Scout Enterprise Management Suite

Version 14.x

Administrator´s Guide

How to manage a client infrastructure through Scout Enterprise console

Date 2017-06-16

0. Legal Information

Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH
Ludwig-Erhard-Allee 26
76131 Karlsruhe
+49 (0) 721 96451-0

1. Introduction

1.1. About Scout Enterprise Management Suite

Scout Enterprise Management Suite is the management solution for Thin Clients or PCs running the operating system eLux. In addition, Windows-based clients can be managed by using basic Scout Enterprise management features.

Scout Enterprise Management Suite consists of several components. The first seven components listed below are included when performing the Scout Enterprise standard installation[1] but can be excluded optionally when performing the custom installation.

Component	Description	Installation
Scout Enterprise Server	The service controls and manages eLux clients as well as Windows clients which have installed Scout Agent for Windows.	`Scout Enterprise.exe`
Scout Enterprise Console	User interface for the management of eLux clients and for the management of Windows-based clients which have installed Scout Agent for Windows Server communication only via database Multiple consoles can be managed with one Scout Enterprise database.	`Scout Enterprise.exe`
Recovery service	Customized TFTP service to realize a PXE recovery environment for eLux clients	`Scout Enterprise.exe`
Scout Enterprise ELIAS	The dialog program eLux Image Administration Service (ELIAS) allows to create individual image definition files (`.idf`) for modular firmware updates of the eLux clients.	`Scout Enterprise.exe`
Scout Enterprise Report Generator	Tool for creating freely definable reports over all currently existing devices, applications and OUs in the Scout Enterprise Console	`Scout Enterprise.exe`
Scout Enterprise PUMA	Package Update Management Agent The service provides fully automated updates of defined eLux packages from www.myelux.com into the eLux container on the web server.	`Scout Enterprise.exe`
Scout Enterprise Statistics Service	Service for the evaluation of client status information and dynamic asset details	`Scout Enterprise.exe`

[1] for Scout Enterprise Management Suite 15.0 and later versions, Dashboard and the Web API are also included

Component	Description	Installation
Scout Enterprise Dashboard	Web-based console for the management of eLux clients and for the management of Windows-based clients which have installed Scout Agent for Windows	`Scout Enterprise.exe`[1]
Web API[2]	Application programming interface for the management of eLux clients and for the management of Windows-based clients which have installed Scout Agent for Windows	`Scout Enterprise.exe`
Scout Enterprise Mirror App	Dialog program allowing to mirror eLux clients without Scout Enterprise Console (Scout Enterprise administrator rights are applied)	separate
Scout Agent for Windows	Service providing an interface for Windows-based clients to be managed through Scout Enterprise Management Suite	separate
Scout Enterprise Command Interface	Command line interface for Scout Enterprise commands	`Scout Enterprise.exe`
Scout Enterprise Configuration File Editor	Dialog program allowing to modify configuration files which have been exported from the Scout Enterprise Console	`Scout Enterprise.exe`
Scout Enterprise Database Connection Editor	Tool allowing to modify database connection settings of the Scout Enterprise Server and Scout Enterprise Console	`Scout Enterprise.exe`

The present guide describes configuration, control and management of the clients using the Scout Enterprise Console. It also covers the Scout Enterprise Statistics Service and mirroring by means of the Scout Enterprise Mirror App.

The following components are covered by separate guides:

- Scout Enterprise ELIAS
- Scout Enterprise Report Generator
- Scout Enterprise PUMA
- Scout Enterprise Command Interface
- Scout Enterprise Configuration editor
- Scout Enterprise Dashboard

Recovery procedures for eLux clients are described in a Short Guide.

[1] separate for Scout Enterprise Management Suite 14.9 and earlier versions
[2] for Scout Enterprise Management Suite 15.0 and later versions

Note

To be able to compose and use your own image files, in addition to Scout Enterprise Management Suite, you need an eLux container. The eLux container is a web server container providing eLux software packages and image definition files. By usingScout Enterprise ELIAS, you then can compile individual image files to update your clients with. The container installation is done through the `AllPackages` bundle of a eLux version and its `setup.exe` file.

1.2. Communication between Thin Client and Scout Enterprise Server

During system start the client devices connect to their Scout Enterprise Server and verify if their configuration data is up-to-date. Updated data can concern device configuration, application definitions, files defined for transfer and advanced file entries. For further information about identifying and transferring updated configuration data, see Configuration method.

The communication between client and server can proceed in three ways:

- Client accesses the Scout Enterprise Server. The Scout Enterprise Server has no updated configuration data. Client continues booting with its configuration.
- Client accesses the Scout Enterprise Server. The Scout Enterprise Server reports new configuration data and transfers the data to the Thin Client. If required, the client restarts using the new configuration.
- Client cannot access the Scout Enterprise Server due to network or other problems which result in a management timeout (see Advanced network settings). The Thin Client continues booting with its configuration.
  Depending on the handshake settings the client retries connecting to be able to synchronize the configuration data. For further information, see Optimizing with handshake.

Updated configuration data can relate to device configuration (setup), application definition, files configured for transfer and advanced file entries.

During operation of a client device there is no data exchange between the Scout Enterprise Server and Thin Client. During shutdown, the client reports its current status to the Scout Enterprise Server.

Exception: VPN Connections.

1.3. Representation

The following representations and conventions for instructions are used throughout the documentation:

Representation	Description
Control element	All graphical user interface controls are displayed in **bold**
Menu > menu command	Whenever running a command involves clicking a series of menus, the single GUI controls such as menu commands or dialog tabs are linked by **>**.
`Value`	All data that have to be entered by the user or data that represent a field value are displayed in `Courier New`. Also, file names and path names are displayed in `Courier New`.
STRG	Keys to be pressed are displayed in CAPITAL LETTERS.
<*Placeholder*>	Placeholders in instructions and user input are displayed in *italics* and in <angle brackets>.
1. Instruction	Procedures to be carried out step by step are realized as numbered steps.
Result	System responses and results are displayed in *italics*.

Abbreviations and acronyms

Abbreviation	Description
EBKGUI	Interface of the eLux Builder Kit (component of Scout Enterprise)
EPM	eLux package module (`.epm`, software package)
FPM	Feature package module (`.fpm`, part of a software package)
FQDN	Fully qualified domain name
GB	Gigabyte
IDF	Image Definition File (`.idf`)
IIS	Microsoft Internet Information Services
MB	Megabyte
OU	Organizational unit Unit or group within the organizational structure
VPN	Virtual Private Network

1.4. Keyboard shortcuts

Keys	Selected element	Description
CTRL+SHIFT+INSERT	Individual OU	Opens the **Advanced settings** of the selected OU
	Applications	Opens the **Application Properties** dialog to define a new application
	Devices	Opens the **Information** dialog to enter a MAC address
CTRL+SHIFT+DELETE	Individual OU	Deletes the selected organization unit
	Individual application	Deletes the selected application
	Individual device	Deletes the selected device
F2	Individual OU	Rename the selected organization unit
	Individual device	Rename the selected device
	Individual application	Rename the selected application
F5	_	Updates the configuration of all devices
CTRL+F	_	Activates the Quick search field for simple search
CTRL+SHIFT+F	_	Opens the Search window for advanced search
CTRL+X	Individual device	Cuts the selected device
CTRL+V	**Devices** or individual device	Pastes the device from the Clipboard to the selected position
CTRL+A	Individual application or device in the **List** window.	Selects all applications/devices in the **List** window
CTRL+E	Individual device	Performs a **setup comparison**
CTRL+P	_	Opens the **Print dialog** to print the list of available devices

2. Installation

2.1. System requirements

Note
We recommend to operate Scout Enterprise Management Suite on a Windows Server system. If you use a Windows workstation instead, you cannot run Scout Enterprise Dashboard.

Minimum requirements for the Scout Enterprise Server:

- Hard disk space 600 MB (only Scout Enterprise Management Suite, the software container requires additional space)
- Microsoft Windows Server 2008 R2, 2012, 2012 R2 or
  Microsoft Windows Server 2016 (requires Scout Enterprise Management Suite 14.9 or later versions) or
  Microsoft Windows 7, Windows 8, Windows 10

  including the relevant software updates provided by Microsoft at the time of installation
- Microsoft .NET Framework version 3.5 and
  Microsoft .NET Framework version 4.5.1 or later
- Suitable ODBC driver
- In order to install the 64-bit version of Scout Enterprise (Scout Enterprise 14.0.0 or later), the Microsoft SQL Server Native Client 11.0 must be installed on the Scout Enterprise Server. The corresponding `MSI` file (`sqlncli.msi`) can be downloaded from the Microsoft website either individually or as part of Microsoft SQL Server Feature Pack. After successful installation of the Microsoft SQL Server Native Client, the driver is displayed in the ODBC data sources.
- Administrator rights for the system Scout Enterprise is running on
- Administrator rights to connect to the TCP/IP network

Requirements for the database system

- Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016
  - for Scout Enterprise Management Suite 14.6.1 and earlier versions: MS JET database engine (mdb) which is included in Windows
  - for Scout Enterprise Management Suite 14.7 and later versions: MS SQL Server Express LocalDB as integrated DBMS based on SQL, included in the Scout Enterprise installation file

Minimum requirements for the container:

- Write access to FTP or HTTP server, local or via network
- The required space depends on the number of provided operating system versions. To install eLuxContainerRP5 (eLux RP 5.5 LTSR), for example, we recommend available disk space of 1 GB minimum.

For further information, see Installing a container in the ELIAS guide.

Support periods and compatibility matrix can be viewed in the download area of our technical portal. For further information, see www.myelux.com.

2.2. System limitations

For all components of the Scout Enterprise Management Suite, we do not know of any system limitations.

On the same system, there can be run other services such as Citrix XenApp.

2.3. Database support

Scout Enterprise requires database software such as Microsoft SQL Server or, for smaller environments, Microsoft SQL Server Express LocalDB (Scout Enterprise 14.7.0 and later versions) and Microsoft JET database (Scout Enterprise 14.6.1 or earlier).

Microsoft SQL Server

As SQL database, you can use any Microsoft SQL Server version that is supported. You are required to create a Scout Enterprise database (any file name you wish) before installing Scout Enterprise. The Scout Enterprise database requires about 50 MB free disk space per 1.000 devices.

If you intend to install the Scout Enterprise Statistics Service along with the Scout Enterprise Management Suite (standard installation), you are also required to create a Scout Enterprise Statistics database before. And, if you intend to install and use Scout Enterprise Dashboard, a third database must be created in Microsoft SQL server before installing Scout Enterprise. For further information, see Installing Scout Enterprise.

The database tables of the databases are created automatically by the installation routine of the Scout Enterprise Management Suite and the Scout Enterprise Dashboard.[1]

Overview of databases:

- Scout Enterprise
  Device configuration, (static) asset data, server settings, management of administrators, consoles and licenses, transaction logging

[1]For Scout Enterprise Management Suite 14.9 and earlier versions, the Scout Enterprise Dashboard is installed separately.

- Scout Enterprise Statistics
  Asset data (dynamic, history)
- Scout Enterprise Dashboard
  Dashboard settings, transaction logging

Microsoft SQL Server Express LocalDB

Using Microsoft SQL Server Express LocalDB or Microsoft JET database respectively, is only recommended for less than 1.000 clients or for test and evaluation environments.

Note
With Microsoft SQL Server Express LocalDB or Microsoft JET Database, you cannot use the Scout Enterprise Statistics Service (keep alive messages and static asset data) nor Scout Enterprise-Dashboard (web console).

The Scout Enterprise database is created automatically during the installation:

- For Scout Enterprise Management Suite 14.6.1 and earlier versions: The Microsoft Server operating systems already include Microsoft JET Database. If you want to use it, during the installation of Scout Enterprise, the Scout Enterprise Server creates the required database of the type `.mdb` with any name you wish.
- For Scout Enterprise Management Suite 14.7.0 and later versions: The Scout Enterprise installation file already includes Microsoft SQL Server Express LocalDB. During the installation, if desired, Scout Enterprise creates the required database of the type `LocalDB`. The database name is defined by the system.

Converting Microsoft JET Database

You can convert and use your Microsoft JET Database (`.mdb`) from now on as **Microsoft SQL Server Express LocalDB**.

1. First, update your existing Scout Enterprise installation to Scout Enterprise Management Suite version 14.6.1 using your mdb database.

   On the restart of the Scout Enterprise service, the database is converted to version 14.6.1 which is the first step.

2. Subsequently, install a later version of Scout Enterprise Management Suite with the same database.

   On the restart of the Scout Enterprise service, the database is automatically converted to a SQL 2014 LocalDB database.

Multiple database connections

By using the database connection editor, you can define various database connections for the Scout Enterprise Console. You then can select one or more of the defined connections when starting the console. From your console, you can use multiple connections to different databases at the same time.

The database connection editor is provided on the Windows Start menu.

Database cleanup

Outdated data can be deleted using the **Database cleanup** feature. For further information, see Database cleanup.

2.3.1. SQL LocalDB

– for Scout Enterprise Management Suite 14.7.0 and later versions –

We recommend using the integrated database Microsoft SQL Server Express LocalDB only for less than 1.000 clients or for test and evaluation environments. The required software modules are included in the Scout Enterprise installation file.

When you update an existing installation to Scout Enterprise 14.7 or later versions, the Microsoft JET Database is converted automatically to Microsoft SQL Server Express LocalDB during the installation of the update. However, the database conversion requires Scout Enterprise version 14.6.1 first.

If you want to use Microsoft SQL Server Express LocalDB, during the installation, you are requested to specify a Scout Windows user that acts as owner of the LocalDB instance. We recommend to use a technical user account that can be used by all users to access the LocalDB database and is provided with a non-expiring password. The account must be provided with the local user right **Log on as a service** and must be member of the local administrator group.

Backup of the LocalDB before installing updates

Before you update an existing Scout Enterprise installation with Microsoft SQL Server Express LocalDB, you can back up the LocalDB in two ways.

Method 1:

- Create a copy of the two files `ScoutEnterpriseLocalDB.mdf` and `ScoutEnterpriseLocalDB_log.ldf` located in the directory `C:\Users\<User name>\`

  After having installed the Scout Enterprise update, copy the database files back to the specified directory.

Method 2 (requires SQL Server Management Studio):

1. In SQL Server Management Studio, connect to
   Database `ScoutEnterpriseLocalDB`
   Instance `(localdb)\.\ScoutEnterpriseManagementSuite_Shared`
2. Use the **Backup** feature to create a backup.

   For further information, see the Microsoft documentation for SQL Server Management Studio such as https://technet.microsoft.com/en-us/library/ms189621.

After having installed the Scout Enterprise update, use the Management Studio feature **Restore** to restore the database.

Limitations of Microsoft SQL Server Express LocalDB compared to Microsoft SQL Server

- The Scout Enterprise Console can only be operated in conjunction with the Scout Enterprise service and the LocalDB database on a server system. Dedicated Scout Enterprise Consoles that can access the LocalDB database remotely are not supported.

- The **Statistics** service (keep alive messages and static asset data) and Scout Enterprise **Dashboard** (web console) cannot be used.
- The **Configuration run** command to prepare the client configuration data is not available.
- The **Database cleanup** feature to delete out-of-date data is only available with Scout Enterprise 14.9 and later versions.

2.3.2. Authentication in SQL Server

If you choose `MS SQL Server` as database type during installation, you can select between the authentication modes for the database engine `Windows authentication` and `SQL Server authentication`.

The SQL or Windows user to be specified must be member of the db_owner fixed database role in SQL Server to be able to perform the relevant configuration and maintenance activities on the database.

Mode	Description
Windows authentication	'Trusted connection', the user identity is confirmed by Windows. The Scout Enterprise service must be run with a user account that has the required access rights in SQL Server (member of db_owner). The login data of the service account can be specified in the dialog of the Scout Enterprise installation.
SQL Server authentication	User name and password must refer to a SQL Server user. The SQL user must have the relevant user rights in SQL Server (member of db_owner). The login data of the SQL user can be specified in the dialog of the Scout Enterprise installation.

2.3.3. Defining application roles for SQL Server

In order to control access from the console to the SQL Server tables, you can define a Microsoft SQL application role. The name of the application role must be defined in the **System** table of the Scout Enterprise database. The name and password can be stored either encrypted or unencrypted.

1. Add one row for the name and one row for the password :

Encrypted	Unencrypted
`ParamName=RName` and `ParamVal=<Name of the role>`	`ParamName=RName2` and `ParamVal=<Name of the role>`
`ParamName=RPass` and `ParamVal=<Password of the role>`	`ParamName=RPass2` and `ParamVal=<Password of the role>`

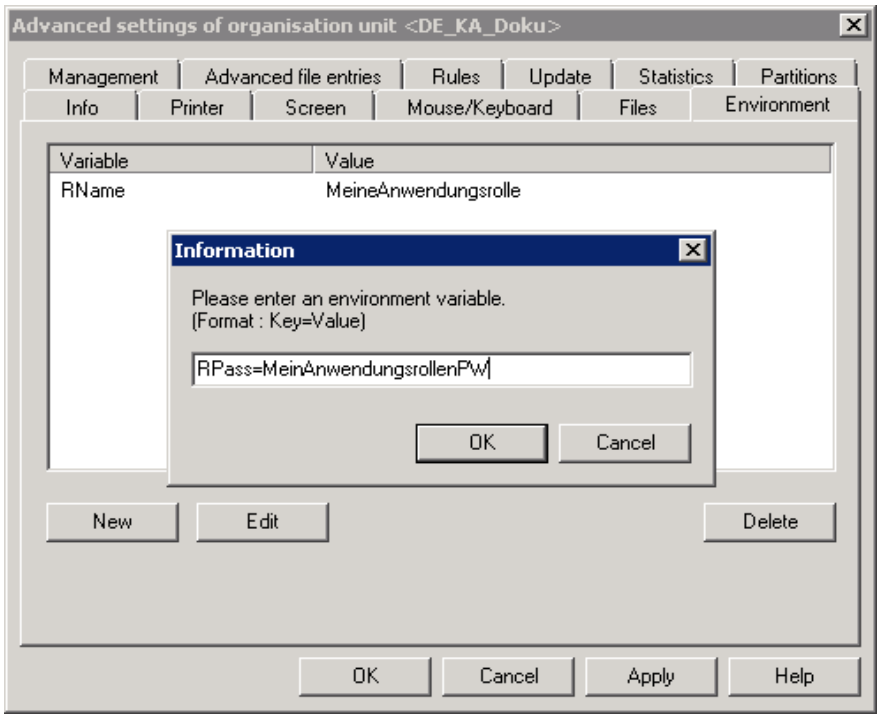
2. If you choose to specify the application role data in encrypted mode, you must encrypt the name and password of the role. For further information, see Encrypting SQL application role values.

During start of the Scout Enterprise Console, these fields are read and the application role is set.

2.3.4. Encrypting SQL application role values

If you want to use a SQL application role with encrypted values, encrypt name and password of the role:

1. In the Scout Enterprise-console, create a temporary OU such as `TEMP`.
2. Open the context menu of the `TEMP` OU and click **Advanced settings > Environment**.
3. Add two new variables for the name and password, and enter the values of the application role.



4. After having created the variables, right-click the variables, and on the context menu, click **Encrypt value**.
5. Select the variables and click **Edit**. Then copy the encrypted value to the clipboard and paste it into the SQL table.
6. Delete the temporary OU.

2.3.5. Scout Enterprise Server cluster

If you use a SQL database, several Scout Enterprise Servers can connect to one Scout Enterprise database concurrently. Concurrent Scout Enterprise Servers enable failure load balancing as well as the possibility to configure load balancing by using DNS entries (ManagerLoadBalancing).

Client devices that connect to the Scout Enterprise Server receive a list of all currently running servers that access the shared Scout Enterprise database.

FailureLoadBalancing

At start-up, the client tries to connect to the Scout Enterprise Server it was connected to last time. If, however, that server is not available, it connects to the next server from the servers list. Subsequently, this one becomes the server the client tries to access by default.

The FailureLoadBalancing mechanism restarts as soon as the client fails to connect to the same Scout Enterprise Server.

ManagerLoadBalancing

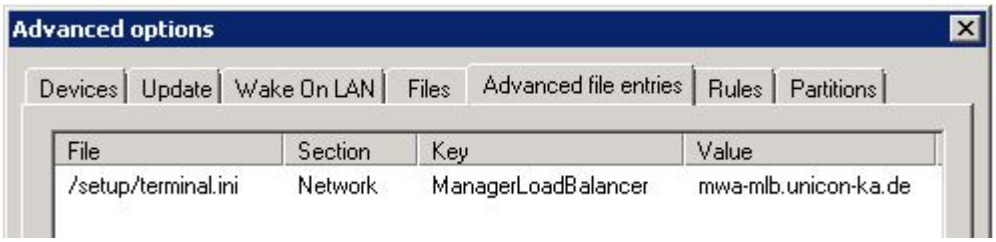
By setting the additional parameter

`ManagerLoadBalancer=`

in the `/setup/terminal.ini` file you can predefine a preferred server the clients are supposed to connect to.

This parameter can be set for all devices, for an OU or an individual device. It is defined by using the Scout Enterprise Console feature **Advanced file entries**.

File	`/setup/terminal.ini`
Section	`Network`
Entry	`ManagerLoadBalancer`
Value	*<FQDN DNS entry>*



`ManagerLoadBalancer` refers to a DNS entry pointing to the relevant Scout Enterprise Server. In a separate step the DNS entry must be defined on the DNS server. The DNS entry allows the assignment of devices to a particular Scout Enterprise Server without modifying the device configuration.

The parameters `ManagerLoadBalancer` is interpreted by the devices on each client restart.

Outline process:

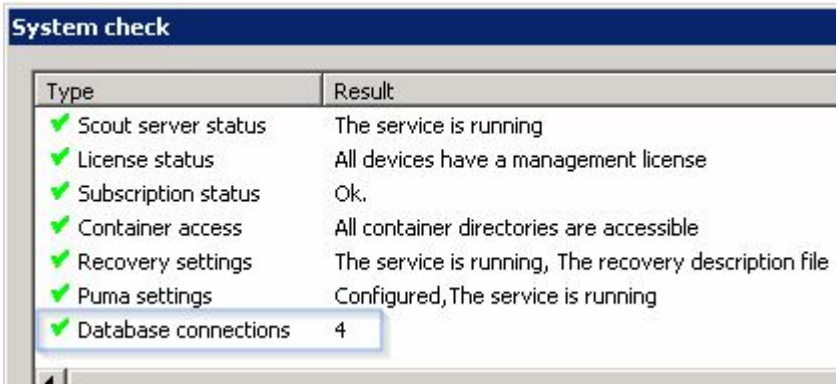
- Thin Client restarts
- DNS entry `ManagerLoadBalancer` is resolved
- Client connects to the determined Scout Enterprise Server

If, however, the Scout Enterprise Server identified by the DNS entry `ManagerLoadBalancer` is not available, the FailureLoadBalancing mechanism described above is used and the client accesses the next server from the list.

2.3.6. Number of ODBC connections

The number of ODBC connections between the Scout Enterprise Server and Scout Enterprise SQL database is defined dynamically at start-up of the server service. Normally, for each CPU kernel two ODBC connections are defined and used.

The number of database connections currently used can be viewed by using the **system check** feature (Scout Enterprise Console **View > System diagnostics > System check**).



From experience, two ODBC connections for each CPU kernel lead to good results considering

- maximum communication performance between Scout Enterprise Server and SQL database and
- optimum CPU utilization.

Static versus dynamic ODBC connections

You can specify a fixed number of ODBC connections, to meet the particular system requirements of a Scout Enterprise installation. For this, you must define the following parameter in the configuration file `eluxd.ini` of the Scout Enterprise Server:

File	`%sys-temdrive%\Users\Public\Documents\UniCon\Scout\Server\eluxd.ini`
Section	`[ELUXD]`
Para-meter	`DatabaseConnections=`
Value	`n` *(n=1-128)*

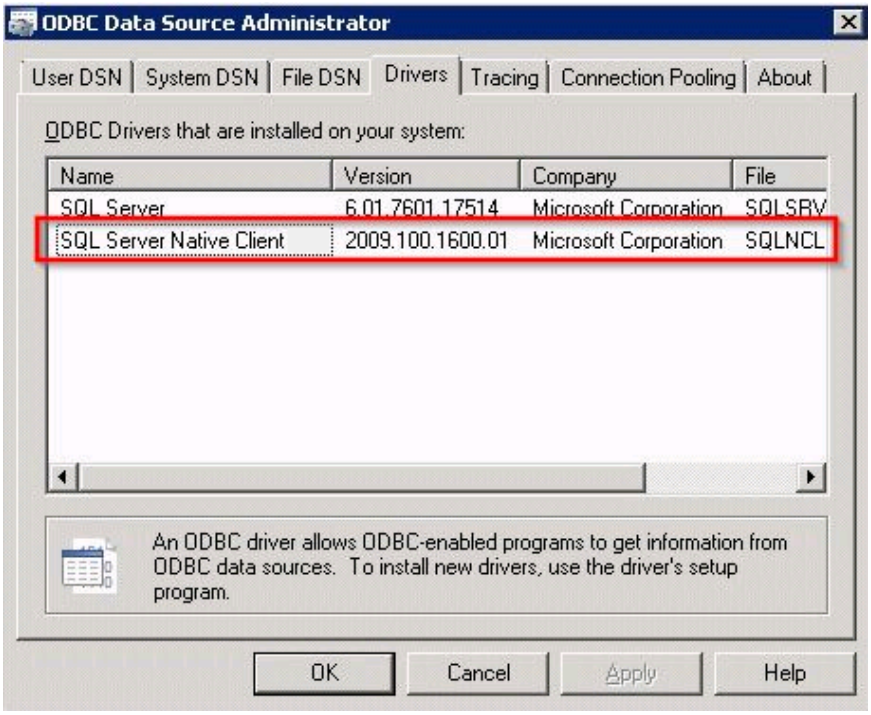
Note
Increasing the number of database connections manually can lead to CPU overload.

For further information on modifying `INI` files, see Advanced file entries.

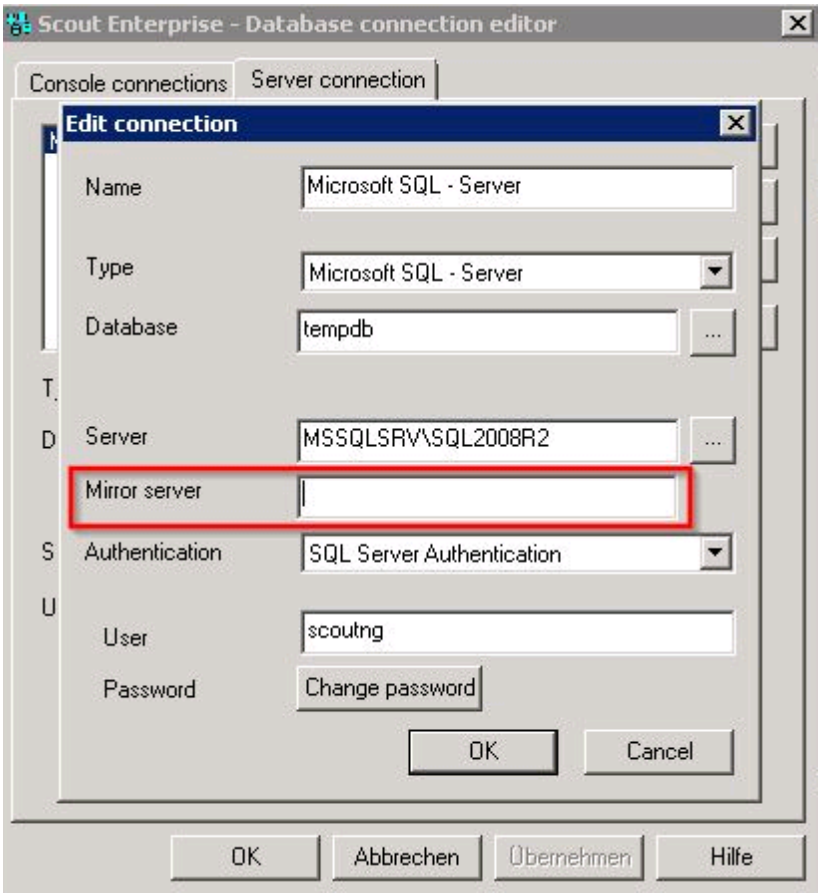
2.3.7. SQL server database mirroring

Scout Enterprise version 14.0.0 up to version 14.5.0 supports the Failover mechanism of the Microsoft SQL Server database mirroring. The SQL database mirroring support requires installing the Microsoft SQL Server Native Clients on the Scout Enterprise Server. The relevant `MSI` file `sqlncli.msi` can be downloaded as part of a Microsoft SQL Server Feature Pack. Alternatively, the file can be downloaded on the official Microsoft website.

After successful installation of the Microsoft SQL Server Native Client, the driver is shown in the ODBC data sources:



Subsequently, the mirroring server can be configured in the Scout Enterprise Database connection editor:



Note

If the Microsoft SQL Server Native Client is not installed on the Scout Enterprise Server, the **Mirror server** box in the **Scout Enterprise Database connection** dialog is hidden.

After successful configuration of the mirroring server, all relevant Scout Enterprise components are able to support the Failover mechanism of Microsoft SQL Server. However, it is important to ensure that the user credentials of the user accessing the database are identical across all affected SQL Server instances including the Security Identifier (SID). For further information on Microsoft SQL server database mirroring, see the Microsoft documentation.

2.4. Installing Scout Enterprise Management Suite

Requires
If you use Microsoft SQL Server, the databases for Scout Enterprise and Scout Enterprise Statistics must be available in Microsoft SQL Server before you start the installation process. The tables, by contrast, are created by the system during installation. For further information, see Support of databases.

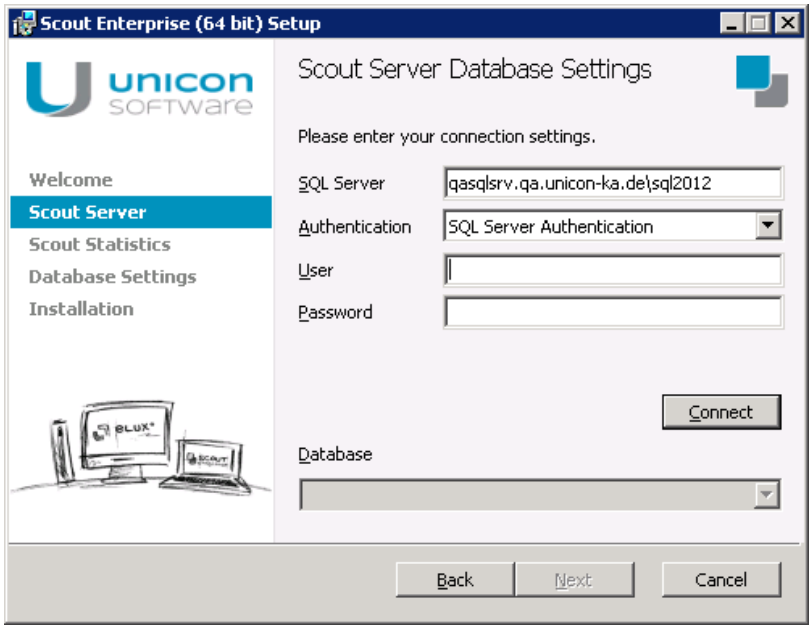
1. Download the latest version of Scout Enterprise from our technical portal www.myelux.com and unpack the `ZIP` file.

   Note
   Run Setup from a local hard drive. Do not use a USB stick, CD-R drive or a network drive.

2. Run the `Scout Enterprise.exe`[1] program as administrator.
3. Select the installation language. Then, select the type of database (`MS SQL Server` or `MS SQL LocalDB`). For further information, see Support of databases.
   Click **Install**.
4. Read and accept the license terms.
5. If you want to exclude particular components from the installation or change the installation directory, click **Customized**. After having edited the provided options, click **Next**.

   To perform the standard installation, click **Install**.
6. If you use Microsoft SQL LocalDB, specify the relevant Windows account name and password. For further information, see SQL LocalDB.
7. If you use Microsoft SQL Server, specify the required data to connect to the already existing **Scout Enterprise** database:
   - *<SQL server\instance>*
   - `SQL Server authentication` or `-Windows authentication`
     For further information, see Authentication in SQL Server.
   - *<SQL user>*
   - *<Password>*

[1] in earlier versions: `setup.exe`



Click **Connect**, and then, in the list-field, select your **Scout Enterprise** database.

In the next dialog, verify or edit the communication data to connect to the already existing **Scout Enterprise Statistics** database. Click **Connect**, and then, in the list-field, select your **Scout Enterprise Statistics** database.

To install the Statistics service, specify the TCP port and the certificate of the Statistics service.

Important

Sending 'keep alive' messages and statistical device data from the devices via HTTPS to the Statistics service requires a valid certificate for server authentication. You can deselect the Statistics service installation by using the **Customized** installation.

8. Enter a first organization unit (OU).
9. Specify the language, keyboard layout, and time zone.
10. If desired, define applications. Applications can be defined later as well. For further information, see Defining applications.
11. Start the installation process.

After successful installation, the default account `administrator` *with password* `elux` *is provided.*

Note

We strongly recommend to change the password at once to prevent unauthorized access:

- Change console password or
- Activate administrator policies

2.5. Unattended installation

Installing Scout Enterprise unattended

- Run the Scout Enterprise `Scout Enterprise`[1] program file along with the required command-line parameters:
  `"Scout Enterprise.exe" /s/v"/qn"`

Note
By performing an attended installation with the required options, the `eluxd.ini` file is created in the Scout Enterprise Server directory. This file contains several Scout Enterprise values that might be useful.

Option	Description
/v"UCPROP_DBTYPE=*2*"	0=Microsoft SQL LocalDB[2] 2= Microsoft SQL-Server
/v"UCPROP_DBNAME=*Scout*"	Scout Enterprise database
/v"UCPROP_DBSERVER=*your-server.your-domain.de\your_instance*"	Database server of Scout Enterprise database
/v"UCPROP_DBUSER=Scout-Admin"	Database user (only for SQL Server authentication)
/v"UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_"	see `eluxd.ini`
/v"UCPROP_OUNAME=*your-OU*"	OU to be created
/v"UCPROP_DESKTOP_LANGUAGE=*de_DE*"	Client desktop language setting
/v"UCPROP_KEYBOARD_LANGUAGE=*de*"	Client keyboard language setting
/v"UCPROP_LANGUAGE=*de*"	Language for the Scout Enterprise Console at startup de=german en=english If the parameter is not set, the language defined in the operating system is used.

[1] in earlier versions: `setup.exe`
[2] for Scout Enterprise Management Suite 14.6 and earlier versions: 0=Jet Engine

Option	Description
/v"UCPROP_DBNAME_STATISTIC=*Scout_Statistics*"	Scout Enterprise Statistics database
/v"UCPROP_DBSERVER_STATISTIC=*your-server.your-domain.de\your_instance*"	Database server of Scout Enterprise Statistics database
/v"UCPROP_DBUSER_STATISTIC=*Scout-Admin*"	Database user (only for SQL Server authentication)
/v"UCPROP_DBPASSWORD_CRYPTED_STATISTIC=*u[D``Gqu[w_"*	see eluxd.ini
/v"UCPROP_STATISTIC_SERVER_PORT=*22124*"	TCP port of the Scout Enterprise Statistics Service
/v"UCPROP_STATISTIC_CERTIFICATES=\"*MyCert_ServAuth*\""	Certificate of the Scout Enterprise Statistics Service
/v"ADDLOCAL=*Component 1,Component 2*" Example: `/v"ADDLOCAL=Console,Server,Report"`	Optional parameter to install particular components. Only the specified components are installed.

Example:

```
"Scout Enterprise.exe" /s /v"/qn" /v"/lv c:\temp\SetupLog.log"
/v"UCPROP_DBTYPE=2" /v"UCPROP_DBNAME=Scout" /v"UCPROP_DBSERVER=your-
server.your-domain.de\instance_sql2012" /v"UCPROP_DBUSER=Scout-Admin"
/v"UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_" /v"UCPROP_OUNAME=MyOU"
/v"UCPROP_DESKTOP_LANGUAGE=de_DE" /v"UCPROP_KEYBOARD_LANGUAGE=de"
/v"UCPROP_DBNAME_STATISTIC=Scout_Statistics" /v"UCPROP_DBSERVER_
STATISTIC=your-server.your-domain.de\instance_sql2012" /v"UCPROP_
DBUSER_STATISTIC=Scout-Admin" /v"UCPROP_DBPASSWORD_CRYPTED_STATISTIC=u
[D``Gqu[w_" /v"UCPROP_STATISTIC_SERVER_PORT=22124" /v"UCPROP_STATISTIC_
CERTIFICATES=\"MyCert_ServAuth\"" /v"ADDLOCAL-
L=Console,Server,Report,Elias,ScoutStatistic"
```

Scout Enterprise components available for installation[1]

Server
Console
Recovery
Elias
Report

[1] for Scout Enterprise Management Suite 14.6 and earlier versions, 32 bit installations require the following different component names: Server32, Console32, Recovery32, Elias32, Report32, Puma32

Puma
ScoutStatistic

Deinstalling Scout Enterprise unattended

- Run the following command:
  `"Scout Enterprise.exe" /x /s /v"/qn"`

2.6. Update to new version

To update your system to a later Scout Enterprise Management Suite version, download the required `ZIP` file from our portal www.myelux.com. Unpack and install the new version specifying your existing database.

Depending on the extent of new features updating to a new version might cause longer run-times when converting the Scout Enterprise database. If so, the relevant release notes on www.myelux.com provide details about that.

2.7. Uninstalling Scout Enterprise Management Suite

- Use the control panel to uninstall Scout Enterprise Management Suite.

Or:

1. Run the `Scout Enterprise.exe`[1] program as administrator.
2. Select **Removing program**.

[1] in earlier versions: `setup.exe`

2.8. Encryption

Encryption between the Scout Enterprise Server and the eLux clients is realized by the proprietary Scout Enterprise Management protocol on TCP-IP using the secure port 22123 and AES (Advanced Encryption Standard) encryption. The clients are required to run eLux or RP.

If you use a firewall, the port 22123 must be enabled.

2.9. Paths

Program path

Scout Enterprise version 14.0 and later is installed in

`%PROGRAMFILES%\Unicon\Scout`

Earlier versions have been installed to

`%PROGRAMFILES%\Unicon\ScoutNG`

File path for server files

Scout Enterprise log files, configuration files and more are saved to a subdirectory of

`%PUBLIC%\Documents\UniCon`

- To open the server files directory in the Windows Explorer, in the Scout Enterprise Console, click **View > System diagnostics > Server files** (only if console and server are installed on the same machine).

File path for user files

User files such as diagnostic files are saved to a subdirectory of the local user directory in

`%USERPROFILE%\Documents\UniCon\`

Note

Depending on your Windows version, the paths might vary slightly.

2.10. Certificates

For several features and applications, certificates must be provided.

- The file name extension must be `.pem` (Base64) or `.crt` (DER).
- Certificates are transferred to the client using the Files feature of the Scout Enterprise Console.
- On the client, the certificates are stored in the local certificate store `/setup/cacerts/` or in a sub-directory. The following table gives an overview:

Feature	Component	Directory
User authorization	ADS (UserAuth)	/setup/cacerts/login
User authorization	ADS+smart card (UserAuth)	/setup/cacerts/login
SSL encryption	Firefox	/setup/cacerts/firefox
SSL encryption	Chromium	/setup/cacerts/browser
SSL encryption	Citrix (ICA client)	/setup/cacerts/ and /setup/cacerts/intcerts
SSL encryption	VMware Horizon View client	/setup/cacerts/
Network login	WPA-/X-Supplicant (xsupplicant) X509/Radius SCEP (Certificate authentication)	/setup/cacerts/ /setup/cacerts/scep
VPN client / OpenVPN	vpnsystem	/setup/openvpn
VPN client / Cisco AnyConnect	vpnsystem	/setup/cacerts/ca and /setup/cacerts/client
Firmware update including certificate check	BaseOS	/setup/cacerts
RDP client	eLuxRDP	/setup/cacerts

Note
StoreFront can be called using a Citrix session or a browser.

