.
2. Specify the name of the **domain**, the **domain controller** and the **page size**.

The page size limits the number of hits (i.e. objects) in the Active Directory on the server side. The standard value is 1,000. Change this value according to your server configuration.

3. Click **Test Connection** to test the connection after entering valid user data.

A number of Active Directories can be linked. You should therefore ensure that you give the correct domain when logging in (e.g. to the UMS Console).

In this document, the terms Active Directory and LDAP are, to an extent, used interchangeably:

- Administrative users / UMS administrators can be imported both from an AD and from an LDAP.
- Shared Workplace users can authenticate themselves only vis-à-vis an Active Directory. An LDAP service cannot be used for this purpose.

14.3.2. Administrative Tasks


Menu path: **UMS Administration > Global Configuration > Administrative Tasks**

You can define administrative tasks for the 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.

Create Administrative Task

Menu path: **UMS Administration > Administrative Tasks**

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:

- *Database backup (only for Embedded DB)* (page 123)
- *Remove Unused Firmwares* (page 125)
- *Refresh Caches* (page 126)
- *Delete logging data* (page 127)
- *Delete task execution data* (page 128)
- *Delete Thin Clients* (page 130)
- *Export view result via Mail* (page 131)
- *Assign profiles to the thin clients of views* (page 132)

3. Click on **Finish**.

The task is defined and will be shown in the content panel.

Database backup (only for Embedded DB)

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Database Backup (only for Embedded DB)"**

You can define a scheduled backup of the database as a task.

General

- **Name:** Name for the task
- **Action: Database Backup (only for Embedded DB)**
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).
 - **Additional recipients:** Other mail addresses to which the mail is 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.
 - The task will not be executed.

Configuration

- **Limit backups to a maximum amount:** If this number of backup files in **Destination directory of database backup** 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.
- **Destination directory of database backup:** Local directory path on the UMS server in which the backup files are saved.



Ensure that the destination 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.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
- **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
- **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.

- **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
- **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .

➔ Further information on the public holiday lists can be found under *Misc* (page 33).

- **Expiration:** Point in time as of which the task will no longer be repeated.

Remove Unused Firmwares

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Remove Unused Firmwares"**

You can define the removal of unused firmware as a task.

General

- **Name:** Name for the task
- **Action:** **Remove Unused Firmwares**
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).
 - **Additional recipients:** Other mail addresses to which the mail is 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.
 - The task will not be executed.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
- **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
- **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
- **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
- **Exclude public holidays:** The task will not be executed on the days listed in the public holiday lists selected via .

➔ Further information on the public holiday lists can be found under *Misc* (page 33).

- **End:** Point in time as of which the task will no longer be repeated.

Refresh Caches

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Refresh Caches"**

You can define a task as a result of which the cache of the UMS server is refreshed.

➔ Information regarding configuration of the cache can be found under *Cache Configuration* (page 136).

General

- **Name:** Name for the task
- **Action:** Refresh Caches
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).
 - **Additional recipients:** Other mail addresses to which the mail is 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.
 - The task will not be executed.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
 - **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
 - **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
 - **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
 - **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
 - **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .
- ➔ Further information on the public holiday lists can be found under *Misc* (page 33).
- **Expiration:** Point in time as of which the task will no longer be repeated.

Delete Logging Data

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete Logging Data"**

You can define the deletion of UMS message and event logs as a task.



The logs for *Secure Shadowing* (page 59) will not be deleted as a result of this administrative task.

General

- **Name:** Name for the task
- **Action:** **Delete logging data**
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).

- **Additional recipients:** Other mail addresses to which the mail is sent. If you enter a number of addresses, you must separate them using a semicolon ";".

Configuration

- **Target directory for log data 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 from the one on which the UMS console is located.

- The logging information will be backed up in the given target directory before it is deleted from the UMS server.
- The logging information will not be backed up.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
- **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
- **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
- **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
- **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .
- ➡ Further information on the public holiday lists can be found under *Misc* (page 33).
- **Expiration:** Point in time as of which the task will no longer be repeated.

Delete Task Execution Data

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete Task Execution Data"**

You can define the deletion of the results of tasks as a task. To do this, the criteria according to which logs are deleted must be specified under **UMS Administration > Task Protocol**; further information can be found under *Task Protocol* (page 135).

General

- **Name:** Name for the task
- **Action:** Delete job execution data
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).
 - **Additional recipients:** Other mail addresses to which the mail is 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.
 - The task will not be executed.

Configuration

- **Target directory for log data backup:** 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 `<InstallDir>\rmguiserver\temp` will be used. The file name for the logging data is structured as follows: `Igel_deleted_job_exec_<date_time>.csv`
 - The results will be backed up in the target directory specified under **Target directory for log data backup** before they are deleted from the UMS database.
 - The logging information is backed up in the default directory `<InstallDir>\rmguiserver\temp`.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
- **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
- **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.

- **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
- **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .

➔ Further information on the public holiday lists can be found under *Misc* (page 33).

- **Expiration:** Point in time as of which the task will no longer be repeated.

Delete Thin Clients


Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Delete Thin Clients"**

You can define a task as a result of which specific thin client will be deleted from the UMS database. Which thin clients are deleted is defined through the criteria of a view. Example: All thin clients that have not been booted for more than a year.

General

- **Name:** Name for the task
- **Action:** Delete Thin Clients
- **Description:** Optional description of the task
- **Send Result as Mail**
 - The result of the task will be sent to the specified recipients via mail.
 - **Send to default recipient ([mail address])**
 - The mail will be sent to the mail address defined under **Mail Settings > Mail Recipients**. Further information can be found under *Mail Settings* (page 138).
 - **Additional recipients:** Other mail addresses to which the mail is 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.
 - The task will not be executed.

Configuration

- **Attach to view:** View which specifies the criteria for deleting thin clients. The view is selected via the  button.
- **View ID:** ID of the selected view.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
 - **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
 - **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
 - **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
 - **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
 - **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .
- ➡ Further information on the public holiday lists can be found under **Misc**
- **Expiration:** Point in time as of which the task will no longer be repeated.

Export View Result via Mail

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Export View Result via Mail"**

You can define a task as a result of which the results of a view will be exported as a mail attachment.




In order for mails to be sent, the UMS mail settings must be correct. Further information can be found under *Mail Settings* (page 138).

General

- **Name:** Name for the task
- **Action:** **Export view result via mail**
- **Description:** Optional description of the task
- **Active**
 - The task will be executed at the set time.
 - The task will not be executed.

Configuration

- **View ID:** ID of the selected view. The view is selected via the  button.
- **Visible columns configuration:** Data fields which the mail will contain.
- **Mail Recipients:** Mail addresses of the recipients. If you enter a number of addresses, you must separate them using a semicolon ";".
- **Result format:** Data format in which the results are sent as a mail attachment

Possible options:

- XML
 - HTML
 - CSV
- **Create archive**
 - The mail attachment will be compressed as a ZIP archive.
 - The mail attachment will retain its data format (XML, HTML or CSV).