2.11. Licensing

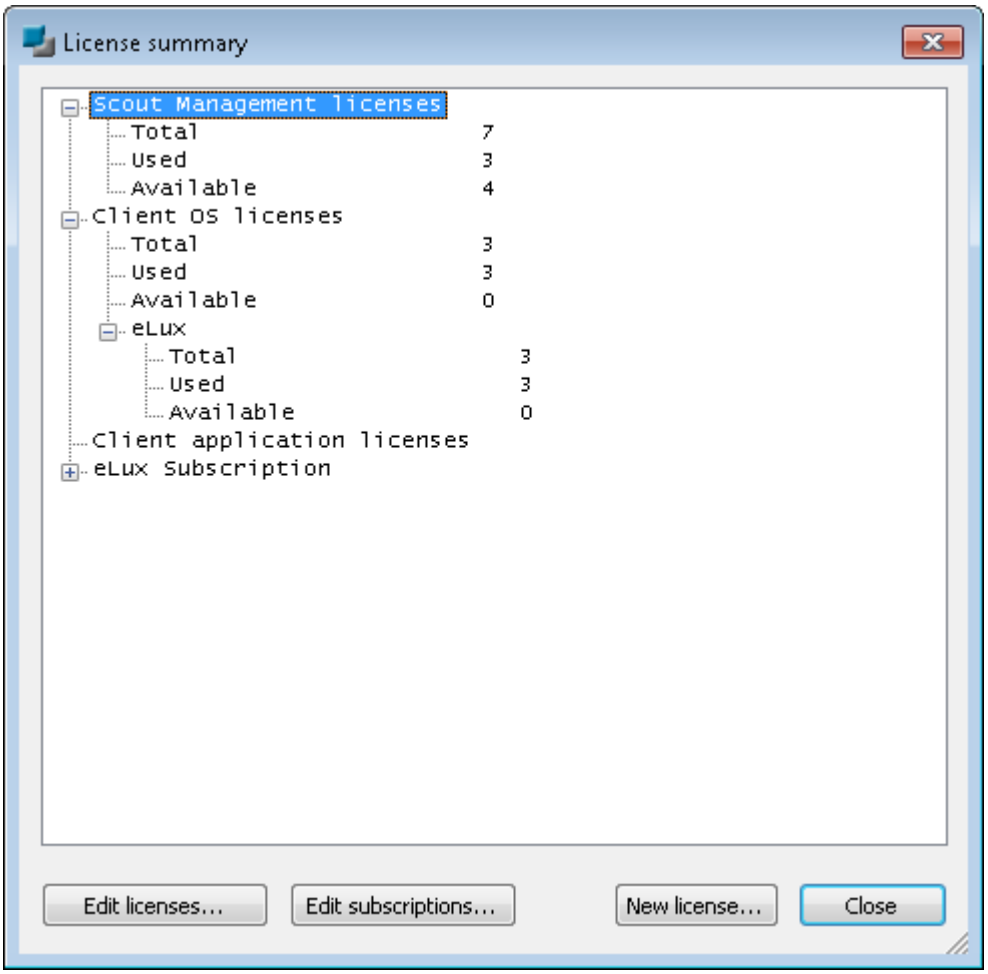
To manage clients with Scout Enterprise, each client requires a Scout Enterprise Management license. For further information on our license model, see the White Paper Licensing and Subscription.

License summary

The Scout Enterprise Server also acts as license server and manages the following license information:

- Scout Enterprise Management licenses
- Client operating system licenses
- Client application licenses
- Subscription

All managed licenses can be viewed in the Scout Enterprise Console in **Options > License information...**



Licenses displayed as **Available** are not yet allocated. They might have been ordered in advance or have been released by removed clients. Available licenses are allocated automatically to new unlicensed clients during their first contact to the Scout Enterprise manager.

New licenses

For new licenses which are not builtin, you need to generate an activation code by using the Product Activation Center of our **myelux.com** portal. You can do that by the help of the License Base Key provided on your license certificate.

In the second step, you enter the new licenses in the Scout Enterprise Console, in **License summary > New license...**, and then activate the new licenses by using the generated activation code.

For detailed instructions, see Activating licenses in our White Paper **Licensing and Subscription**.

2.12. Troubleshooting

Error message	Reason	Solution
File access error while checking HTTP/FTP server (error number = 404)	Possibly caused by missing MIME type entries for the file extensions `.idf`, `epm`, `.fpm` and `gz` as text/plain on the web server	Add the Scout Enterprise Mime types to Microsoft Internet Information Server (IIS) by executing the VB script `ScoutAddMimeToIIS.vbs`, see below.

Adding MIME types in IIS through VB script

1. Download from www.myelux.com **eLux Software Packages > eLux RP Container > Released packages >** *<Latest version>* **> Bundles > eLuxRP-*_AllPackages** the file `AllPackages.zip`. Follow the next instructions in order to execute the VB script `ScoutAddMimeToIIS.vbs` which will add the Scout Enterprise MIME type to the IIS. The VB script must be run with administrator rights.
2. Open the `zip` file and the subfolder `Support`. Copy the file `ScoutAddMimeToIIS.vbs` to `C:\temp`.
3. Execute the VBS script with admin rights.

   *The message **Add Scout MIME types to Internet Information Server** is shown.*
4. Confirm with **OK**.

   *The message **Added MIME types successfully** is shown.*

> **Note**
> Where required, the VB script must be run in the Windows command shell in C:\TEMP by using the command `wscript ScoutAddMimeToIIS.vbs`.

Troubleshooting for an installation with LocalDB

Error message	Reason	Solution
Your Microsoft Jet Database Engine (MDB) database is not up-to-date	MDB databases are not supported with later versions of Scout Enterprise Management Suite. To convert them to LocalDB, Scout Enterprise 14.6.1 is required.	First, install Scout Enterprise Management Suite version 14.6.1 with your MDB database and start the console. Subsequently, install a later version with the same database. On the first start, the database is converted automatically to Local DB.
The user verification failed	The specified user name or password are not correct.	Make sure that the specified user is available. We recommend to use a technical user account.
The user does not have the right to log on as a service	The account must be provided with the local user right **Log on as a service**.	Use a technical user account provided with the right **Log on as a service** to access the LocalDB database
The user does not have administration rights	The user must be member of the administrator group.	Make sure that the relevant account is provided with administrator rights.
Windows 2008 R2 Server oder **Windows 7 Professional**: The user does not have administration rights (in spite of being member of the administrator group)	Known bug in the operating system: The query if a user is member of the administrator group fails.	Install the Microsoft Hotfix https://support.microsoft.com/de-de/kb/2830145

3. Interface

3.1. Organizational structure

The main window of the Scout Enterprise Console shows a tree view in the upper left corner that reproduces the organizational structure with all managed devices. When you log in for the first time, you will see the organizational units **Lost&Found** and **Enterprise**[1] which are created by default. The latter serves as the top node of your organizational structure.

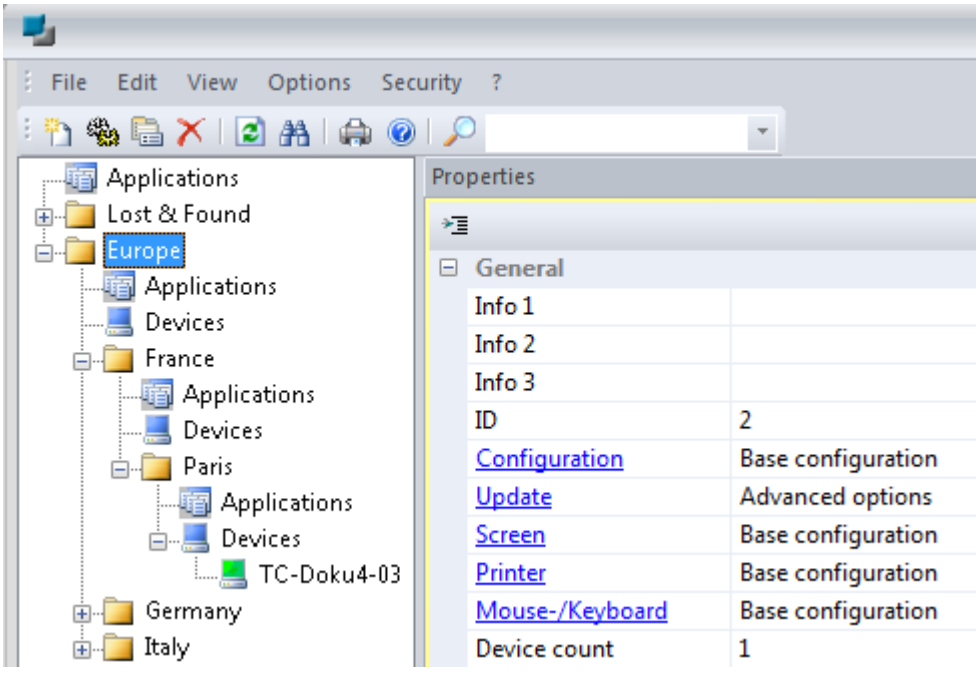
At the top level, three applications are provided that you can use to connect to a back-end:[2] **RDP**, **StoreFront** and **VMware Horizon**. For further information, see Defining applications.

To each organizational unit – hereafter referred to as OU – you can add applications, devices and other OUs. Each OU can contain subordinate OUs, applications and devices.

By default, inheritance is active. Application definitions are inherited by subordinate OUs and configuration data defined at top level is inherited by the devices.

If you add a new device to an OU, it will receive all application definitions and configuration data from this OU.

Individual devices and applications can be moved from one OU to another by using a drag-and-drop operation or the Clipboard. The devices then are assigned the properties of the new OU (if inheritance is active). For further information, see Setup/Concept.



For the element selected in the tree view, you can view several details in the **Properties** window.

[1] for Scout Enterprise Management Suite 15.0 and later versions
[2] for Scout Enterprise Management Suite 15.0 and later versions

Adding a new OU

1. For the relevant OU, open the context menu and click **Add > Organization unit...**

   *The **Advanced settings** dialog opens.*
2. Enter a unique name for the new OU.
3. If required, enter further information into the **Info** fields and edit fields on the other tabs.
4. Confirm with **Apply** and **OK**.

The new OU is shown in the tree structure. It provides the folders  *Applications and*  *Devices.*

3.2. Icons in the tree view

Icon	Description
	Organization unit (OU)
	Applications
	Device, has not connected to Scout Enterprise yet (Example: Device import)
	Device, running
	Device, switched off or not available
	Device, desktop is initializing or the log-on screen is shown
	Device, update is running
	Device, missing license to manage this device

3.3. Windows

Next to the organizational structure you can show further windows by clicking **View > Windows**:

Window	Description
Properties	Properties of the selected application, OU or device
Assets (only for devices)	Hardware information
Dynamic Client Groups	Shows the defined Dynamic Client Groups
Independent setups	OUs and devices which do not use the parent configuration For further information, see Blocking inheritance - independent configuration
Compare setups	Shows differences in the configuration between devices or OUs

Window	Description
OU devices/applications	Devices or applications of an OU in list view without icons Double-clicking on a device shows the corresponding device in the tree view. This feature an be disabled, see below.
All devices	Shows all devices in list view without icons The device data are only loaded from the Scout Enterprise database when you click the **Refresh** button. This is to avoid unintentional loading of huge data amounts. Multiple devices can be selected by pressing CTRL or SHIFT to perform bulk operations provided on the context menu such as commands. Double-clicking on a device shows the corresponding device in the tree view. This feature can be disabled, see below. To search the window content, use the **Search** field of the tool bar, type (the beginning of) a name and press SHIFT+RETURN. Press SHIFT+F3 to find the next match. For further information, see Searching for applications, devices or OUs.

Sorting columns

- Click a column header for sorting the rows.

Showing/Hiding properties

- Click the  button to define which properties you want to show.
  Alternatively, use the context menu.

Additional options in the Properties window of devices and OUs

Selected element	Option	Description
Device	**Configuration**	Double-click opens the relevant **Device setup**.
Device	**Image**	Double-click opens ELIAS with the IDF configured for the device in the relevant container.
Device	**Update State**	Double-click or **...** opens the **Update-Info** for the device providing information on performed updates. For further information, see Update-log.
OU	**Configuration**	Double-click opens the relevant **Device setup**.

Selected element	Option	Description
OU	Update	Double-click opens the relevant **Update** settings in the **Advanced Settings** for this OU.
OU	Screen, Printer, Mouse/Keyboard	Double-click opens the relevant setup (**Device setup** or **Advanced settings**) for Screen, Printer or Mouse/Keyboard.
OU	ID	Shows the ID of this OU. In addition to the decimal value you can show the hexadecimal value. This requires a new registry entry: Key: HKEY_CURRENT_USER\Software\UniCon\Scout\Settings Value name: `DisplayHexOUID` Value type: `DWORD:32` Value data: `1`

Note
Make use of the links shown in blue to quickly browse the relevant configuration and information in each context.

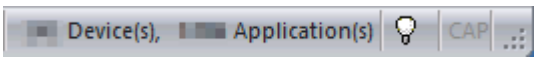
Disabling the Double-click shows device feature

By default, double-clicking a device within a device list causes the tree view to show the corresponding device. This behavior can be disabled.

- Define the following registry entries with value type `DWORD:32` and value `1`:

  HKEY_CURRENT_USER\Software\UniCon\Scout\Settings
  DisableDoubleClick_OUDevices_View
  DisableDoubleClick_AllDevices_View
  DisableDoubleClick_DCG_View

3.4. Status bar



The status bar shows on the right the total number of devices and applications.

The lamp icon can be double-clicked to view the alert messages (Error, Warning, Info) such as **Scout Enterprise Server terminated** or **Could not write Scout server log file**. The colour of the lamp icon changes to yellow as soon as there is a new entry.

3.5. Searching for devices, OUs or applications

Note
The search applies the search parameters set in the **Find** dialog.

Quick search

1. In the tree view, click to set the focus.
2. Press CTRL+F or click into the **Search** field of the tool bar.
3. Type the name of an application, device or OU.

   If configured, you can type partial words.

4. Press RETURN or click the magnifier icon.

   The first matching object is shown in the tree view.
5. To find the next match press F3 or click the magnifier icon.

Quick search in the All devices window

1. In the **All devices** window, click to set the focus.
2. Press CTRL+F or click into the **Search** field of the tool bar.
3. Type the name of a device.

   If configured, you can type partial words.
4. Press RETURN or click the magnifier icon.

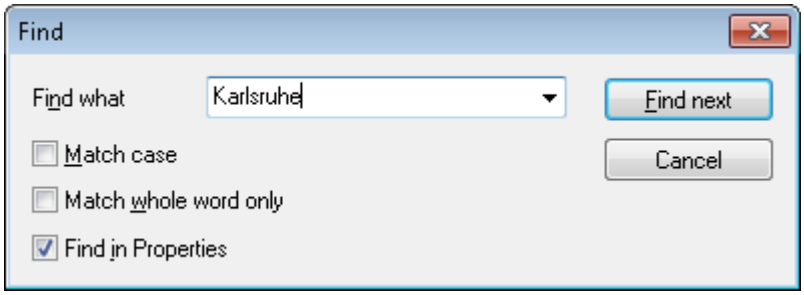
   *The first matching object is shown in the **All devices** window.*
5. To find the next match press F3 or click the magnifier icon.

Note
There is no need to have the focus on the **All devices** window if you press SHIFT+RETURN to start searching for the specified object, and if you press SHIFT+F3 to find the next match.

Searching the tree view and setting search parameters

1. Press CTRL+SHIFT+F or click **Edit > Find...**

   *The **Find** window opens.*



2. Type the name of an application, device or OU.

   If configured, you can type partial words.

3. If required, modify the search parameters.

Option	Description
Match case	Search is case-sensitive
Match whole word	Only exact matches are found, no partial words.
Find in properties	Search is also applied to **Properties** and **Assets** fields. This allows you to search for a vendor or a MAC address.

Note
The search parameters remain active after search and are also applied to the **Quick search**.

The first matching object is shown in the tree view.

4. To find the next match click **Find next** or press F3.

3.6. Moving and copying elements

Devices, OUs and applications can be moved from one OU to another OU within the tree view of the organizational structure. If inheritance is active, each device or OU after moving receives the properties of the new parent OU.

Moving devices, OUs or applications

1. Show the source and target position of the relevant element in the tree view.

   The target position can be the icon of the target OU or any valid position subordinate to the target OU.

2. Use a drag-and-drop operation to move the element from the source to the target position.
   or
   Move the element via context menu or CTRL-X to the Clipboard and paste it via context menu or CTRL-V at the target position.

3. Confirm with **Yes**.

The element is moved to the target OU.

Copying applications

Note
Applications in the tree view are application definitions and do not include software. The software must be configured and provided separately via IDF.

1. Show the source and target position of the relevant application in the tree view.

   The target position can be the icon of the target OU or the **Applcations** node subordinate to the target OU.

2. Use a drag-and-drop operation while pressing CTRL to move the application from the source to the target position.
   or
   Copy the application via context menu or CTRL-C to the Clipboard and paste it via context menu or CTRL-V at the target position.

3. Confirm with **Yes**.

The application is copied to the target OU.

Note
Applications can also be copied from any client device to a Scout Enterprise OU. For further information, see Uploading applications from client to Scout Enterprise.

3.7. Switching OU to top-level

Note
This feature can only be applied to an OU.

- For the relevant OU, open the context menu and click **Edit > Convert to base-OU**.

The relevant OU is moved to the highest level. It is one of the base-OUs. Configuration and inheritance remain as defined. If inheritance is active, it gets all settings from the base configuration.

3.8. Printing device list

Note
With Scout Enterprise 14.9 and later versions, the print feature is not available any more. Use Scout Enterprise Report Generator to create device lists according to your criteria.

1. Click **File > Print**

   *The **Print** dialog opens.*

2. Define printer and printing option.
3. Confirm with **OK**.

4. Device management

To be able to manage client devices with eLux or other operating systems, Scout Enterprise must know their MAC addresses. There are several approaches to register new clients:

- Self-registration of devices
- Discovery:Searching for devices
- Reverse Discovery: Searching for a Scout Enterprise Server

New devices must be assigned to an organizational unit (OU). You can configure if new devices

- are added to a specified OU (**default OU**)
- are assigned automatically by the OU filter according to definable criteria
- are created in terms of proxy profiles even before connecting (Reserving device profiles).

The way you want to deal with new devices is mainly defined in **Options > Advanced Options >** Devices.

Note
As the devices are organized hierarchically in OUs you can use Dynamic Client Groups to apply commands to several devices irrespective of their OU.

4.1. Self-registration of devices

By default, the first time a Thin Client boots, it automatically searches for an available Scout Enterprise Server. The client requires the IP address of the Scout Enterprise Server.

Requirements for self-registration:

- Thin Client must be in initial state (either upon delivery or by performing a factory reset)
- Thin Client must be connected to the network
- The Scout Enterprise IP address must be configured in one of the following ways:
  - DHCP: A configured DHCP option is set to the IP address/name of the Scout Enterprise Server. You can also specify more than one Scout Enterprise Server and a destination OU. For further information, see DHCP configuration.

  or

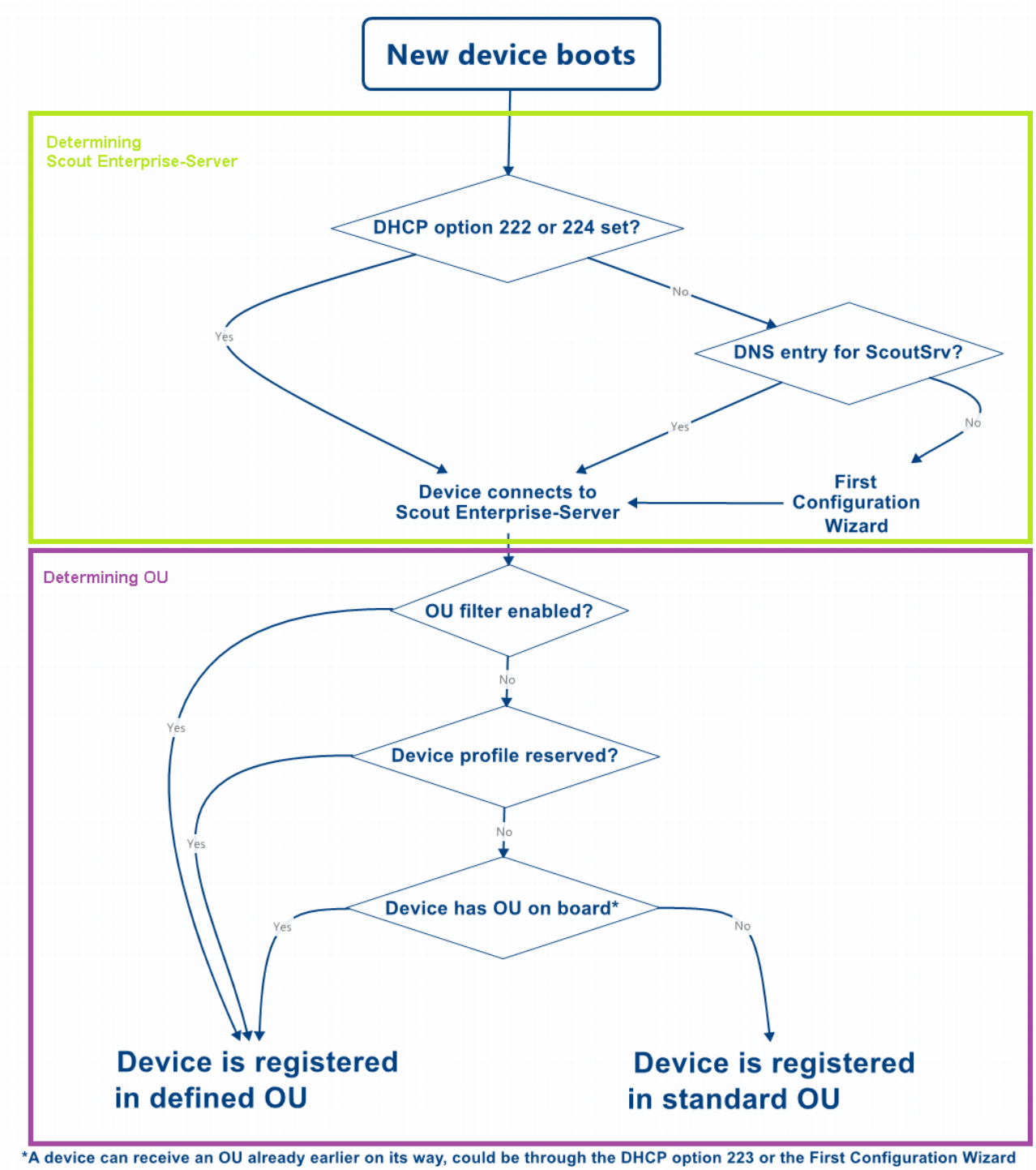
  - DNS: The DNS server resolves the host name `ScoutSrv` (no case-sensitivity).

If the Scout Enterprise Server's IP address cannot be determined, neither by the DNS nor by DHCP, a First Configuration Wizard automatically runs on the Thin Client to help the local user through the initial configuration.

Registering a device automatically

- Turn the Thin Client on.

If the requirements for self-registration are met, the device contacts the Scout Enterprise Server and enters itself in the defined OU or the standard OU. It receives the configuration of the OU and is restarted with the new configuration.



*A device can receive an OU already earlier on its way, could be through the DHCP option 223 or the First Configuration Wizard

The flow chart roughly shows the way a new device is assigned to a Scout Enterprise Server and to an OU. Details such as the **Accept only known devices** have not been considered.

4.2. DHCP configuration

Note
DHCP options can only be applied to eLux clients.

A new client booting for the first time can retrieve the following information from a DHCP server:

- IP address or name of the Scout Enterprise Server (option 222)
- List of Scout Enterprise Servers (option 224)
- ID of the destination OU on the Scout Enterprise Server (option 223)

This requires configuring the DHCP server by using one of the two following methods.

In Method 1 (recommended), you define a new vendor class, set the new options, and apply the values. Method 2 uses the DHCP Standard Options 222, 223 and 224.

The following instructions are based on the DHCP manager of Windows Server 2008.

Method 1: Defining user-defined vendor class

Requires
DHCP server compliant with RFC 2132, supporting user-defined vendor classes. Otherwise use Method 2.

1. Open the DHCP manager.
2. Select the relevant DHCP server, and then click **Action > Define...**
3. Click **Add...** to create a new class:

Option	Value
Display name	eLux NG
Description	eLux specific options
Code (in **ASCII** column)	ELUXNG *The entry is automatically extended with the related hexadecimal number (45 4C 55 58 4E 47).*

4. Click **Action > Set Predefined Options...**, and then, in the **Option class** list field, select `eLux NG`.
5. If you want to define a Scout Enterprise Server, click **Add...** to create a new option:

Option	Value
Name	Scout Enterprise Server
Data type	String

Option	Value
Code	222
Description	Name or IP address of the Scout Enterprise Server

6. If you want to define more than one Scout Enterprise Server, click **Add...** to create a new option:

Option	Value
Name	Scout Enterprise Server list
Data type	String
Code	224
Description	Server names/IP addresses, comma-separated

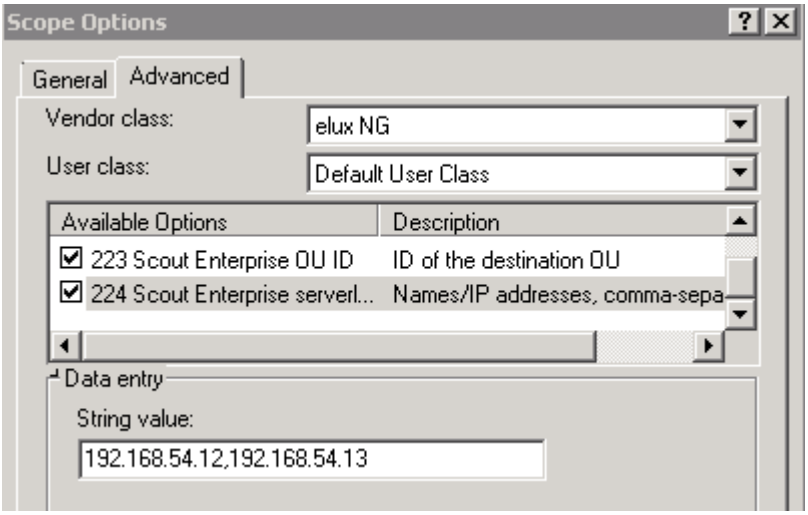
7. If you want to assign new devices to a specific OU, click **Add...** to create a new option:

Option	Value
Name	Scout Enterprise OU ID
Data type	Long
Code	223
Description	ID of the destination OU

8. To assign the options, for the relevant DHCP server, select either the **Server Options**, the **Scope options** or the **Reservations**, and then click **Action > Configure Options... > Advanced**.

   In the **Vendor class** list field, select `elux NG`. Select each of the defined options and enter its value into the **Data entry** field:

Option	Value
222 Scout Enterprise Server	*<Name or IP address of the Scout Enterprise Server>*
223 Scout Enterprise OU ID	*<ID of the destination OU>*
224 Scout Enterprise Server list	*<Names or IP addresses of the Scout Enterprise Servers, separated by comma>*



Method 2: Using DHCP Standard Options

Requires

The DHCP Standard Options `222`, `223` and `224` must be available. Otherwise use Method 1.

1. Open the DHCP manager.
2. Select the relevant DHCP server, and then click **Action > Set Predefined Options...**. In the **Option class** list field, select `DHCP Standard Options`.
3. Click **Add...** to create the following Standard Options, as described for Method 1:
   - Scout Enterprise Server, String, 222
   - Scout Ernteprise server list, String, 224
   - Scout Enterprise OU ID, Long, 223
4. To assign the options, for the relevant DHCP server, select either the **Server Options**, the **Scope options** or the **Reservations**, and then click **Action > Configure Options... > General**.

   Select each of the defined options and enter its value into the **Data entry** field:

Option	Value
222 Scout Enterprise Server	*<Name or IP address of the Scout Enterprise Server>*
223 Scout Enterprise OU ID	*<ID of the destination OU>*
224 Scout Enterprise Server list	*<Names or IP addresses of the Scout Enterprise Servers, separated by comma>*

4.3. Searching for devices (Discovery)

Based on the IP address, you can search for devices throughout the entire network or within particular subnets. Any matching devices are registered automatically to Scout Enterprise and are added to the specified OU (**Destination group**). The devices are restarted and receive the configuration of the destination group (device configuration, application definitions, files defined for transfer and advanced file entries).

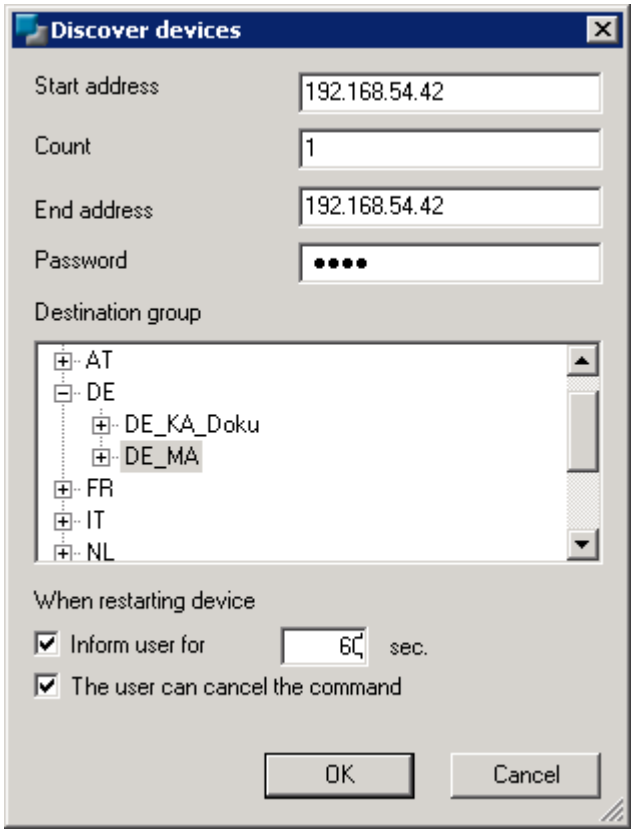
Note
If the OU filter is active, the filter specifies the destination group or groups. For further information, see Advanced settings/Devices.

Requirements:

- The devices are turned on and connected to the network.
- The devices are provided with valid IP addresses.
- The device password is known.

Searching and registering devices

1. Make sure that the destination group is configured correctly.
2. Select **Options > Search devices**.



3. Edit the following fields:

Start address	First IP address of the range
Count	Number of IP addresses within the range (restricted to 255)
End address	Last IP address of the range
Password	Device password (default: `elux`) The password must match the password currently set on the particular clients.
Destination group	OU the devices should be assigned to Default is the predefined `Lost&Found` group with the base configuration.
	Important If the **Destination group** field is disabled, the OU filter is active and the matching devices are assigned according to the OU filter rules.
Inform user	The user is informed by a message about the upcoming client restart. Specify in seconds how long the message shall be displayed.
User can cancel the command	Allows the user to suppress the client restart. The configuration is not updated until the client is restarted.

4. Confirm with **OK**.

The matching devices receive the IP address of the managing Scout Enterprise Server. The devices are assigned to their destination group and are restarted. The devices inherit the configuration of their new OU. If there has been any local non-protected configuration, it is overridden. With immediate effect, on each restart, the clients connect to their Scout Enterprise Server and, if available, are given the latest configuration and application definition data.

If a device profile for a client had been reserved previously, the predefined profile is assigned automatically at Discovery.

To modify response time and maximum searching time for the Discovery feature, use **Options > Advanced options > Devices > Discover devices**.

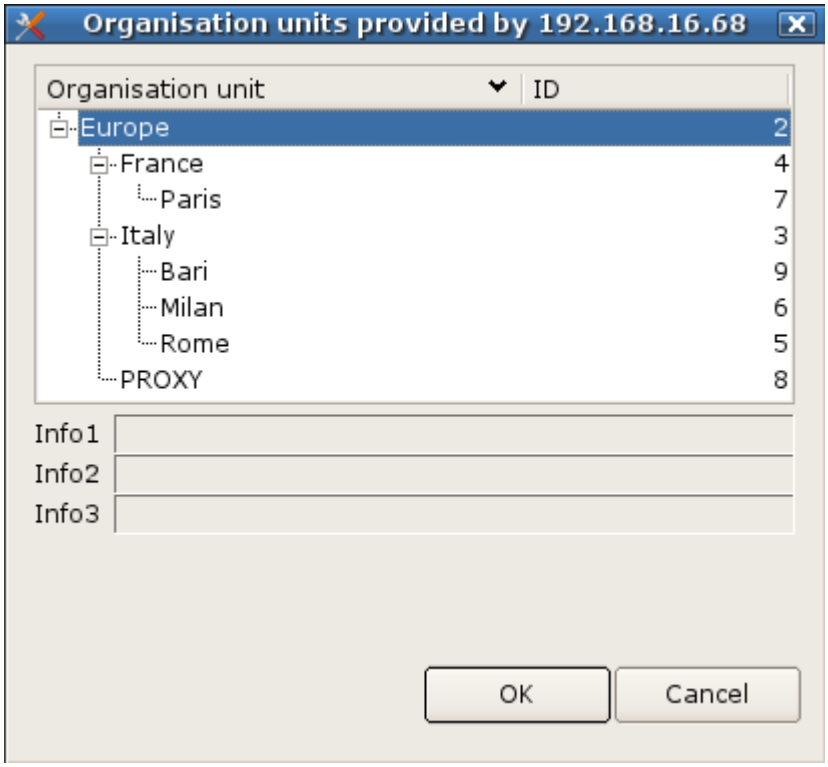
Note
Devices already registered to Scout Enterprise are not modified, only their status is updated when connected.

4.4. Executing the Reverse discovery

A client can search for its destination OU by using the **Reverse discovery** feature.

1. In the eLux control panel, click **Setup > Security**.
2. In the **Scout Enterprise** box, enter name or IP address of the Scout Enterprise Server.
3. Click **...**

   A window shows all OUs available on the specified Scout Enterprise Server.



4. Select an OU.
5. Confirm with **OK** and **Apply**.

After restarting the device it is assigned to the selected OU. The host name of the decvice is registered in Scout Enterprise as device name.

If a device profile for the client had been reserved previously, the pre-defined profile is assigned automatically at Reverse Discovery.

4.5. Reserving device profiles

Devices can be assigned to OUs even before the devices connect to Scout Enterprise for the first time.

By creating devices manually in the Scout Enterprise Console, you reserve a device profile in terms of the MAC address. As soon as such a manually created device contacts its Scout Enterprise Server for initial start-up, the already registered MAC address is recognized and the device is entered. The configuration data of the relevant OU are transferred to the device.

Reserving device profiles can be applied for the following device registration procedures:

- Discovery
- Reverse Discovery
- DNS alias name `ScoutSrv`
- DHCP option `222` for the Scout Enterprise Server

Note
If an OU filter is active, the OU filter precedes device profile reservation.

Reserving a device profile

1. Select the relevant OU you want to assign the device to, and show its sub tree.
2. Open the **Devices** context menu within the OU and select **Add...**
3. Enter the 12-digit MAC address of the device, without hyphens.
   *If the MAC address is valid, the **Setup** dialog opens. The **Use parent** option is selected by default.*
4. Confirm with **OK**.

Scout Enterprise reserves a profile for the device with the relevant MAC address. The actual registration is made at the time of the first client connection.

Note
Importing devices does also result in the reservation of device profiles within the OU structure. If you aim to create new devices in a greater number we recommend to use the **Import** feature. For further information, see Import/Export.

4.6. Secure device management with Scout Enterprise

For adding new clients to Scout Enterprise there is provided an enhanced security level.

Clients that are registered with their MAC addresses in the Scout Enterprise database (reserved device profile) are accepted by the Scout Enterprise Server and can be integrated to the Scout Enterprise management. In contrast, clients having an unknown MAC address are not accepted and therefore cannot be managed by Scout Enterprise. Unknown clients are not provided with a license from Scout Enterprise's license pool.

Accept only known clients:

1. In the Scout Enterprise Console, select **Options > Advanced options > Devices > New**
2. Select the **Accept only known devices** option.

If an unknown device tries to contact the Scout Enterprise Server, an error message is displayed on the client saying that the connection to the Scout Enterprise Server was denied.

Note

Only the requests of those clients are accepted whose MAC addresses are already saved to the Scout Enterprise database by a device import or device profile.

4.7. OU filter

The OU filter can be used for automatic assignment of devices to an organization unit (OU) based on defined criteria. This is particularly helpful with the registration of new devices and for relocating devices.

You can configure the OU filter in two ways:

- The Subnet filter uses the client network address for filtering
- The User-defined filter uses any configured asset information of the devices for filtering

You can only use one of the two filters at the same time. For each filter, you can define multiple filter rules and specify the sequence you want the rules to be processed.

Once defined, the filter rules are retained until you delete them explicitly. Deactivate filter rules which are currently not required but which you want to keep for future use.

The OU filter has precedence over

- OU assignment of devices by using the DHCP option 223
- Discovery of new devices via Scout Enterprise
- selecting the OU in the First Configuration Wizard locally on the Thin Client
- the default OU specified in **Advanced options > Devices**.

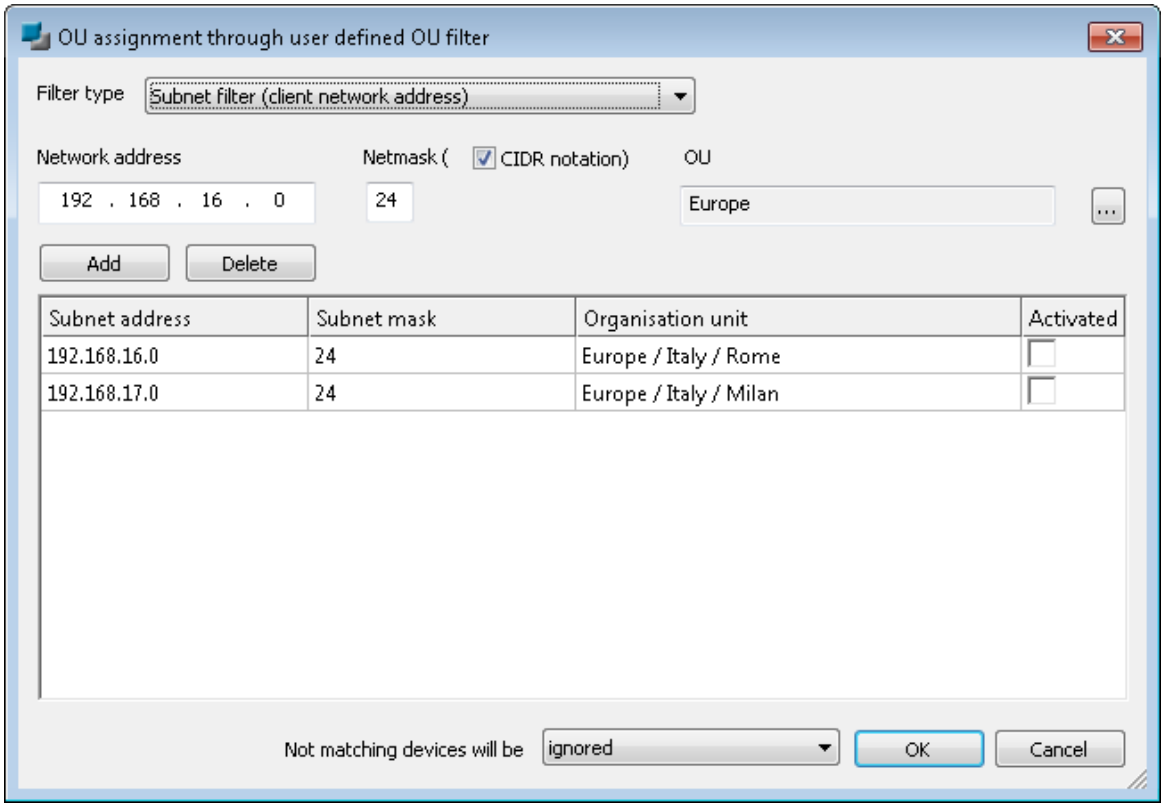
OU filters are included when exporting the data category **Advanced options**. For further information, see Import/Export.

4.7.1. Setting up an OU filter as subnet filter

You can use the OU filter to filter on client network addresses and assign the matching devices to an OU.

1. Click **Options > Advanced options... > Devices**.
2. Under **New devices**, select the **Assign OU depending on the OU filter** option.
3. Click the **...** button to configure the filter.
4. In the **Filter type** list, select `Subnet filter (client network address).`
5. In the **Network address** box, enter the scope of IP addresses.
   Example: `192.168.16.0` covers all IPs starting with `192.168.16.`
6. In the **Netmask** box, enter the relevant network prefix.
7. In the **OU** list, select the OU the devices should be assigned to. Click **...** to browse.
8. Click **Add**.

   The filter rule is displayed in the field below.



9. If required, add more filter rules and configure them. For further information, see Editing OU filter rules.
10. In the **Non-matching devices will be** list , select where you want the non-matching devices to go.

Important

If you select `assigned to the default OU`, all non-matching devices and even devices already assigned to other OUs are reassigned to the default OU.

11. Review all active filter rules thoroughly to avoid unintentional assignments.
12. Confirm with **OK**.

All active filter rules are processed. On the next restart, the matching devices are assigned to the OUs as defined by the OU subnet filter. If there exist user-defined filter rules in parallel, they are of no relevance.

4.7.2. Setting up an OU filter as user-defined filter

You can filter on configured asset information of the devices to assign the matching device to the appropriate OUs.

Devices with eLux RP version 4.6.0 and later send a **OU filter text** field containing device information about themselves to the Scout Enterprise Server. You can use the **OU filter text** field in the report generator and for the user-defined OU filter. It includes the values for the following features:

Host name, OS name, OS version, serial number, supplier, device type, BIOS, CPU speed, model,kernel version, flash type, flash size, RAM size, graphics.