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
 - **One server (select one):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
 - **One server (random):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
- **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
- **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
- **Exclude Public Holidays:** The task will not be executed on the days listed in the public holiday lists selected via .

➡ Further information on the public holiday lists can be found under *Misc* (page 33).

- **Expiration:** Point in time as of which the task will no longer be repeated.

Assign Profiles to the Thin Clients of Views

Menu path: **UMS Administration > Administrative Tasks > Dialog Create Administrative Task > Action "Assign Profiles to the Thin Clients of Views"**

You can assign profiles to thin clients that you have filtered via a view or search and update this assignment regularly using a schedule.

➔ Please also note the instructions in *Assign profiles to a view* (page 104).


General

- **Name:** Name for the task
- **Action:** Assign profiles to the thin clients of views
- **Description:** Optional description of the task
- **Send result as mail**
 - The assignment will be sent via mail.
Send to default recipient: This address is specified in the *mail settings* (page 138).
 - The assignment is sent to the main recipient.
Additional recipients: Mail address of the recipient if the recipient is not the main recipient. Several mail addresses must be separated by a semicolon.
- **Active**
 - The task will be executed at the set time.
 - The task will not be executed.

Select views / thin client searches

➤ Click on  to select views or thin client searches that will be assigned to one or more profiles.

Select profiles

➤ Click on  to select one or more profiles to which you would like to assign the views or thin client searches.

Server assignment

- **Assignment type**




This setting is only relevant to HA (High Availability) environments.

Possible options:

- **All servers:** The task will be executed by all servers.
- **One server (direct assignment):** You can select a specific server for this task. The available servers are listed under **Assigned servers**.
- **One server (random selection):** The server for this task will be automatically selected from the servers listed under **Assigned servers**.
- **Assigned servers:** List of servers that are available for this task.

Schedule

- **Start:** Point in time at which the task is executed.
 - **Task starts every [number of time units]**
 - The task will be repeated at the set time interval.
 - The task will not be repeated at the set time interval.
 - **Weekdays:** The task will be executed on the activated weekdays at the point in time specified under **Start**.
 - **Exclude public holidays:** The task will not be executed on the days listed in the public holiday lists selected via .
- ➔ Further information on the public holiday lists can be found under *Misc* (page 33).
- **Expiration:** Point in time as of which the task will no longer be repeated.

14.3.3. License configuration

In this area, you are given an overview of the availability and status of all licenses and a list of registration data.

14.3.4. Automatic UDC license deployment

From **Version 5.02.100**, the UMS offers the option of using an IGEL thin client as a license server in order to automatically allocate licenses to devices converted using UDC2.

- ➔ A best practice describes the entire procedure for setting up the automatic deployment of UDC licenses.
- **Enable automatic UDC license deployment:**
 - UDC2 devices newly registered on the UMS will automatically receive a license.
 - Do not enable.

- **License server:** Select one of the license servers shown.
- **Connection status:** Indicates whether a network connection to the license server exists.
- **License type:** The licenses available on the license server
- **License OS:** Operating system for which licenses are available
- **Number of licenses:** Number of licenses still available
- **Check license server again:** Checks the network connection to the license server again, for example if you have switched on the server in the meantime.
- **Deployed licenses:** List of licenses deployed by the selected license server since it was last restarted.
 - **License deployed at:** Date and time when the license was deployed
 - **Unit ID:** Unique ID of the thin client or converted device

14.3.5. Universal Firmware Update

The setup procedure is described in the chapter *Universal Firmware Update* (page 114).

14.3.6. Logging

You can set up logs relating to two different areas:

Message log settings:	Logging for actions prompted by the user
Event log settings:	Logging for actions prompted by the thin client

Each log type – independently of one another – can be:

- enabled or disabled,
- saved for a limited time, for a limited number of entries or indefinitely,
- set up and the actions which are to be registered controlled.

Some tips when working with logs:

- You can register detailed information along with messages.
- You can also record the name of the UMS administrator who performed the particular action.
- You can enable or disable actions that are to be logged in the log level configuration.
By default, all actions are recorded when the logging function is enabled.
- Click **System>Logging** to bring up the current log and the exported information in the UMS Console.
The log information can be manually exported there too.

The Administration area of the UMS Console also allows you to set up an **administrative task** in order to backup and delete the logs automatically on a regular basis.

14.3.7. Task Protocol

Menu path: **UMS Administration > Job Protocol Settings**

You can specify the criteria according to which task protocols are deleted.

- **Never delete:** Task protocols will not be deleted.
- **Keep no more than [number] executions per job:** If the number of protocols for a specific task is reached, the oldest protocol will be deleted when a new protocol for this task is created.
- **Delete executions older than [number] days:** Protocols that are older than the number of days specified here will be deleted.

14.3.8. Cache

The cache is integrated into the UMS GUI Server and is configured from the UMS Administrator. It is designed to improve overall performance when the thin client retrieves its settings. Furthermore, the UMS can provide the thin client settings even if the UMS Database is not running. Please bear in mind, however, that you cannot change thin client settings if the database is not enabled.

Enable cache	Enable or disable cache
Delete stray files	Deletes entries in the cache that cannot be found in the database.
Add all thin clients	When the cache is updated, you can add to it the settings for all thin clients which are known to the UMS. Otherwise, only the settings of the thin clients which have connected at least once to the UMS of the current host will be added.
Update cache when the server is launched	The cache is updated when the server is launched. To make detailed changes to the update settings, go into the UMS Console and click Administrative Tasks in the UMS Administration .

- Select **Misc>Manage Cache** in the UMS Console menu.

Various details about the cache are shown in the dialog window. These include which entries can be found in the cache, when the next update will take place etc.

A number of cache actions can also be performed here:

Update cache	Updates all cache contents immediately
Empty cache	Removes all cache entries immediately
Update view	Provides an updated view of the cache information

The Administration area of the UMS Console also allows you to set up an **administrative task** in order to update the cache automatically on a regular basis.

14.3.9. Wake-on-LAN

Menu path: **UMS Administration > Global Configuration > Wake On LAN Configuration**

Thin clients can be wakened via the network using magic packets. A magic packet contains the MAC addresses of the thin clients that are to be wakened. In order for a thin client to be wakened, it must be in either S3 (suspend to RAM – STR), S4 (suspend-to-disk – STD) or S5 (soft-off) mode. In the UMS administration, you can specify the network addresses to which the magic packets are sent.

For scenarios where the UMS is outside the thin clients' network and broadcast packets from the WAN are not allowed, you can define one or more Linux thin clients as a Wake-On-LAN proxy.



The Wake-On-LAN proxy function is supported by Linux thin clients from **Version 5.09.100**.

- **Broadcast address**


- The magic packet will be sent to the broadcast address of the network.

- **Last known IP address of the Thin Client**

- The magic packet will be sent to the last known IP address of the thin client.

- **All defined subnets**

- The magic packet will be sent to the network addresses of all subnets that are defined for the UMS. To add a subnet, proceed as follows:

- a) Click on  in the area below **All defined subnets**.