1. Click **Options > Advanced options... > Devices**.
2. Under **New devices**, select the **Assign OU depending on the OU filter** option.
3. Click the **...** button to configure the filter.
4. In the **Filter type** list, select `User-defined filter (configured asset information)`.
5. In the **Filter rule** box, enter one or more filter criteria. A filter criterion is composed of three parts:
   - an asset information string as specified in the **OU filter text** field
   - the logical operator =
   - the value you want to filter by.

   Example: `ELUX_OSNAME=eLux RP`

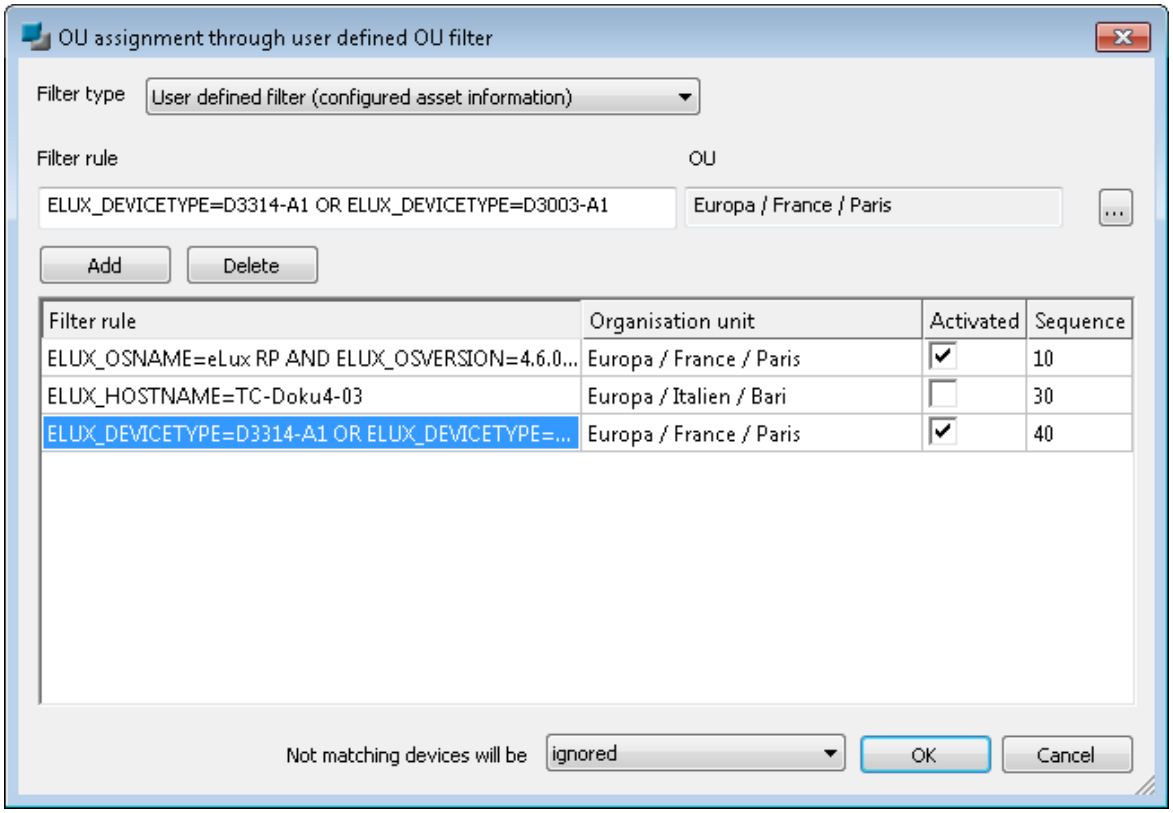
   Use the logical operators AND and OR to link together several filter criteria. Make sure to use capital letters for the operators.

   Wildcards are not supported, but all matches are found that begin with the specified string.

   Example for the values of an **OU filter text** field:
   `ELUX_HOSTNAME=Inga;ELUX_OSNAME=eLux RP5;ELUX_OSVERSION=5.3.0; ELUX_SERIAL=44015379;ELUX_SUPPLIER=FUJITSU;ELUX_DEVICETYPE=D3314-A1; ELUX_BIOS=V4.6.5.4 R1.4.0 for D3314-A1x;ELUX_CPU=998;ELUX_PRODUCT=D3314-A1; ELUX_KERNEL=3.4.71;ELUX_FLASH=4GB NANDrive;ELUX_FLASHSIZE=3849; ELUX_MEMORY=2048;ELUX_GRAPHICS=ATI AMD Radeon HD8210E`

   Examples for filter criteria:
   Example 1: `ELUX_OSNAME=eLux RP5 AND ELUX_OSVERSION=5.2`
   Example 2: `ELUX_DEVICETYPE=D3314-A1 OR ELUX_DEVICETYPE=D3003-A1`
6. In the **OU** list next to the **Filter rule** box, select the OU the devices should be assigned to. Click **...** to browse.
7. Click **Add**.

   The filter rule is displayed in the field below.



8. If required, add more filter rules and configure them. For further information, see Editing OU filter rules.
9. In the **Non-matching devices will be** list, select where you want the non-matching devices to go.

Important

If you select `assigned to the default OU`, all non-matching devices and even devices already assigned to other OUs are reassigned to the default OU.

10. Review all active filter rules thoroughly to avoid unintentional assignments.
11. Confirm with **OK**.

All active filter rules are processed in the specified order. On the next restart the matching devices are assigned to the OUs as defined by the OU user-defined filter. If there exist subnet filter rules in parallel, they are of no relevance.

4.7.3. Editing OU filter rules

Once you have defined OU filter rules they remain until they are deleted explicitly. You can edit the filter rules in the following ways:

1. Click **Options > Advanced options... > Devices**.
2. Under **New devices** next to **Assign OU depending on OU filter**, click **...** to open the **OU filter** dialog.
3. In the **Filter type** list, select the required option.

4. Use the following features:

Option	Action	Description
Add	Click button	**User-defined filter**: The filter criteria of the **Filter rule** field and the destination OU selected in the **OU** field are added as new filter rule to the list. Syntax for a filter criterion: `<String from OU Filtertext>=<Wert>` You can combine two or more filter criteria by using one of the logical operators `AND` or `OR`. Make sure to use capital letters for the operators. For examples, see Setting up an OU filter as user-defined filter. **Subnet filter**: The data from the fields **Network address**, **Netmask** and **OU** are added as new filter rule to the list.
Delete	Click button	The selected filter rule is deleted.
Edit filter rule	Select filter rule and press F2 or double-click	You can modify the filter rule right in the list.
Activate / Deactivate	Select/Clear **Activated** option	Deactivated filter rules are not executed. Newly added filter rules are active by default.
Change sequence of processing (user-defined filter)	Edit **Sequence** field	Filter rules with low sequence number are processed prior to filter rules with high sequence number.

5. In the **Non-matching devices will be** list, select where you want the non-matching devices to go.

Important

If you select `assigned to the default OU`, all non-matching devices and even devices already assigned to other OUs are reassigned to the default OU.

6. Review all active filter rules thoroughly to avoid unintentional assignments.
7. Confirm with **OK**.

All active filter rules are processed in the specified order. On the next restart the matching devices are assigned to the OUs as defined by the OU filter.

4.7.4. Deactivating OU filters for particular devices

If the OU filter is enabled, all active filter rules are executed and the matching devices are assigned to the specified OU on their next restart. If you want to except an individual device from the filter, you can deactivate the OU filter for that device.

1. For the relevant device, open **Advanced settings > Management**.
2. Under **New devices**, select the **Ignore OU filter** option.
3. Confirm with **OK**.

Or:

1. By using a drag-and-drop operation, move the device to another OU.
2. Confirm with **OK**.

The device is assigned to the new OU and the OU filter is deactivated for this device.

4.8. Dynamic Client Groups

Dynamic Client Groups enable administrators to run cross-OU commands for freely definable device groups. For example, you can send a message to all devices with a particular image throughout the whole organization. Or, you can run a BIOS update on all devices with a particular BIOS version, across all OUs. Even client relocation to another Scout Enterprise Server can be applied to a Dynamic Client Group.

Dynamic Client Groups are based on reports created in the Scout Enterprise Report Generator which extract the desired devices. These reports are exported to the Scout Enterprise Console once, and from that point onward, are displayed as a **Dynamic Client Group**. Any commands applicable to OUs or to individual devices can be applied to a dynamic Client Group.

Dynamic Client Groups are displayed in the Scout Enterprise Console in a special window and remain there for re-use until they are deleted. They can be updated any-time with a click.

When you create Dynamic Client Groups, access rights are respected as defined in administrator management.

4.8.1. Requirements for Dynamic Client Groups

- Scout Enterprise Management Suite 13.4.2 or later
  Download on www.myelux.com.
- Scout Enterprise Report Generator of Scout Enterprise Version 13.4.2 or later
- Report layout must include the MAC address. The report type must be **List of devices** or **List of asset entries**.

For further information on defining Dynamic Client Groups, see Creating Dynamic Client Groups in the Scout Enterprise Report Generator guide.

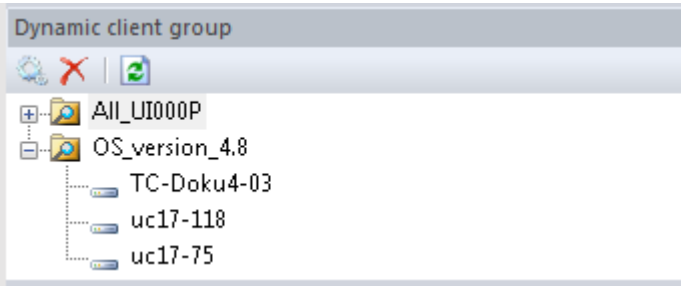
4.8.2. Using Dynamic Client Groups

Dynamic Client Groups are usually based on reports that have been created in Scout Enterprise Report Generator and exported to the Scout Enterprise Console.

For further information on defining and exporting, see Creating Dynamic Client Groups in Scout Enterprise Report Generator guide.

Displaying Dynamic Client Groups

1. In the Scout Enterprise Console, click **View > Window > Dynamic Client Groups...**.



*The **Dynamic Client Groups** window is displayed. The Dynamic Client Groups can be expanded to show the matching devices.*

Note
The Dynamic Client Group shows those devices that have matched the criteria at the time of the latest report generation. Make sure that the Dynamic Client Group is up-to-date.

For a selected Dynamic Client Group, the **Properties** window shows the **Creation date**, **Number of devices** and **Filter** criteria of the used report. The creation date refers to the date of the latest generation of the report the Dynamic Client Group is based on, and thus indicates if the Dynamic Client Group is up-to-date.

If, for example, new devices have been integrated into the database and these devices match the criteria of the report, the Dynamic Client Group is not up-to-date any longer. You can, however, update the Dynamic Client Group by re-creating the report right from the Scout Enterprise Console.

If a Dynamic Client Group is not needed anymore, you can delete it by using the button. The report the Dynamic Client Group was based on remains unaffected.

Updating Dynamic Client Groups

1. In the **Dynamic Client Groups** window, select the relevant client group.
2. On the toolbar of the **Dynamic Client Groups** window, click the **Recreate** button .

*The relevant report is re-created and exported. The resulting devices are shown below of the Dynamic Client Group as extracted from the database. In the **Properties** window, in the **Creation date** field, the current point of time is displayed.*

Note
The **Refresh** button refers to the view only. The report is not updated by this command.

Applying commands and notifications to Dynamic Client Groups

1. In the **Dynamic Client Groups** window, select the relevant Dynamic Client Group, and then check the information shown in the **Properies** window.
2. Update the Dynamic Client Group by using the **Re-create** button to make sure that exactly the currently matching devices are affected.
3. Open the context menu of the Dynamic Client Group and select a command or notification.

Commands and notifications are applied to the matching devices, irrespective of their OU. The available commands can also be scheduled for later execution.

4.8.3. Special form of Dynamic Client Groups by import

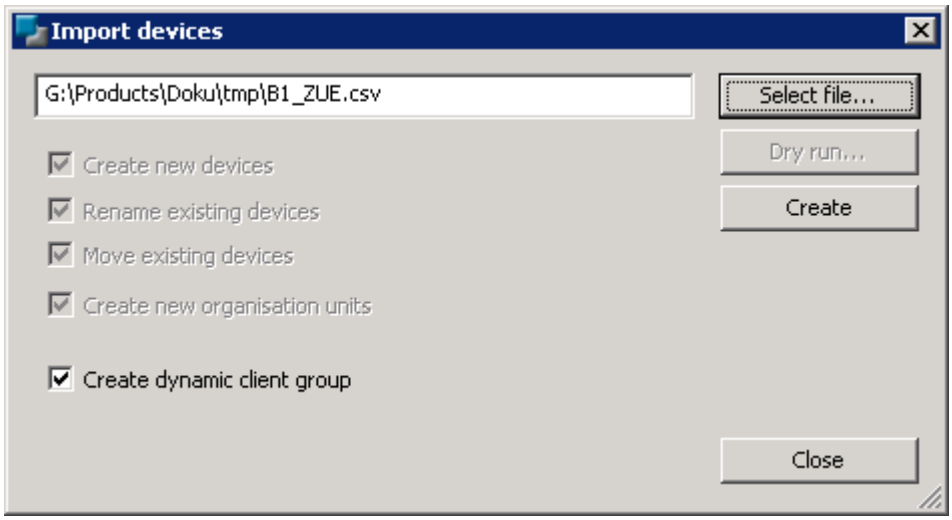
– with Scout Enterprise 14.9 and later versions–

To create a Dynamic Client Group, instead of using Scout Enterprise Report Generator, you can use the **Import** feature of the Scout Enterprise Console to make up a client group based on a device list containing MAC addresses. The advantage is that you are completely free to select any devices you want, they just must be registered in Scout Enterprise. Note that you use the **Import** feature but do not perform an import of devices.

Creating Dynamic Client Groups by import

Requires
The relevant devices must be listed with their MAC addresses in a `.csv` file. Each line must begin with a MAC address. The lines may contain further information but only the MAC address is evaluated.

1. In the Scout Enterprise Console, click **File > Import > Devices...**.



2. In the **Import devices** dialog, in the bottom section, select the **Create Dynamic Client Group** option.

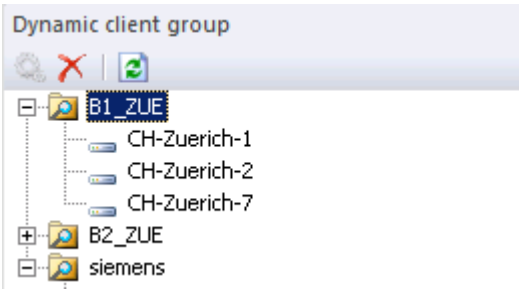
   All options related to the device import are disabled.

3. Click **Select file...** and select the relevant `.csv` file from the file system.
4. Klicken Sie auf **Erstellen**.

Die `.csv`-Datei wird ausgewertet. Scout Enterprise erstellt eine neue Dynamische Gerätegruppe, die alle Geräte der `csv`-Liste enthält, deren MAC-Adresse in Scout Enterprise registriert ist. Die Dynamische Gerätegruppe übernimmt den Namen der `csv`-Datei.

Displaying Dynamic Client Groups

- In the Scout Enterprise Console, click **View > Window > Dynamic Client Groups...**.



*The **Dynamic Client Groups** window is displayed. The Dynamic Client Groups can be expanded to show the matching devices.*

Note

Dynamic Client Groups that have been created cannot be updated by using the **Re-create** button. To update the client group, after having modified the device list, you are required to perform a new import in the way described above using the modified `*.csv` file under the same name.

For a selected Dynamic Client Group, the **Properties** window shows some information such as the **Creation date** and **Number of devices**. The **Filter** field shows the entry `created by device import`.

Applying commands and notifications to Dynamic Client Groups

1. In the **Dynamic Client Groups** window, select the relevant Dynamic Client Group, and then check the information shown in the **Properies** window.
2. Open the context menu of the Dynamic Client Group and select a command or notification.

Commands and notifications are applied to the matching devices, irrespective of their OU. The available commands can also be scheduled for later execution.

4.9. Client relocation between servers

Relocating devices from one Scout Enterprise Server to another can be very helpful in different scenarios relating to device migration. For example, if you want devices to be relocated from a test/QA server to a production server or if several Scout Enterprise Servers are to be consolidated to a single server (server fusion).

With Scout Enterprise version 14.6 and later, client relocation can be performed with and without the clients verifying the availability of the target server. A so-called 'offline' relocation does not require the target server to be physically available at the point in time of the relocation.
Example:External suppliers, in their environment, set up devices to be used in the customer's environment.

Client licenses and their Subscription can either be included in the transfer or left on the source server.

Requirements:

- Scout Enterprise version 14.5.0 or later
- eLux RP version 4.10.0 or later

4.9.1. Relocation procedure

The relocation procedure is initiated by the source server (device-releasing server) and completed by the target server (device-receiving server). The actual relocation procedure, however, is performed by the client and includes the required testing of the surrounding conditions, and - if required -the transfer of client licenses and a proportion of the remaining Subscription validity.

Relocation is triggered by the notification **Initiate client relocation** for the relevant devices in the Scout Enterprise Console of the source server. The notification includes all required details. On the next client restart, the configuration data of the target server is replicated and the clients evaluate the relocation notification.

The clients then check if the transmitted target server's address is available via the network. Moreover, the clients verify, if the Scout Enterprise version of the target server is version 14.5.0 or later.If both results are positive, relocation can take place and the clients are deleted from the source server.

By default, the clients transmit the information on their licenses and proportional Subscription validity they had been provided with by their source server to the target server, and this license and Subscription information is deleted on the source server along with the clients and added on the target server. The target server's amount of licenses and Subscription is updated accordingly. If, however, you want to leave the license and Subscription information on the source server to be used by other devices, you can specify that in the notification.

The new clients are assigned to the specified OU on the target server. If you have not specified a particular destination OU, the default OU or the OU according to the OU filter rules is used (configured in **Options > Advanced options > Devices > New devices**).

The relocation procedure is completed by an automatic restart of the devices to activate the configuration of the target server. If the OU filter is used, an additional restart of the clients is provoked by the system right after assignment.

Important

Do NOT reserve device profiles by entering the MAC addresses of the new devices on the target server before client relocation. If the devices are already registered on the target server, licenses and Subscription will NOT be updated.

4.9.2. Relocation procedure / offline

– Requires Scout Enterprise version 14.6 and later –

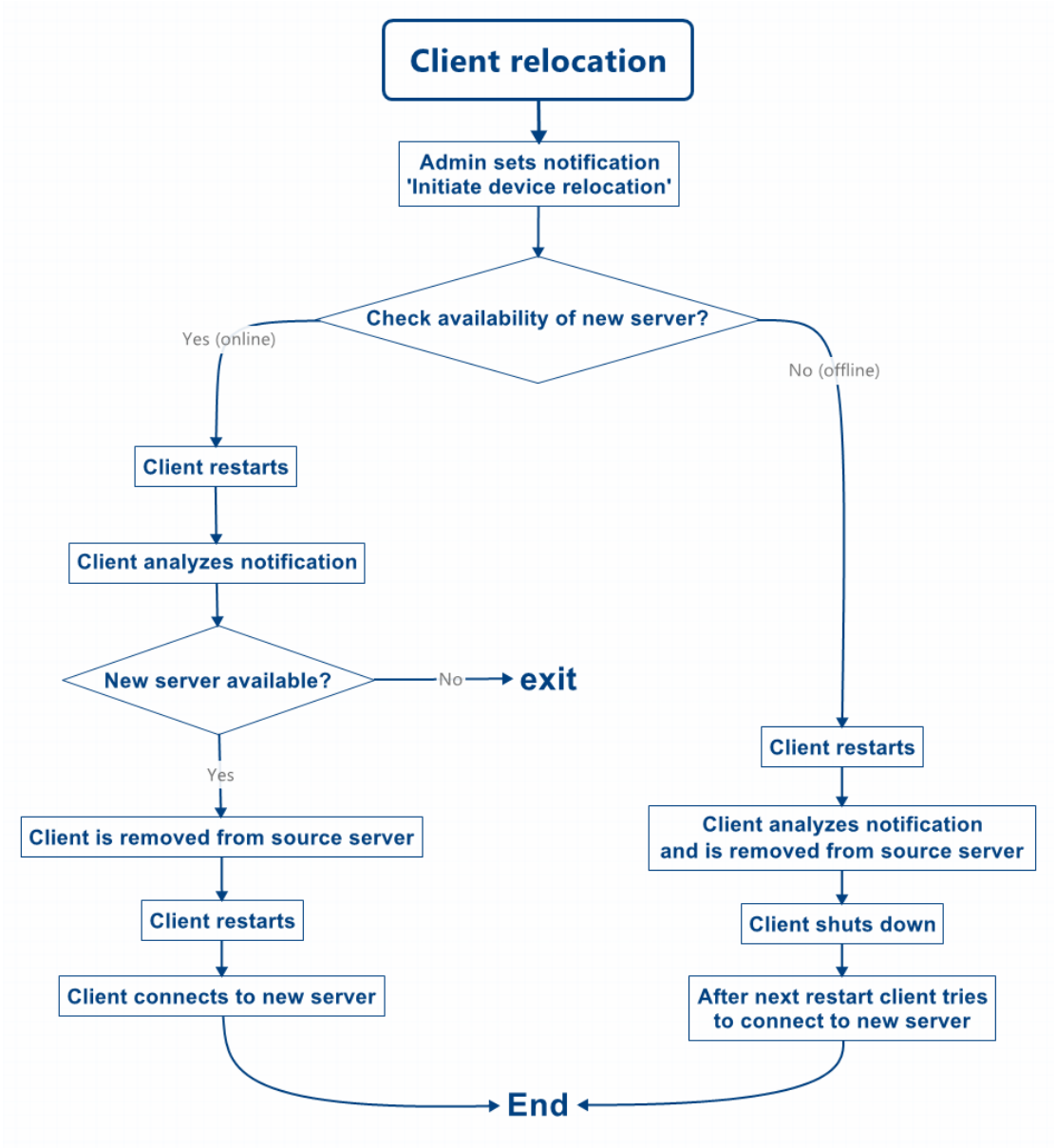
The relocation procedure is initiated by the source server (device-releasing server) and completed by the relevant client devices. Performing an offline relocation the clients do not verify if the target server (device-receiving server) is available and ready to take the devices.

The administrator still triggers the relocation by setting notification **Initiate client relocation** for the relevant devices in the Scout Enterprise Console of the source server. The notification includes all required details. On the next client restart, the notification is analyzed and the configuration data are updated.

The relevant devices are removed from the source server without further verification.

Client licenses and their Subscription can either be included in the transfer or left on the source server.

4.9.3. Relocation flow chart

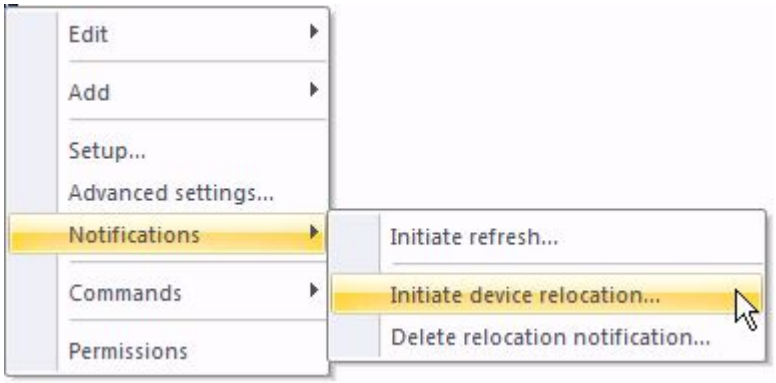


4.9.4. Initiating client relocation

Requires

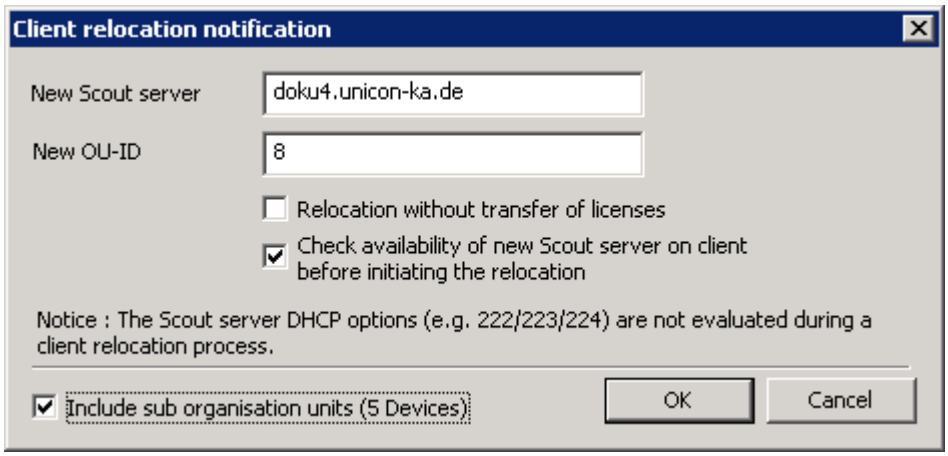
- In **Advanced Options > Devices**, clear the **Accept only known devices** option on the target server, if selected.
- To ensure relocation success, the DHCP options of the client are not checked during relocation. If, however, some of the Scout Enterprise Server DHCP options for the source server have been defined (222/223/224), on the target server, in **Setup > Network > LAN > Edit > Advanced** you must select the **Ignore DHCP options** option.

1. Select a device, an OU, a Dynamic Client Group or devices within the **All devices** window.
2. On the context menu, click **Notifications > Initiate client relocation...**.



*The **Client relocation notification** dialog opens.*

3. In the **New Scout Enterprise Server** field, type the name (FQDN) or the IP address of the target server.
4. In the **New OU-ID** field, type the ID of the desired destination OU on the target server.



If you do not specify a destination OU, the devices are assigned to the default OU or to the OU according to the OU filter rules.

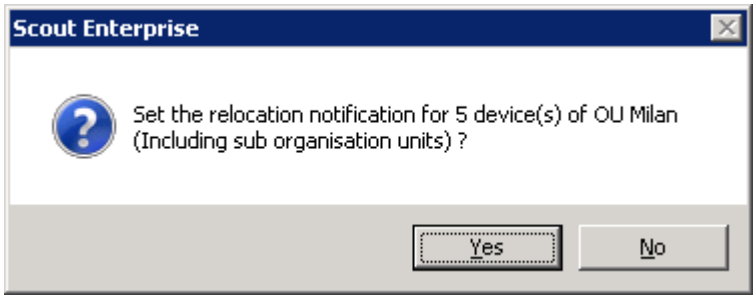
5. If you want to leave the licenses of the relocating devices on the source server, select the **Relocation without transfer of licenses** option.

If you select this option, the client licenses stored on the devices are deleted and made available for other devices on the source server. Likewise any proportion of valid Subscription remaining for the devices is left on the source server.

If you do not select this option, the client licenses as well as the proportional Subscription are kept with the devices and move to the target server.

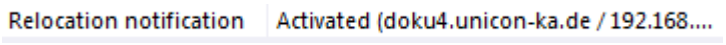
6. To have the availability of the target server verified before relocation ('online' relocation), make sure the **Check availability of new Scout server** option is active.
7. If you want to include the devices of all subordinate OUs, select the option **Include sub organisation units**.

   The number of devices shown in brackets is updated dynamically.
8. Confirm the notification and confirmation.



If you perform an 'online' relocation, the name of the target server is resolved, or the IP address is verified, respectively.

*The notifications for client relocation are set. For the relevant devices, in the **Properties** window, the **Relocation notification** field shows the value* `Activated`.

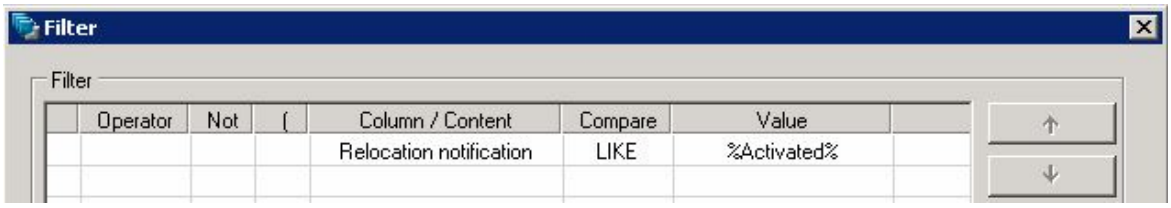


*If a device is not involved in a relocation, the **Relocation notification** field remains empty.*

Note

If the **Relocation notification** field in the **Properties** window is hidden, click  to define which fields you want to show.

By using the Scout Enterprise Report Generator, you can analyze those devices having an activated relocation notification:



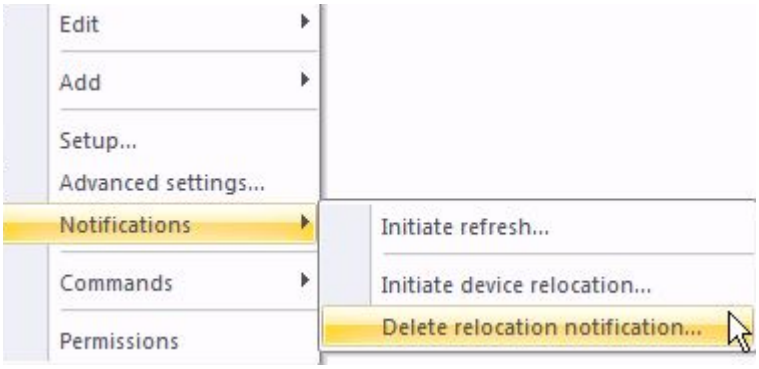
9. If you want to control and schedule the execution of the client relocation, use the Report Generator to identify and export the relevant devices to a dynamic client group, and then run the command **Restart device...** on that group.

The relevant devices are restarted at the point in time defined by you and get their configuration data from the target server. This way you can ensure that relocation takes place beyond working hours and that all relevant devices are relocated at the same time (for online relocation).

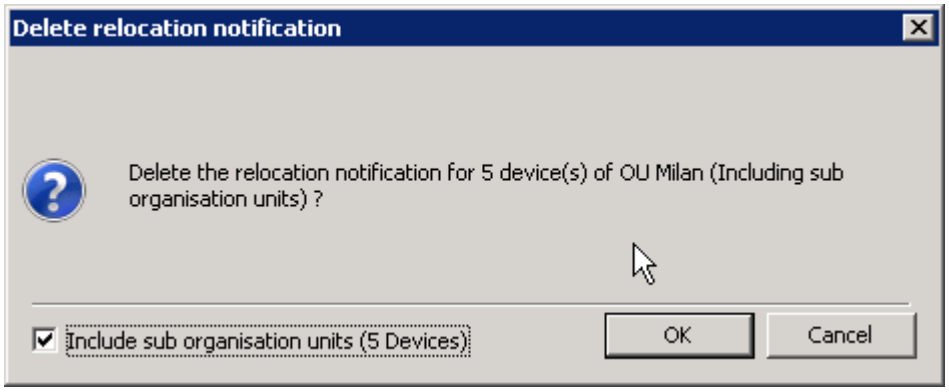
If you perform the relocation offline, the relevant devices connect to their new server as soon as it is available.

4.9.5. Deleting relocation notification

1. For the relevant OU, device or dynamic client group, open the context menu and select **Notifications > Delete relocation notification...**.



2. If you want to include the devices of all subordinate OUs, in the **Delete relocation notification** message, select the **Include sub organisation units** option .



The number of devices shown in brackets are updated dynamically.

3. Confirm with **OK**.

*After refreshing the **Properties** window, the **Relocation notification** status for the relevant devices has been deleted.*

5. Device configuration (Setup)

5.1. Concept

Device configuration is the key to managing a large number of Thin Clients efficiently. Configuring as many clients as possible in the same way keeps IT processes simple, and costs low. All the same, numerous different locations, heterogeneous hardware environments and additional requirements do not allow for a unified device configuration.

Scout Enterprise Management Suite reflects this situation by using inheritance. By default, the base configuration defined at top level gives its properties down to the devices.The concept of inheritance helps you keep configuration consistent and efficient. To define any variations, just modify the relevant settings. Scout Enterprise provides flexibility to override any settings on all levels.

Note
Any changes to device configuration take effect on the next restart of the relevant clients.

Important
The configuration of the clients depends on the software packages installed on the client.

5.1.1. Inheritance of configuration

Base configuration and the configuration of OUs can be inherited to lower instances.

The base configuration is the top level instance. Lower instances can be other OUs or individual devices.

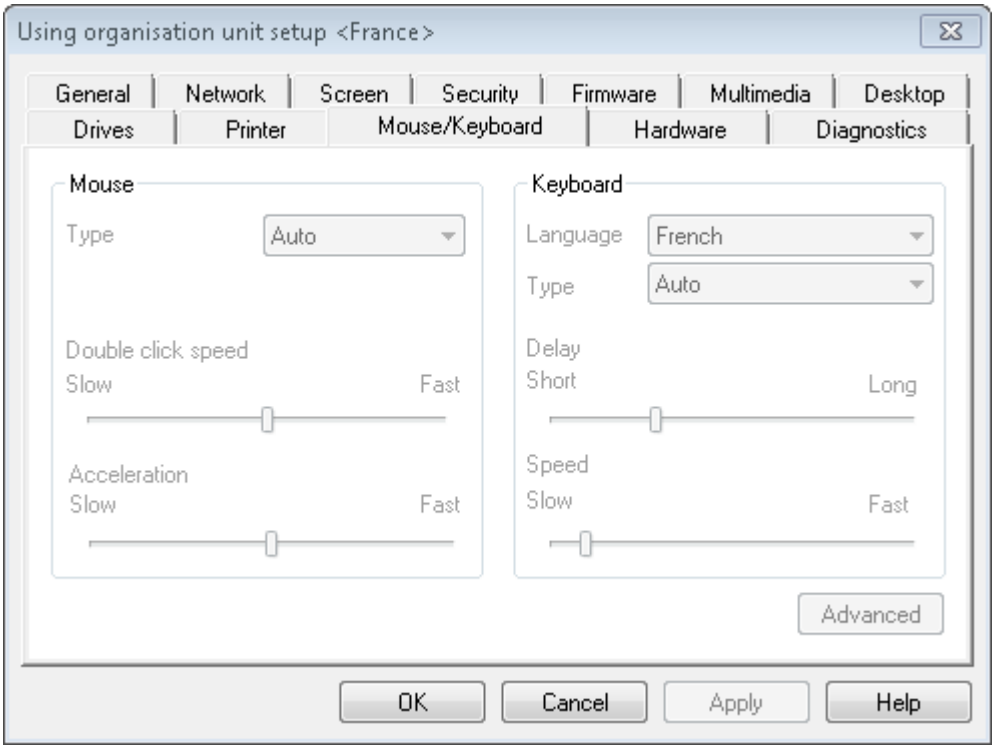
If the option **Use parent** is active, the configuration of the superior element of the hierarchy is applied to the current instance. By default, the option **Use parent** is active, so that a device inherits its configuration from the base configuration.

Settings of the configuration can be edited on three levels in the Scout Enterprise Console:

- Base configuration (**Options > Base configuration**)
- OU (**context menu > configuration**)
- Device (**context menu > configuration**)

On every level you can inherit the configuration from the superior level or define independent settings. To be able to override settings, you must block inheritance, that is disable the use of the parent configuration.

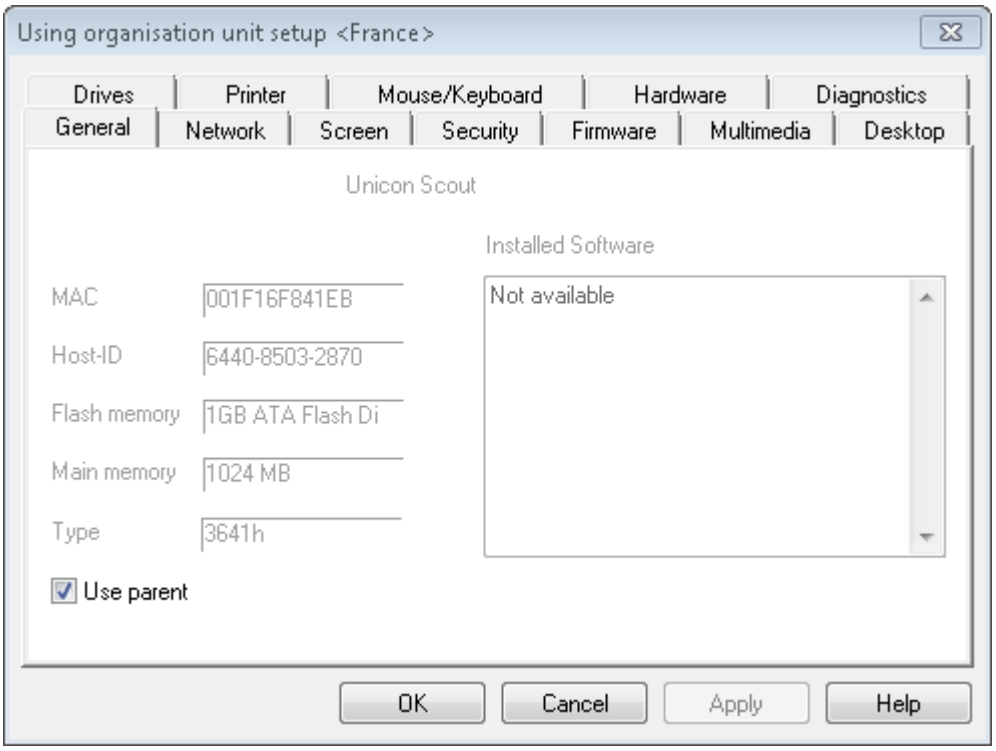
Note
Pay attention to the configuration dialog title. It indicates the location of the current configuration. This can be the base configuration or a superior OU or a particular device.



Example: If inheritance is active and you open the configuration dialog of a device or OU subordinate to `France`, the title bar shows **Using organisation unit setup <France>**. To modify any settings you must open the `France` configuration dialog.

5.1.2. Blocking inheritance - independent configuration

If you want to define independent settings for a particular OU or device, you have to block inheritance for that instance.



1. Open the context menu of the relevant instance (OU or device) and click **Setup...**.

   *The **Setup** dialog opens and the title bar shows the currently active configuration instance. This can be the base configuration or a superior OU. For further information, see* Opening setup dialogs.

2. On the **General** tab, clear the **Use parent** option.

Inheritance is disabled. The title bar of the dialog shows the currently edited instance and the available options are editable. This instance and all subordinate instances can be configured independently of the superior instances.

Note

The **Independent setups** window shows all OUs and devices that do not use their parent configuration.

In **View > Settings...**, you can specify that after modifying any configuration all subordinate independent configurations are checked. This feature lists all configurations with the relevant parameters and allows you to assign the modifications in a convenient way to all or selected instances.

5.1.3. Supporting local configuration

User rights for modifying the local device configuration can be set for OUs and devices, even for individual fields. You can lock and disable particular fields or tabs for security reasons whereas other features such as monitor management can be allowed. For further information, see Changing user rights.

If individual (local) configuration is allowed, make sure that the relevant configuration data are prevented from being overridden when the Scout Enterprise configuration is reloaded on the next restart of the devices.

Preventing local configuration from being overridden:

1. Click **Options > Advanced options... > Devices**.
2. Under **Update of fields**, select **Only locked fields are updated.**

When the Scout Enterprise configuration data are reloaded, only locked tabs and fields are updated. Local user configuration data in unlocked fields are kept.

In case of a defective user configuration, however, the administrator, in the Scout Enterprise Console, can set a flag to override all configuration data on the next restart of the device.

Initiating update of all configuration data

- In Scout Enterprise, for the relevant device, open the context menu and select **Notifications > Initiate reload...**

The relevant device is marked for obtaining a complete copy of the relevant Scout Enterprise configuration data including unlocked fields, on the next restart.

5.1.4. Accessing device configuration

Opening Base configuration

- In Scout Enterprise, select **Options > Base configuration...**

*The **Base configuration** dialog opens. It contains the global device configuration applying to all devices unless there are defined independent configuration instances.*

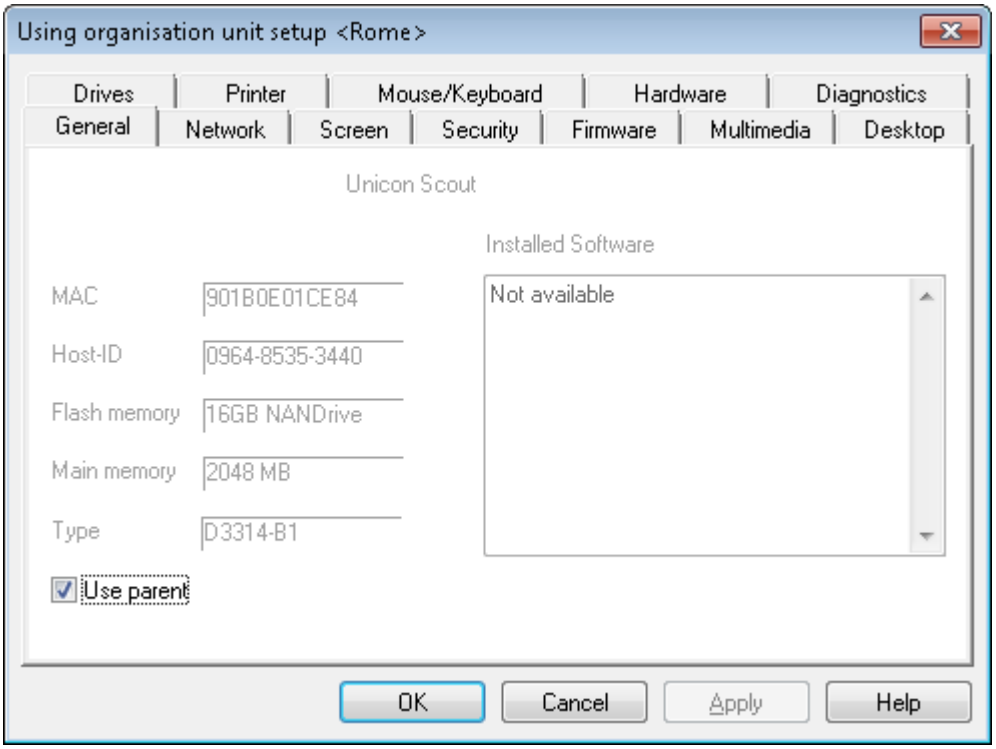
Opening Setup dialog for OUs and devices

- Select the relevant element in tree view, and then and click **Edit > Configuration...**

or

- For the relevant element, open the context menu, and then click **Setup...**

*The **Setup** dialog of the selected element opens. Possibly, the options are disabled as the **Use parent** option is selected. In this case, the relevant OU or the base configuration is specified in the dialog title.*



Opening the relevant Setup dialog (from where configuration data are applied)

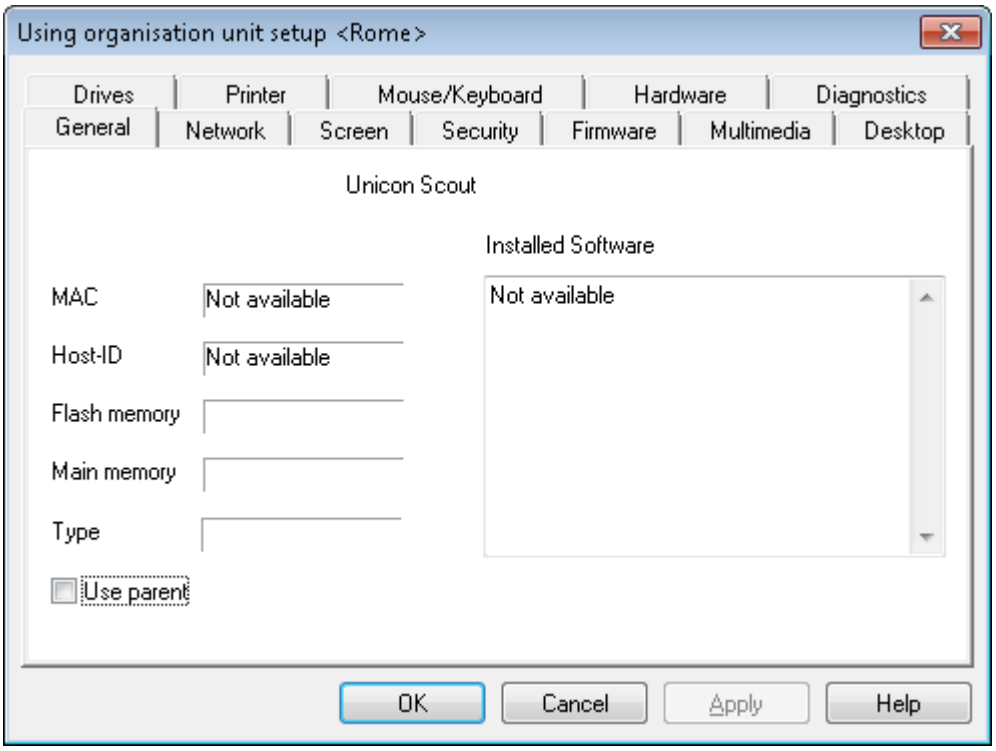
1. Select an element in the tree view.
2. To show the **Properties** window, click **View > Window > Properties**.

   *In the **Properties** window, next to **Configuration**, the instance is displayed from where con-*

figuration data are applied to the selected element.

3. In the **Properties** window, double-click **Configuration**.

*The **Setup** dialog of the displayed instance opens containing the configuration data applied to the selected instance.*



5.1.5. Comparing configurations between OUs or devices

The configuration of different OUs or devices can be compared by using a dedicated window.

1. Click **View > Window > Compare setups**.

   *The window **Compare setups** is shown as permanent window in the lower part of the console window.*

2. Drag two or more OUs or devices into the **Compare setups** window by using a drag-and-drop operation.
   Or:
   On the context menu of the relevant OU or device, click **Edit > Add to setup compare...**.

3. On the icon bar of the **Compare setups** window, click the  icon.

   The configurations of the listed OUs or devices are compared. Differences in the main properties are shown.

4. To view all of the information, on the icon bar of the **Compare setups** window, click the  icon.

   All properties are shown.

Note
To compare actual and target settings of an individual device, use the relevant command. For further information, see Comparing target and actual settings.

5.2. Configuration method

During system start of the clients managed by Scout Enterprise they connect to their Scout Enterprise Server and check if there are updated configuration data. Updates can relate to the device configuration (setup) but also to application definitions, files configured for transfer and Advanced file entries. If there are updated configuration data they are transferred to the clients. For further information, see Communication between Thin Client and Scout Enterprise Server.

5.2.1. Configuration run

If, when checking for updated configuration, the system identifies updated configuration data for a client, the particular modified data are identified, compressed and saved to the database, and then transferred to the client in one step. For modifications on the configuration of a huge number of clients such as changes in the application definitions when moving to another back-end infrastructure, you can initiate the identification and compressed storage in advance, for example at night. The required configuration data then can be prepared to be ready for transfer on the next restart of the clients which might be on the next working day.

To prepare the configuration data in this way, you can run the **Configuration run** command on the relevant OU or Dynamic Client Group. The command can be scheduled or executed immediately. You can view the processing progress in the **Command history**.

The configuration run only prepares configuration data for those clients a configuration delta has been identified.

5.2.2. Snapshot method (Scout Enterprise Management Suiteversion 14.5)

The feature described below is only provided in Scout Enterprise Management Suite version 14.5.

Note

For Scout Enterprise Management Suite 14.6.0 and later versions, the crucial advantages of the snapshot method have been integrated into the default procedure and have improved the overall performance. The new procedure combines

- the identification of the configuration data at run-time and
- the transfer of the compressed configuration data

By default, the **Determine at runtime** method is applied.

Enabling Snapshot method

- In the Scout Enterprise Console, click **Options > Advanced options > Devices > Configuration method > Snapshot method**.

As of now, each time a client running the required eLux RP version connects to Scout Enterprise, only the snapshot ID is verified.

Note
After enabling the Snapshot method, to provide configuration data for the clients, the administrator should create an initial configuration snapshot.

Snapshot method

– Optional method for Scout Enterprise Management Suite version 14.5 –

Identifying configuration data and transferring them to the clients is done in two independent steps:

- Identifying the configuration data of **all** clients and saving them to the Scout Enterprise database (Configuration snapshot) at a freely definable point in time
- Transferring updated configuration data to the clients in one consolidated step when the clients connect to the Scout Enterprise Server after restarting (if required only)

This method uncouples identification of the configuration data from the point in time the clients connect to the Scout Enterprise Server. This way, the risk of incomplete configuration transfer with high server load and adverse conditions can be excluded to a great extent.

The configuration data are identified by creating a configuration snapshot for all managed devices

- through the Scout Enterprise administrator
- at any point in time
- in the Scout Enterprise Console

The configuration data for each client are identified and saved with a unique snapshot ID to the Scout Enterprise database.

Each time a client connects to the Scout Enterprise Server, the server verifies if the client is already provided with the latest snapshot ID. Otherwise, the compressed configuration data of the latest snapshot is transferred to the client in one step.

Determining configuration data at runtime is obsolete.

Note
When executing an **Update** command, the core information is the URL that is transferred to the client. The URL is created by using the values set in **Setup > Firmware** at the time when the command is run. This applies even if these data are not yet included in the latest configuration snapshot. For further information, see Planning an update.

Requirements

- Scout Enterprise version 14.5.x
- eLux RP 4.10 and later versions

or
eLux RP 5.1 and later versions

Clients running earlier eLux RP versions are not able to process the snapshot configuration data. These clients are provided with the old **Determine at runtime** method.

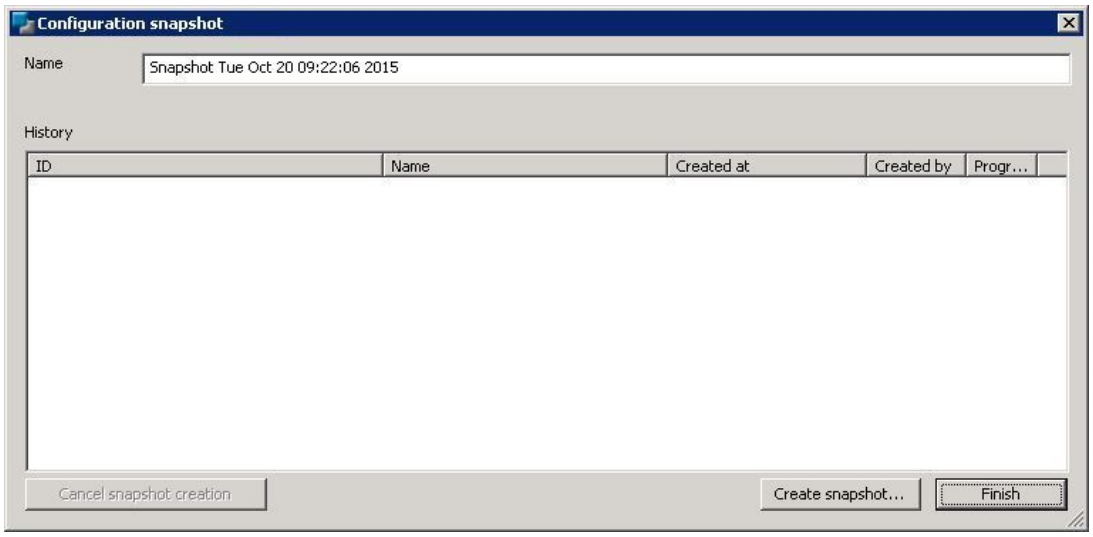
For clients running the required eLux RP version but having been integrated after the last snapshot, a dynamic snapshot is created. For further information, see Dynamic snapshot.

Creating a configuration snapshot

Requires
The relevant menu permissions for the Scout Enterprise administrator

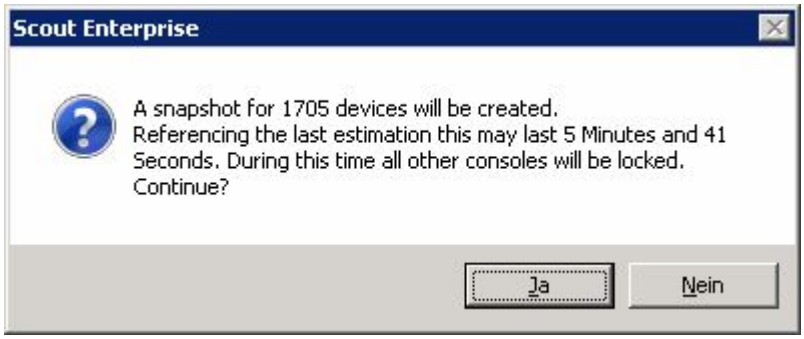
Important
While a snapshot is created, all Scout Enterprise Consoles (including the own) are locked.

1. In the Scout Enterprise Console, click **File > Create Configuration snapshot...**



2. Complete or replace the predefined snapshot name and confirm with **Create snapshot...**.

   The Scout Enterprise service calculates the estimated processing time of creating a snapshot for all devices:

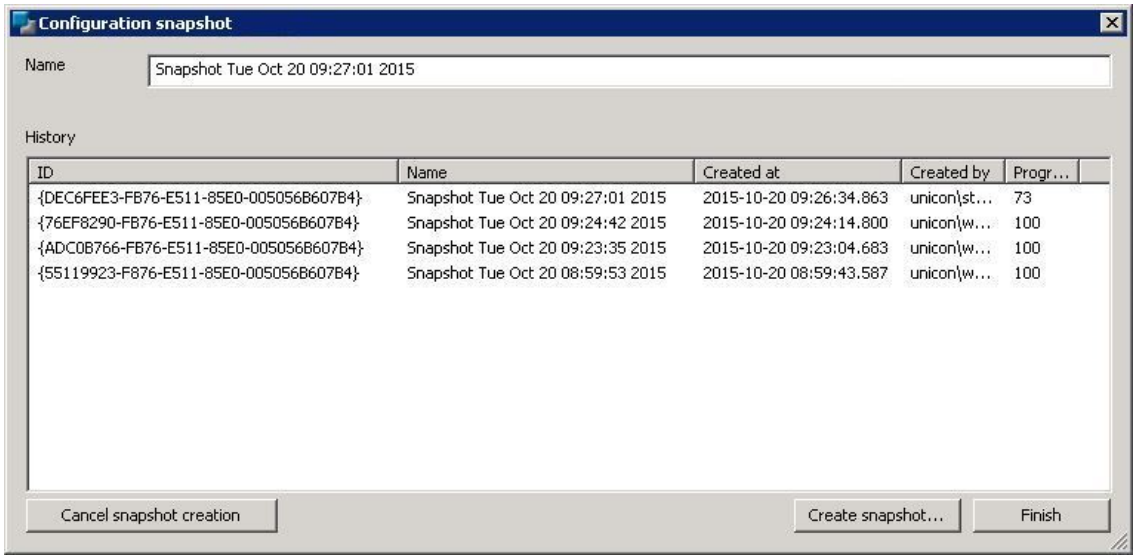


3. Confirm with **Yes**.

   The snapshot is listed in the history and the processing progress is shown in the **Progress %** column.

   While the snapshot is created, all Scout Enterprise Consoles are locked and the **Lock information** dialog is displayed:

4. If desired, in the **Lock information** dialog, click **Snapshots...** (visible only with the required permissions) to return to the **Configuration snapshot** dialog:



   You can cancel the process of snapshot creating anytime. Any configuration data created so far are deleted.

A snapshot with a unique ID is created for all devices. From now on, clients running the required eLux RP version need only verify the snapshot ID when connecting to the Scout Enterprise Server.

Note

As soon as you modify device configuration, application definitions, configured file transfer, or advanced file entries, you are required to create a new snapshot.

Dynamic snapshot

When operating clients initially with Scout Enterprise or when relocating clients to another Scout Enterprise Server, if you have enabled the **Snapshot** method, the following situation might occur:

Devices running the required eLux RP version (version 4.10 or later, version 5.1 or later) are integrated into Scout Enterprise after the last snapshot has been created. For these devices, the Scout Enterprise Server creates a dynamic snapshot which means that the configuration data identified by the old **Determine at runtime** method are saved to the Scout Enterprise database and then transferred to the client.

So, a dynamic snapshot is a snapshot created after the last snapshot of the administrator, for devices that have 'missed' the general snapshot. If the configuration data have been modified after the last configuration snapshot, the dynamic snapshot already includes the modifications. As soon as the Scout Enterprise administrator recreates a configuration snapshot, the configuration data for all devices are harmonized.

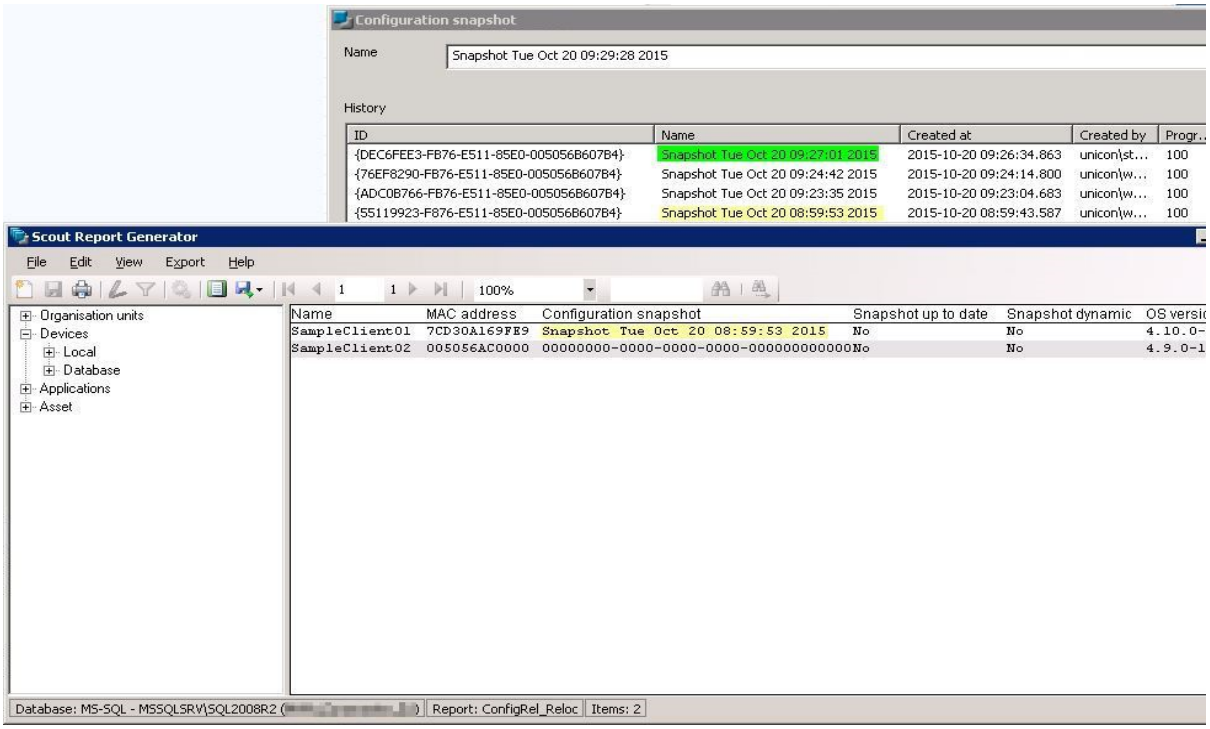
By using a report you can identify those devices that do not use the latest configuration data of the last snapshot, or those devices that have been integrated into Scout Enterprise after the last snapshot. For further information, see Evaluating configuration data.

Evaluating configuration data (Scout Enterprise Management Suite14.5)

Note

The following information on evaluating configuration data of the clients relates to the snapshot method.

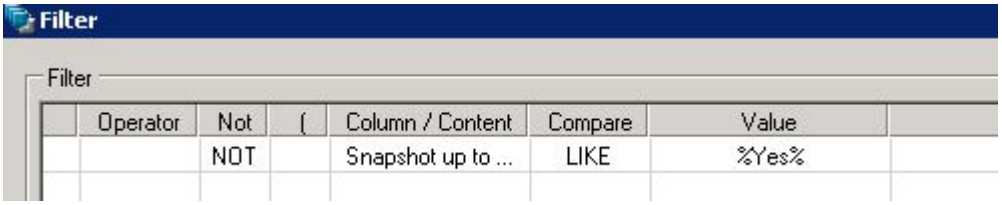
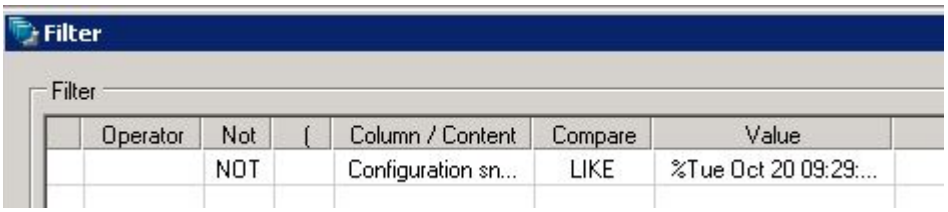
By using the Scout Enterprise Report Generator, you can identify all devices that do not use the latest configuration data of the last snapshot:



Note

For devices running earlier eLux versions, the value for the **Configuration snapshot** field is shown as `00000000-0000-0000-0000-000000000000` and the value for the **Snapshot up-to-date** field is shown as `No`.

You can use the following fields to filter by:

Field	Example/Description
Snapshot up-to-date	
Configuration snapshot	
Snapshot dynamic	Identify devices that have been integrated into Scout Enterprise management **after** the last snapshot (for example new devices or relocated devices from another Scout Enterprise Server). For further information, see Dynamic Snapshot.

5.2.3. Determine at runtime

– Method used by Scout Enterprise Management Suite 14.4 and earlier versions –

As soon as a client restarts and connects to Scout Enterprise, the updated configuration data considering inheritance are identified and transferred to the client. The transfer might be performed in several steps depending on the complexity of the configuration.

The Scout Enterprise Server determines the relevant configuration data at runtime. That means that all modifications made to configuration in the Scout Enterprise Console up to now are concerned and are transferred to the client immediately.

Simultaneous connections of a great number of clients to the Scout Enterprise Server may lead to a high load of the Scout Enterprise Server – according to the number of clients and to the system performance of the server or database. In extreme cases, if, let's say, several thousands of devices are turned on simultaneously and the sever/database performance is insufficient, the transfer of the configuration data to the clients might fail or be incomplete.

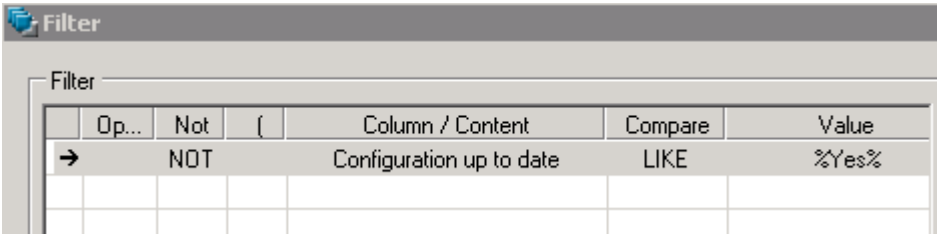
Note
Independent of the configuration method you can ensure and optimize the configuration data transfer by using the **Handshake** feature. For further information, see Optimizing with Handshake.

5.3. Evaluating configuration data

By using the Scout Enterprise Report Generator, you can identify all devices that do not use the latest configuration data.

Note

For devices running earlier eLux versions, the value for the **Configuration up-to-date** field is shown as `No`.



5.4. General tab

On the **General** tab, the **Use parent** option is provided. If this option is selected, all other fields of the dialog are disabled.

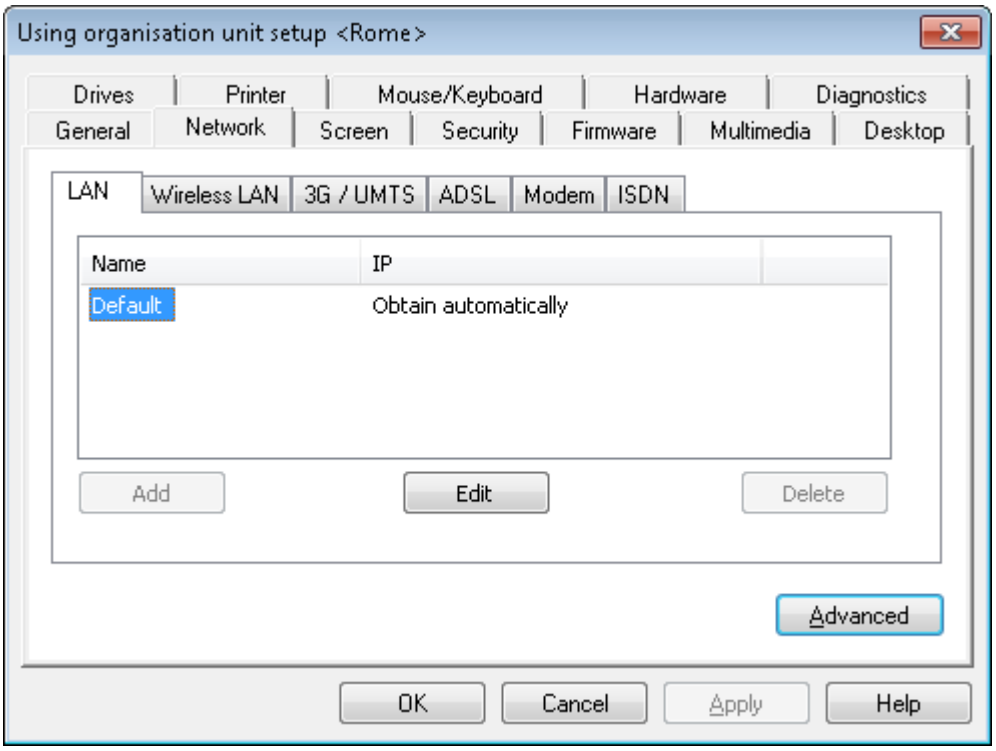
Note
In particular situations, it might be useful to disable the **Use parent** option temporarily. For further information, see Blocking inheritance.

The **Setup** dialog of an individual device provides some additional information about the hardware. For further device properties, see the **Properties** window of the Scout Enterprise Console.

Option	Description
MAC address	Device address of the hardware (MAC=Media Access Control)
Host-ID	eLux Host-ID assigned to the device, required for the licensing process
Flash memory	Short description of the flash memory type and size.
Main memory	Main memory size in megabytes.
Type	Product details provided by the hardware manufacturer (character string)

5.5. Network tab

Depending on the installed image and the hardware used you can set up different network profiles. The user then can choose from the defined network connections on the client systray.



5.5.1. Advanced network settings

In **Setup > Network > Advanced** you will find the host list as well as features related to all network connections.

Defining a timeout for a connection

- Under **Management timers**, in the relevant fields, enter the desired timeout in seconds
  - when establishing a connection.
  - when the connection is in idle state.

After the indicated time, the connection is terminated.

The option **Send Keepalive packet** ensures that the client sends keepalive signals to the Scout Enterprise Server in the specified time interval. For further information, see Defining status messages (keep alive messages).

Defining a host list for networks without DNS server

If the network is not equipped with a domain name server (DNS), host names can be resolved locally by the device. All you need is to keep your host list up-to-date.

1. Click **New**.
2. Enter a host name and the IP address.
3. Confirm with **OK**.

The host list is transferred automatically on the next restart.

5.5.2. Defining a LAN profile

1. In Scout Enterprise, for the relevant device or OU, open **Setup > Network**.
   In eLux, in the control panel, click **Setup > Network**.
2. Select the **LAN** tab and click **Add**.

   *The **Edit network profile** dialog opens.*
3. On the **Ethernet** tab, determine whether the IP address is dynamic or edit the IP address data.
4. On the **Advanced** tab, you can set further options regarding DHCP, DNS and IEEE 802.
5. Confirm with **OK**.

5.5.3. Defining a WLAN profile

The following configuration options are provided:

A. In the Scout Enterprise Console, in the device configuration, a WLAN profile can be created for a device, OU or all devices, see below.
   EAP authentication is not supported for this method.

B. Users can create individual WLAN profiles locally on the client. For eLux RP 5.6 and later versions, local profiles and profiles created in Scout Enterprise can be merged automatically to make them connect depending on the location.

C. Corporate WLAN: A WLAN configuration can be distributed throughout the entire company network by using a WPA configuration file with and without 802.1x. This method requires configuring a dummy WLAN profile in the device configuration that can be hidden for the clients.[1]
For eLux RP 5.6 and later versions, users can create individual WLAN profiles locally on the client, on top. Configured WLAN networks can connect automatically depending on location and priority. For further information, see WPA support and Corporate WLAN.

Creating a WLAN profile in the Scout Enterprise device configuration

1. In the Scout Enterprise Console, for the relevant OU, open **Setup > Network**.
2. On the **Wireless LAN** tab, click **Add**.
3. In the **Edit network profile** dialog, select the **Connect automatically** option.

Note
If the **Connect automatically** option is not selected, there is no automatic use of any WLAN connection.
In this case, the user must start the WLAN manually from the systray.

4. On the **IP** tab, determine whether the IP address is dynamic or edit the IP address data.
5. On the **Medium** tab, edit the following fields:

Option	Description
SSID	Service Set Identifier Name of the WLAN
Timeout	Time period in seconds waiting to connect
Channel	Selected automatically by default
Encryption	Authentication mode Select `WPA` or `WPA2` with pre-shared key (PSK). Do not use `WPA-EAP` or `802.1x`. To authenticate via EAP (Extensible Authentication Protocol), use a WPA configuration file. For further information, see WPA support.

6. On the **Advanced** tab, you can set further security options regarding DHCP and DNS.
7. Confirm with **OK**.

[1] for eLux RP 5.6 and later versions

Note
To create an individual WLAN profile locally on the client (B), the same steps can be applied in the eLux control panel, the relevant user rights provided.

Displaying WLAN profile editor on the client

Available WLAN networks can be viewed on the client using the network icon of the systray. In addition, the WLAN profile editor can be shown in a popup window when an unknown WLAN network is detected:

- Use the **Advanced file entries** feature of the Scout Enterprise Console:

File	`/setup/terminal.ini`
Section	`Layout`
Entry	`NotifyNewWLAN`
Value	`true`

For further information, see Advanced file entries.

5.5.4. WPA support

To secure your your WLAN, you can use WPA encryption wit the help of the `WPA-supplicant` software. This software provides key negotiation with the WPA Authenticator, and controls association with IEEE 802.11i networks. WPA is using IEEE 802.1X, and WPA2 is using IEEE 802.11i.

Authentication can be performed either with a pre-shared key (PSK) or, for IEEE 802.1x, over the Extensible Authentication Protocol (EAP).

WPA is configured using the text file `wpa.conf` that can list accepted networks and security policies. The configuration file is saved locally on the clients in the */setup/wlan/* directory.

`WPA-supplicant` is a free software implementation. For further information see http://w1.fi/wpa_supplicant/.

Providing WPA configuration file

1. Create a text file named *wpa.conf* by using the **wpa_supplicant** program. An example is shown below.
2. For the relevant devices, configure the file transfer to the clients using the Scout Enterprise feature Advanced configuration\Files.
3. In the **Add file entry** dialog, select the **Import file to database** option and then click the **...** button to select the newly created *wpa.conf* file as source file from the file system.
4. In the **Destination file** box, set the path for the client to */setup/wlan/wpa.conf*.
5. Confirm with **OK** and **Apply**.

For further information see Advanced configuration\Files.

Note
In addition, the configuration of a dummy WLAN profile is required. For further information, see Corporate WLAN.