The **Define subnets** dialog will open.

- b) In the **Subnet** field, enter the network address of the subnet.

- c) Under **CIDR (Classless Inter-Domain Routing)**, select the suitable suffix for the network mask.



Values between 8 and 28 are appropriate.

Example 1: The network address 10.43.8.0 with the suffix 24 corresponds to the CIDR notation 10.43.8.0/24 with the network mask 255.255.255.0. This network corresponds to a Class C network. The addresses that can be used by hosts lie between 10.43.8.1 and 10.43.8.254.

Example 2: The network address 10.43.8.64 with the suffix 28 corresponds to the CIDR notation 10.43.8.64/28 with the network mask 255.255.255.240. The addresses that can be used by hosts lie between 10.43.8.65 and 10.43.8.78.

- d) If you wish, add a **Comment**.

- e) Click on **OK**.

- **Network address of the last known IP address**

- The magic packet is sent to the network address of the network in which the last known IP address of the thin client is located. In order for this network address to be determined, you will need to specify a network mask for each of the possible networks.

To add a network mask, proceed as follows:

- a) Click on  in the area below **Network address of the last known IP address**.

The **Define network mask** dialog will open.

- b) Enter the **network mask**.
 c) If you wish, add a **Comment**.
 d) Click on **OK**.

- **Wake On LAN Proxies**

- The magic packet will be sent to the thin clients 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 thin client, All defined subnets and Network address of the last known IP** settings have no effect on the Wake-on-LAN proxy.

- The magic packet will not be sent to the thin clients defined as Wake-On-LAN proxies.




Thin clients configured as a Wake-on-LAN proxy will retain their role, even if **Wake-On-LAN proxies** is disabled.

To define one or more thin clients as a Wake-On-LAN proxy, proceed as follows:

- a) Click on  in the area below **Wake On LAN Proxies**.

The **Edit Wake On LAN Proxies** dialog will open.

- b) Highlight the desired thin client in the left-hand column.

- c) Click on  to select the thin client.


- d) Click on **OK**.

The thin client will now function as a Wake-On-LAN proxy.




A thin client 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 thin client receives the settings from the UMS.

To undo the configuration as a Wake-On-LAN proxy, proceed as follows:

- e) Click on  in the area below **Wake On LAN Proxies**.

The **Edit Wake On LAN proxies** dialog will open.

- f) Highlight the desired thin client in the right-hand column.

- g) Click on  to deselect the thin client.

- h) Click on **OK**.

The thin client will no longer be configured as a Wake-On-LAN proxy as soon as the setting is sent to the thin client.

14.3.10. Mail Settings

Menu path: **UMS Administration > Global Configuration > Mail Settings**

The mail settings described here are required for the following functions:

- *Send view as mail* (page 102)
- *Export view result as mail* (page 131)
- Export results of the following administrative tasks as mail:
 - *Database backup (only for Embedded DB)* (page 123)
 - *Remove unused firmwares* (page 125)
 - *Refresh caches* (page 126)
 - *Delete logging data* (page 127)
 - *Delete task execution data* (page 128)
 - *Delete thin clients* (page 130)
 - *Assign profiles to the thin clients of views* (page 132)


➡ If you would like to use Gmail for sending mails, read the Mail Settings for Gmail Accounts best practice.

- **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 Auth**
 - The UMS will log on to the SMTP server in order to send mails. The logon data must be defined under **SMTP User** and **SMTP Password**.
- **SMTP User:** User name when logging on to the SMTP server
- **SMTP Password:** Password when logging on to the SMTP server
- **SMTP Port:** Port for the connection between the UMS and the SMTP server. For unencrypted SMTP, Port 25 is used by default. For SMTP-SSL, the default is Port 465.
- **Activate SMTP-SSL**
 - The mails will be sent with SMTPS encryption.
- **Activate SMTP-Start TLS**
 - TLS encryption for transporting mails will be enabled in accordance with the STARTTLS procedure.
- **Send Test Mail:** If you click on this button, the UMS will send a test mail.
- **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 Recipient:** 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 ";".

14.3.11. Thin Client Attributes

Menu path: **Setup > UMS Administration > Global Configuration > Thin Client Attributes**

In this area, you can set up additional attributes for thin clients which you can reuse in views and as a search criterion.

➤ Click on  to set up a new thin client attribute.

- **Name:** Name of the attribute
- **Type:** Data type of the attribute

Possible values:

String

Number

Date

- **Description:** Optional description of the attribute

- Using the **up** and **down arrows**, you can change the order of the additional attributes.
- In the thin client system information display, you can give the attributes values.



The additional attributes are used when displaying thin client system information, in views and in searches.

14.3.12. VNC

Menu path: **Setup > UMS Administration > Global Configuration > VNC**

In this area, you can centrally allocate graphic settings for the shadowing of thin clients.

Secure VNC

- **Activate global secure VNC**
 - Secure VNC shadowing will be activated globally.
- **Log user for secure VNC**
 - User names will be saved in the VNC logs.

The settings configured below override the individual parameters set under **Menu Bar > System > VNC Viewer**.

- **Preferred encoding:** Specifies the encoding.

Possible values:

- **Tight**
- **Raw**
- **PRE**
- **Hextile**
- **Zlib**


- **Color depth:** Specifies the default color depth.

Choose between **8 bit** and **24 bit**.

- **Refresh period:** Interval at which images are refreshed. Preset: 20 ms.
- **Compression level:** If you use the **Tight** coding, you can influence the level of compression here.
- **JPEG quality:** If you use the **Tight** coding, you can influence the quality of JPEG graphics here.
 - **Use "Draw Rectangle" mode**
 - If windows are moved, only the frame will be shown and not the entire window.

- **Override VNC viewer settings:**
 - Overrides the local VNC viewer settings. You can no longer configure your own settings on the console.
 - Does not override the local VNC viewer settings. Under **Menu Bar > System > VNC Viewer**, you can overwrite the server settings once again.



The settings configured here will only take effect if you save them, ideally by clicking on  in the symbol bar.

➔ See also our best practice regarding Secure Shadowing


14.3.13. Misc Settings

Menu path: **Setup > UMS Administration > Global Configuration > Misc Settings**

Further global parameters can be found here:

- **Recycle Bin**
 - **Enable recycle bin**
 - The recycle bin will be enabled. If an object is deleted in the navigation tree, it will be moved to the recycle bin.
- ➔ See also *Deleting objects in the UMS / recycle bin* (page 43)
- **Template Profiles:** Enables support for *template profiles* (page 85).
 - **Enable template profiles**
 - Template profiles will be enabled.
 - Do not enable
 - **Master Profiles:** Allows the use of *master profiles* (page 80).
 - **Enable master profiles:**
 - Master profiles will be enabled
 - **User Login History:** Records logon and logoff activities if desired.
 - **Enable user login history**
 - User logons will be enabled.
 - **Add last thin client users to quick search**
 - The user who logged on last will be added.
 - **Add only still logged in users:**
 - Only users who are currently logged on will be added.