Example for a WPA configuration file with 802.1x

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1
network={
    ssid=__MYSSID__
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=TLS
    identity=__IDENTITY__
    priority=6
    ca_cert="/setup/cacerts/serverca.pem"
    client_cert="/setup/cacerts/client.pem"
    private_key="/setup/cacerts/client.key"
        }
```

5.5.5. Corporate WLAN

A corporate WLAN providing access to internal resources can be secured by 802.1x and provided with firewall policies tailored to specific needs.

After having set up your WPA configuration file, you can deploy it where-ever you want it to be used. For further information, see WPA support.
In addition, define a dummy WLAN profile in the device configuration of the Scout Enterpriseconsole, see below.

If you use a corporate WLAN, you can decide to allow the users to create their own WLAN profiles in parallel.[1] For example, a mobile Thin Client could use the provided LAN connection when it is attached to the docking station on the job, but change automatically to the corporate WLAN when undocked. Once the device is started in the home office, eLux connects to the manually configured WLAN.

Configuring corporate WLAN

1. In the base configuration, in **Nework > Wireless LAN**, create a new WLAN profile. This profile serves as a dummy profile and is invisible on the client:[2]

[1] for eLux RP 5.6 and later versions
[2] for eLux RP 5.6 and later versions

Option	Wert	Beschreibung
Name	`#Dummy#`	This name ensures that the WLAN profile on the client is invisible for the user.[1] The name is mandatory.
Connect auto-matically	selected	mandatory
SSID	*<DummySSID>*	Use any value.
Timeout		Use the default value.
Channel		Use the default value.
Encryption	`WPA (PSK)`	Do not use `WPA-EAP` or `802.1x`.
PSK	*<Password>*	Use any string with eight or more characters.

For further information, see Defining a WLAN profile.

2. Define an advanced file entry to merge the WLAN profiles:

File	`/setup/terminal.ini`
Section	`Network`
Entry	`MergeWLANProfile`
Value	`true`

For further information, see Advanced file entries.

3. Distribute your corporate WLAN configuration with a WLAN configuration file.

   To define higher priority as the manually created WLAN profiles have (priority `5`), set the **Priority** value to `6` or higher.

   For further information, see WPA support.

Users can create individual WLAN profiles on the local client in addition to the corporate WLAN:

Creating a local WLAN profile

1. In the eLux control panel, in **Setup > Network > Wireless LAN**, add a new profile.

   If there is no network connection available, the WLAN profile editor pops up.

2. In the **Edit network profile** dialog, select the **Start automatically** option.
3. Edit the remaining fields. For further information, see Defining a WLAN profile.
4. To connect to the defined WLAN for the first time, use the network icon of the systray and click the **Connect** button.

[1] for eLux RP 5.6 and later versions

If a network connection is available, the connected network is shown in the systray when the mouse pointer is moved over the network icon.

5.5.6. G3/UMTS profile

Option	Description
Name	Name for the network connection
APN	Access Point Name, system access point of the provider
Timeout	Timeout value in seconds before the connection is aborted by eLux
User name	User name assigned by your provider
Password	Password assigned by your provider
PIN or SIM card	PIN of your SIM card assigned by your provider
Secured	Local users are not allowed to modify the profile.
DNS server 1	Name server, if required
DNS server 2	Name server, if required

5.5.7. ADSL profile

Option	Description
Name	Name for the network connection
Timeout	Timeout value in seconds before the connection is aborted by eLux
User name	User name assigned by your provider
Password	Password assigned by your provider
Identification	Protocol used by your provider
Secured	Local users are not allowed to modify the profile.

eLux supports the dynamic change of IP addresses.

5.5.8. Modem profile

Option	Description
Name	Name for the network connection
Telephone number	Telephone number of your provider
Timeout	Timeout value in seconds before the connection is aborted by eLux
User name	User name assigned by your provider

Option	Description
Password	Password assigned by your provider
Identification	Protocol used by your provider
Tempo	Baud rate,value must be greater than the fastest baud rate of the modem.
Secured	Local users are not allowed to modify the profile.

eLux supports the dynamic change to IP addresses.

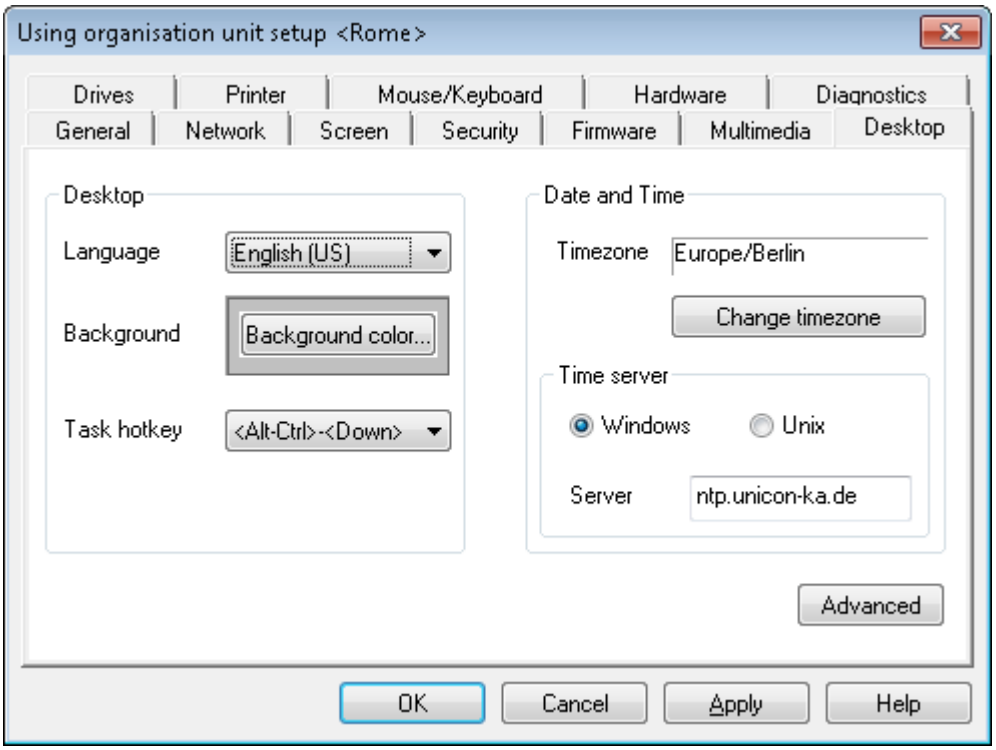
5.5.9. ISDN profile

Option	Description
Name	Name for the network connection
Telephone number	Telephone number of your provider
Timeout	Timeout value in seconds before the connection is aborted by eLux
User name	User name assigned by your provider
Password	Password assigned by your provider
MSN	Number for multiple ports. If you use the call back feature, type your telephone number without prefix If you do not use call back, type 0 (zero).
Identification	Protocol used by your provider
Recall	Select the option if your provider offers call back.
Using IP address	Only if your provider reserves a static IP address for your eLux terminal
Secured	Local users are not allowed to modify the profile.

eLux supports the dynamic change of IP addresses.

5.6. Desktop

On the **Desktop** tab, you can modify the eLux interface and configure time and date.



5.6.1. Configuring desktop

1. In Scout Enterprise, for the relevant device or OU, open **Setup > Desktop**. The same dialog works for eLux on the client.
2. In the **Language** list, click the preferred desktop and application language.

> **Note**
> The language is related to the display of desktop elements but not to text services and input. To ensure correct performance, the applications have to support the selected language.

If you select `German`, the eLux user interface elements such as start menu and control panel are displayed in German. If you select any other language they are displayed in English.

3. Click the **Background color** button to select a background color.

> **Note**
> The selected background color comes only into effect, if the option **Classic Desktop** is checked, see Advanced desktop configuration.

4. In the **Task Hotkey** list, select a shortcut to switch between the sessions.

   The default is `ALT+CTRL+↑` to avoid any conflict with the shortcut `ALT+TAB` which is used to switch between the tasks within one session.

5.6.2. Configuring time zone and time server

- To define the time zone, click **Setup > Desktop**, and then under **Date and time** select the relevant time zone.
- To specify a time server, click **Setup > Desktop**, and then under **Date and time** and **Time server** type the relevant server name or IP address.

5.6.3. Advanced desktop settings

In **Desktop > Advanced** the following options are available:

Option	Description
Interactive Desktop	Icons displayed on the desktop
Desktop writable	Users are allowed to place icons on the desktop.
Classic Desktop	The eLux Modern User Interface is deactivated. The **Background colour** selected on the **Desktop** tab is shown.
Window manager	If the **Animated Windows** option is selected, the windows' content is displayed while moving them. If the **Maximize/Fullscreen**option is selected, and you have connected multiple monitors, you can assign each application (ICA and RDP) to a dedicated monitor.
Taskbar	Settings for the taskbar at the bottom of the screen
Quick Setup (Systray)	Systray icons to be displayed in the taskbar. **Multimedia**: Selecting input and output devices, Volume control, Test sound **Mouse/Keyboard**: Mouse and keyboard speed, left-handed mouse, keyboard language **Screen**: Information, resolution, alignment **USB mass storage devices**: Information about USB devices **Show network status**: LAN/WLAN, network information, disconnect/connect, configuration **Device information**: MAC, IP, name, serial number, free information fields **Date/Time**: Display and configuration of date, time and time zone

Option	Description
Background image (only Scout Enterprise)	There are two ways to define background images: • In the **Server file** field, type the picture file name including its path relative to the Scout Enterprise Server directory (`...\UniCon\Scout\Server`) • Click **Load** to browse and select the picture file. The picture file is imported into the database. This option has precedence over a file referenced in the file system. Click **Delete** to remove the current background image from the database. Files that you import into the database are saved with the SQL database backup. Files that you reference in the file system provide the opportunity to be replaced by other content as long as the file name remains. The background image is not reloaded on each restart, but after changes have been made in file configuration or in the files themselves.
	Note Make sure to have enough space on the client flash card. The background image is stored in the `/setup` directory of the flash card.
Autostart	The control panel is started after the system start with the defined delay in seconds
Work spaces	Number of desktops

5.6.4. eLux Modern User Interface

The Modern User Interface layout can be used as an alternative to the classic desktop. It provides the usesr with resources of Citrix StoreFront Stores and the Citrix Webinterace but also with all other applications configured for the client.

Enabling Modern User Interface

Requires
On the clients, eLux RP 4.8.0 or a later version, and the ICA client V13.1.3 or a later version must be installed.

- In the device configuration, in **Desktop > Advanced**, clear the **Classic desktop** option.

You can customize the Modern User Interface to your needs. For example, you can change the size of the application icons or display your own logo on the desktop.

Customizing the layout of the Modern User Interface

1. For the relevant devices, use the Advanced file entries feature of the Scout Enterprise Console to modify the client file `/setup/terminal.ini`:

File	`/setup/terminal.ini`
Section	`Layout`
Entry and value	see table below

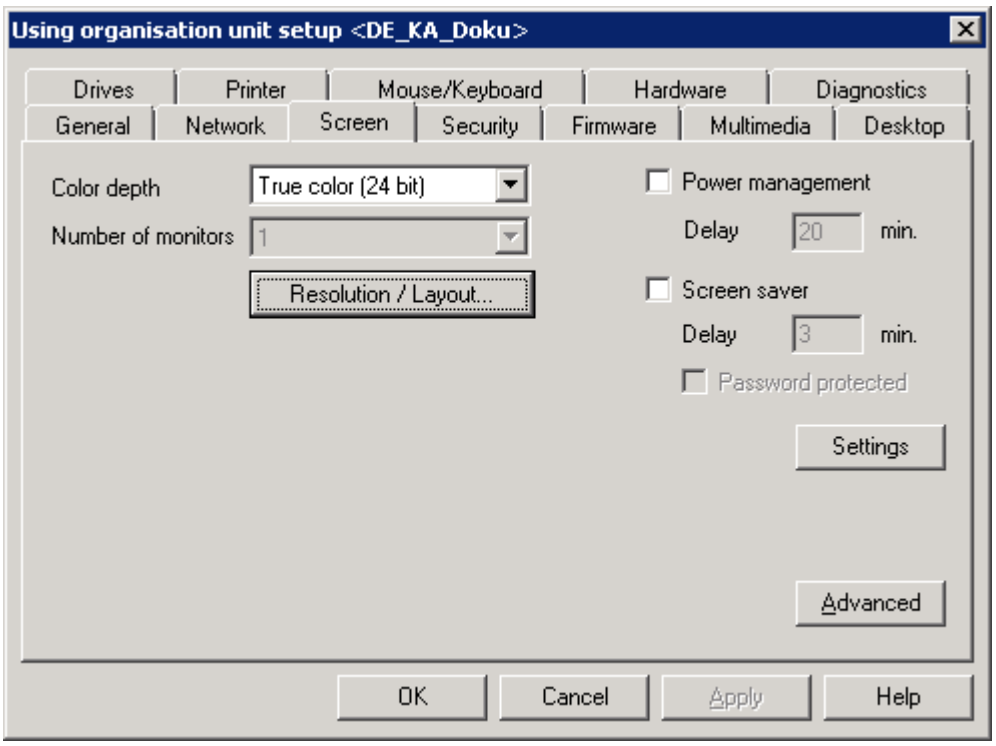
2. Add the following new entries and specify the relevant values:

Entry	Value range	Default	Description
DesktopLayout	small, medium, large	medium	size of the application icons on the desktop
DesktopLogo	*Path and name of the picture file*	*eLux-Logo*	Replaces the eLux Logo in the upper left by the specified picture file. Example: `setup/public/myPic.png`
	Note The picture file must be configured for file transfer. For further information, see Advanced Setup/Files		
DesktopTextColor	#<*rgb*>	#ffffff	Text colour of application icons
DesktopBackgroundColorMenu	#<*rgb*>	#000000	Background colour of menus

Confirm each entry with **Add**.

3. To display a background image on the Modern User Interface, configure the relevant picture file in the device configuration. For further information, see Advanced desktop settings.

5.7. Screen tab



5.7.1. Screen settings and multiple monitors

On the **Screen** tab, you can define the color depth, energy saving options and screen saver.

Further basic settings such as screen resolution, frequency and rotation are defined in the **Resolution/Layout** dialog. This dialog also serves for the configuration and layout of multiple monitors (up to eight monitors with Scout Enterprise 14.9 and later versions[1]).

Note
High screen resolution and high color depth require more graphics and main memory capacity. This might limit the number of parallel opened applications.

If you use adapters or if you use the analog VGA port to connect monitors to Thin Clients, no warranty is given for the operation of these clients, because combinations of that kind are not part of functional acceptance tests.

Defining multiple monitors

1. Click **Resolution/Layout** to open the dialog of the same name.

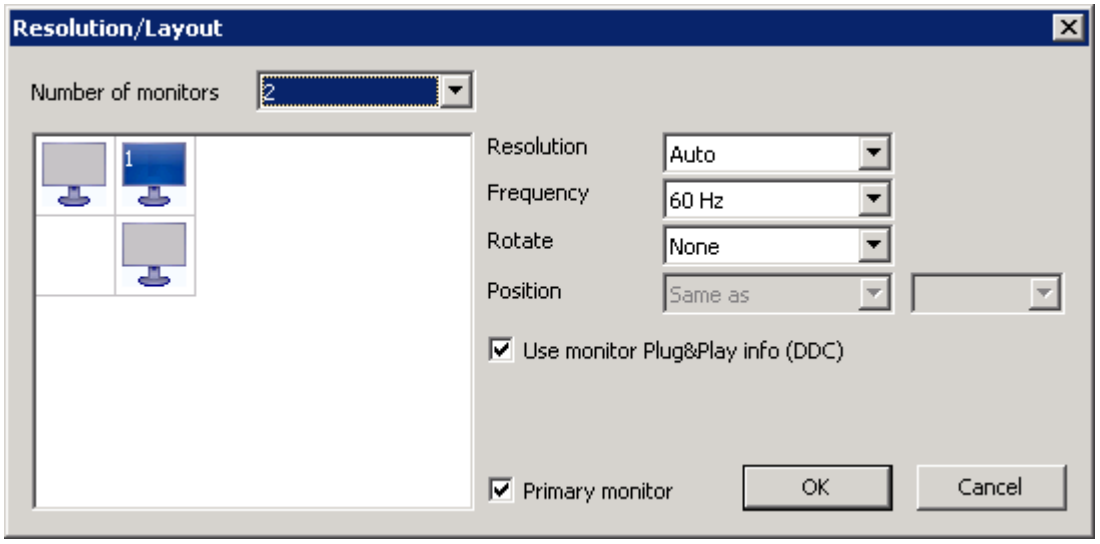
   *In the field **Number of monitors**, by default, `1` monitor is specified. This monitor, in the field below, is shown as blue monitor icon with number `1`. By default, the first monitor is defined as primary monitor (see option in the lower section).*

[1] up to four monitors with Scout Enterprise 14.8 and earlier versions

If you want to be free in the position of the first monitor, see the instructions below.

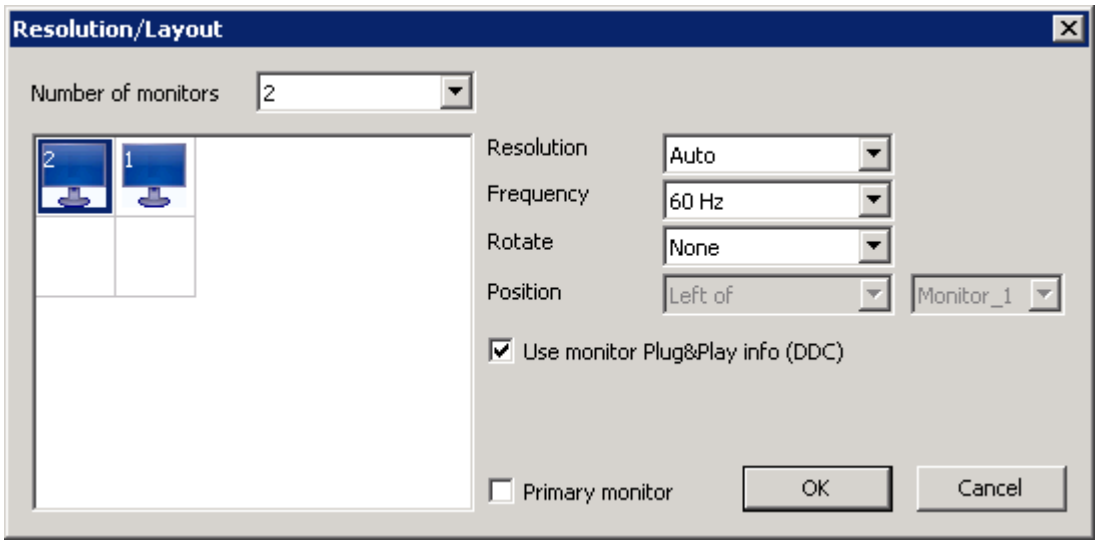
2. In the **Number of monitors** list, select how many monitors you want to connect to the Thin Client.

   Once you have defined more than one monitor, for each additional monitor, its possible positions (horizontal and vertical) are shown as gray monitor icons.



3. Double-click the gray monitor icon that shows the position of the second monitor.

   The selected monitor icon is shown in blue and with the number 2.



4. If you have specified more than two monitors, double-click the desired gray monitor icons, one after the other.

   Each of the defined monitors is shown as blue monitor icon with its number.

Note

Four monitor setup is supported on the following devices: Dell Z50QQ, Hewlett-Packard t620 Plus and Hewlett-Packard t730.

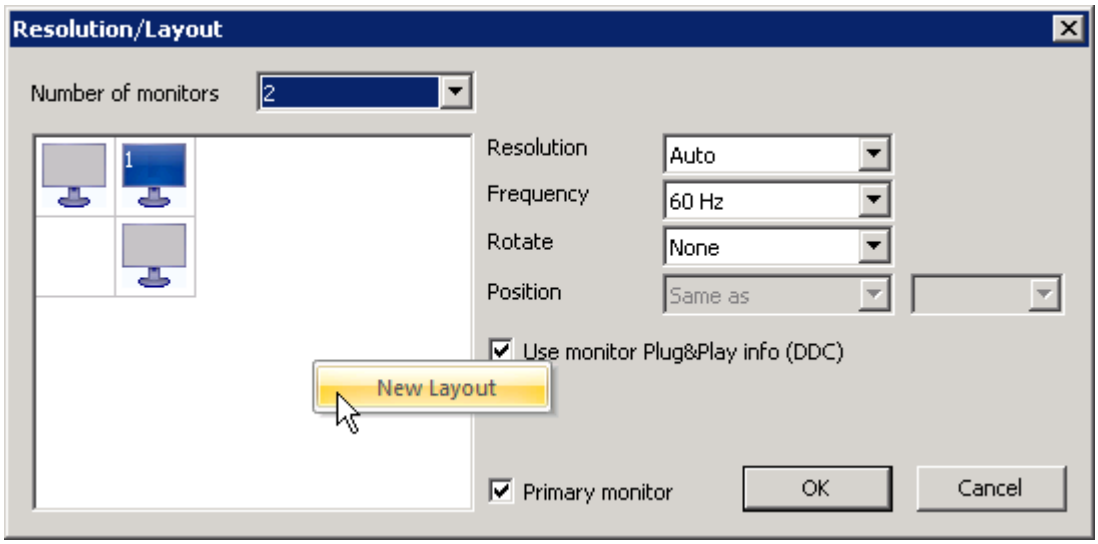
Defining positions of all monitors freely

If you want to be free in the position of the first monitor, use a new layout.

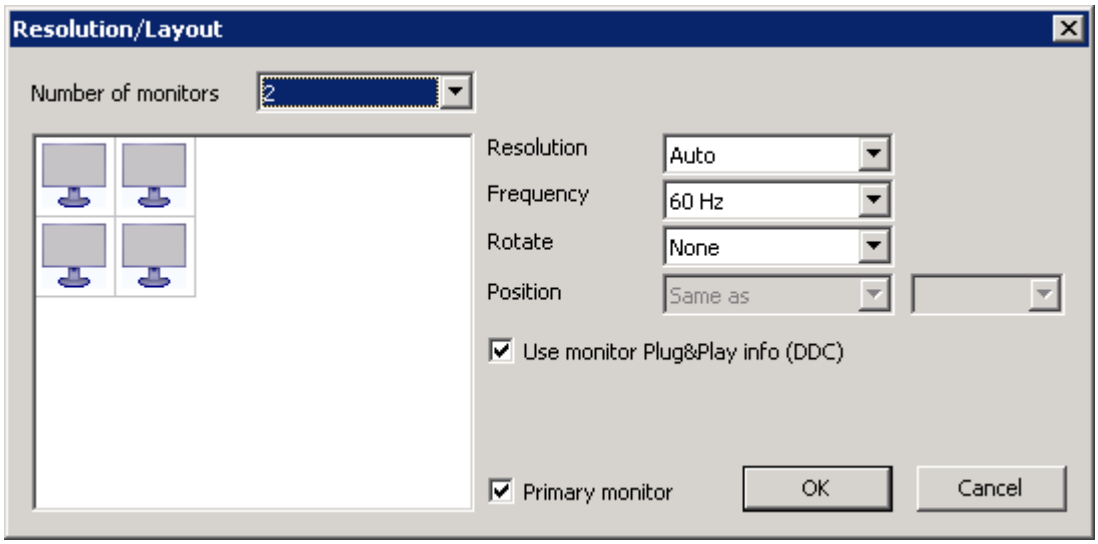
1. In the **Resolution/Layout** dialog, in the **Number of monitors** list, select how many monitors you want to connect to the Thin Client.

   The first monitor is shown as blue monitor icon, and for each additional monitor, its possible positions (horizontal and vertical) are shown as gray monitor icons.

2. Right-click in the white area next to the monitor icons, and on the context menu, click **New layout**.



For the number of monitors selected, all possible positions are shown as gray monitor icons:



3. Double-click the desired monitor position for the first monitor. Then, double-click the desired monitor positions of the remaining monitors.

Configuring extended desktop or cloned mode

If you have specified more than one monitor, the system configures the monitors to be used as extended desktops (one continuous desktop over all monitors), by default. Alternatively, for individual monitors, you can activate the Clone mode (same display on multiple monitors):

- Right-click a blue monitor icon, and on the context menu, click **Same as** *x*.

You can deactivate the Clone mode by using the **New Layout** feature (see above).

Editing screen settings

1. Select one of the blue monitor icons.
2. For the selected monitor, specify the screen resolution, frequency and rotation by using the list-fields on the right.

Note

To use screen resolutions that are not provided by the list, you can add the relevant resolution to the database table `dbo.Resolution`. After modifying the table you need to restart the Scout Enterprise Console.

3. If you want the values supported by the monitor to be processed by the client, select the **Use monitor Plug&Play Info (DDC)** option.
   If you clear the option, the **Monitor class** field becomes active.
4. If you want the selected monitor to be the primary one, select the **Primary monitor** option.
5. Confirm with **OK** and **Apply**.

Important

If your monitors do not support the settings you have defined, you might have to set back the client to initial state and modify the desired screen settings again.

5.7.2. Setting a screensaver

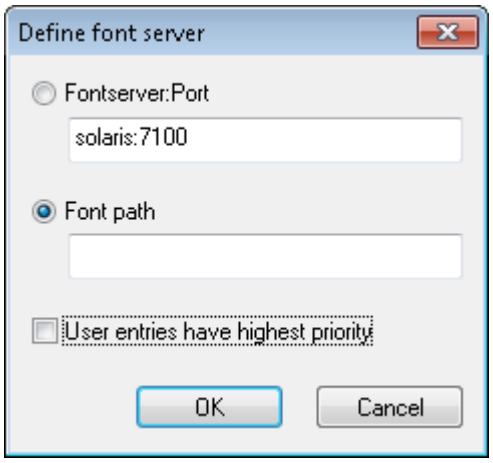
1. On the **Screen** tab, select the **Screen saver** option.
2. In the **Delay** box, type a time period in minutes, to define when you want the screensaver to come up.
3. (Only Scout Enterprise:) Select the **Password protected** option to force authentication for unlocking the screen.

   This feature requires user access authorization. The password is set to `$ELUXPASSWORD`. For further information, see Where to apply user variables.
4. Click **Settings...** to select and configure a screen saver.
5. Confirm with **OK** and **Apply**.

5.7.3. Configuring a font server

To manage different fonts, they can be saved on the server and requested by a Thin Client on demand.

1. On the **Screen** tab, click **Advanced**.
2. In the **Advanced Screen Settings** dialog, click **New**, **Edit** or **Delete** to define, modify or delete a font server.
3. If you define a new font server, in the **Font server** dialog, in the **Font server:Port** box, enter the IP address or name of the font server and then the port number. Use the following format:
   `<Font server name/IP-Address>:<Port number>`.
   Example: `192.168.10.23:7100`
   Or: In the **Font path** box, enter the installation path of the fonts.
   Example: `/smb/g/fonts`.



4. Confirm with **OK** and **Apply**.

5.7.4. Backingstore

Backingstore saves the screen information locally on the X11 server of the Thin Client. The `pixmap` picture of every window is stored on the X server regardless of whether it is visible or not.

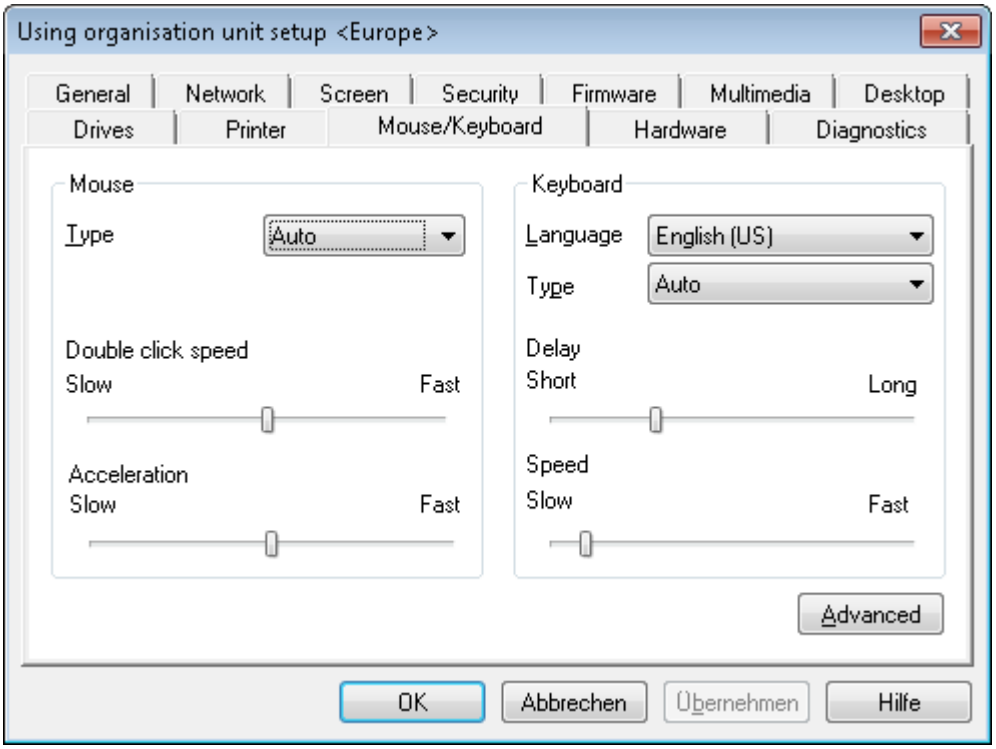
The basic idea is, when reactivating a hidden window, the window layout does not need to be recreated by the application because it is saved by the X server. This way, the screen layout can be recreated much faster, especially for slow network connections.

We recommend to use this feature with slow network connections like ISDN. The individual pixmaps are saved in the main memory, that means X server needs more memory space. Backingstore requires at least 128 MB main memory capacity.

Turning on Backingstore

1. On the **Screen** tab, select **Advanced**.
2. Select the **Backingstore** option.
3. Confirm with **OK** and **Apply**.

5.8. Mouse/Keyboard tab



5.8.1. Configuring mouse settings

1. On the **Mouse/Keyboard** tab, under **Mouse**, select your Mouse type or `Auto`.

   Normally, the type of the mouse is recognized automatically.

2. Under **Double click speed**, move the slider to the right to increase the speed.

   Double click speed defines the time interval between the two clicks to be identified as a double-click.

3. Under **Acceleration**, move the slider to the right to increase acceleration of the mouse pointer.

   The faster the mouse pointer, the smoother the movements.

5.8.2. Configuring the keyboard

1. On the **Mouse/Keyboard** tab, under **Keyboard**, in the **Language** list, select the required keyboard layout.
2. In the **Type** list, select `Auto`.

   The type of the keyboard is identified automatically.

3. Under **Delay**, move the slider to the right to increase the delay.

   The delay controls how long a key needs to be pressed until the letter is retyped.

4. Under **Speed**, move the slider to the right to increase speed.

   The speed controls how fast a letter will be retyped while a key is pressed.

5.8.3. Advanced mouse and keyboard settings

1. On the **Mouse/Keyboard** tab, click **Advanced**.
2. Edit the following fields:

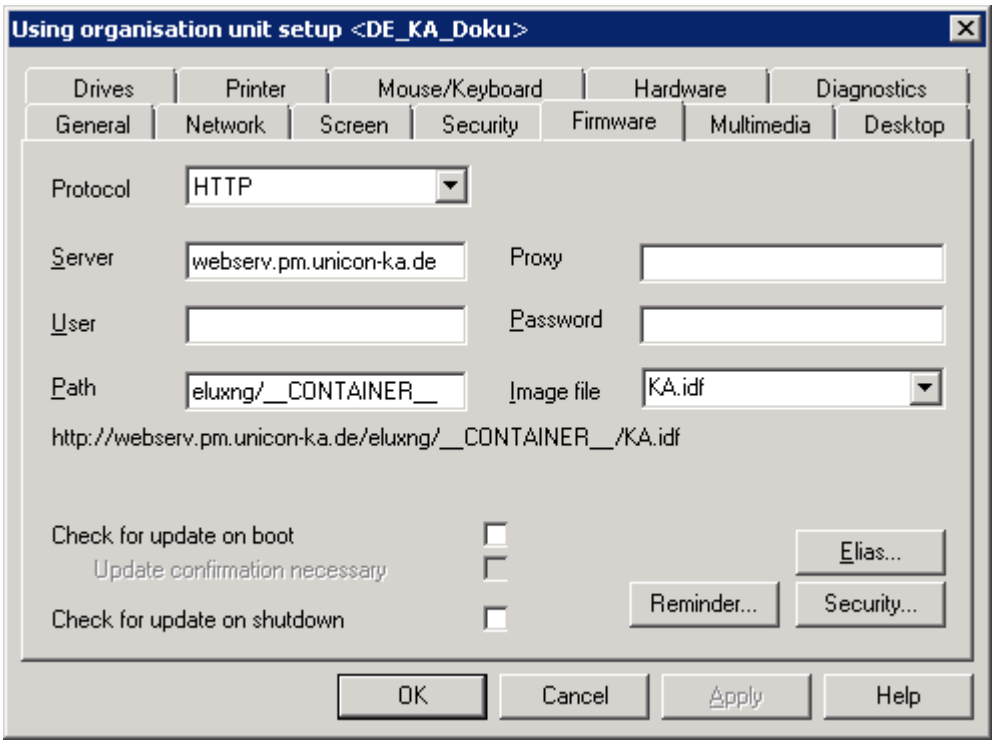
Option	Description
3 button emulation	Emulates the third mouse button for 2-button mice: Press the left and right mouse button simultaneously.
Left-handed	Reverse mouse buttons
Dead Keys	Dead keys only produce visible output when they are followed by a second key-stroke. Accent keys are dead keys as the need to be pressed before you press a character key (`+ A => à). By default, the option is active. If you use an application which is incompatible with dead keys, clear the option. Note: Some hardware platforms do not provide this option.
Numlock	Enables the numeric keypad on the client on start.
Console switch	The user can switch between the consoles by using key combinations. If the option is not active, console 1 (eLux desktop) is always shown. For further information, see Shortcuts in the eLux manual.
Multimedia/Extended keys	Enables multimedia keys and other keys with special functions on the key-board.

3. Confirm with **OK** and **Apply**.

The modifications become active on the next restart of the Thin Client.

5.9. Firmware tab

On the **Firmware** tab, you configure the firmware update settings for software updates of the clients via network.



The image definition file (IDF) defines the software to be installed on the Thin Client. The **Firmware** tab provides the required information to access the relevant IDF.

The IDF is created by using the ELIAS application, and then made available on a web server.

5.9.1. Requirements

- Web server (like IIS) which provides the eLux Software packages and Image Definition Files via HTTP or FTP.
- Software container with eLux software packages on the web server (installation component of the bundles eLux[version]_AllPackages.zip from www.myelux.com)
- ELIAS tool (eLux Image Administration Service) to create and modify Image Definition files in the software container on the web server (component of the Scout Enterprise-Installation)
- Scout Enterprise Console to configure firmware updating for the clients (component of the Scout Enterprise installation)

5.9.2. Configuring firmware update

1. For the relevant device or OU, open **Setup > Firmware**.
2. Edit the following fields:

Option	Description
Protocol	Network protocol of the web server for the software package transfer to the clients (`HTTP, HTTPS, FTP, FTPS`)
Server	Name (FQDN) or IP address of the web server containing the eLux software packages and the image definition file
Proxy (optional)	IP address and port (f3128) of the proxy server Format: `IP address:port` Example: `192.168.10.100:3128`
User and Password (optional)	User name and password (if required) to access to the eLux software container of the web server
Path	Directory path of the eLux software packages on the web server / FTP server Use slashes `/` to separate directories. Example: `eluxng/UC_RP5` corresponds to the IIS web server directory `C:\inetpub\wwwroot\eluxng\UC_RP\5` To handle different eLux versions the container directory can be parametrized by the container macro.
Image file	Name of the image definition file (`.idf`) on the web server which is used for firmware updates Do not use spaces. The file name is case-sensitive and requires the file extension `.idf`. Example: `myImage.idf` If you have both, UEFI devices and non-UEFI devices, use the BIOS macro within the IDF name.
	Note The fields **Protocol**, **Server**, **Path** and **Image file** are used to build a URL-address, which is used by the clients when starting the transmission of Image Definition file and eLux software packages for a firmware update. The URL address is displayed below of the **Path** field.
Check for update on boot / shutdown	The Thin Client checks during start or shutdown, if there are firmware updates available and necessary. You can set the option **Update confirmation nesessary** to let the user decline the update, if required..
Elias... button	Starts the ELIAS tool and opens the Image Definition file indicated in the **Image file** field.
Security... button	The **Security settings** let you define signature check before update through the client. Signature check can be performed for the Image Definition files and/or for the eLux software packages.

Option	Description
Reminder... button	The **Reminder Settings** let you define if a user is allowed to defer a firmware update and for how long. Moreover, you can specify time intervals for the update reminder. For further information, see Update deferment by user.

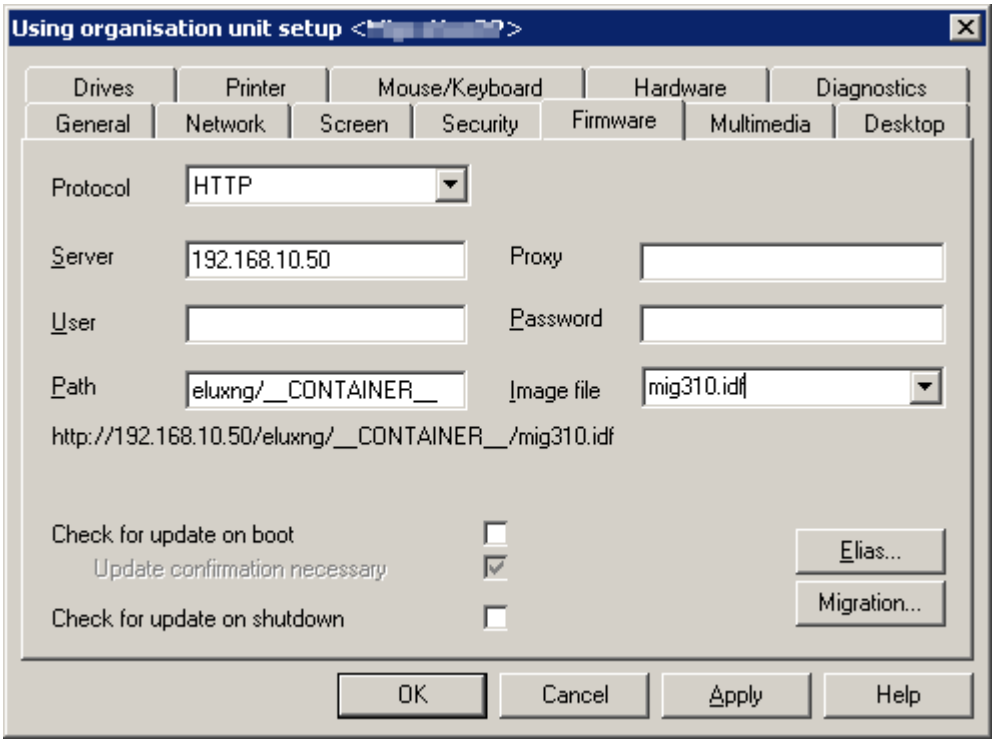
3. **Only eLux**: Click **Update** to test the Firmware-settings. For further information, see Updating firmware in the eLux guide.

   If the settings have been defined correctly, a connection to the Scout Enterprise Server is set up to check if an update is necessary.

Note
We recommend to test the Firmware settings on a client (see step 3) before configuring the clients in Scout Enterprise.

5.9.3. Different eLux versions

By default, after you have installed an eLux container, in **Setup > Firmware > Path** of a newly installed Scout Enterprise Console or eLux control panel, you will find the container macro parameter `__CONTAINER__`.



The `__CONTAINER__` string is part of the directory path and parametrizes the relevant software container (directory) on your web or FTP server. This can be very helpful if you have more than one eLux version in use.

Example:

If you run devices with both, eLux RP4 and eLux RP5, the eLux RP4 clients require the `UC_RP` container while the eLux RP5 clients require the `UC_RP5` container. To provide all clients with their

according software, in **Setup > Firmware > Path** of all clients, you will use the `__CONTAINER__` macro parameter. The clients then resolve the container macro according to their installed eLux version to `UC_RP` or `UC_RP5`, respectively. The advantage is that only one Image Definition file can be used for the two `IDFs` that have been defined for eLux RP4 and for eLux RP5 in ELIAS.

Note
In some cases, it can be useful to replace the container macro name by a fixed container name. In this case, the entry in the **Path** field must correspond to the actual container name on the web server.

Spelling of the container macro name

To replace a fixed container name by the container macro name, make sure to use the correct spelling:

Two underscores followed by the word `CONTAINER` (all uppercase) followed by two more underscores.

Note
You can use the container macro in the firmware configuration and in the recovery settings **Options > Recovery setttings...**.

5.9.4. Different BIOS systems (UEFI)

Note
eLux RP 5.3 and later versions support devices with UEFI (Unified Extensible Firmware Interface).
For these devices, the image file must contain the 64 bit kernel eLux package with integrated UEFI support (such as `kernel-4.4.x-1.UC_RP5-1.0.zip`).

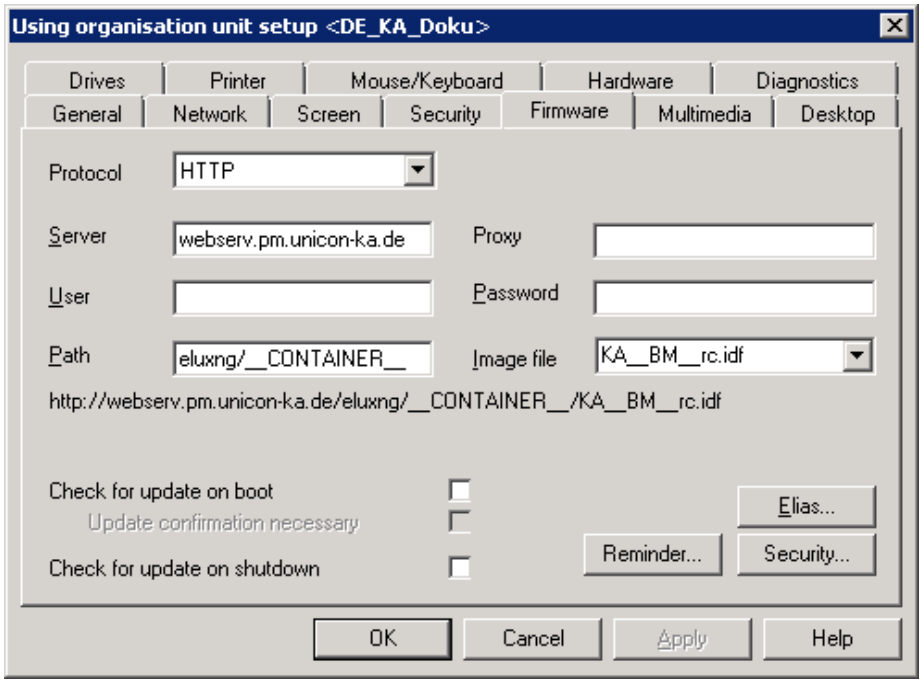
To be able to update UEFI devices and at the same time devices with the traditional BIOS in one step, the BIOS macro `__BM__` (BIOS mode) is provided to be used for the shared firmware configuration. The macro is inserted into the IDF file name. Whenever an update command is run, the client resolves the BIOS macro due to its BIOS system (device with UEFI | device without UEFI).

Configuring firmware updates for mixed environments

1. In ELIAS, create an IDF for the UEFI devices. Make sure to include the 64 bit kernel package. The IDF file name must contain the string `EFI` at any position.
   Example: `KAEFIrc.idf`
2. In ELIAS, create a second IDF for the devices without UEFI. The IDF name must correspond to the one for UEFI devices but excluding the string `EFI`.
   Example: `KArc.idf`

> **Note**
> The image files for UEFI devices and for non UEFI devices may be located in different containers if they are used for different eLux versions. The container macro then evaluates the relevant container.

3. In the Scout Enterprise Console, for the relevant OU, open **Setup > Firmware**.
4. In the **Image file** field, enter the file name of your IDF. At the position of the `EFI` string within the file name, insert the string `__BM__` for the BIOS macro instead. The file name extension `.idf` and the rest of the file name must be maintained.



   The image file specified in the figure above requires the IDFs `KArc.idf` for devices without UEFI and `KAEFIrc.idf` for UEFI devices to be available.

5. Edit the further fields of the **Firmware** tab. For further information, see Configuring firmware update.

When an update command is run on the relevant OU, the clients of the OU evaluate the BIOS macro due to their BIOS system and convert the macro string either to `EFI` or to an empty string. In the example shown above, the following URLs are generated:

UEFI devices: `http://webserv.pm.unicon-ka.de/eluxng/UC_RP5/KAEFIrc.idf`

Devices without UEFI: `http://webserv.pm.unicon-ka.de/eluxng/UC_RP5/KArc.idf`

Impact of the BIOS macro on clients running earlier eLux RP versions

Clients running firmware versions earlier than eLux RP V.5.3 cannot resolve the BIOS macro. Any firmware updates configured with a `__BM__` string in the URL fail because the specified IDF cannot be found in the containers `UC_RP` or `UC_RP5`.

Solution:

- Save an additional copy of your IDF – for eLux RP4 in the `UC_RP` container, for earlier eLux RP 5 versions in the `UC_RP5` container – using the same file name but including the unresolved macro string.

Exxample: `W:\Inetpub\wwwroot\eluxng\UC_RP5\KA__BM__rc.idf`

Spelling of the BIOS macro string

Make sure to use the correct spelling:

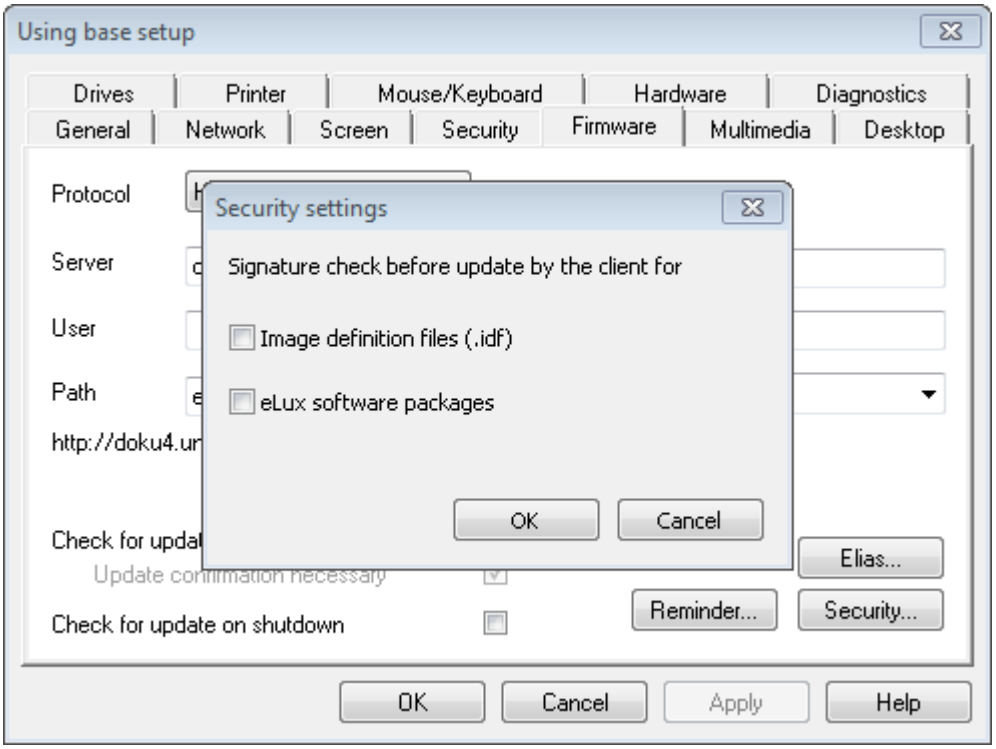
Two underscores followed by the string `BM` (all uppercase) followed by two more underscores.

Note
You can use the BIOS macro in the firmware configuration and in the recovery settings **Options > Recovery setttings...**.

5.9.5. Firmware security through signature

You can configure Scout Enterprise to make the client check signatures each time before an update is performed. In this case an update is performed only if the signature of the Image Definition file (IDF) and/or the signature of the eLux software packages have been verified successfully. The update can't be run, however, if the IDF or one of the eLux software packages to be installed, do not have a valid or verifiable signature.

Activating signature check



1. In **Setup > Firmware**, click **Security...**...
2. Under **Signature check before update**, select the **Image Definition file** option and/or the **eLux software packages** option.

*The result of the signature verification is documented in the update log file on the client. After having performed an update, the update log file is sent to the Scout Enterprise Server and can be viewed for the selected device in the **Properties** window by double-clicking the **Update status** field.*

Verifying the IDF signature on the client side requires the root certificate, but also the signature certificate in the local client directory /SETUP/CACERTS. If you use own certificates for signing IDFs or individually composed eLux packages, you can configure their transfer by using the Scout Enterprise command **Options > Advanced options... > Files**. For those eLux packages provided by Unicon, all required certificates are included in BaseOS eLux RP 4.7.0 or later.

For further information on how to create IDF signatures, see Signing an IDF in the ELIAS guide.

Note

Signature check of eLux software packages requires an update partition on the client computer. On devices without update partition, signatures can only be checked for Image Definition files but not for eLux software packages.

5.9.6. Update deferment by user

This feature allows the users to determine the update time by themselves as soon as the administrator runs an **Update** command. This allows the users to avoid firmware updates while using the device.

The client reports the current update process status to the Scout Enterprise Server. The status can be viewed in the Scout Enterprise Console in the **Update State** field of the relevant **Properties** window.

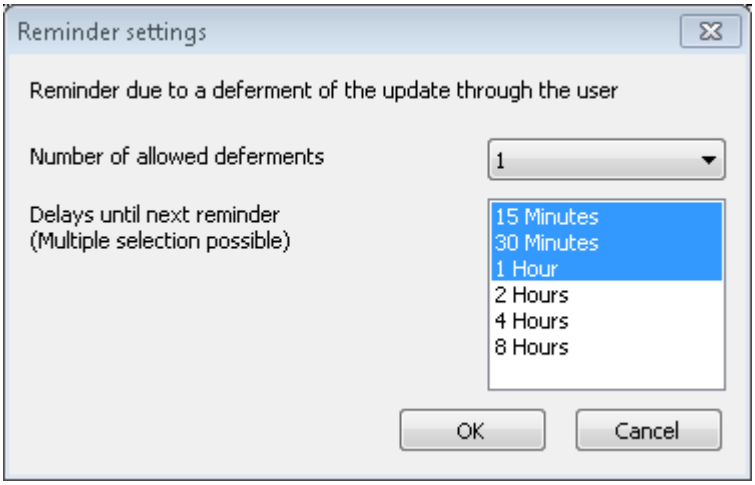
In addition, you can use the Report Generator to evaluate the **Update State** field by the value `Deferred` (other: `Successful`,`Not successful`,`Not necessary`).

Configuring update deferment option for the users

1. For the relevant device or OU, open **Setup > Firmware > Reminder...**

   *The **Reminder settings** dialog opens.*

2. Select the **Number of allowed deferments** from the list.
3. In the **Delays until next reminder** list, click one or more time intervals from which the user can select the delay for the next reminder.

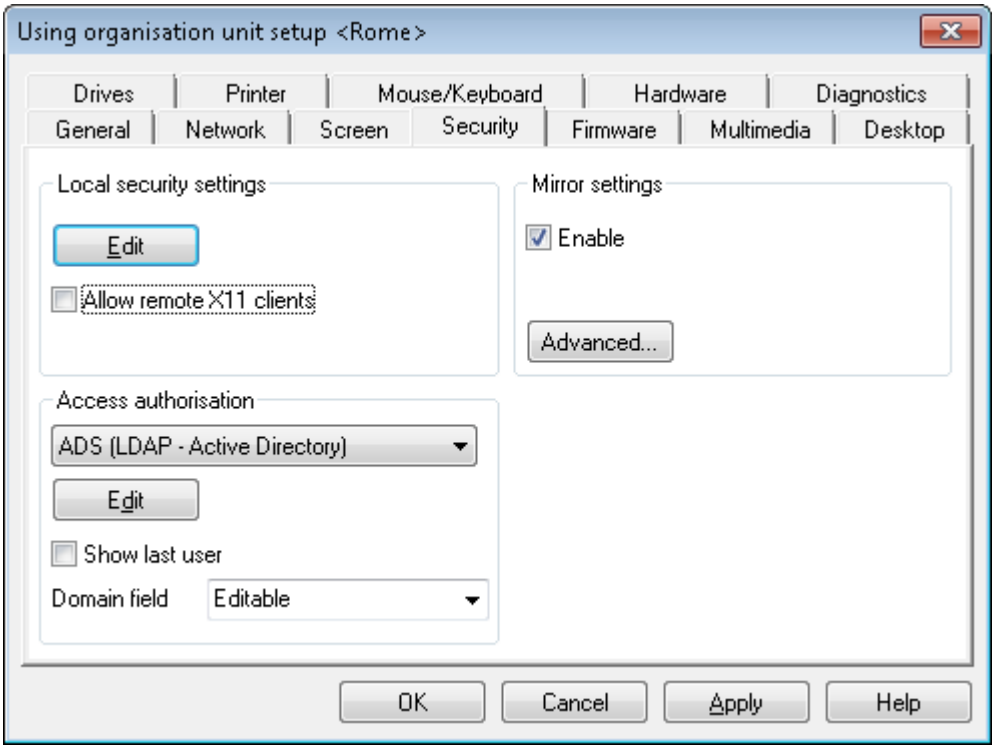


*The possibility of update deferment for the user is enabled. If the admin configures an Update command with the **Inform user** option selected, the user will get a system message including a deferment option. For further information, see* Impact of the user deferment option.

Important

Update deferment must be configured once on the **Firmware** tab and, additionally, in the **Command** dialog, for each **Update** Command you run. For further information, see Performing updates via command.

5.10. Security tab



5.10.1. Configuring mirroring

1. In **Setup > Security > Mirror settings**, select **Enable** .
2. Click **Advanced** for configuration:

Option	Description
Password (optional)	Enter a password (eight characters maximum) that is requested when a mirror session is started.
Read access only	Allows read access only
Confirmation needed	Before mirroring, the user is requested to confirm.
Transfer mirroring information	Enables recording of the mirror session
Encrypted transmission	Uses encrypted transmission
Allow Scout Enterprise only	Mirroring is only allowed from the Scout Enterprise Console or the Scout Enterprise Mirror App.
Logoff after disconnect[1]	Automatic logoff as soon as the connection is aborted
XDMCP	Enables the XDMCP protocol

3. Confirm with **OK** and **Apply**.

[1] for Scout Enterprise Management Suite 14.8 and later versions

For further information, see Mirroring.

Note

The user can cancel a mirror session at any time.

5.10.2. Local Security

To prevent users from configuring defective or unwanted settings locally on the client, you can deactivate or restrict the user rights for local device configuration.

User rights can be configured for OUs and for individual devices, even for individual fields. For example, for security reasons, you might wish to disable all tabs, but allow only particular options such as some screen settings. For further information, see Supporting local configuration.

Tabs and fields that you disable for editing appear dimmed on the client.

Changing user rights

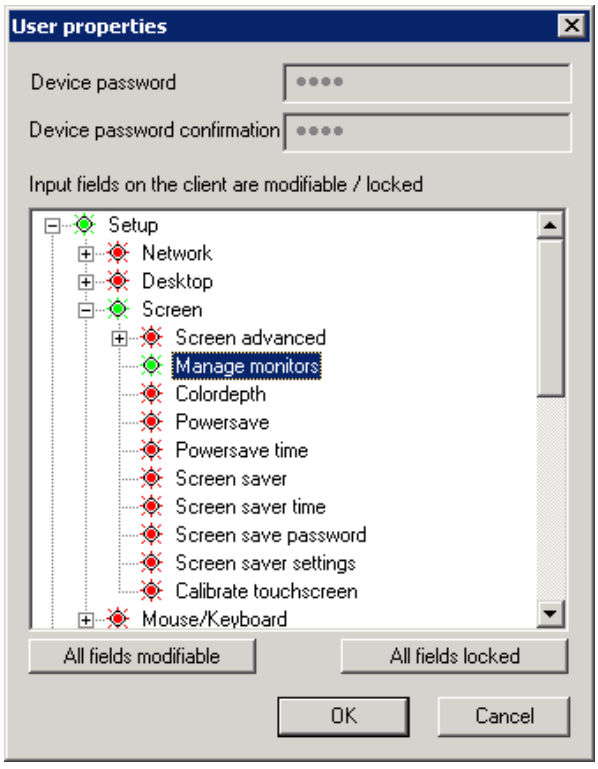
The eLux control panel provides a **Configuration** tab containing the application definitions for the installed applications, and a **Setup** tab containing the device configuration. For both tabs, you can edit the user rights related to the features shown there. Additionally, some general features such as **Logoff** are provided. Each feature can be allowed or locked.

Note

If you allow local configuration for some features, you can prevent the relevant fields and tabs from being overridden by updated configuration data of Scout Enterprise. For further information, see Supporting local configuration.

Modifying user rights for device configuration

1. On the **Security** tab, under **Local Security**, click **Edit**.



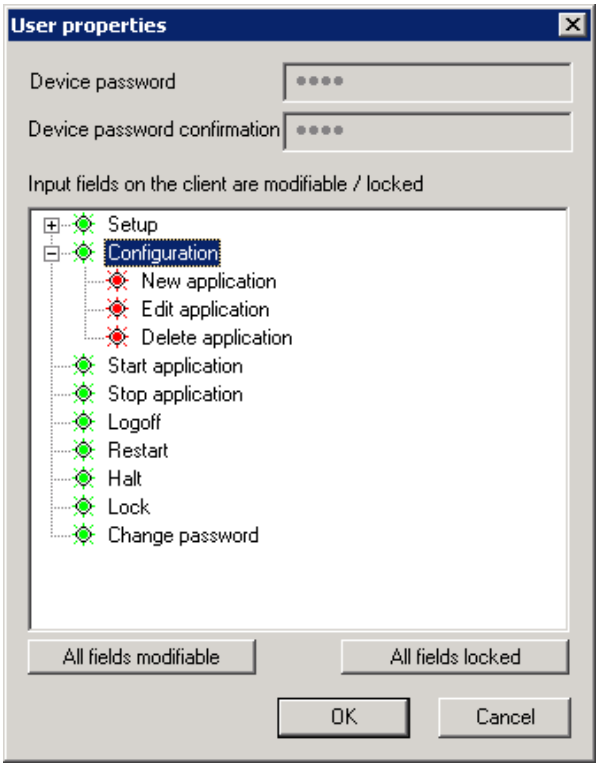
*The **Setup** node refers to the device configuration and its structure corresponds to the tabs and fields of the eLux control panel.*

2. Expand the nodes below of **Setup** as required.
3. Modify the status of the relevant features by double-clicking or pressing the SPACE key.

Allowed features are displayed in green, locked features are displayed in red. Modified user rights become active on the next restart of the client.

Modifying user rights for application definitions

1. On the **Security** tab, under **Local Security**, click **Edit**.



*The **Configuration** node refers to the defined applications.*

2. Modify the status of the features subordinate to **Configuration** by double-clicking or pressing the SPACE key, depending on whether the users are allowed to create, edit or delete an application definition.
3. If you lock the **Configuration** node, the **Configuration** tab of the client control panel is disabled and the users cannot view the application definitions.

Note

If you protect local configuration and lock the three application features, we recommend to lock also the **Configuration** node to ensure that the application definition data are updated correctly.

Allowed features are displayed in green, locked features are displayed in red. Modified user rights become active on the next restart of the client.

Allowing remote connections to X11 clients

Due to the activation of X11 applications which are hosted on remote servers, these applications can be shown in eLux..

- On the **Security** tab, under **Local security settings**, select **Allow remote X11 clients**.