In the event of configuration changes, the page will need to be reloaded by clicking on  in order to apply the settings.

In order to view the user history for a thin client, click on the relevant device in the navigation tree under **Thin Clients**. All information regarding the client will now be shown in the content panel. If you scroll right to the bottom, you can open up the last point – **User login history**. The following information is recorded here:

- **User name:** Logon name of the user who logged on to the client.
- **Login time:** Time at which the user logged on
- **Logoff time:** Time at which the user logged off
- **Logon type:** At the moment, this can be Shared Workplace or Kerberos/Active Directory.



In the case of Linux thin clients where firmware older than **Version 5.09.100** is installed, the **Logoff time** column will be empty. Up until this version, only logons and only those under Shared Workplace were logged.

15. 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 is described *above* (page 122). When importing user accounts, only connected ADs are available for selection.

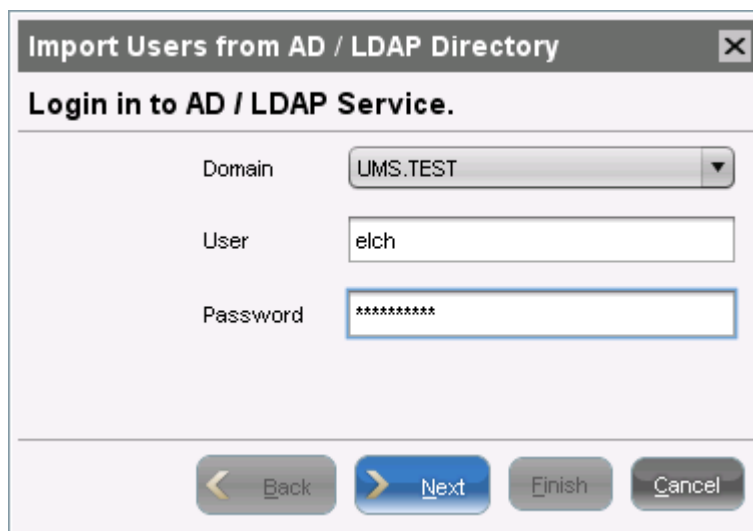


Figure 73: Login to Active Directory

3. Click **Continue**.

The Active Directory browser will open.

4. Select individual users or groups from the structure 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.

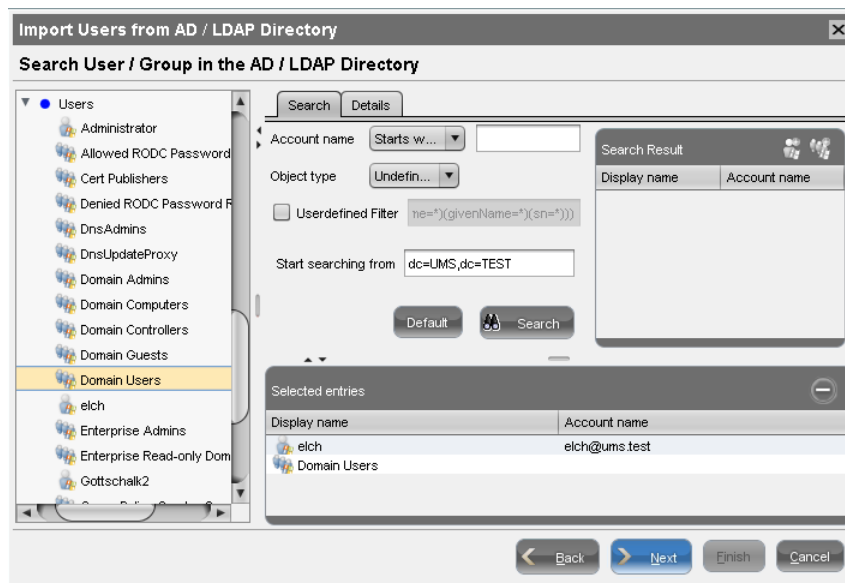


Figure 74: AD Import Filter

As an alternative to navigating in the structure tree, you can also highlight and add users or groups to the selection via the **Search** function.








5. Click **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.

15.1. Explanation of symbols

The symbols in the AD structure tree have the following meanings:

-  User account in the Active Directory
-  User group in the Active Directory
-  User account added to the selection
-  User group added to the selection
-  Computer in the Active Directory
-  Organizational unit (OU) in the Active Directory
-  Any object which is not a user or a group

The context menu allows the following actions to be performed on tree elements:



Adds a user (or group member) to the selection



Adds a user group to the selection

Sets an element as a starting point for searching in the AD

Shows the properties (details) of the element

Some tips:

- By holding down the **Ctrl** key when dragging and dropping a group, the group members and not the group itself will be selected.
- If an organizational unit is selected, only the members will be added, not the OU itself.
- The **Ins** and **Del** keys can be used to add and remove elements from the selection.
- If a user is both an administrator and a group member in the UMS, the user's own authorizations will take precedence.

15.2. Searching in the Active Directory

The options in the AD structure tree have the following meanings:

Account	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
Filter	Filter criteria in accordance with the RFC-2254 standard
Starting point	Element within the tree where the search begins
Reset	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:



Adds a user (or group member) to the selection



Adds a user group to the selection

Shows the properties of the element

Shows a tool tip (object properties with a mouse-over)

Via the context menu, you can once again bring up the properties of the objects selected for import and remove objects prior to the import if necessary.

15.3. 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.

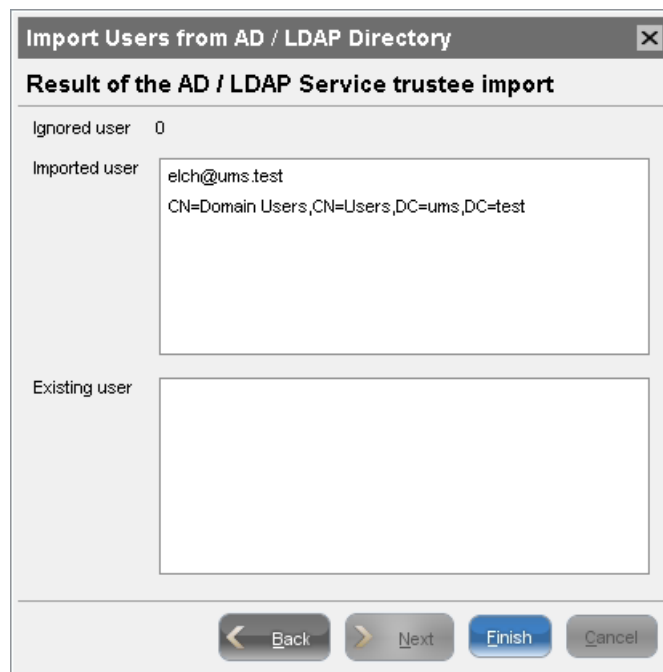


Figure 75: Result of Import

16. Administrator accounts and access rights

For the purpose of logging in to the UMS Console, you can either import UMS administrator accounts from a linked Active Directory or create, organize and remove accounts manually.

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

16.1. Administrators and groups

- Click **System>Administrator Accounts** to manage the IGEL UMS administrator accounts.

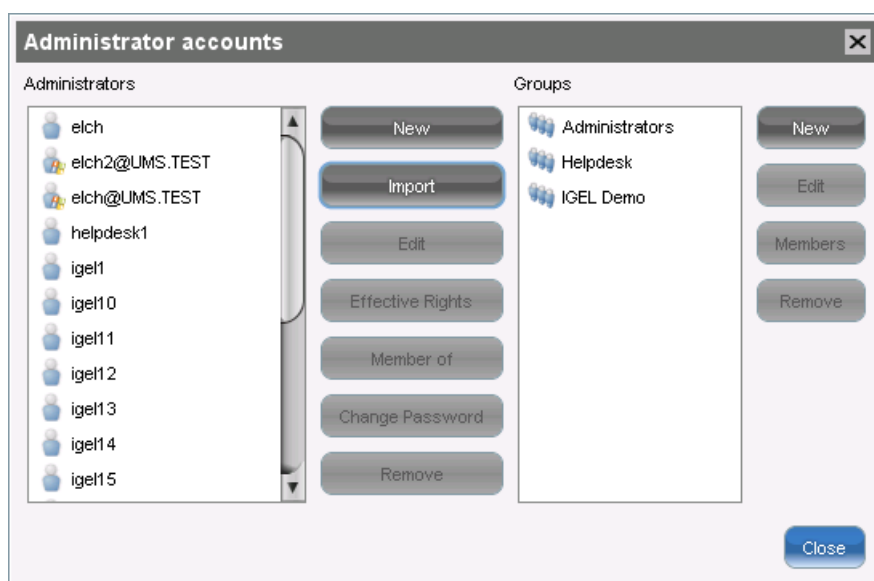


Figure 76: IGEL UMS Administrator Accounts

All available accounts are listed in the left-hand column, while the available groups are listed in the right-hand column. To the right of each column you will find the associated buttons such as **New**, **Edit** and **Remove**. For administrator accounts, you can also **change the password** and show group memberships. Details of the **members** who make up a selected group can also be shown. **Effective Rights** provides an insight into the rights that were directly or indirectly granted to a user or taken away from them.

16.2. Access rights

Authorizations in the IGEL UMS include:

- General rights which can be granted to an administrator or denied either directly via the account or indirectly on the basis of group membership,
- Access rights to objects in the navigation tree,
- Actions within the UMS Console.

The indirect rights given to an administrator on the basis of their group membership can be changed further for each administrator in the group. In this case, rights that were granted directly have precedence over those granted indirectly.

An administrator can be a member of several groups and receive the corresponding rights. If authorizations contradict each other, the withdrawal of an authorization takes precedence over the granting of it. If a prohibition regarding an action or object from a group is issued, it will overrule all rights from other groups.

Generally speaking, the same authorization settings are used for groups and administrators. The following description of individual configuration options for administrators therefore applies equally to groups too.

16.2.1. Basic authorizations

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 (thin clients, profiles...) or nodes in the administration area of the 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	

Figure 77: Basic access rights

Example 1:

In order to be able to change the configuration of a thin client, a user requires authorization to **search** the thin client's directory path and **configure** the thin client itself.

Example 2:

In order to be able to configure a scheduled backup of the internal database, an administrative user requires **search**, **Global Configuration** and **write** authorization for administrative tasks (reading authorization is automatically set at the same time).

16.2.2. General administrator rights

The general administrator rights essentially relate to actions in the menu of the console:

	Allow	Deny
'System' Menu		
Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
Event and log messages	<input type="checkbox"/>	<input type="checkbox"/>
Firmware management	<input type="checkbox"/>	<input type="checkbox"/>
License management	<input type="checkbox"/>	<input type="checkbox"/>
Snapshot management	<input type="checkbox"/>	<input type="checkbox"/>
'Thin Clients' Menu		
Scan for Thin Clients	<input type="checkbox"/>	<input type="checkbox"/>
'Misc' Menu		
Cache management	<input type="checkbox"/>	<input type="checkbox"/>
Default Directories	<input type="checkbox"/>	<input type="checkbox"/>
Host Assignment (Jobs)	<input type="checkbox"/>	<input type="checkbox"/>
Public Holidays Management	<input type="checkbox"/>	<input type="checkbox"/>
Sql Console	<input type="checkbox"/>	<input type="checkbox"/>
'Help' Menu		
Save support information	<input type="checkbox"/>	<input type="checkbox"/>

Figure 78: General administrator permissions

Administrator accounts are particularly important here. This is the system for managing authorizations itself. An administrator with this authorization can grant themselves and others rights, take away those rights and set up new accounts. This authorization should only be granted to users who are to have full access to all objects and actions in the UMS.

The individual items:

Administrator Accounts	Authorization management may be performed.
Events and messages	The event and message log may be viewed if Logging is enabled.
Managing firmware	Firmware versions can be imported, exported and removed from the database.
Manage Licenses	IGEL firmware licenses can be allocated to thin clients.
Manage Snapshots	Snapshots for IGEL thin clients can be registered on the UMS Server and removed again.
Scan Thin Clients	The network can be scanned for thin clients, for example if they are to be registered on the UMS Server.
Manage Cache	The UMS Server cache can be viewed, updated and deleted.
Managing public holiday lists	Public holidays can be defined in order to plan tasks.
Host assignment	Planned tasks can be assigned to various hosts.
SQL Console	The SQL Console may be run. Warning: The SQL Console can cause considerable damage to the database!
Default Directories	Directories and rules for automatically sorting thin clients can be created and deleted.
Saving support information	Database and server log files can be exported for support purposes.

16.2.3. Object-related access rights

Administrators and administrator groups can be granted specific rights with regard to objects in the navigation tree. These authorizations are inherited "downwards", e.g. from a folder to the thin clients within this folder.

You can change the authorization settings after selecting an object in the following ways:

- via the context menu of the object
- or via the authorization symbol in the tool bar
- or via the menu item **Edit>Authorizations**