Important

If you allow remote X11 clients, X11 tools can be used to access the client screen and to create screen shots.

5.10.3. Configuring user authentication

Note
User authentication requires that the **User authorisation modules** are installed on the clients.

1. On the **Security** tab, under **Access authorization**, choose from the following authentication methods:

None	Disables user authorization
ADS (LDAP - Active Directory)	Active Directory-Server Client data can be stored on the server.
LDAP (LDAP server)	Lightweight Directory Access Protocol-Server
SMB (Windows NT 4.0)	Windows NT Primary Domain Controller (PDC)
ADS + smart card	Smart card with ADS
Smart card (Smarty)	Authorization by using personalized smart cards – not supported any more
Smart card (X.509)	Smart card with LDAP

2. Click **Edit**. Specify server, server list or domains. For further information, see below. If required, define user variables. For further information, see User variables. Confirm with **Apply** and **OK**.
3. Select the **Show last user** option, if you want to help the users log in quickly.
4. In the **Domain field** list, choose if you want to allow the users to modify the specified domain or if you want to hide the domain.
5. Confirm with **OK**.

If you have configured an authentication method, the user name and password are requested when the users log on after the next restart.

Note
For devices not managed by Scout Enterprise, the administrator can log on with the user name `LocalLogin` and device password to correct any settings, if required.

Active Directory (AD)

With Scout Enterprise 14.8 and later versions, you can define more than one domain. In the client logon dialog, the users then can choose between default and alternative domains. The domain entries can be displayed with friendly names.

Note
To enable the users to log on to different domains, the following software packages must be installed on the clients:

userauth >= 3.0.0-8
securitylibs >= 1.6.0.2-2
baseosrp >= 5.4.0-1

Directory tab

- Create one or more entries by clicking **Add**, and then edit the entry (F2 or double-click).

Option	Description
Name (optional)[1]	Display name for the domain
Server	IP address or name of the domain controller To specify more than one server, separate them by spaces. If the server is not located in the same subnet as the client, enter the fully qualified domain name (FQDN). If you define more than one domain[2], the user can choose from a list. The domains are shown with their display name. The first entry is the default domain in the AD login dialog on the client.
Search base[3]	Directory tree node to be used as the base node for the LDAP queries Example: `DC=YourDomain,DC=com` **Only eLux**: Click **Find values** to search and specify the server automatically.

Note
We recommend to use a Windows time server machine. If the system time of the domain controller and client differ, Active Directory queries cannot be run successfully.

[1] for Scout Enterprise Management Suite 14.8 and later versions
[2] for Scout Enterprise Management Suite 14.8 and later versions
[3] right-click the display name for Scout Enterprise Management Suite 14.8 and later versions

Server profile tab (only Scout Enterprise)

The **Use server profile** option bundles and stores user profile data (only data that are not managed by Scout Enterprise) on the server when the user logs off. On the next logon, these data are restored. This feature helps provide the users with their user data independently of the device they use. The profile directory must be defined in the AD using the UNC format.

Note
On shutdown, triggered by the **Shutdown** button of the control panel, the **Change Password** option is provided.

Lightweight Directory Access Protocol (LDAP)

LDAP is a TCP/IP based protocol providing access to distributed directory information services.

Option	Description
Server	IP address or name of the LDAP server To specify more than one server, separate them by spaces. If the server is not located in the same subnet as the client, enter the fully qualified domain name (FQDN).
Search base	Directory tree node to be used as the base node for the LDAP queries Example: `o=<company>,l=<your city>,c=<your country>` **Only eLux**: Click **Find values** to search and specify the server automatically.
Version	LDAP version

SMB (Windows NT 4.0)

User information is managed centrally on the PDC and can be replicated on a BDC.

Option	Description
Domain	NT domain
Primary	Host name of the PDC (=NetBIOS name) IP address is not allowed.
Secondary	Host name of the BDC (=NetBIOS name) More than one BDC is not allowed. IP address is not allowed.

Smart card

Smart card tab

Option	Description
Behaviour of smart card on removal	If you choose `Lock screen`, ensure that in **Setup > Screen > Screen saver** the **Password protected** option is selected.
Allow user/password log-on	Smart card application allows user/password log-on by pressing the ESC key.

Certificate tab

Certificate-based log-on requires verification of the user certificate against the root certificate.

- Select one or more root certificates, and then click **Add...**.

The selected certificates are transferred to the client.

5.10.4. User variables

The values of user variables are used by the authentication server for the log-on process. User variables also can be used in some fields of the eLux control panel.

Pre-defined user variables are `$ELUXUSER`, `$ELUXDOMAIN` and `$ELUXPASSWORD`. They are used for log-on if user authorization is active.

For LDAP or Active Directory authentication, you even can define your own variables.

Note
If you want to use user variables, the **User authorisation modules** package and related components such as **Open LDAP** are required to be installed.

Where to apply user variables

User variables can be applied in the following fields if user authorization is active.

Note
User variables are defined without a leading `$`, but when they are applied they must begin with `$`.

Configuration

Command	Function	User variable
Start > Lock	Manual activation of the screen lock	The password is pre-assigned the default value of `$ELUXPASSWORD`

Setup

Tab	Field	User variable
Drives	User name	`$ELUXUSER`
	Password	`$ELUXPASSWORD`
	Directory, Server, Share	Any `$ELUX` variable
	Browser home directory	Any `$ELUX` variable
Screen	Screen saver > Password protected	`$ELUXPASSWORD`

Applications

Tab	Field	User variable
ICA/RDP	Server	Any `$ELUX`variable
	User name	`$ELUXUSER`
	Password	`$ELUXPASSWORD`
	Domain	`$ELUXDOMAIN`
Browser	Proxy type, Proxy port	Any `$ELUX`variable
Tarantella	Server	Any `$ELUX`variable
Local / Custom application	Parameter for all programs run from the command line Example: `eluxrdp /v:MyHost.MyDomain.de /u:$ELUXUSER /p:$ELUXPASSWORD`	Any `$ELUX`variable

Defining new user variables

If you use ADS or LDAP access authorization, you can define your own user variables (local variables). The variables are based on the LDAP attributes and are defined using the pattern `Local variable = LDAP variable`

1. On the **Security** tab, under **Access authorization**, select `ADS` or `LDAP`.
2. Click **Edit**.

3. On the **User variables** tab, edit the following fields:

Option	Description
Local variable	The name of the local variable must begin with the string `ELUX` (but without `$`), which can be followed by any characters. Example: `ELUXFULLNAME` More than one entry can be transferred if you append a `#` sign to the variable name. Example: `ELUXmemberOf#`
LDAP variable	To be able to use the LDAP variables, the relevant LDAP variable names are assigned to the individual variable as an attribute. Example 1: `ELUXFULLNAME` = `displayName` Example 2: `ELUXmemberOf#` = `memberOf` If there are several `memberOf` values within the seach base on the authentication server, they are assigned to the local variables `ELUXmemberOf_1`, `ELUXmemberOf_2` etc.

4. Confirm with **OK** and **Apply**.

Note
User variables are defined without a leading `$`, but when they are applied they must begin with `$`.

5.11. Multimedia tab

The audio **output** devices are grouped in classes depending on their connector:

USB	USB port
Analog	TRS audio jack (phone connector) or integrated devices
Digital	DisplayPort or HDMI

For each device class, you can control the volume level and **Mute** separately.

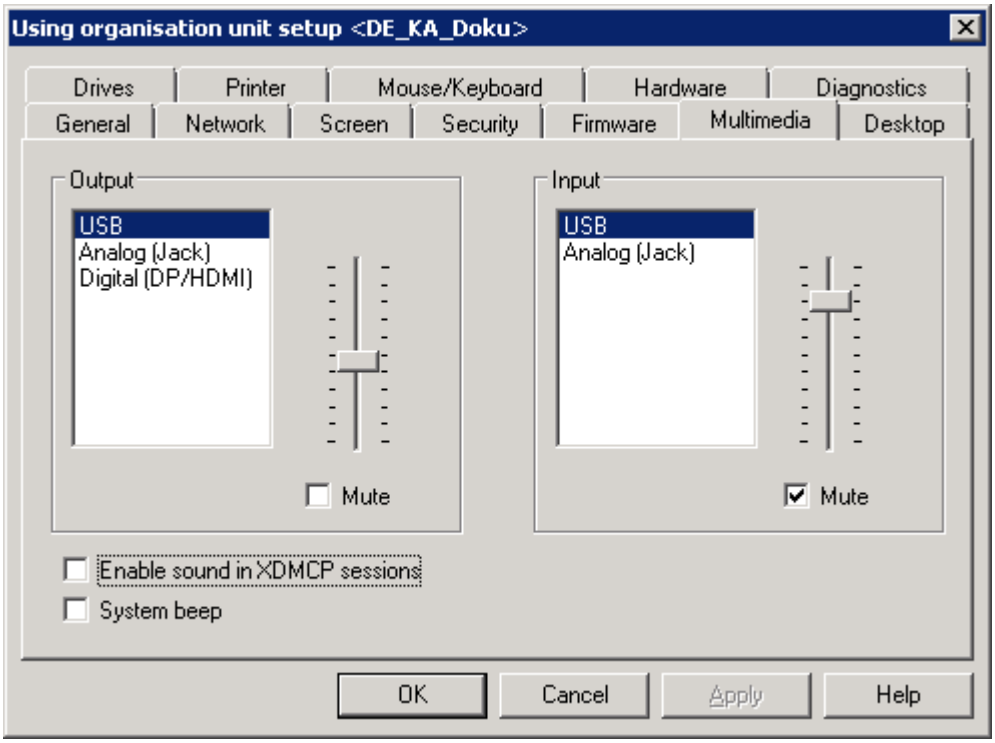
By default, the priority is defined: USB – Analog – Digital. To change priority, move the list entries by using drag-and-drop operations.

The audio **input** devices are grouped in classes depending on their connector:

USB	USB port
Analog	TRS audio jack (phone connector) or integrated devices

For each device class, you can control the sensitivity and **Mute** separately.

By default, the priority is defined: USB – Analog. To change priority, move the list entries by using drag-and-drop operations.



Option	Description
Volume (Output)	Slider to control the playback sound level for the selected device class (0 to 100)
Sensitivity (Input)	Slider to control the level of sensitivity for recording for the selected device class (0 to 100)
Mute (Output and input)	No sound is reproduced / recorded
Enable sound in XDMCP sessions	Sound can be rendered by using a X-server
System beep	Acoustic feedback signal when switching off the client

5.12. Drives tab

Define shared network directories on you Windows server as drives that can be accessed by the clients. Any drive defined this way can for example be used as browser home directory.

5.12.1. Defining a network drive

1. In **Setup > Drives > SMB Drives**, click **New**.
2. Edit the following fields:

Option	Description
Directory	Any name for the directory
Server	Name of the server including the path
Share	Windows share name
User name and password	Windows user name and password to access the directory
Domain	Can alternatively be specified in the **User** field: `<Domain\User>` or `<User@Domain>`
AD authentication (only Scout Enterprise)	The Active Directory login data is used to access the directory. The fields **User name** and **Password** are disabled.
Test (only eLux)	Checks if the network share can be accessed with the specified data

> **Note**
> To access network drives with AD authentication, for eLux RP 5.3, the software packages **userauth-3.0.0-3** and **securitylibs-1.6.0.2-1** must be installed on the clients. For eLux RP 5.3 and later versions, the software package **Network drive share** and the included feature package **Linux Key Management Utilities** must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

3. Click **OK** and **Apply**.

The directory path `/smb/` is added automatically just in front of your directory name. The data is provided on the local flash drive under `/smb/<Name of directory>`.

Note
Here, you can apply LDAP user variables. For further information, see Where to apply user variables.

To make browser settings such as bookmarks available on a permanent basis, define a network drive as browser home directory. For further information, see Browser home directory.

5.12.2. Mount points

Mount points are used to access local resources through an application. The following mount points are provided by eLux:

Samba	`/smb`
NFS	`/nfs`
Internal CD-ROM	`/media/cdrom`
USB devices	`/media/usbdisk*`

*For USB devices the mount points are assigned chronologically: The first device gets `/media/usbdisk`, the second one gets `media/usbdisk0` and so on.

Mounted devices are shown in the systray if the option **Desktop > Advanced > Taskbar** is enabled.

Note
Due to security reasons, the **Allow mass strorage devices** must be selected on the Hardware tab.

Note
Drive mapping to access local resources must be defined in the relevant application definition. For Citrix ICA applications see ICA software defaults, for RDP applications see Advanced RDP settings.

5.13. Printer tab

The eLux print service supports printing from local applications both to locally connected printers and to network printers. In addition, other workstations or servers within the network can use a locally installed printer on a Thin Client running eLux. The printer has to support LPR and TCP direct print.

In the Scout Enterprise Console, you can define and configure local printers with logic names. These printers can be accessed within the network.

The option **Print service** makes the print service start on the client.

5.13.1. Selecting printer as standard printer

1. In Scout Enterprise for the desired OU or device, open **Advanced settings > Printer**.
2. In the **Default printer** list, select the printer that you want to be the default printer.

   The list provides all defined printers. If the desired printer is not in the list, you have to define it on the **Printer** *tab of the base configuration or of a parent OU first.*

5.13.2. Defining a network printer

1. Enable the Windows LPD service (Line Printer Demon).

   The TCP/IP printer service is installed and started. The service is required to address the printer.
2. In Scout Enterprise-console, open **Setup > Printer** for the relevant devices (see Accessing device configuration). In eLux, open the Control panel and **Setup > Printer**.
3. Click **New**.

   The ***Define printer*** *dialog opens.*
4. Enter a **Name** for the network printer.
5. In the **Connection type** list, click `Network`.
6. In the **Filter** list, click one of the following options:

Option	Description
None	Enables printing from a remote session. Printing data from the session are forwarded to the printer in unfiltered RAW format. The printer driver name has to match the name in the server's drivers list(case-sensitive).
Text	Enables printing from a local shell.
PCL2	Enables printing for web sites and PDF files opened with the local Firefox in eLux.. The connected printer must supportthe language **PCL2**, **PS** (Postscript) or **PDF**.

Note

If a printer is defined on the client, you can print in different scenarios. For example, you can print text from a local shell or a PDF file out of eLux' Firefox browser. Furthermore, you can print from a remote session. When printing from a Citrix session, the filter `None` is used automatically . Hence eLux is able to send the preprocessed data directly to the defined printer. For further information, see Citrix auto-created printers in the Scout Enterprise Administrator's Guide.

7. In the **Printer address** field ,enter the IP address of the server.
   Or:
   Enter a host name from the local hosts file on the client in **Setup > Network > Advanced**.
8. In the **Printer queue** field, enter the share name of the printer.
9. In the **Driver name** field, enter the printer's driver name.

Important

Make sure that the printer driver name is identical to the one of the printer installed on the server.The name is case-sensitive and sensitive to blanks. If the names do not match, the server cannot identify the driver.

10. Confirm with **OK** and **Apply**.

5.13.3. Citrix auto-created printers

Citrix XenApp provides automatic configuration of printers (dynamic printer mapping) That means, when logging in via ICA an automatic printer definition is created on the XenApp server. This printer definition is valid only for the duration of the ICA session. After closing the session the definition is deleted. It can only be used by the logged-on user.

XenApp can auto-create local printers connected on the client device or a generic printer, the Citrix Universal Printer, which is not tied to any specific device.

Configuring local printer for auto-creating on the client:

1. In **Configuration > Printer**, specify one or more printers.
2. In the **Define Printer** dialog, in the **Name** box, enter the Microsoft Windows printer's name exactly in the same way it is in the drivers list of the server.The name is case-sensitive.

When the user starts an ICA connection to the Citrix XenApp server, the user can see icons for the automatically created client printers in the **Start > Settings > Printer** *dialog with*

`Client\`*<Hostname>#\<Printer>*

<Hostname> is the hostname of the Thin Client and <Printer> is the name of the printer defined in Scout Enterprise.
If the specific driver is not installed on the application server or the name is not identical, the client printer can not be created. In this case the universal printer is used.

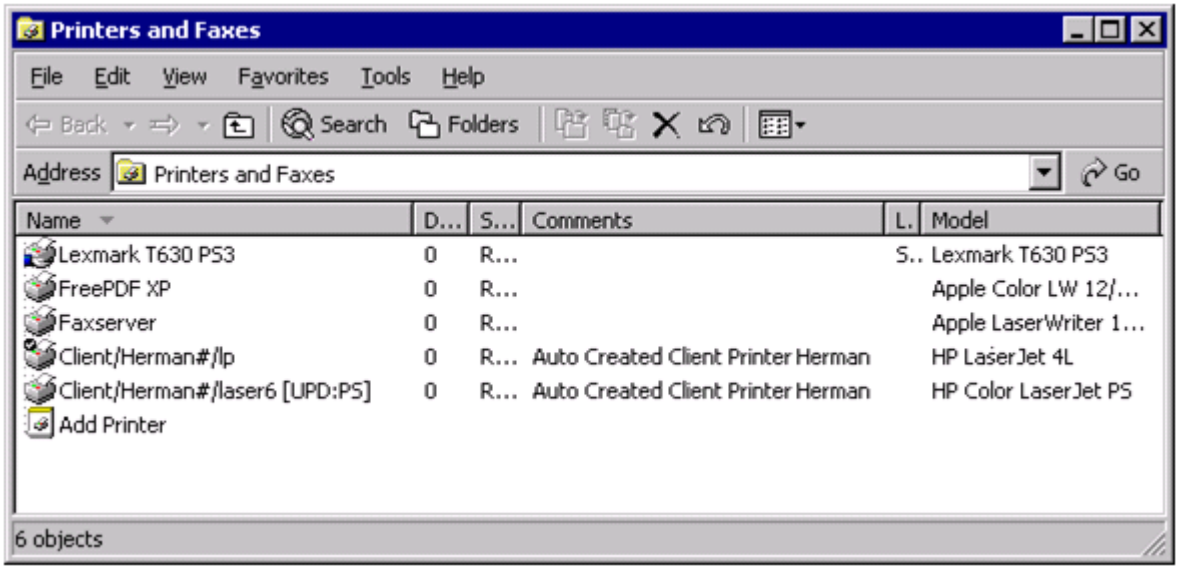
Configuring Universal Citrix Printer on XenApp server

This feature requires the current Citrix ICA client for Linux. The generic driver is the XenApp universal driver.

1. Sign in as administrator on the XenApp server.
2. Open the management console for XenApp.
3. On the context menu of **Printer Management**, click **Properties**.
4. In the left-hand panel, click **Printers**, and then configure the auto-creation of client printers. For further information, see the Citrix documentation.
5. In the left-hand panel, click **Drivers**, and then configure the driver:

Option	Description
Native drivers only	A client printer is created by using the native printer driver defined in Scout Enterprise. If this driver is not installed on the XenApp server, the client printer won't be created.

Option	Description
Universal driver only	A client printer is created. The printer driver defined in Scout Enterprise is replaced by the generic driver.
Use universal driver only if native driver is unavailable	A client printer is created by using the native printer driver defined in Scout Enterprise. If the native driver is not installed on the XenApp server, the generic driver is used.
Both universal and native drivers	Two versions of each client printer are created, one supported by the generic driver and one supported by the native driver already defined in Scout Enterprise.
Automatically install native drivers for auto-created client and network printers	Native printer drivers will automatically be installed on XenApp servers if **Autocreation** is active.



If a universal printer driver is used, the text

`[UPD:<generic driver name>]` is appended to the printer name, where <generic driver name> is `PS` in the example.

In the figure above, the client printer `client/Herman#/lpis` created by using the native driver `HP LaserJet 4L` and `Client/Herman#/laser6` is created using the generic driver for PostScript, as the specified driver `HP LaserJet PS` is not installed on the application server.

For detailed information on server-side settings for universal drivers, see **Citrix Product Documentation** for XenApp.

5.13.4. Using TCP direct print

In TCP direct print, data is sent directly to the printer. There is no spooling of print jobs on the Thin Client and the data are not modified before printing. The flow is controlled by TCP/IP.

- On the print server, type in the IP address of the particular Thin Client, the printer's name and port number

5.13.5. ThinPrint

ThinPrint® software from ThinPrint GmbH in Germany allows optimized network printing across various platforms. The software consists of a server component and a client component. The ThinPrint server processes and compresses print data for the target printer and sends it to the client. The ThinPrint client receives the print jobs from the server, decompresses them and sends them to the selected printer. ThinPrint server and client are connected via TCP/IP. Unlike TCP direct, LPR or CUPS, ThinPrint is a print protocol that allows you to specify the bandwidth. Therefore it is suited for networks with small bandwidth.

Configuring ThinPrint

1. Install the ThinPrint client on the Thin Client.
2. Connect the desired printer.
3. If you use Windows CE clients, in the **Setup > Printer** dialogue at **Thin Print** select the relevant protocol.
4. In **Setup > Printer > New**, define the printer and under **ThinPrint** check the **thinprint** option. Optionally enter a class name of up to 7 characters.
5. Configure the ThinPrint server. For further information, see the ThinPrint® documentation on www.thinprint.com.

5.13.6. CUPS

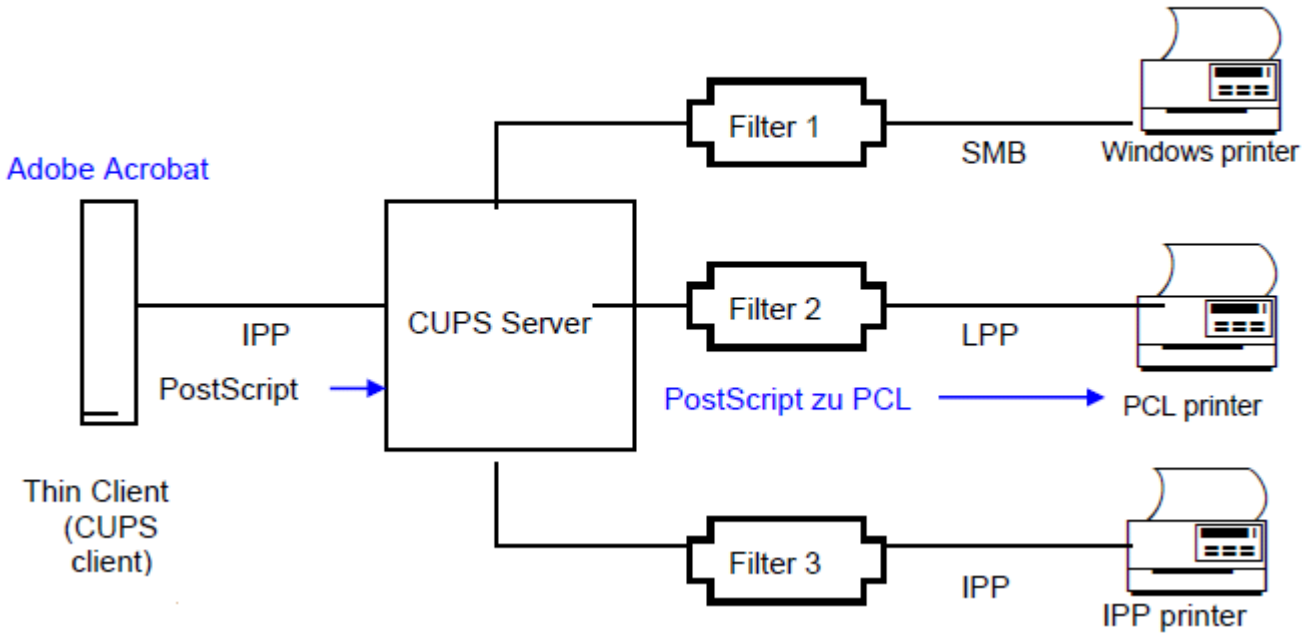
The Common UNIX Printing System™ (CUPS™) is a software solution from Easy Software Products. It provides a common printing interface within local networks and dynamic printer detection and grouping. The advantage of CUPS is that all configuration is done on the CUPS server instead of locally on the client. The CUPS server contains a list of back-ends including serial and parallel ports, USB and network (LPD).

On the Thin Client, when the CUPS client is installed, it replaces the local LPD printing system. All local printer definitions in Setup > Printer are ignored.

The CUPS client and server are provided free of charge. Commercial add-ons and support for the CUPS server can be purchased from Easy Software Products.

CUPS is particularly useful to print from local applications on the Thin Client (for example from Adobe Acrobat or a local browser). These local applications have PostScript as output format. If you do not have a PostScript printer, you are required to install a filter (for example, PostScript to PCL) on the CUPS server.

CUPS procedure



1. Adobe Acrobat generates the output file (PostScript format) and sends it to CUPS server via IPP.
2. CUPS converts PostScript to PCL by using preinstalled filter.
3. CUPS sends print job to printer using preinstalled backend (parallel, serial, network etc.).

Configuring CUPS on the Thin Client

Requires
The package **Print Environment (CUPS) (baseprinter)** must be installed on the client.

1. Install and configure the CUPS server on a computer of your choice.

   For further information, see www.cups.org.

2. Define the following environment variables in Scout Enterprise as follows:

Option	Description
CUPS_SERVER	Host name or IP address of the CUP server.
CUPS_OPTIONS (optional)	Allows you to preset user-dependent print options. These options are defined in the printer's `.ppd` file. Contact a CUPS administrator for this value. For example: CUPS_OPTIONS=-o OutputBin=Bin2. **Tip:** In the case you use LDAP or ADS, in place of the environment variable CUPS_OPTIONS set in Scout Enterprise you can use the user variable ELUX_PRINTEROPTIONS set on the LDAP or ADS server.

3. Transfer the environment variables to the Thin Client.

Printing from a local browser

1. Start Firefox.
2. Open a website that you want to print from.
3. Click **File > Print**.

   The browser's **Print** *dialog opens.*

4. Leave the settings and click **OK**.

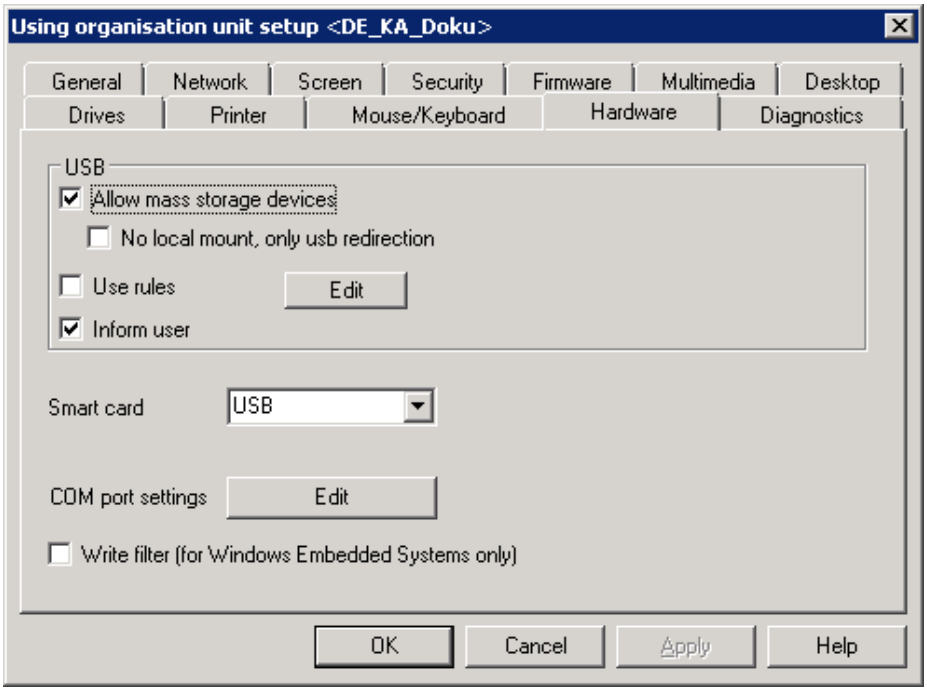
   The CUPS dialog **Print** *opens.*

5. In the **Name** list, select a printer (the provided printers depend on the server-side settings).
6. If required,edit further settings.
7. Click **OK**.

   The printing process starts.

8. After printing, click **OK** to close the **Print information** dialog .

5.14. Hardware tab



5.14.1. USB mass storage devices and card readers

Option	Description
Allow mass storage devices	Allows using the connected USB mass storage devices
No local mount, only USB redirection[1]	Restricts the use of USB mass storage devices to USB redirection within configured sessions on a backend. There are no mount points provided to use USB mass storage devices locally on the eLux client.
Use rules	Restricts the use of USB mass storage devices according to defined rules: Using USB mass storage devices can be restricted to devices with specified VID (Vendor ID) and/or PID (Product ID) such as an individual USB stick model. Moreover, the USB rules can be applied to further USB device classes like smart card readers.
Edit	Opens the USB rules dialog: Define rules to explicitly allow or deny individual device models.
Card reader	Enables a card reader on the selected port
Inform user	When a USB mass storage device is connected, a systray message is displayed.
COM port settings	Set particular COM port settings such as speed, parity, stop bits

[1] for eLux RP 5.4 and later versions

Option	Description
Write filter (only Windows Embedded)	The user is not allowed to store local data on their Windows Embedded client.

Note

If you use defined USB rules, the **Hardware > USB mass storage devices** option is enabled for clients with Lux RP 4 (beginning with version 4.1) and USB mass storage devices can be used. This applies even if the USB rules comprise only entries for other device classes such as smart card readers. To deny USB mass storage devices all the same, use the USB rule `DENY: CLASS=8`.

To use USB rules with eLux 5.4 clients and Scout Enterprise 14.7 or earlier, a `terminal.ini` entry is required:

- For the relevant clients, in **Advanced settings > Advanced file entries**, define the following entry:

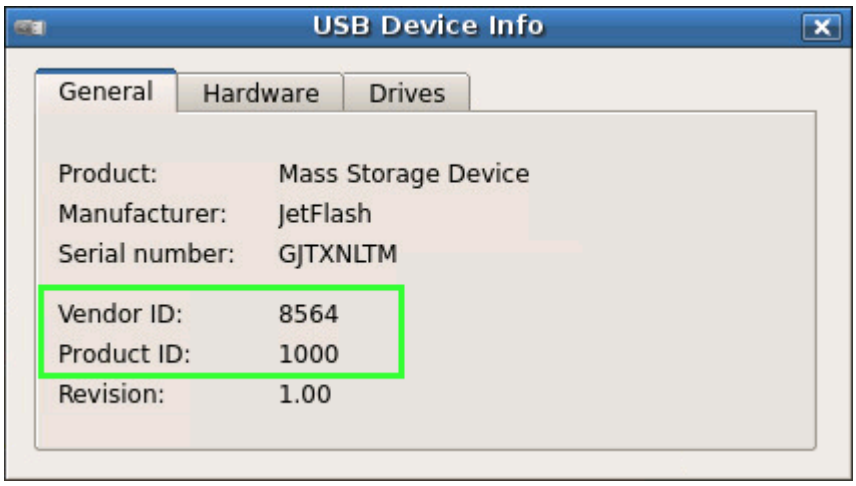
File	`/setup/terminal.ini`
Section	`Global`
Entry	`USBUseRules`
Value	`true`

For further information, see Advanced file entries.

5.14.2. Defining USB rules

1. For the relevant OU or device, open **Setup > Hardware > USB > Edit**.
2. In the list-field, select a set of predefined rules as template.
3. Double-click into the relevant line, or select a line and press F2.
4. Modify the rule by using the example rules below.

   The values of the manufacturer ID (VID) and product ID (PID) can be found in the **USB device info** dialog of the taskbar.



5. Confirm with **OK**.

Example rules:

Rule	Code
Allow a specific USB mass storage device model only	`ALLOW: VID=0781 PID=5151` # Allow particular USB model (Example: SanDisk Cruzer Micro) `DENY: CLASS=08` # Deny all devices of the class MASS STORAGE DEVICES.
Deny a specific smart card model only	`DENY: VID=18a5 PID=0302` # Deny particular smart card model (Example: Omnikey CardMan 3821) `ALLOW: CLASS=0B` # Allow all devices of the class SMARTCARD
Deny all printers, mass storage devices, smart card readers.	`DENY: CLASS=07` # Deny all devices of the class PRINTERS `DENY: CLASS=08` # Deny all devices of the class MASS STORAGE DEVICES `DENY: CLASS=0B` # Deny all devices of the class SMARTCARD
Deny all devices	`DENY:` # Deny all devices.

The syntax of the USB rules corresponds to the one of the Citrix USB policy rules.

Important

The USB rules affect all USB device classes including `03 HID` (Human Interface Devices). Denying the `03 HID` class, deactivates mouse and keyboard. Denying all classes (`DENY: # Deny all devices`) affects also internal USB hubs and devices with manufacturer-specific device classes such as WLAN modules, on the client. For particular hardware configurations, you might encounter issues during the boot process of the client. We strongly recommend performing tests before using this option.

Configuring USB redirection rules

For Citrix Receiver 13.x and later versions, and for VMware Horizon 4.1 and later versions, you can define USB filtering rules für USB redirection.

1. Type the required USB filtering rules into the appropriate configuration files.

   Citrix USB filtering rules:

Configuration file	Code (Example)
/setup/ica/usb.conf	`ALLOW: VID=0781 PID=5151` `DENY: CLASS=08`

   VMware USB filtering rules:

Configuration files	Code (Example)
/setup/elux/.vmware/default-config /setup/elux/.vmware/config /setup/elux/.vmware/view-userpreferences	`viewusb.ExcludeFamily = "storage"` `viewusb.IncludeVidPid = "vid-0781_pid-5151"`

   For VMware, all three VMware configuration files must contain the rules.

2. To transfer the configuration files to the clients, use the Scout Enterprise feature **Files configured for transfer**. For further information, see Advanced settings > Files.

On the next restart of the relevant clients, the USB redirection rules become active.

5.14.3. Key combination for safe removal of USB devices

Any connected USB mass storage devices should always be removed by using the **Remove safely** feature to ensure that all data are saved.

To make it easier for the users you can define a key combination that removes all connected USB mass storage devices savely:

ALT+WINDOWS LOGO KEY+S

Define the key combination by using the **Advanced file entries** feature of the Scout Enterprise Console for the `terminal.ini` file:

File	`/setup/terminal.ini`
Section	`Layout`
Entry	`UsbUnmountHotKey`
Value	`<Alt><Mod4><Hyper>s`

For further information, see Advanced file entries.

5.15. Diagnostics tab

By using the **Diagnostics** tab you can enable or disable enhanced debugging on the client.

If the **Debug level** is active, the feature **Device diagnostics** helps you run predefined commands on the client and retrieve a set of configuration and log files to a greater extent than without enhanced debugging.

If you require technical support from Unicon, switch on enhanced debugging before you perform **Device diagnostics**.

Device diagnostics is performed by using an online command, for further information, see Device diagnostics.

Note

Make sure to switch off the **Debug level** after having performed device diagnostics. Otherwise, you risk to exceed the memory capacity of the Thin Client.

5.16. Troubleshooting

Error / problem	Reason	Solution
When you use USB multimedia devices such as headsets or webcams, the screen freezes or the window cannot be focused.	The USB operating elements register themselves as keyboard or mouse devices in the system.	Prevent the registration as keyboard or mouse devices by defining a `terminal.ini` entry. To do so, use the Scout Enterprise feature Advanced file entries: File: `/setup/terminal.ini` Section: `Xorg` Entry: `IgnoreUsbInput` Value: `VendorID_1:ProductID_1,VendorID_2:ProductID_2` Example: `0b0e:034c,047f:c01e` The basic functionality of the operating elements is not affected.
Multimedia USB devices, connected via DisplayPort, do not play back sound.	Sound reproduction via DisplayPort ist disabled.	Enable sound reproduction by defining a `terminal.ini` entry. To do so, use the Scout Enterprise feature Advanced file entries: File: `/setup/terminal.ini` Section: `Screen` Entry: `Radeon.Audio` Value: `true` Alternatively, use a separate audio cable.
When you use a touch screen, the location of a fingertip touch is not recognized precisely.	The monitor is not calibrated exactly.	To calibrate the monitor, configure a custom application by using the parameter `calibrator`, and then start the application.
Display/graphics issues	The feature package for hardware acceleration **HwVideoAccDrivers**[1] is not installed.	Activate the **HwVideoAccDrivers** FPM[2] within the **XOrg** package in the IDF.

[1] for eLux RP 5.5 and earlier versions: **HwVideoAcc Libraries and Drivers** FPM
[2] for eLux RP 5.5 and earlier versions: **HwVideoAcc Libraries and Drivers** FPM

Error / problem	Reason	Solution

	Hardware acceleration (installed with the **HwVideoAccDrivers** FPM[1]) is not supported by the device and causes problems.	To exclude individual device types from hardware acceleration,[2] create a blacklist that is transferred and locally saved to the clients by using the Scout Enterprise feature Files:
		`/setup/hwaccBlacklist`
		In the text file `hwaccBlacklist`, list the relevant device types, one per line. The name of the device type must be identical to the string that is shown in the Scout Enterprise Console, in the **Properties** window under **Asset > Hardware information > Type**.
		Example:
		`FUTRO S920`
		`D3314-B1`
		`HP t620 Dual Core TC`
		For all device types listed in the blacklist, hardware acceleration is disabled.

Note
After the `sessions.ini` file has been updated on the client, one more client restart might be required to enable the new setting.

[1] for eLux RP 5.5 and earlier versions: **HwVideoAcc Libraries and Drivers** FPM
[2] for eLux RP 5.6 and later versions

6. Advanced settings

The settings of the device configuration that you have defined in **Options > Base configuration** or for particular OUs or devices, respectively, can be

- overridden for particular devices or OUs
- extended by further specific options

by using the **Advanced settings**.

Opening Advanced settings

- To override or to add settings for all devices, in Scout Enterprise click **Options > Advanced settings**.
- To override or to add settings for a particular OU or device, open the relevant context menu and click **Advanced settings...**.

Note
Inheritance is used for the Advanced settings, either. By default, the **Use parent advanced settings** option is selected. You can, however, clear the option on some of the tabs.

6.1. Devices

– only globally available for all devices (**Options > Advanced settings**) –

Option	Description
Maximum ping-time (milliseconds)	Maximum response time in milliseconds by which clients should respond to a `ping` command.
Maximum search time (seconds)	Total time for searching devices for Discovery. After the indicated time has expired, Discovery is stopped.
Only locked fields are updated on the client.	Editable fields are free for individual configuration and are not overridden by Scout Enterprise. When loading an updated configuration from Scout Enterprise, only the locked fields are updated. For further information, see Supporting local configuration.
	Note If users have set defective configuration data, you can, however, override unlocked fields and set a flag for the relevant device in the Scout Enterprise Console to reload all configuration data. For further information, see Supporting local configuration.
Default OU	OU new devices are assigned to, by default
Assign OU depending on OU filter	Activates the OU filter for new devices Click the **...** button to configure the OU filter. The OU filter has priority over other methods but can be ignored for individual devices. For further information, see OU filter.
Deactivate new devices	Deactivates newly added devices
Allow dynamic change of groups	Allows dynamic assignment of devices via DHCP
Accept only known devices	The Scout Enterprise Server accepts only devices with known MAC addresses. For further information, see Reserving device profiles.
Use the client's host name as device name	The device name is the client host name and cannot be changed in the Scout Enterprise Console permanently.
To avoid duplicate names, change name of existing entry	When a new device with already existing name is added, the name of the existing device instead of the name of the new device is changed.
Name template	Name template for new clients Can be overridden for particular OUs (**Advanced settings > Management**)
Apply name template only on new devices	Name templates are not applied when you move or relocate devices.

6.2. Update

– not available for individual devices –

Option	Description
Maximum number of parallel updates	Restriction for performance reasons
Maximum time to connect	Time for connection build up

Note

The optimum values depend on the system.

6.3. Wake On LAN

– only globally available for all devices (**Options > Advanced settings**) –

Wake On LAN is a feature supported by Scout Enterprise that helps you start turned-off Thin Clients.

The Scout Enterprise Server sends a so-called magic packet that is identified by the network adapter of the turned-off Thin Client (requires the Thin Client to support Wake On LAN and have configured it in the BIOS settings).

The magic packet for Wake On LAN is sent as broadcast (UDP, eLux port 20000 incoming/outgoing) within the current network subnet, it cannot operate across the entire network. To wake up Thin Clients in remote subnets, the following methods are provided:

Integrated eLux RP Wake On LAN server

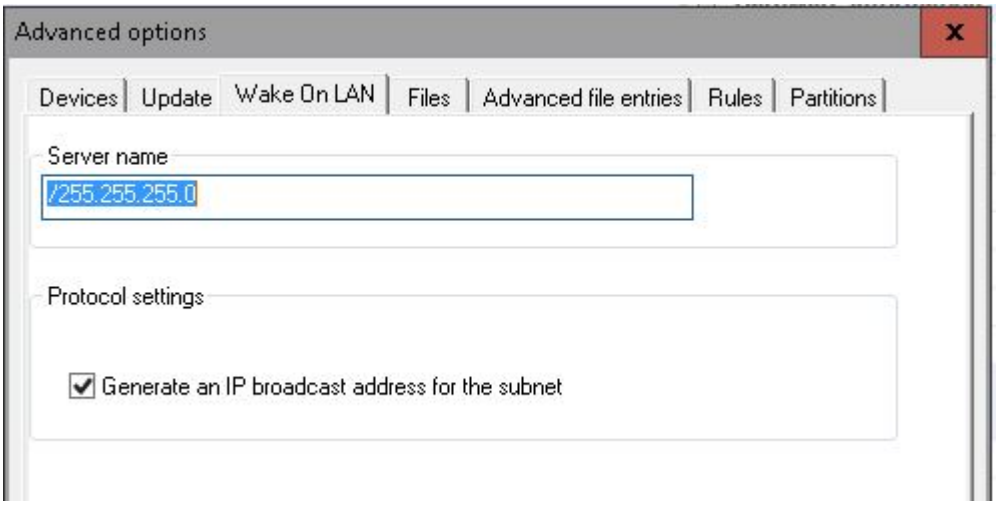
The Scout Enterprise Server always checks if there is any turned-on device in the subnet of the Thin Client to be woken up. In this case, the Scout Enterprise Server transfers a Wake On LAN job containing the MAC address of the destination client via IP to the turned-on Thin Client. The receiving Thin Client then acts as Wake On LAN server, creates a magic packet with the MAC address of the destination client, and broadcasts the magic packet within its subnet (UDP).

The Wake On LAN server is an integral feature of eLux RP and is ready-to-use without configuration.

Subnet directed broadcasts