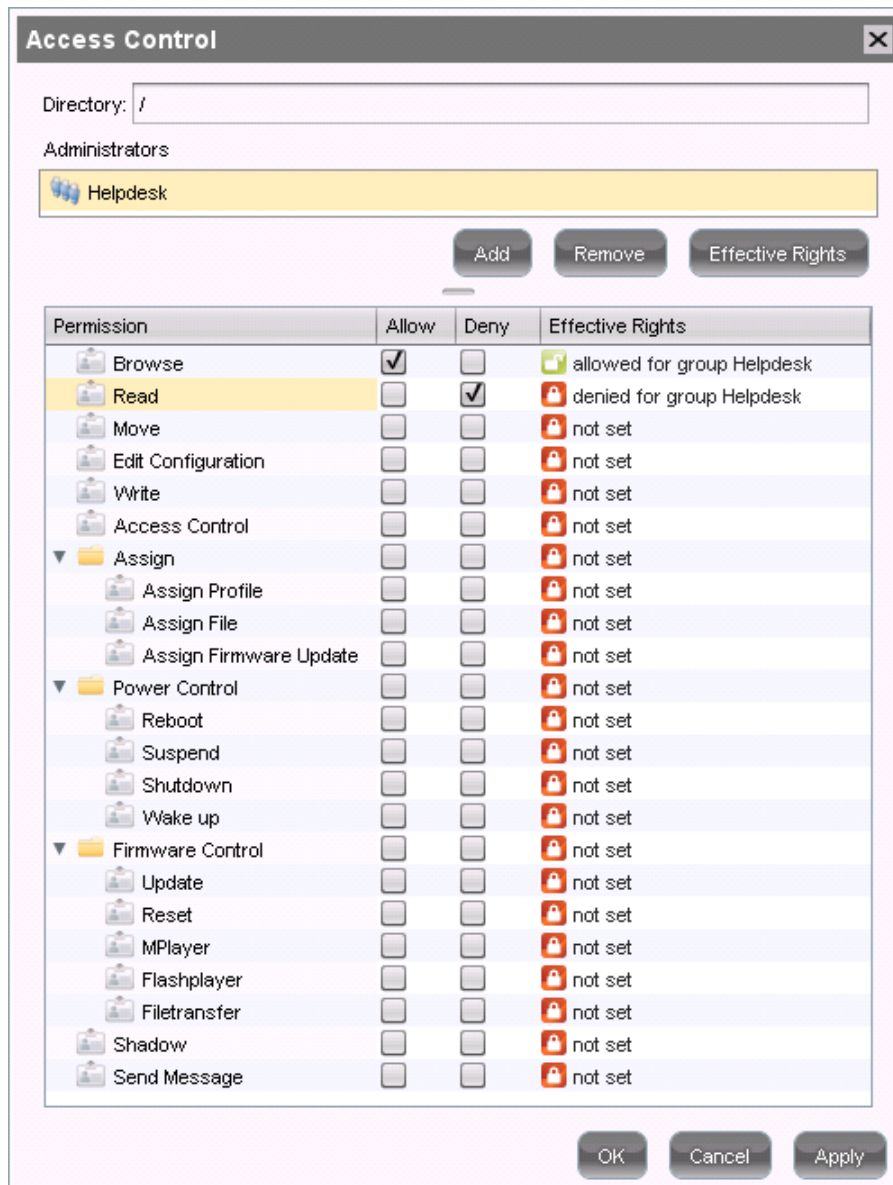


Figure 79: Object related permissions

The above list contains all object-related authorizations available in the UMS navigation tree. Only one selection is available for each selected object. For example, a view cannot be assigned updates and cannot be shut down.

Associated authorizations are automatically set together but can be changed manually later on. Enabled authorizations or denials relating to nodes affect all objects within the node.

The overview shows a selected administrator's rights to an object. Details can be found under **Effective Rights**. The rules for determining rights are also shown here, e.g. whether an authorization was granted directly or whether it is granted via a group or an inheritance within the tree structure.

The screenshot shows a dialog box titled "Effective Rights" with a close button (X) in the top right corner. On the left side, there is a tree view of administrators and groups. The "Support 1" entry is selected and highlighted in yellow. The right side of the dialog contains a table with two columns: "Permission" and "Reason".

Permission	Reason
Browse	allowed for group Helpdesk
Read	not set
Move	not set
Edit Configuration	not set
Write	not set
Access Control	not set
Assign	not set
Assign Profile	not set
Assign File	not set
Assign Firmware Update	not set
Power Control	not set
Reboot	not set
Suspend	not set
Shutdown	not set
Wake up	not set
Firmware Control	not set
Update	not set
Reset	not set
MPlayer	not set
Flashplayer	not set
Filetransfer	not set
Shadow	not set
Send Message	not set

An "Ok" button is located at the bottom right of the dialog box.

Figure 80: Effective permissions

Available rights

General	Search	Visibility of the object in the navigation tree (path as far as the object must also be allowed!)
	Read	Read authorization in respect of folder contents and object attributes
	Move	Thin clients can be moved without write authorization.
	Edit configuration	Write authorization for the configuration of a thin client (TC Setup)
	Write	Write authorization in respect of folders and object attributes (not TC Setup)
	Authorizations	The authorization settings for the object can be changed.
	Shadowing	VNC access to the thin client
	Send message	The thin client's message function
Assignment	Assign profile	A profile may be assigned to the object.
	Assign file	A file may be assigned to the object.
	Assign update	A firmware update may be assigned to the object.
Energy	Reboot	Rebooting the thin client.
	Idle state	Putting the thin client into the idle state.
	Shut down	Shutting down the thin client
	Wake up	Waking up the thin client using wake-on-LAN.
Firmware	Update	The firmware update may be carried out.
	Reset	Resetting the firmware to the factory defaults.
	Media Player	Downloading Media Player codec licenses.
	Flash Player	Downloading an Adobe Flash Player license.
	File transfer	An assigned file may be transferred to the thin client.

16.2.4. Access rights in the administration area

In the administration area of the console, you can **search**, **read** and **write** general authorizations and grant or deny **authorizations** for administrator accounts. Authorizations should only be granted to users who will actually perform administrative tasks on the UMS.

17. User logs

The logging system is used by the UMS and the registered thin clients 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 thin client.

17.1. Administration

The administration settings for the logging procedure are configured in the IGEL UMS Administrator under **Settings>Logging**.

Log message settings

Activate message logging Log administrator data

Log level: Message body and details Log Level Configuration

Never delete

Keep no more than 10,000 Messages

Delete messages older than 5 days

Log event settings

Activate event logging Log Level Configuration

Never delete

Keep no more than 10,000 Events

Delete events older than 5 days

Delete and export options

Export to file before deleting C:\DOCUME~1\igel\LOCALS~1\Temp\ ...

Check the log data at 03:00 o'clock

Daily check the log data on Mon Tue Wed Thu Fri Sat Sun

Figure 81: Log configuration

- **Messages** can be logged either with or without details.

There are no details for **events**.

- Old messages can automatically be deleted from the list. You can specify how many messages are kept and for how long. You can set up an export procedure in order to backup messages before they are automatically deleted.
- With the **Log Level** buttons, you can enable logging for selected commands. Logging for all possible commands is selected as standard.

Apply saves your settings and applies them for the purposes of the RMGuiServer service.

17.2. Logging dialog window

Information regarding **messages** and **events** can be displayed in the 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

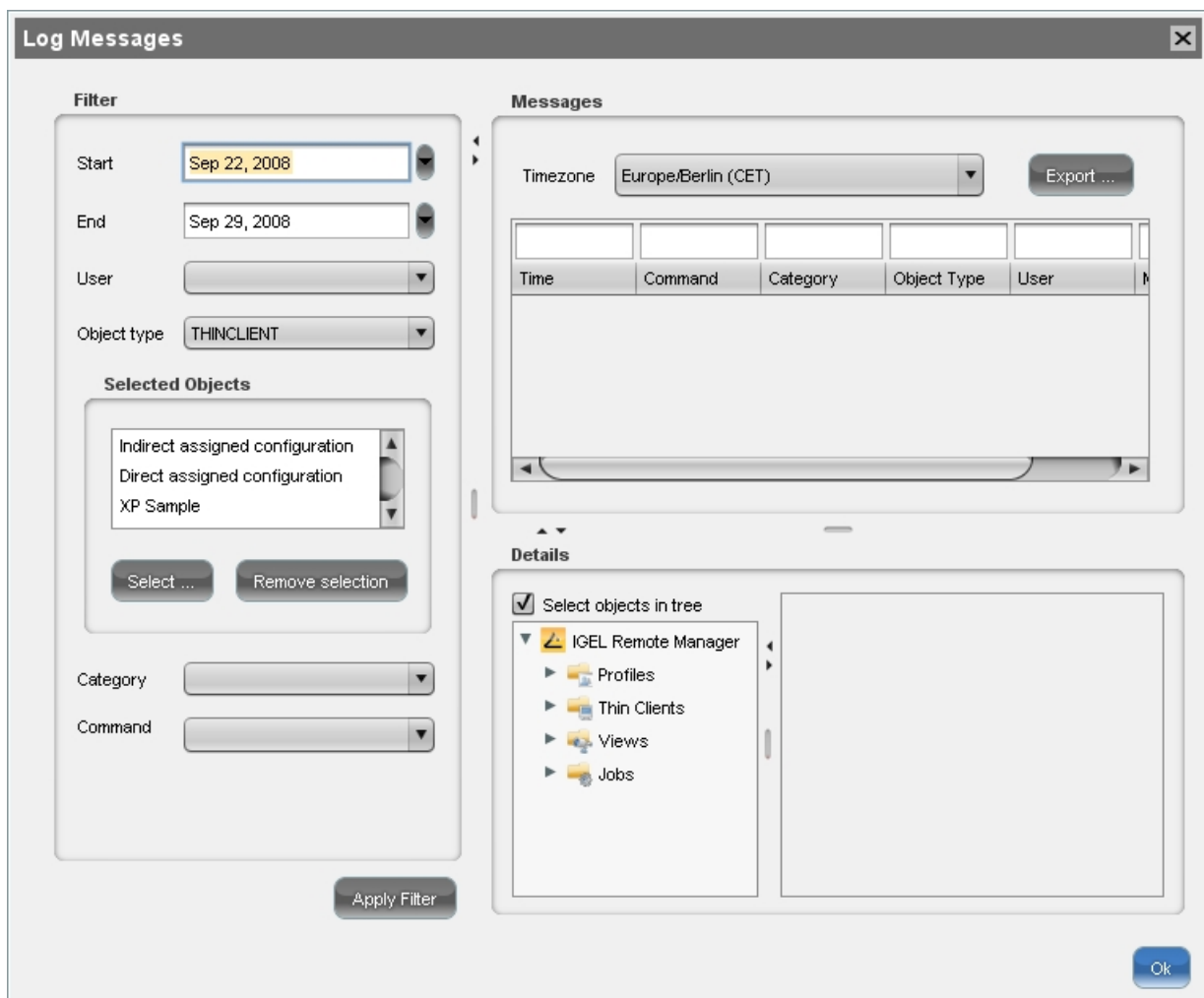


Figure 82: Message logging

17.2.1. 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 thin clients can be selected.

2. Click **Use 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

To set a filter for events, proceed as follows:

1. Specify the **command** if you know what it is.
2. Specify the **MAC address** of the thin client for which you wish to display the events.

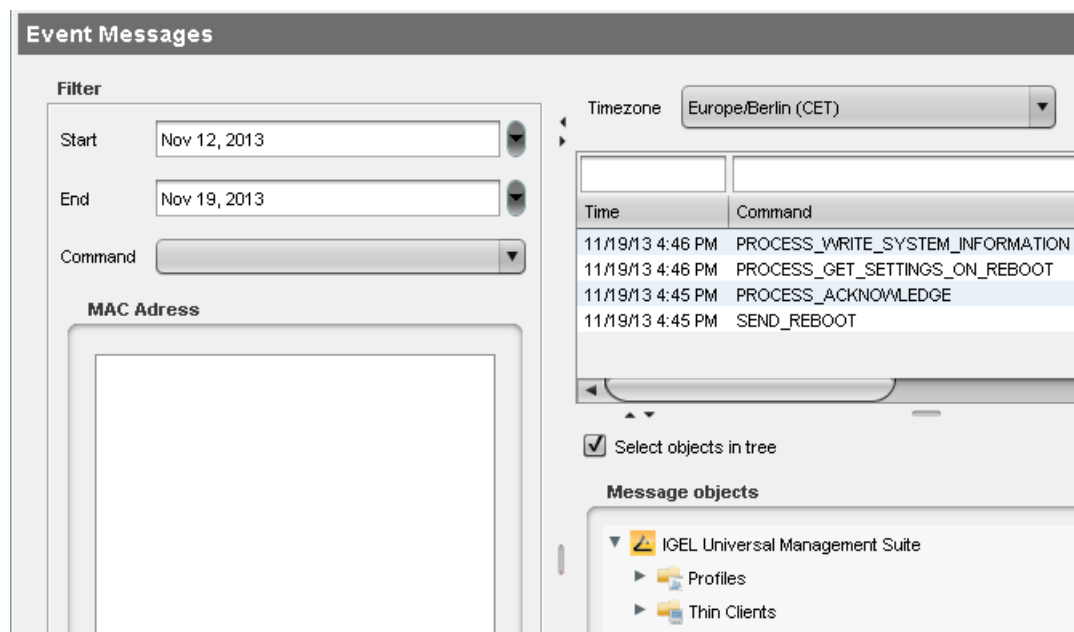


Figure 83: Event logging

Filter for messages

User	Select the name of the UMS administrator who is responsible for the message. If this field is left empty, the messages of all users will be shown.
Object type	Specify an object for which you would like to display the messages. If this field is left empty, the messages for all object types will be shown.
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.

Comments

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 thin client 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 thin clients 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.

18. Send log file to Support

If you have problems with the IGEL UMS and contact your service provider, you can send various UMS log files to Support. The *Support Wizard* (page 158) will help you here.

IGEL Support and Knowledge Base

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 at the *IGEL Support Portal*
<https://www.igel.com/en/members-area/login-logout.html>.

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 also our notes regarding support and service information.

Please visit our *IGEL Knowledge Base* <http://edocs.igel.com> to find additional Best Practice and How To documentation as well as the *IGEL Support FAQ*
<http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQExplorer;CategoryID=3>.

18.1. Support Wizard


Menu path: **Menu Bar > Help > Save support information**

With the Support Wizard, you can collect the log files which are important for your support case and send them as a mail to IGEL Support.



In order to send log files using the Support Wizard, the mail settings must be correct; further information can be found under *Mail settings* (page 138). The support ID must also be valid.

To send log files using the Support Wizard, proceed as follows:

1. Enter the **Support ID** for your support case.
2. Click on **Next**.
3. Highlight the thin clients where the problem has occurred.
4. Click on  to select the highlighted thin clients.
5. Click on **Next**.
6. Under **Number of days back**, specify the maximum age in days of the log entries to be sent.
7. Click on **Next**.
8. Using **Look in**, select the directory in your file system in which the zipped log files are to be saved.
9. Click on **Next**.



If the zipped log files have already been saved, you will be asked whether the existing ZIP file should be overwritten.

If the mail settings are configured, entry fields for the mail will be shown.

If the mail settings are not configured, a confirmation will be shown.

10. 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 **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.

11. Check the information in the mail and click on **Send**.

12. Click on **Finish**.

19. Optional add-ons

You will find comprehensive information regarding the optional IGEL UMS add-ons here:

IGEL UMS High Availability (HA)

Universal Customization Builder (UCB)

IGEL Management Interface (IMI)

Universal Management Agent (UMA)

20. Index

A

About this document.....	5
Access rights	149
Access rights in the administration area	155
Activate template profiles	86
Activating a data source	47
Activating IGEL Shared Workplace	76
Administration.....	156
Administration area.....	124
Administrative Tasks.....	126
Administrator accounts and access rights.....	149
Administrators and groups.....	149
Allocating profiles.....	71
Apache Derby	19
Assign profiles to a view	104
Assign Profiles to the Thin Clients of Views.....	135
Assign template profiles and values to the thin clients.....	94
Assigned objects	39
Assigning a user profile.....	76
Assigning an update to a thin client	119
Assignment	110
Attributes of the IGEL UMS	7
Automatic UDC license deployment.....	137
Available rights	154

B

Backup on the command line	46
Backups.....	45
Basic authorizations.....	150

C

Cache	138
Certificates.....	48
Changing server settings	117
Checking profiles	71

Commands for Tasks.....	106
Comments.....	159
Compare profiles	72
Configuration in the UMS Console	75
Configuring profile settings	69
Configuring thin clients.....	55
Connecting external database systems	17
Connecting the UMS console to the server.....	19
Content panel	37
Context menu	40
Context Menu of a Search Query	120
Copy session	56
Copying a data source	47
Create Administrative Task.....	126
Create keys and values in the profile	91
Create template keys and values.....	87
Creating a Backup	45
Creating a directory	49
Creating a new view	98
Creating profiles	66
Creating/editing a directory rule	52

D

Data sources	46
Database backup (only for Embedded DB).....	126
Defining rules for stipulated directories.....	52
Delete Logging Data.....	130
Delete Task Execution Data	131
Delete Thin Clients.....	133
Deleting a Backup	46
Deleting a directory	51
Deleting objects in the UMS / recycle bin	42
Deleting profiles.....	72
Details	108
Distributing UDC2 licenses.....	60

E

Edit.....	31
-----------	----

Enabling master profiles.....	80	Importing thin clients	23
Establishing conditions	52	Installation	11
Example of how to create a view	99	Installation requirements	11
Examples.....	53	Installation under LINUX.....	14
Explanation of symbols.....	146	Installation under Windows	13
Export View Result via Mail.....	134	Installing a UMS server	13
Exporting a profile and firmware	67	Installing server certificates.....	122
Exporting and importing profiles.....	67		
External VNC viewer	58	L	
		Launching a VNC session	57
F		License configuration.....	137
Files.....	113	License management.....	59
Filter for messages.....	159	Linking an Active Directory	75
Firmware licenses	59	Linking an Active Directory / LDAP	125
First steps.....	19	Logging.....	137
Formatting and meanings.....	5	Logging dialog window	157
Further settings	44	Logout and change of user	78
G		M	
General administrator rights	151	Mail Settings	141
Global configuration	125	Managing certificates	122
		Managing thin clients	49
H		Master profiles	80
Help.....	35	Menu bar	30
		Messages	38
I		Microsoft SQL Server	17
IGEL UMS components	8	Misc.....	32
IGEL VNC Viewer	57	Misc Settings.....	143
Import results list.....	147	Moving thin clients	51
Import with IGEL serial number	26		
Import with long format	25	N	
Import with short format	24	Navigation tree	35
Important Information	2	New profile - options.....	67
Importing a console certificate.....	122		
Importing a directory.....	50	O	
Importing a profile and firmware	68	Object-related access rights	152
Importing Active Directory users.....	145	Optimizing the active Embedded DB.....	47
Importing from a local source	118	Optional add-ons	162
Importing from the UMS WebDAV.....	119	Oracle.....	17
Importing profiles with unknown firmware	68	Order of priority for profiles.....	64, 77, 81

Order of priority for settings	64	Setting a filter	158
Overview.....	7	Setting a filter for categories	159
Overwriting sessions.....	70	Setting a filter for events	158
P		Setting up a Data Source	46
Parameters configurable in the user profile	79	Setting up a new task.....	106
Ports/time limits.....	43	Setting up and using the feature	75
PostgreSQL.....	18	Setting up thin clients manually	28
Profiles.....	63	Shadowing (VNC)	56
R		Special case – structure tag	55
Recycle Bin.....	120	Status bar.....	39
Refresh Caches	129	Support Wizard.....	160
Registering a file on the UMS server	113	Symbol bar.....	36
Registering thin clients	23	System	30
Registering thin clients automatically	27	T	
Registering thin clients manually	27	Task Protocol	138
Registering thin clients on the UMS server	20	Tasks	106
Remove Unused Firmwares.....	128	Template profiles.....	85
Removing a Certificate	122	The console window	28
Removing a file from a thin client	115	The IGEL UMS Administrator	42
Removing assigned profiles from a thin client	72	Thin Client Attributes.....	142
Restoring a Backup	45	Thin Clients	31, 49
Results	111	Tip & Trick.....	46
S		Transferring a file to a thin client	114
Saving a certificate.....	122	Transferring a file to the UMS Server	115
Saving the view results list	102	Transferring a file without assignment.....	115
Scan for Thin Clients.....	22	U	
Schedule	109	UD Linux device-specific parameters	79
Search for objects in the UMS.....	40	UD W7 device-specific settings	79
Search History.....	120	UDC2 test licenses	60
Searching for and downloading updates.....	118	UMS Administration	38
Searching for thin clients in the network	21	UMS Administrator.....	9
Searching in the Active Directory	147	UMS Console.....	10
Secure Shadowing (VNC with SSL/TLS).....	59	UMS console via Java Web Start	12
Send log file to Support	160	UMS network.....	124
Send view as mail	103	UMS Server	9, 125
Server settings	43	Universal Firmware Update.....	117, 137

Updating UMS installation.....	15
Updating under LINUX.....	16
Updating under WINDOWS.....	15
Upgrading licenses.....	62
Use template keys in profiles	93
User login.....	77
User logs	156
User profiles - IGEL Shared Workplace.....	74
Using a directory rule	53
Using profiles.....	66
V	
Value groups.....	95
Views	98
VNC.....	142
W	
Wake-on-LAN.....	139
What is new in 5.02.100?	5
Working with the IGEL UMS	28