Subnet directed broadcasts can directly address the subnet of the Thin Client to be woken up via IP. The IP broadcast address of the relevant subnet is determined by the IP address of the client and the configured subnet mask. The magic packet for Wake On LAN is broadcasted (UDP) only within the addressed subnet.

The use of an IP broadcast address for the subnet must be configured once as gloabl setting.



This option is only available in the global Advanced options.

Option	Description
Server name	Subnet mask for subnet directed broadcasts (for earlier versions: IP address of Wake On LAN server – option also available in the Advanced settings of devices and OUs)
Generate an IP broadcast address for the subnet (in global Advanced options only)	The packet is sent to the relevant subnet (dedicated subnet). Requires a subnet address in the **Server name** field using the format `/255.255.255.0` (Note the leading slash). Example: To wake up a device with IP address `192.168.10.44`, enter `/255.255.255.0` in the **Server name** field. This causes Scout Enterprise to generate the IP broadcast address `192.168.10.255` for the subnet. By default, this option is not active.

6.4. VPN

– only available for individual devices –

Note
The **VPN** tab is only provided in the **Avanced settings** of the devices but not of an OU.

Scout Enterprise supports the following VPN (Virtual Private Network) clients for secure communication:

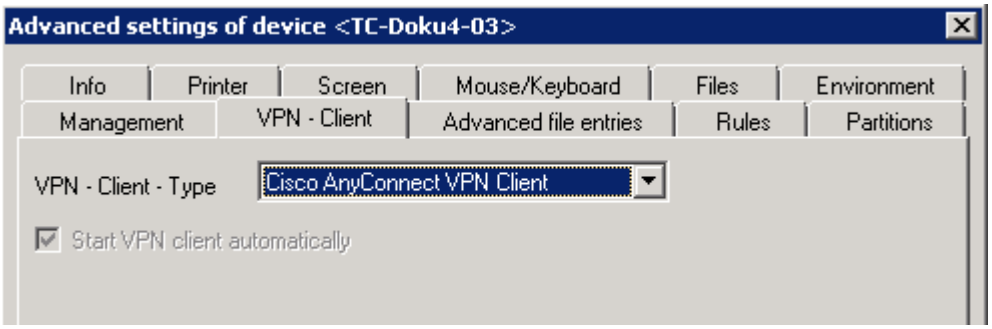
- Cisco AnyConnect
- VPNC (only for eLux RP version 4)
- OpenVPN

Depending on the VPN client used the client devices must have a configuration file. You can modify the configuration file by using the Scout Enterprise feature Advanced file entries.

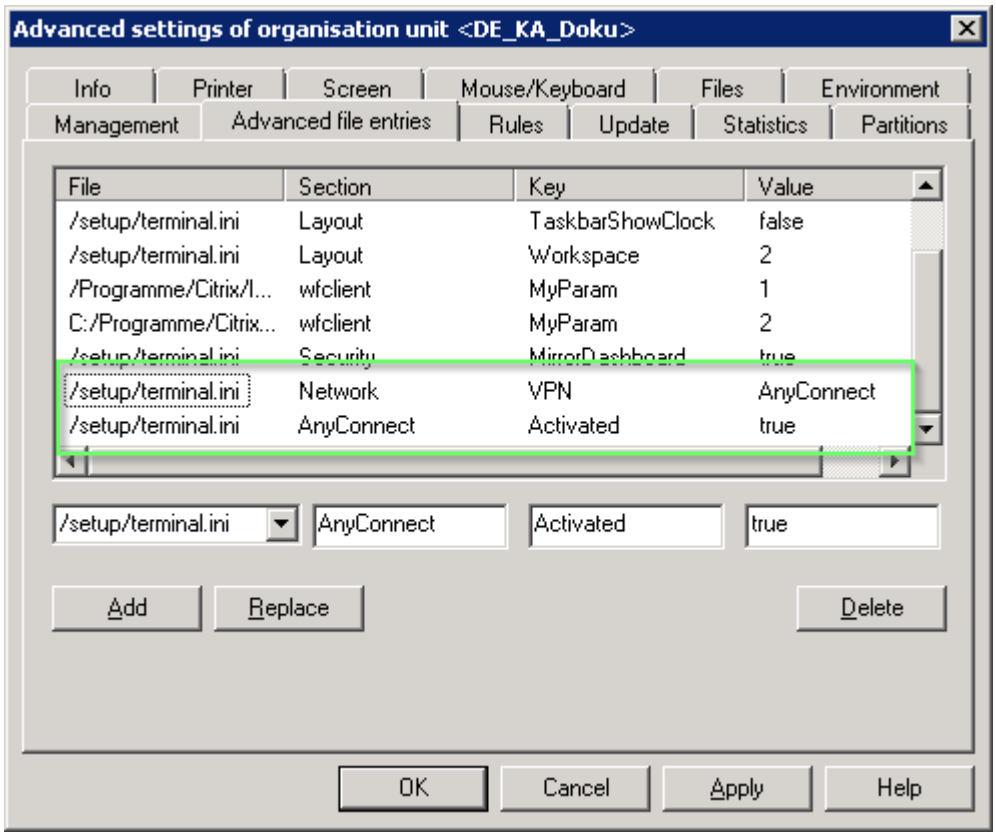
6.4.1. Configuring Cisco AnyConnect

Requires
The IDF must contain the **vpnsystem-*x*** software package, and in the package, the **Cisco AnyConnect** component must be selected. For further information, see Creating an IDF in the ELIAS guide.

1. If you want to configure Cisco AnyConnect for an individual device, right-click the relevant device and click **Advanced settings > VPN client**, and then, in the list-field, select `Cisco AnyConnect VPN Client`.

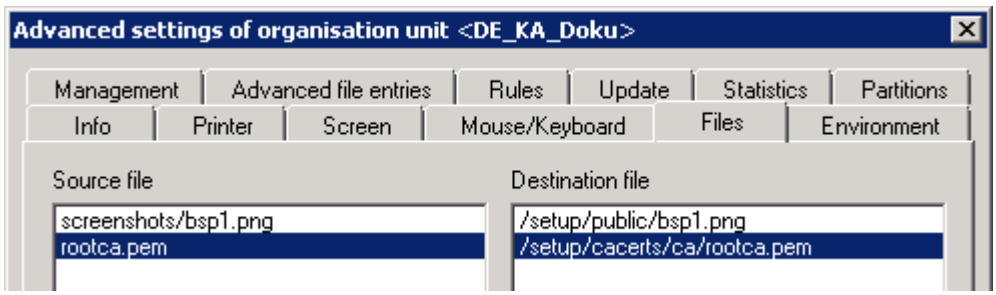


2. If you want to configure Cisco AnyConnect for an OU, for the relevant OU, open **Advanced settings > Advanced file entries** and add the following `terminal.ini` entries:



The clients of the relevant OU receive their Cisco AnyConnect configuration via `terminal.ini`.

3. To configure the transfer of the required certificates, for the relevant client or OU, open **Advanced settings > Files**. Add the source file and destination file with destination path `/setup/cacerts/ca`.



Note
The certificates that are transferred from the VPN server are stored in `/setup/cacerts/client`.

4. Restart the relevant clients twice. (The second restart is required to activate the VPN configuration data locally on the client.)

   The Cisco AnyConnect dialog opens. The dialog can also be called from a shell by using `vpnui` or as local custom application.

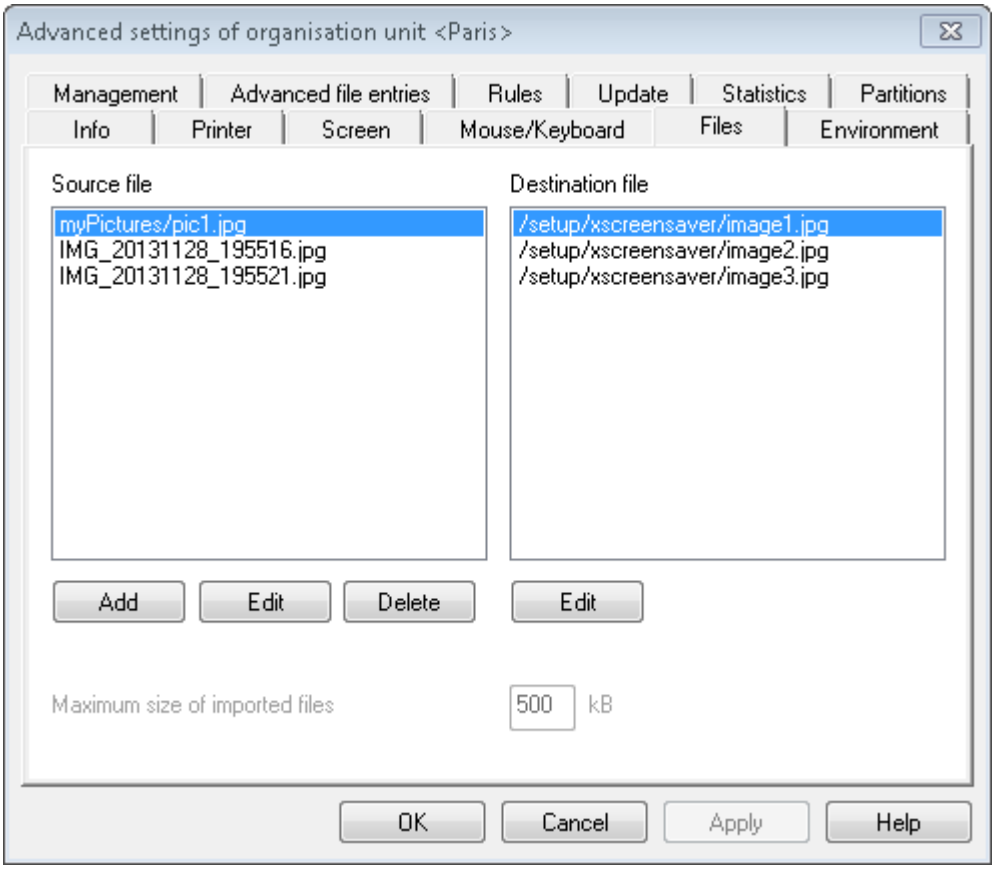
5. Enter the address of the Cisco back-end and click **Connect**.

Note
As an option, you can create an AnyConnect configuration file or copy one from a reference client, and then transfer the file to `/setup/elux/.anyconnect` by using the Scout Enterprise feature **Files**.

6.5. Files configured for transfer

This feature helps you transfer files to the client. You can define files to be transferred on the next restart for all devices, for individual devices or for OUs.

The source files can be referenced in the file system or imported to the Scout Enterprise database.



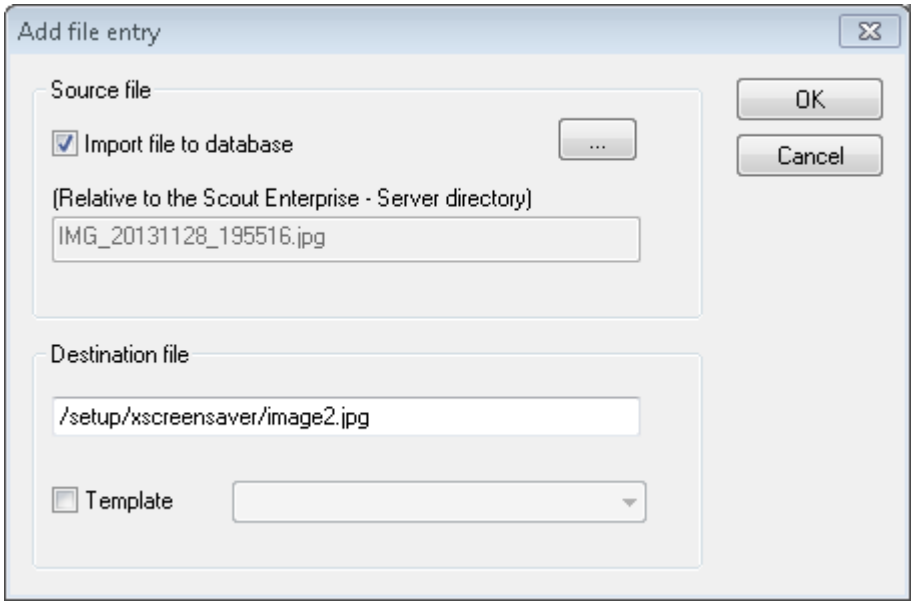
Example: You might wish to copy one or more picture files to the clients to be used as screen saver.

Defining files for transfer

1. If you want to configure file transfer to all devices (global file list), click **Options > Advanced Settings...**.
   If you want to configure file transfer to the devices of a particular OU or to an individual device (individual file list), open the context menu of the relevant OU or device and click **Advanced settings...**

Note
Individual file lists have precedence over global file lists.

2. Click the **Files** tab.
3. Click **Add**.



*The **Add file entry** dialog opens.*

Note

Files that you import into the database are saved with the SQL database backup.
Files that you reference in the file system provide the opportunity to be replaced by other content as long as the file name does remain the same.

4. Under **Destination file**, modify target path and file name, as you like to save it on the client.

   The file name may differ from the one of the source file.

5. Confirm with **OK**

Source and destination are defined. The files are transferred on the next restart of the clients.

The files will only be reloaded after changes have been made in file configuration or in the files themselves.

6.6. Advanced file entries

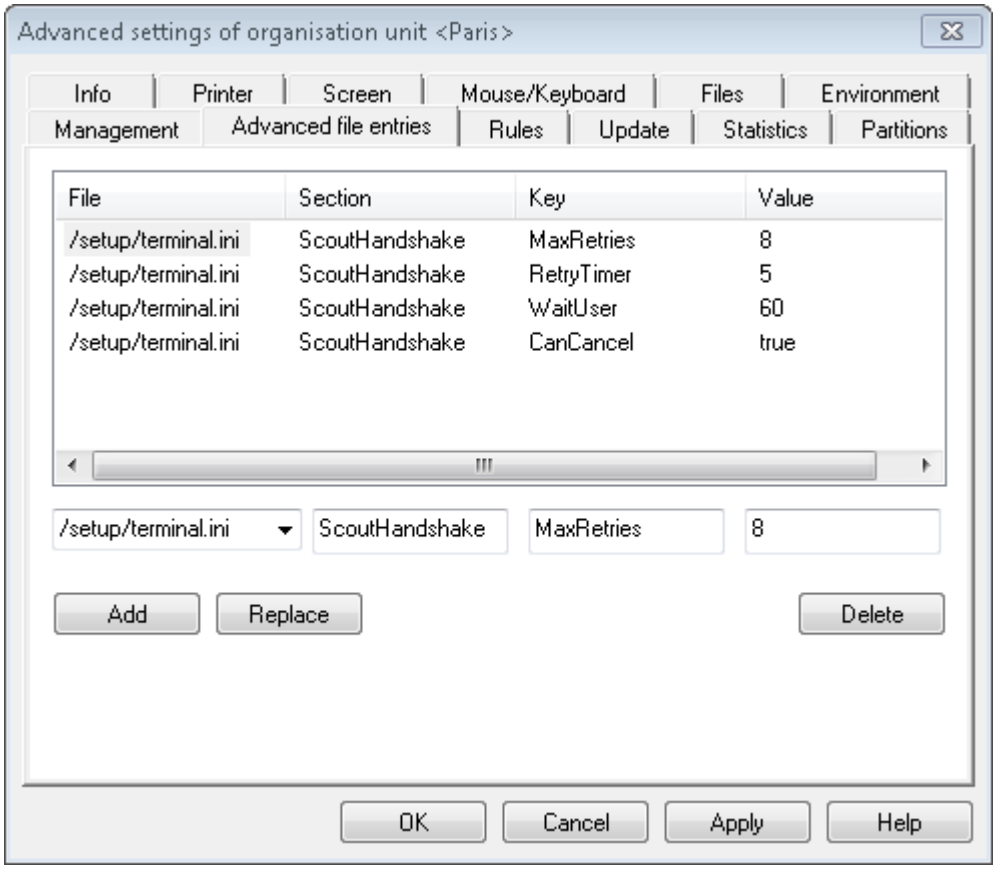
The **Advanced file entries** tab allows you to set parameters that cannot be set by using the graphical user interface. For example, you can set special parameters for the Citrix ICA client configuration files.

Configuration files must have the file format `.ini`.
Moreover, the `INI` file editor of Scout Enterprise places the following requirements:

- `.ini` files contain at least one section. Every section contains zero or more keywords.The keywords contain zero or more values.
- Each section is headed by a symbolic name that is enclosed in square brackets.
- Each keyword and its value are in the same line and are separated by an equal sign (=).
  One keyword can have more than one value.
- If a section name is used more than once in the same file, or if a keyword is used more than once in the same section, the last occurrence has precedence.

6.6.1. Defining individual file entries

1. In Scout Enterprise, click **Options > Advanced Options**.
   Or:
   Open the context menu of the relevant OU or device and click **Advanced settings...**
2. Click the **Advanced file entries** tab.



3. Edit the following fields:

Option	Description
File	Enter the full path including file name or select from the list: Citrix ICA: `/setup/ica/wfclient.ini` and `/setup/ica/appsrv.ini` Terminal: `/setup/terminal.ini`
Section	Section heading without brackets
Entry	Keyword
Value	Value you want to assign to the keyword. Blanks, hyphens and multiple values are allowed. Example: `valueA,valueB,valueC;comment`

4. Click **Apply**.

The new entries are written to the .ini file on the next restart of the client.

6.6.2. Changing values of individual file entries

1. In **Advanced settings > Advanced file entries**, select the entry of which you want to change the value.
2. Below, in the **Value** box, replace the current value.
3. Click **Replace**.

The new values are written to the .ini file on the next reboot of the client.

6.6.3. Deleting individual file entries

1. In **Advanced settings > Advanced file entries**, define a new entry: Enter **File**, **Section** and **Entry** of the relevant file entry, but leave the **value** box empty.
2. Click **Add**.

The 'empty' file entry overrides previous instructions. The file entry is deleted from the relevant section on the next reboot.

Note
If you use the **Delete** button to delete a selected row from the list, this only means that Scout Enterprise does not update the relevant entry anymore.

6.6.4. Deleting complete sections

1. In **Advanced settings > Advanced file entries**, define a new entry: Enter **File** and **Section** of the relevant file entry, but leave the **Entry** and **Value** boxes empty.
2. Click **Add**.

The 'empty' section overrides previous instructions. The section is deleted from the file on the next reboot even if it contained file entries.

6.7. Rules

Using this feature helps you define rules which can be executed when closing the last application or during the first contact with Scout Enterprise.

Option	Description
After terminating the last application execute the following action	Select between the options of the list-field
Display a message on the device for	Enter a time period in seconds to inform the user
After first management contact execute the following action	Select `Update the device`, if you want to ensure new devices being up-to date at once.

Note
For OUs and devices, the `Use parent action` option is set by default to enable the rules defined for a higher OU level.

6.8. Environment variables

– only available for individual devices and OUs –

Environment variables can be used locally on the client. They are strings.

Defining environment variables

1. Click **New**.
2. Enter the required variable using the format:
   `Variable name=value`
   and confirm with **OK**.

   The new variable is shown in the list.
3. If you want to encrypt the value of the variable, right-click the variable, and on the context menu, click **Encrypt value**.

Note
When you apply variables, the name of a variable must begin with a dollar sign: `$<Variable name>`.

7. Defining applications

The clients can be supplied with the following types of applications:

- Applications providing access to back-end systems
- Local applications

The definition of applications and the installation of the related software are independent of each other. Defining applications means to configure the applications provided for the users. Additionally, to enable the users to operate the applications, the relevant software packages must be installed on the client via IDF configuration. For further information, see Creating an IDF in the ELIAS guide.

Note
The term **Applications** refers to application definitions.
The term **Software** refers to the required software packages.

Applications can be inherited from the top of the organization structure to subordinate OUs. The lowest level to define an application is an OU, the highest level is the root level.

7.1. General

7.1.1. Adding applications

1. In the tree view, right-click on the **Applications** icon of the relevant OU.
2. On the context menu, click **Add**.

*The **Application Properties** dialog opens. This dialog provides several tabs, each of them relating to a particular application type.*

The following options of the **Application Properties** are available for most application types:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console **Note** Applications are identified by their name. Make sure to use a unique name for them.
Display name[1] (optional)	Name of the application shown on the client (control panel, start menu)
Server	Name of the server to which the application connects

[1] for Scout Enterprise Management Suite version 14.7 and later

Option	Description
Login	The user is automatically logged on to the terminal server by using predefined credentials (user name, password, domain).
Pass-through login	The values of the local user variables `$ELUXUSER`, `$ELUXPASSWORD` and `$ELUXDOMAIN` are used for logon on the authentication server. This allows to use the AD login data of the eLux desktop for automatic login to the configured applications (single sign-on). For further information, see User variables.
Application restart	The application is immediately restarted after it has been closed either unexpectedly or by the user.
Start automatically after	The application is automatically started after the eLux desktop has been loaded. Optionally, you can delay the auto-start process by specifying the required number of seconds.
Desktop icon	Provides an additional desktop shortcut for the application (icon and display name) except for PN Agent
Free Parameters	Individual parameters for program start

Note
Application definitions also can be

- copied from one OU to another
- exported from one OU and imported to another OU (context menu > **Edit**).

7.1.2. Editing application properties

- Open the context menu of the relevant application and click **Properties**.

*The **Application Properties** dialog for the application opens.*

Note
Properties of the selected application can be displayed in the **Properties** windows of the Scout Enterprise Console. They can't be modified there.

7.1.3. Defining free application parameters

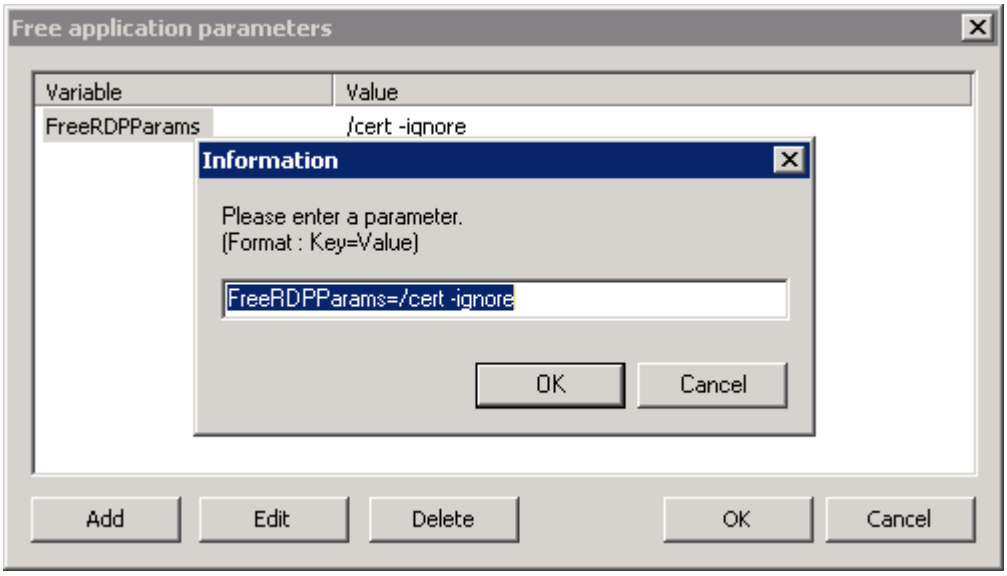
Free application parameters are individual parameters which can be used to start an application. You can define free application parameters for all applications, except for SAP-GUI and Emulation.

1. Open the **Application properties** of the relevant application.
2. Click **Free Parameters**.
3. Click **Add**, enter the relevant parameter using the specified format, and then confirm with **OK**.

The new parameter is saved with the application definition and shown in the dialog.

4. To define more parameters, repeat the last step.
5. Confirm with **OK**.

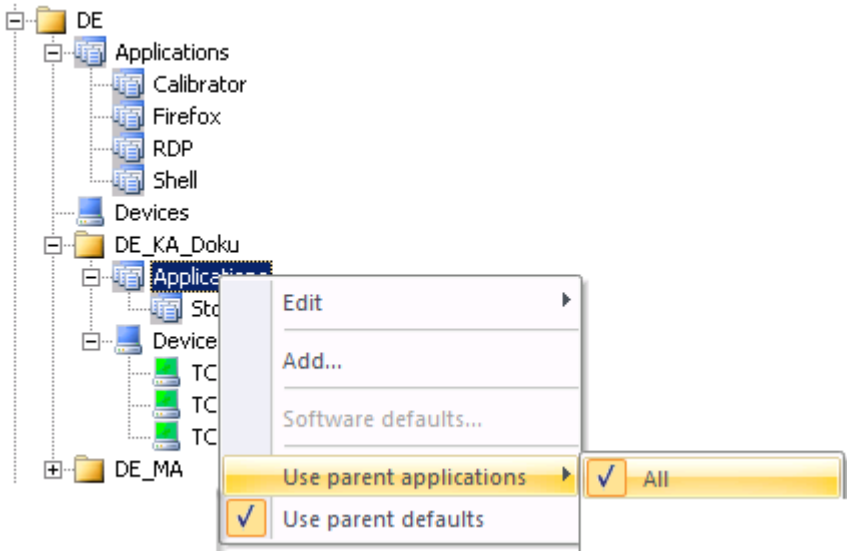
The defined parameters are inserted into the file `\setup\sessions.ini` *for the relevant application.*



7.1.4. Using parent applications

By default, applications are inherited to subordinate OUs. This allows you to define applications in only few but central places.

For the subordinate OUs, in the tree view, on the **Applications** context menu, the option **Use parent applications > All** is enabled (check mark). With the check mark set, all applications are active that have been defined for higher-level OUs or for the top-level OU. In addition to these applications you can define more applications valid for that particular OU (and subordinate OUs).



Disabling inheritation of applications

1. For an OU that you do not want to receive higher-level applications, open the context menu.
2. Click **Use parent applications > All** to remove the check mark.

The OU cannot use higher-level applications and cannot inherit them to subordinate OUs any-longer. Only applications defined within that OU are active.

Inheriting only individual applications

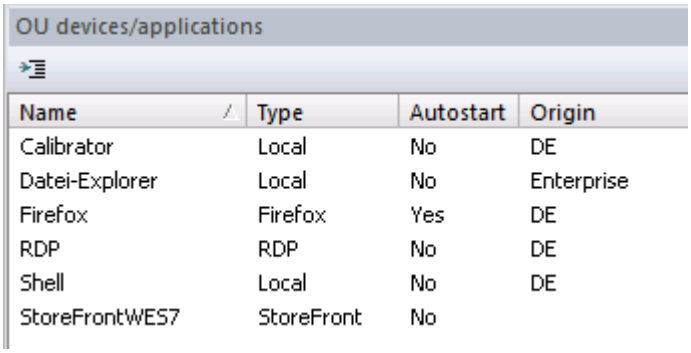
1. For the OU that you want to receive some of the applications defined for a higher-level OU or at top-level, open the context menu.
2. Make sure that the option **Use parent applications > All** is cleared (no check mark).
3. On the submenu **Use parent applications**, under **All**, select the application you want to inherit from above.

The selected application, on the submenu, receives a check mark, and its definition is provided on the next restart of the clients for that OU.

Show defined applications for an OU

1. Click **View > Window > OU devices/applications** to display the relevant window.
2. In the tree view, click the **Applications** icon below of an OU.

*For the selected OU, all defined applications are listed. The **Origin** column shows the OU from which an application is inherited. Top-level applications show the value `Enterprise`.*



Name	Type	Autostart	Origin
Calibrator	Local	No	DE
Datei-Explorer	Local	No	Enterprise
Firefox	Firefox	Yes	DE
RDP	RDP	No	DE
Shell	Local	No	DE
StoreFrontWES7	StoreFront	No	

The selected OU of the figure above has one own application (no entry in the **Origin** column), four applications from the higher-level OU **DE**, and one top-level application.

Note
To apply also the default settings of the parent applications, on the **Applications** context menu, select the **Use parent defaults** option.

7.1.5. Defining software defaults

Software default settings for all applications of the same type can be defined centrally or on OU-level. Software default settings are available for Citrix applications (Citrix Rreceiver) and for browsers[1].

We recommend to apply the default settings at top-level (root applications) to use inheritance over all OUs.

1. In the tree view, for the relevant level, open the  **Applications** context menu and click **Software defaults...**

   Note
   If inheritance is enabled, you can only open and modify the **Software defaults...** of the top-level instance or parent instance. To use different default settings for different OUs, inheritance must be disabled.

2. In the list-field, select the relevant software and click **Edit**.
3. Edit the relevant options on the tabs and confirm with **OK**.

[1] for Scout Enterprise Management Suite 15.0 and later versions

7.1.6. Uploading applications from Thin Client to Scout Enterprise

Application definitions of a reference client with an up-to-date eLux version can be uploaded to the Scout Enterprise Console and assigned to any OU.

Important

If you upload applications to an OU, all existing applications in this OU will be deleted.

Uploading from any client (outside of Scout Enterprise Management Suite

1. In Scout Enterprise, click **File > Application upload...**.

   *The **Application upload** dialog opens.*
2. Enter the IP address or name of the client device you want to upload application definitions from.
3. Select the **Destination** OU.
4. Click **Start**.

The application definitions of the specified Thin Client (of its OU) are uploaded to the specified OU. Already existing applications are deleted.

Uploading from a client managed by Scout Enterprise Management Suite

1. In the Scout Enterprise Console, select the device you want to upload application definitions from.
2. Click **File > Application upload...**.

   *The **Application upload** dialog opens. The IP address of the selected device is already set in the field **IP-name or IP-address of the device**.*
3. Select the **destination** OU to which the application definitions are to be copied.
4. Click **Start**.

The application definitions of the specified Thin Client (of its OU) are uploaded to the specified OU. Already existing applications are deleted.

7.1.7. Defining application icons

You can define custom icons for applications to be displayed on the client desktop. For the icon files, the file types `XPM`, `ICO` and `GIF` are supported.

1. In the tree view, for the root-level  **Applications**, open the context menu.
2. Click **Define application icons...**.
3. Click **Add** and select the relevant file from the file system.
4. Confirm with **Open** and **OK**.

The application icon is shown in the dialog. The icon is defined but not assigned yet.

7.1.8. Assigning custom application icons

Note
Before you assign an application icon other than the default icon, make sure that the icon is already defined. For further information, see Defining Application Icons.

1. For the relevant application, open the context menu and click **Properties...**.
2. Select the **Desktop icon** option.
3. Click **...** and select one of the icons.
4. Confirm with **OK** and **Apply**.

The application icon is shown for the selected application on the next client restart.

7.2. Connecting to a Citrix farm

Users can connect to sessions running on a Citrix back-end. Once the connection has been made, the user can access published desktops and applications.

Connecting from the Thin Client to a Citrix back-end is performed by one of the following applications:

- by a StoreFront application to a StoreFront server
- by the Citrix Self-Service user interface to a StoreFront server
- via browser to a StoreFront server or Webinterface server
- by a PNAgent application to a StoreFront server (XenApp Services Support must be enabled on the Citrix farm) or Webinterface server
- by an ICA application to a virtual desktop or published applications

Note
Access via the **ICA** application type is deprecated and only supported up to XenApp version 6.x by Citrix.

Requirements

- The eLux package **Citrix Receiver for Linux, V13.5.x** must be installed on the clients. .
- To connect via HTTPS, for the application types **Storefront**, **Self Service** and **PNagent**, the relevant root and intermediate certifcates must be available on the clients.
  - Root certificates must be transferred to `/setup/cacerts`.
  - Intermediate certificates must be transferred to `/setup/cacerts/intcerts`.

  For further information, see Certificates.
- To connect via HTTPS, for the application type **Browser**, the relevant root and intermediate certifcates must be available on the clients.
  - Firefox: Root certificates and intermediate certificates must be transferred to `/setup/cacerts/firefox`.
  - Chromium: Root certificates and intermediate certificates must be transferred to `/setup/cacerts/browser`.
- The eLux taskbar should be enabled on the clients if published applications are provided as **seamless applications**. Seamless applications behave like local applications and users can only restore them from minimized window size by using the taskbar. For further information, see Advanced desktop settings.

7.2.1. StoreFront application

By using the application type **StoreFront** users can connect to a StoreFront server. Virtual desktops and published applications are aggregated and provided through stores. As Citrix products, mainly XenApp und Citrix XenDesktop are used. StoreFront sites can be accessed via HTTP or HTTPS.

Being integrated into the Modern User Interface of eLux RP, StoreFront enables users to access Citrix resources of one or more stores together with other configured applications such as **RDP** or **Browser** sessions by using only one interface, the Modern User Interface. For further information, see eLux Modern User Interface.

Defining a StoreFront application

Note
HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and click the **StoreFront** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application shown in the Scout Enterprise Console
Stores	Specify the URL of one or more stores ▶ Click **Add** and replace the automatically created default value by your individual value (double-click or F2) Example: (`https://CtrXd76.mastertec-01.-com/Citrix/Store33/discovery`)
Logon	The user is automatically logged on to the store by using the specified credentials (user name, password, domain).
Pass-through logon	The user is logged on to the store via single sign-on. The AD user credentials are used. If AD users log on via smart card, and if Citrix Receiver for Linux 13.4.x or later versions are used, the authentication method **Domain pass-through** on the Citrix server must be disabled.
	Note For pass-through logon, the eLux package **Citrix Receiver Extensions** and the included feature package **Dialog Extension** must be installed on the clients.

Option	Description
Show last user[1]	The user credentials (except for password) of the last logon are displayed in the XenApp login dialog. This option has no effect if you specify fix user credentials for automatic logon under **Logon**.
Autostart	Specify the names of those StroreFront applications you want to have started automatically. Make sure to spell the names exactly in the way they are in StoreFront. To separate more than one application name, use a semicolon. Example: `MyApp1;MyApp2`
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start see Defining free application parameters.

3. If you want to delete an entry from the **Stores** list, select the entry and click **Delete**.
4. To configure further settings, click **Advanced** and edit the following fields:

Option	Description
Windows properties	Desktops can be launched in full-screen or window mode.
Timed logoff	To enable automatic logoff from the StoreFront server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last StoreFront application has been closed.
Application reconnection	Determine the actions to be done on a reconnect to the StoreFront server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.

[1] Scout Enterprise 14.7 and later versions

Option	Description
Manual logoff	Determine the actions to be done on logoff from the StoreFront server **Logoff only server**: Logoff is performed only from the StoreFront server **Logoff server and applications**: Logoff is performed from the StoreFront server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the StoreFront server but the virtual desktop session is only disconnected. This enables the user to reconnect later on.

5. Confirm with **Apply** and **OK**.

Smart card authentication for StoreFront

If you use smart card authentication for StoreFront, you can configure the behavior of the smart card when it is removed.

Note
Using a smart card requires the smart card middleware to be installed on the client. In addition, smart card authentication must be enabled on the Citrix farm. If Citrix Receiver for Linux identifies smart card middleware on the client, smart card logon has precedence over logon with user name and password.

Define the following entry by using the Scout Enterprise feature Advanced file entries:

File	`/setup/sessions.ini`
Section	`ICADefaults`
Entry	`SmartcardRemovalAction`
Value	`noaction` | `forcelogoff` (Default: `noaction`)

Access to published resources

After users have logged on to a StoreFront server or Web Interface server, they can access the provided resources through the eLux Start menu or through the control panel and the **Applications** tab: The **StoreFront** node can be expanded to view the resources provided on the server.

7.2.2. Self-Service user interface

The Self-Service user interface (UI) replaces the configuration manager **wfcmgr** and allows access to Citrix services providing published ressources. After they are set up with an account, users can subscribe to desktops and applications, and then start them.

Defining Citrix Self-Service as local application

Note
The eLux package **Citrix Receiver for Linux** and the included feature package **Self-service** must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select `Custom`.
Parameter (manatory)	Enter the following program name to start the application: `selfservice`

3. Confirm with **Apply** and **OK**.

Note
The `selfservice` application cannot be configured individually. If you want to use configuration options, use the Self-Service UI with extensions (`ucselfservice`) alternatively.

7.2.3. Self-Service user interface with extensions

The Citrix Self-Service user interface (UI) can also be used in an extended version with further functionality[1]

- Configuration of the stores
- Logoff and reconnect options
- Dialog and window layout

Defining Citrix Self-Service UI with extensions

Note

The eLux package **Citrix Receiver for Linux V13.5.x** must be installed on the clients.
The eLux package **Citrix Receiver Extensions V2.x** must be installed on the clients.
Depending on the desired features, the following included feature packages must be installed on the clients:
Self-service wrapper
Dialog Extension (for modifications on the Citrix dialog design)
Self-service dialog themes (for modifications on the Citrix dialog design)

This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select `Custom`.
Parameter (mandatory)	Enter the following program name to start the application: `ucselfservice`
Free parameters	Define parameters and values for the stores to be called, window properties and connection options as listed in the table **Parameters for the Self-Service extensions** below. For further information, see Defining free application parameters

3. Confirm with **Apply** and **OK**.
4. If you want to change the design of the Citrix dialogs for all Citrix connections, use the Scout

[1] for eLux RP 5.6 and later versions

Enterprise feature **Advanced file entries** to set the following entries:

File	Section	Entry	Value
/setup/sessions.ini	ICADefaults	UiDialogTheme	`ucselfservice`
/setup/sessions.ini	ICADefaults	UiDialogDecorated	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogKeepAbove	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogKeepBelow	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogColorHover	<*color*> Example: `#b0b0b0`
/setup/sessions.ini	ICADefaults	UiDialogColorUnselected	<*color*> Example: `#a0a0a0`
/setup/sessions.ini	ICADefaults	UiDialogColorSelected	<*color*> Example: `#c0c0c0`

For further information, see Advanced file entries.

Note
After the `terminal.ini` file has been updated on the client, one more client restart might be required to enable the new setting.

Parameters for the Self-Service extensions

Parameter	Description	Origin
`StoreUrl1=`<*URL to store1*>	Storefront URL	Citrix/Unicon
`StoreUrl2=`<*URL to store2*>	Storefront URL	Citrix/Unicon
`StoreUrl3=`<*URL to store3*>	Storefront URL	Citrix/Unicon
`SharedUserMode=`<*true|false*>	**Shared User Mode** allows to use one system user account for multiple users. When users log off or close the UI, the user data are removed.	Citrix
`FullscreenMode=`<*0|1|2*>	0 Not full-screen 1 Full-screen 2 Maximized and undecorated, taskbar remains visible This can be useful as users can launch seamless applications. Default: 0 (not full-screen)	Citrix

Parameter	Description	Origin
`SelfSelection=<true|false>`	Used to disable the search box and the self-selection panel Disabling prevents users from subscribing to extra applications. Default: false	Citrix
`ReconnectOnLogon=<true|false>`	Tries to reconnect to all sessions, for a given store, immediately after logon to that store	Citrix
`StoreGateway=<store gateway>`	If required, specify a gateway	Citrix
`ReconnectOnLaunchOrRefresh=<true|false>`	Tries to reconnect to all sessions when an application is launched or the store is refreshed	Citrix
`SessionWindowedMode=<true|false>`	true: Display desktops windowed false: Display desktops in full-screen	Citrix
`UseLogoffDelay=<0|1>`	To activate automatic logoff, set `UseLogoffDelay=1`.	Unicon
`LogoffDelay=<seconds>`	Delay in seconds for automatic logoff	Unicon
`ForcedLogoff=<1|2>`	1 Logoff timer is started with logon 2 Logoff timer is started when the latest Citrix app is closed.	Unicon
`LogoffInfoTimeout=<seconds>`	During logoff (selfservice restart), an info dialog can be shown to the user for some seconds.	Unicon

7.2.4. Browser session to access published resources

Users can access applications and desktops that have been published through a store on the Citrix StoreFront server or through Citrix Web Interface by using a local browser.

Defining a browser application to access published resources

Note
To provide the users with a browser application to be used directly on the client, the relevant software package for Firefox or Chromium must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

Note
HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and click the **Browser** tab.
2. Edit the following fields:

Option	Description
Name	Name for the browser session
Browser type	Firefox or Chromium

Called page	URL of the Web Interface homepage or StoreFront store.
	Examples:
	`https://<Servername>/Citrix/StoreWeb`
	`https://<Servername>/Citrix/XenApp`

3. For the remaining parameters, see Defining a browser application.

The local user starts the browser and is forwarded to the defined page. After successful logon to the StoreFront server or Web Interface server, the available published applications, desktops and contents are shown in the browser window.

7.2.5. PNAgent application

An application of the type **PNAgent** (Program Neighborhood Agent) enables users to access published resources through a server running a XenApp Services site. Published resources can be published applications, published desktops, or published contents (files).

Customizable options for all users are defined in the configuration file `config.xml` which is stored on the Web Interface server (by default in the directory `//Inetpub/wwwroot/Citrix/PNAgent`). When a user starts one of published programs, it reads the configuration data from the server. The configuration file can be configured to update the settings and user interface regularly.

The `config.xml` file affects all connections defined by the XenApp Services site. For further information, see the Citrix eDocs on http://support.citrix.com.

Defining a PN Agent application

Note
HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and click the **PN Agent** tab.
2. Edit the following fields:

Option	Description
Name	Name of the application

Option	Description

Server	Specify the address of the configuration file on the Web Interface server (URL).
	If you use the default directory and port 80, the server address is sufficient.
	
	Examples:
	`https://CtrXd.mastertec-01.-com/Citrix/PNAgent/config.xml`
	`https://192.168.10.11:81`

Login	The user is automatically logged on to the Web Interface server by using the specified credentials (user name, password, domain).
Pass-through logon	The user is logged on to the store via single sign-on. The AD user credentials are used. Note: Kerberos authentication is no longer supported with Citrix Receiver for Linux 13.x.
Autostart application/folder	Specify the names of hose applications you want to have started automatically. Alternatively, you can specify an autostart folder containing the relevant published applications. The folder must have already been created on the Web Interface server.
Show last user	The user credentials (except for password) of the last logon are displayed in the PNAgent logon dialog. This option has no effect if you specify fix user credentials for automatic logon under **Logon**.
Allow cancel	Allows the user to close the PNAgent logon dialog box.
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start Example: `PNATimeout=60` brings Citrix Receiver to try for 60 seconds to enumerate the published applications and desktops. To configure dual-monitor mode, you can also use the **Free parameters**, see below. For further information, see Defining free application parameters.

3. To configure further settings, click **Advanced** and edit the following fields:

Option	Description
Window properties	For resolution/window size, color depth and audio output, select **Use default** (server settings) or select one of the values from the list-field.
Timed logoff	To enable automatic logoff from the Web Interface server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last PNAgent application has been closed..
Application reconnection	Determine the actions to be done on a reconnect to the Web Interface server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.
Manual logoff	Determine the actions to be done on logoff from the Web Interface server **Logoff only server**: Logoff is performed only from the Web Interface server **Logoff server and applications**: Logoff is performed from the Web Interface server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the Web Interface server but the virtual desktop session is only disconnected. This enables the user to reconnect later on.

4. Confirm with **Apply** and **OK**.

Program Neighborhood variables

For example, variables can be used to define a unique client name for a Citrix XenApp session. To log on to a Web Interface server with Program Neighborhood, you can use the following variables:

`$ICAUSER`	User name
`$ICADOMAIN`	Domain for this user
`$ICAAPPLICATION`	Name of the PNAgent application definition

Creating a domain list

For PNAgent applications, you can create a domain list from which the user can select.

1. Create the text file `icadomains` without file name extension.
2. Enter the required domain names, one domain per line.
3. Save the file to the Scout Enterprise installation directory.
4. Transfer the file to the `/Setup` directory on the Thin Client by using the Scout Enterprise feature Files.

If some of the configuration data are missing, when a PNAgent application is started, the missing data is requested by a Citrix Web Interface login dialog. The defined domains are listed in a drop-down list.

Note
In the PNAgent application definition, you can predefine a specific domain.
Example: `work.mastertec-01.com`.

Settings for dual monitor mode

For PNAgent sessions, you can configure dual-monitor mode by using one of the following methods. The Citrix session can be transferred to the first monitor, to the second monitor, or to both of them.

Method 1:

- Use the **Advanced file entries** feature of the Scout Enterprise Console and modify the ICA software defaults:

File	`/setup/sessions.ini`
Section	`ICADefaults`
Entry	`Xinerama`
Value	`-1|0|1`

For further information, see Advanced file entries.

Method 2:

- In the Scout Enterprise Console, in the application definition, set the following **Free parameters**:

```
Key = Xinerama
Value = -1|0|1
```

For further information, see Free parameters.

The values mean the following:

-1	both monitors
0	first monitor
1	second monitor

7.2.6. Defining an ICA application

Note
Access via the **ICA** application type is deprecated and only supported up to XenApp version 6.x by Citrix.

1. Add a new application and click the **ICA** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
Published application	Configures direct access to a published application To provide access to complete desktops, clear the option.
Server	IP address or name of the Citrix server (terminal server)
Application	Only relevant if you have selected the **Published application** option Name of the Windows application including path (see Citrix server) Note: The **Browse** option applies to the Citrix farm but is not supported anymore.
Working directory (optional)	Only relevant if you have selected the **Published application** option Working directory for the application
Login	The user is automatically logged on to the Citrix server by using the specified credentials (user name, password, domain).
Pass-through logon	The user is logged on to Citrix server via single sign-on. The AD user credentials are used. Note: Kerberos authentication is no longer supported with Citrix Receiver for Linux 13.x.
Smart card logon	The client uses a smart card for logon.

Option	Description
Application restart Start auto-matically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters.
Connection options Advanced (eLux)	Opens the configuration dialog of Citrix Receiver for Linux (`wfcmgr`) Edit the relevant options. The Citrix Receiver configuration is saved to the file `/setup/ica/wfclient.ini` on the Thin Client and can be viewed from the Scout Enterprise Console by using the **Diagnostic files** feature.

3. Confirm with **Apply** and **OK**.

A published application is displayed on the eLux client in the same way as local applications.

7.2.7. Citrix software defaults

For all Citrix applications, in the Scout Enterprise Console, you can define Citrix Receiver software defaults that are applied to all devices of the relevant OU and subordinate OUs if configured.

The following options are available:

- Client drive mapping
- COM port mapping
- Firewall settings
- Citrix keyboard shortcuts
- Window properties
- Connection options
- Bitmap caching

To edit the software defaults, see Defining software defaults.

Some of the Citrix default options are described below. For further information, see the Citrix documentation.

General tab

Option	Description
TW2StopwatchMinimum	Scrolling speed for remote applications (such as Adobe Acrobat Reader, Excel) The higher the value, the slower the speed when scrolling Note for Excel: A low value increases scrolling speed but delays as soon as a selection is drawn down out of the visible screen area. Default = 25
Client name template	Definition of the client name in the Citrix session Note: You can use the Program Neighborhood variables `$ICANAME` and `$ICADOMAIN` to set a unique client session name. This is required for Citrix Roaming and some XenApp programs. For further information, see PNAgent application.

Drive Mapping tab

Option	Description
A-Z	The letters A to Z represent the logic drive names on the terminal server. In the field on the right, you can assign a local resource to a drive letter that is to be shown in the Citrix session. Enter the mount point relating to the local access path of the resource. The mount points are provided by eLux: `/media/usbdisk` or `/media/cdrom`
Attributes E / R / W	Type of access permission • E = enable • R = read • W = write
Enable Drive Mapping	Must be selected to enable the defined drive mappings
Enable Dynamic Mapping	Available mass storage devices are assigned to the next free drive letter.

For further information, see Mount points.

COM Ports tab

To connect via COM port, the device name of the Thin Client COM port is required.

The COM port device name always begins with the string `/dev`. Device names are case-sensitive.

Examples:

Port device name	COM port
`/dev/ttyS0`	COM1
`/dev/ttyS1`	COM2

The availability of COM ports depends on the hardware platform

Note
The client ports must be mapped on the Citrix resource (such as desktop) accordingly. You can use a `net use` command for that.
Example: `net use com1: \\Client\COM2: /persistent:yes`

7.2.8. ICA Connection Center

By means of the ICA Connection Center, users can see all current server connections and can log off, disconnect or close them without operating the application. In addtion, the connection transport statistics can be viewed which might be helpful for slow connections.

The Connection Center is provided as systray icon in the task bar.

Defining the Citrix Connection Center

Note
The eLux package **Citrix Receiver Extensions** and the included feature package **Connection Center** must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select `ICA Connection Center`.
Parameter (optional)	Command-line parameters for program start

3. Confirm with **Apply** and **OK**.

7.3. Additional software for Citrix environments

7.3.1. Installing HDX RealTime Optimization Pack

The HDXRealTime Optimization Pack enables better audio and video quality for VOIP and video chat.

1. Download the `citrix_hdxrtme` package from our portal www.myelux.com.
2. In ELIAS, import the package into your Container. For further information, see Importing packages to a container in the ELIAS guide.
3. In ELIAS, add the package to your `IDF`, and then save the new `IDF`.For further information, see Creating an IDF in the ELIAS guide.
4. Perform an eLux update using the new `IDF`. For further information, see Firmware Update.
5. Configure Microsoft Lync or Skype for Business in the back-end environment.

7.3.2. Configuring Adobe Flash Player

For eLux RP 5.4 and later versions, Adobe Flash Player is provided in a special version that includes HDX MediaStream Flash Redirection supported by Citrix and in a general version that might be more up-to-date.

Configuring Flash Player for ICA

- Edit the file `mms.cfg`, and then use the **Files** feature of the Scout Enterprise Console to transfer the configuration file to the target directory `/setup/adobe/` on the client.

  For further information, see Files.

7.3.3. Installing Cisco VXME

Cisco Virtualization Experience Media Edition (VXME) extends the Cisco collaboration experience to virtual deployments. With supported versions of Cisco Jabber for Windows, users can send and receive phone calls on their hosted virtual desktops (HVD). The VXME software routes all audio and video streams directly from one Thin Client to another, or to a phone, without going through the HVD.

1. Download the `Cisco VXME` package from the Cisco website.
2. Download the `VXME_utils` package from our portal www.myelux.com..
3. In ELIAS, import the package into your Container. For further information, see Importing packages to a container in the ELIAS guide.
4. In ELIAS, add the package to your `IDF`, and then save the new `IDF`. For further information, see Creating an IDF in the ELIAS guide.
5. Perform an eLux update using the new `IDF`. For further information, see Firmware Update.
6. Follow the Cisco Deployment and Installation Workflow on the Cisco website in order to configure the VXME system environment.

VXME 11.5 eLux Edition

VXME 11.5 eLux Edition Release Notes

7.3.4. Installing Lumension package

1. Download the package "Lumension Endpoint Security Agent Control" from the technical portal www.myelux.com > Software Packages. Make sure that you download the package for the corresponding eLux version.
2. With the aid of ELIAS you are able to add this package into the corresponding container.
3. Add this package into your IDF and save this new IDF.
4. Execute an eLux update onto new IDF.
5. Change to the particular server on which the Lumension software is running on the server-side.
6. Finish the service **Lumension Endpoint Security Command and Control**.
7. Copy the file `LDI64.dll` into the folder `Program Files\Lumension\Endpoint`.
8. Start the service **Lumension Endpoint Security Command and Control** again.

You can find the log file at **%windir%\Temp\ldi.log**.

For further information, see the website of Lumension Security Inc.

7.3.5. Installing CenterTools DriveLock

CenterTools DriveLock provides endpoint security for USB interfaces on the Thin Client.

1. Download the `DriveLock` package from our portal www.myelux.com.
2. In ELIAS, import the package into your Container. For further information, see Importing packages to a container in the ELIAS guide.
3. In ELIAS, add the package to your `IDF`, and then save the new `IDF`.For further information, see Creating an IDF in the ELIAS guide.
4. Perform an eLux update using the new `IDF`. For further information, see Firmware Update.
5. Configure the DriveLock back-end environment.

7.4. RDP

This connection type corresponds to the ICA functionality but is using the Microsoft Remote Desktop Protocol (RDP) to connect to a Microsoft Terminal Server. The provided RDP client is **eLuxRDP** that is based on the free software implementation **FreeRDP**.

There are two ways for configuration:

- Windows Desktop: The user accesses the desktop of a terminal server by using a remote desktop session. The user can use any application available on the desktop.
- Individual / seamless application: The user can only access one particular application of the terminal server.

7.4.1. Defining an RDP Windows desktop session

1. Add a new application and click the **RDP** tab.
2. Edit the following fields:

Option	Description
Name	Name for the RDP application
Server	IP address or name of the server
Application	Leave the field empty.
Working directory	Leave the field empty.
Logon	The user is automatically logged on to the server by using the specified credentials (user name, password, domain).
Pass-through login	The user is logged on via single sign-on. The AD user credentials are used.
Free parameters	Allows to define any parameters supported by **eluxRDP** in the format: `FreeRDPParams=<Parameter>` Example: `FreeRDPParams=/cert -ignore` To view the provided parameters enter the `eluxrdp` command in a shell.

3. Confirm with **Apply** and **OK**.

Note
Defining a server-independent application as local hidden application named `RDP_TEMPLATE` allows you to configure a connection template without backend. The user starts `rdpconnect` from the shell and, subsequently, specifies the server to be connected to. This feature requires the software package **RDPConnect**.

7.4.2. Defining an RDP application

To configure an individual application via RPD, the Windows desktop definition requires additional data about the relevant application.

1. Add a new application and click the **RDP** tab.
2. Edit the following fields:

Option	Description
Name	Name for the RDP application
Server	IP address or name of the server
Application	Name of the Windows application including path name System variables are allowed Example: `c:\Program Files\Microsoft Office\Office\EXCEL.EXE` `%SystemRoot%\system32\notepad.exe`
Working directory (optional)	Working directory of the Windows application
Logon	The user is automatically logged on to the server by using the specified credentials (user name, password, domain).
Pass-through logon	The user is logged on via single sign-on. The AD user credentials are used.

3. Confirm with **Apply** and **OK**.

For the user, the application runs full-screen in the session window.

7.4.3. Advanced RDP settings

- To access the advanced RPD settings, in the **Application properties** dialog of an RDP application, click the **Advanced** button.

View tab

Option	Description
Window size	Full-screen or a specific resolution
Full-screen on Monitor	If you have selected the window size `Full-screen`, select if you want to display on one specific or all monitors.
Colors	Color depth for the RDP session (8-32 Bit

Note
If you have connected multiple monitors, and if you want to display on one specific monitor only, in **Setup > Desktop > Advanced > Windowmanager**, the **Maximaize/fullscreen to single monitor** option must be selected.

Local Resources tab

Note
– for terminal servers supporting RDP protocol version V5.2 or later –
The settings take effect only if, on the **Advanced** tab, the value of the **Protocol** field is not set to `RDP V4`.

Option	Description
Drive mapping	Select drive, mount point and drive letter that you want to be shown in the RDP session. The mount points correspond to the local access paths of the resources and are provided by eLux. For USB devices the mount points are `/media/usbdisk`, `/media/usbdisk0` and so on. For further information, see Mount points.
Connect printer	Up to four printer definitions can be created automatically for a session. The printers must be configured on the Printer tab in the eLux control panel and they must have the correct driver name as defined on the server (case-sensitive!). The first four profiles can be used with drivers. To define a default printer, enable the option **Standard** in the **eLux Printer** settings.
Sound	Using the **Play local** option, the sound can be reproduced locally on the client. **Play remote** provokes the sound to be played remotely on the server.
Connect ports	Makes the defined port connections accessible in the RDP session.
Enable smartcard	Smart cards based on a certificate can be used for log in.

Advanced tab

Option	Description
Protocol	Enables setting to protocol 4 or 5. Normally, the protocol is recognized automatically.
Keyboard language	Defines the keyboard layout within an RDP session. The default is **Auto** which corresponds to the keyboard setting of the eLux control panel.
	Important If you define a particular language, it has to be identical with the keyboard language defined in the eLux control panel.
Deactivate Window-Manager Decorations	The frames of the eLux windows are hidden.

Option	Description
Deactivate encrypting	The server does not accept encrypted sessions. You can use this option to increase performance. By default the option is disabled.
Deactivate mouse move events	Mouse position data are not transferred to the server constantly, but only with every mouse click. This increases system performance and is especially helpful for connections with small bandwidth. By default the option is disabled.
Show connection bar on full screen	Shows connection list in full screen mode.
Bandwidth	Choose from `standard`, `modem`, `broadband` or `LAN`.

7.4.4. Configuring RemoteFX

Microsoft® RemoteFX™ is a feature that is included in Windows Server 2008 R2 (SP1) and later versions. RemoteFX delivers rich user experience for Virtual Desktop Infrastructure (VDI) by providing a virtual 3D adapter, intelligent codecs and the ability to redirect USB devices to virtual machines.

1. Open the **Application properties** dialog of your **RDP** application and click **Advanced**.
2. On the **Advanced** tab, in the **Bandwidth** field, select `LAN`.
3. Confirm with **Apply** and **OK**.

Note
RemoteFX will only work if the server supports RemoteFX and is configured in the right way. The only parameter to be configured on the client is bandwidth.

7.5. Browser

Supported browsers are Mozilla Firefox and Google Chromium[1].

Note
If you use Chromium, we recommend to provide your Thin Clients with 2 GB of RAM.

7.5.1. Defining a browser application

1. Add a new application and click the **Browser** tab.
2. Edit the following fields:

Option	Description
Name	Enter a name for the browser. This name is shown in the Scout Enterprise Console.
Browser type	Select `Firefox` or `Chromium`[2].
Start page	Web page (URL) that opens whenever you click **Home**
Called page	Web page (URL) that opens after starting the browser

Proxy type	• `No proxy`
	• `Manual (Proxy:Port)`: Proxy server and port
	Example: `proxy.mastertec-01.de:3800`
	For manual proxy type, you can specify exceptions[3] in the **Advanced browser settings**.
	• `Auto (URL)`: Proxy configuration file
	Examples:
	`http://www.wpad.mastertec-01.com/wpad.dat`
	`http://www.proxy.mastertec-01.com/proxy.pac`

Application restart Start auto-matically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start see Defining free application parameters

3. For manual proxy type, to define destinations that you do not want to access via proxy, click

[1]For Scout Enterprise Management Suite 14.8 and later versions
[2]Chromium is provided with Scout Enterprise Management Suite 14.8 and later versions
[3]for Scout Enterprise Management Suite 14.8 and later versions

Advanced > Proxy exception list, and then enter the relevant addresses.

4. To enable **Kiosk** mode, see Configuring Kiosk mode.
5. Confirm with **Apply** and **OK**.

Note
By default, all browser files (cache, history, bookmarks, etc.) are saved temporarily to the flash memory but are deleted with each restart. We recommend to configure the browser home directory on a network drive. For further information, see Browser home directory.

Further browser-specific preferences can be set through policies (Chromium) or configuration file entries (Firefox.). For further information, see the Scout Enterprise guide

Preferences Chromium

Preferences Firefox

Deploying SSL certificates for the browser

- Use the Scout Enterprise feature **Files configured for transfer** to transfer certificate files to the required target directory on the client:

Mozilla Firefox	`/setup/cacerts/firefox`
Google Chromium	`/setup/cacerts/browser`

For further information, see Advanced settings > Files.

Note that a second boot of the client is required to assign the certificates that have been transferred during the first boot to the certificate store of the browser.

7.5.2. Preferences Chromium

By using policies you can set mandatory (managed) and recommended preferences for the Chromium browser. Mandatory preferences define fixed values that cannot be changed by the user. Recommended preferences define default values that can be changed by the user. For further information, see https://www.chromium.org/administrators/.

- Use the Scout Enterprise feature **Files configured for transfer** to transfer policy files (`.json`) to the required target directory on the client:

Fixed values	`/setup/chromium/managed`
Default values	`/setup/chromium/recommended`

For further information, see Advanced settings > Files.

7.5.3. Preferences Firefox

Firefox-specific preferences exceeding the options provided within the application definition can be defined by using the configuration file `/setup/firefox/user.ini` on the client (Firefox 38.5.2.1 and later versions).

You can use all options that are available in the Mozilla configuration editor for Firefox (`about:config` page). The required options including the relevant entry and value are transferred to the client by using the Scout Enterprise feature **Advanced file entries**.

Setting preferences for Firefox by using about:config

1. In Firefox, open the `about:config` page. The **Preference Name** column shows the available options, and the preference name itself provides the basis for the strings to be entered under **Section** and **Entry** in the next step.
   For further information, see Configuration Editor for Firefox on the Mozilla Support site.
2. In the Scout Enterprise Console, for the relevant clients, open **Advanced settings > Advanced file entries**.
3. Define the following entry:

File	`/setup/firefox/user.ini`
Section	*<preference name as indicated in the configuration editor –first part of the string, left of the last dot>*
Entry	*preference name as indicated in the configuration editor –second part of the string, right of the last dot>*
Value	*<required value>*

Example:
You want to set the value for **browser.tabs.closeWindowWithLastTab** to `false`.

File	`/setup/firefox/user.ini`
Section	`browser.tabs`
Entry	`closeWindowWithLastTab`
Value	`false`

For further information, see Advanced file entries.

7.5.4. Browser home directory

By default, the browser settings are temporarily saved to the flash memory but are deleted with each restart.

If you define a browser home directory on the network, browser settings such as bookmarks can be saved and made available to the user after each client restart. Use a network share that you have configured for access:

Requires
Configured Windows network share (**Defined drive**). For further information, see Defining a network drive.

Defining browser home directory for Firefox

- On the **Drives** tab, under **Browser home directory**, enter the name of one of the defined drives of the list on the left. The name must correspond to the one of the list. Example: `/smb/share`

Firefox saves the browser files within the specified Windows directory to the `mozilla` directory.

Defining browser home directory for Chromium

Requires
- eLux RP 5.4 or later
- The network directory must support `SMB 2.1` (Windows Server 2008 R2 or later).

- Define the following entry using the Scout Enterprise feature **Advanced file entries**:

File	`/setup/terminal.ini`
Section	`Chromium`
Entry	`Home`
Value	`<Defined drive>*`

*Samba share as specified in Configuration > Drives in the list. Example: `/smb/share`

For further information, see Advanced file entries.

Chromium saves the browser files to the specified Windows directory.

7.5.5. Kiosk mode

Note
Kiosk mode is only supported for Firefox at this time.

The kiosk mode starts the browser in full-screen mode and with limited user rights. The user cannot open other windows and cannot exit the browser.

The browser window is displayed without address bar and navigation buttons, by default. So users are forced to stay on the predefined web page and cannot exit.

Kiosk mode is suitable if the users should only see one website and are not supposed to use further applications on the Thin Client. For correct use of the Kiosk mode, we recommend to disable related functions of the Thin Client such as rebooting and opening the control panel. For further information, see Setup>Security.

Configuring Kiosk mode

1. In the application properties of your browser application, click **Advanced**.
2. On the **Kiosk mode** tab, edit the following fields:

Option	Description
Enable Kiosk mode	Enables kiosk mode
Display navigation bar	Allows using browser tabs despite kiosk mode The users can view multiple web pages of the defined web site concurrently
Add print button	Allows using browser tabs and provides a **Print** feature despite kiosk mode
Add address bar	Allows using browser tabs and provides the address bar including navigation buttons despite kiosk mode

3. Confirm with **Apply** and **OK**.

On the next restart, the browser opens in kiosk mode.

7.6. Local and user-defined applications

Defining local commands is particularly important as they enable the definition of applications which can be launched within a shell. This feature assumes knowledge about the commands that average users may not have.

Note
Make sure that the user is authorized to start the application. All commands are executed by the UNIX user **eLux** (UID = 65534).

Some of the local applications are predefined. If you miss an application, you can define your own application or command by using the `Custom` option of the **Local Application** list-field.

Error messages will not be shown. If your command does not include an X client application, no messages are shown during execution. For this reason, we recommend to run the command first within an XTerm session for testing purposes.

7.6.1. Defining predefined local applications

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console
Local application	In the list-field, select a predefined application.
Parameter (optional)	Command-line parameters for application start
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start see Defining free application parameters.

3. Confirm with **Apply** and **OK**.

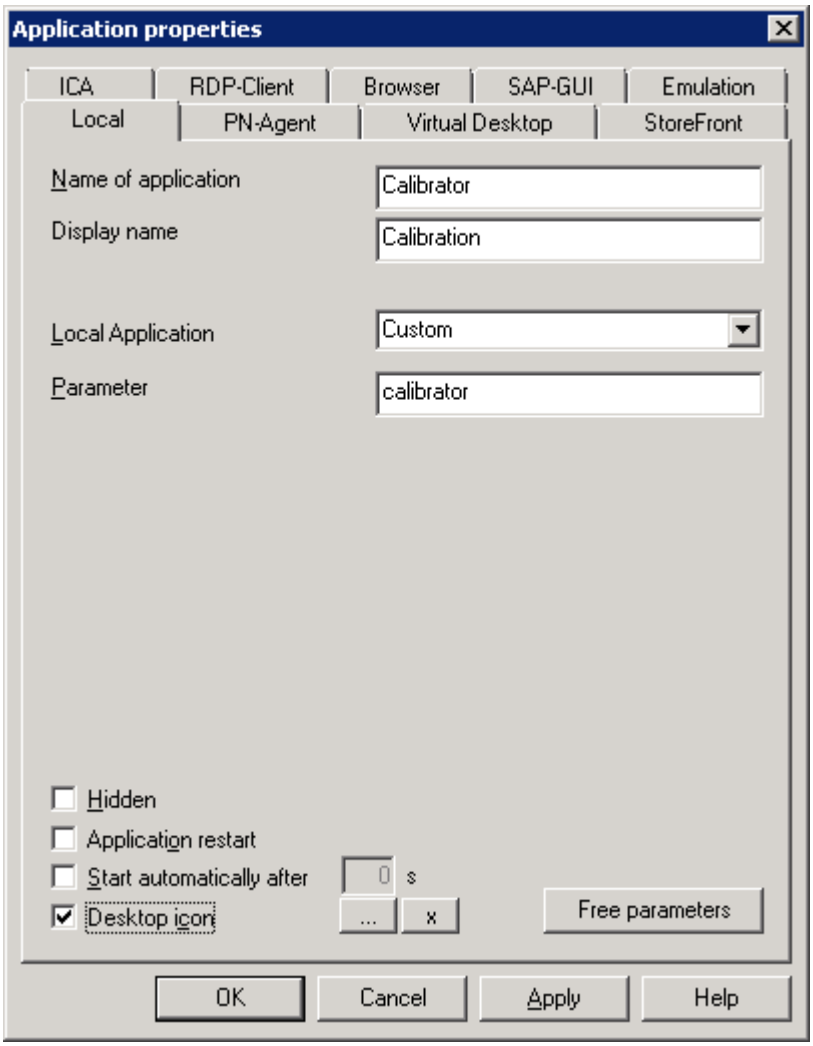
7.6.2. Defining custom applications

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console
Local application	Select `Custom`.

Option	Description
Parameter (mandatory)	Enter the program name required to start the application. If desired, add start parameters Example: `calibrator` calls the **Calibrator** tool `squid` calls the **Squid** application `squid /tmp/mycache` calls **Squid** using the specified cache directory
Hidden	The application is not shown on the **Application** tab of the client control panel. The option **Start automatically** or **Application restart** must be active.
Application restart Start automatically Desktop icon	See Adding applications.
Free parameters (optional)	Individual parameters for application start see Defining free application parameters

3. Confirm with **Apply** and **OK**.



The figure shows the application definition for the calibration tool **Calibrator**. After the next client restart the **Calibration** application is provided on the client and can be started using the control panel, start menu, or desktop icon (provided that the **Calibrator** tool is included in the image).

7.6.3. Configuring Ekiga SIP Softphone

Ekiga is a free software implementation for audio and video telephony (VoIP) supporting the SIP protocol. Configuration is based on a SIP account.

1. Add a new application and select the Local tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
Application	`Custom`
Parameter	`ekiga`

3. Click **Free parameters** and then **Add** to define the following free parameters:

Variable	Value
account	*<Name of the SIP account>*
server	*<server URL>*
user	*<SIP user name>*
password	<password>
outbound_proxy	*<proxy URL >*

Example: `password=424242`
For further information, see Using free application parameters.

4. In the **Free application parameters** dialog, right-click the variable name `password` and click **Encrypt**.
5. Confirm with **Apply** and **OK**.

7.7. Virtual Desktop

The **Virtual Desktop** tab helps you define Citrix or VMware connections with with a VD broker. For Citrix XenDesktop, the logon data is defined according to an ICA connection.

7.7.1. Defining a virtual desktop

1. Add a new application and click the **Virtual Desktop** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
VD Broker	Choose the desired Broker from the list
Server	Enter the IP address (or the name) of the server
Logon Pass-through logon	See Adding applications
Protocol (VMware View only)	Choose between `RDP` and `PCOIP`

3. To configure further settings, click **Advanced**. For further information, see depending on the selected broker or protocol
   - Advanced XenDesktop settings or
   - Advanced RDP settings
4. Confirm with **Apply** and **OK**.

7.8. Emulation

The following emulations are available:

Emulation	Description
PowerTerm InterConnect	PowerTerm® InterConnect from Ericom® Software is an emulation suite that allows you to connect to IBM mainframes, IBM AS/400, Unix, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000 and Data General. The **PowerTerm InterConnect** (powerterm) package is required for installation. PowerTerm InterConnect is a licensed product and available from our distribution partners.
eterm	eterm is a terminal emulation suite including the following emulations: Siemens 97801 (7 & 8 bit), ANSI, AT386, BA-80, VT320. The **Eterm 97801 terminal emulation** (eterm) package is required for installation. eterm is included in licensed eLux software free of charge. For information on configuration and how to modify the key mapping, see the eterm Administrator's Guide, available in the Archive on the uDocs Download page.
Virtual Network Computing	Virtual Network Computing (VNC) is a remote display system which allows you to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. The remote machine to be viewed must have a VNC server installed and the local machine a VNC viewer. On the **Emulations** dialog, you can configure the VNC viewer, which is open source and included free of charge in the eLux software. The **VNC client** (vnc) package of the eLux package **Mirror eLux Desktop** is required for installation. For further information, see Mirroring in the Scout Enterprise guide.
XDMCP	The X Display Manager Control Protocol (XDMCP) is used by X terminals (and X servers in general) to set up an X session with a remote system over the network. The XDMCP functionality is included in the BaseOS. By default, the XDMCP session runs in its own console. To enable sound, open **Setup > Multimedia** and select the **Enable sound in XDMCP sessions** option. Note: The application must be e-sound system compatible.

Emulation	Description
X11	The X Window System (X11) is the de facto standard graphical engine for the UNIX and Linux operating systems. It provides common windowing environment bridging heterogeneous platforms. It is independent of the operating system and hardware. The X11 server developed by The XFree86 Project, Inc (www.xfree86.org) is included in the **Xorg** package and is part of the BaseOS.
Tarantella	Tarantella allows users to access their applications over a Web-based interface. The **Tarantella Client** (tarantella) package is required for installation. The server is licensed, the client is free. For further information, see www.tarantella.com.

For further information, see Configuring PowerTerm InterConnect and Configuring X11 application in the Scout Enterprise guide.

7.8.1. Defining an X11 application

1. Add a new application and click the **Emulation** tab.
2. In the **Emulation type** list, select **X11**.
3. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console Do not use blanks within the name.
Server address	Enter the IP address or name of the UNIX server.
User name	Enter the name of the user registered on the UNIX system.
Application	Enter the application name including its complete path.
Use SSH	The X11 session is started via Secure Shell (SSH) protocol Public key authorization only

4. Confirm with **Apply** and **OK**.

7.8.2. Configuring PowerTerm InterConnect

The configuration of PowerTerm InterConnect is carried out in two steps:

- Defining a PowerTerm application on a reference client and transferring the created configuration files
- Defining a PowerTerm application for all clients by using the configuration files created on the reference client

Defining a PowerTerm InterConnect application for a reference client

The PowerTerm software package must be installed on the reference client

1. Define on the reference client locally or in the Scout Enterprise Console a PowerTerm application containing only the application name. (for details see below).
2. Start PowerTerm on the reference client and configure the application manually.

   The configuration is saved to the local client directory `/setup/PowerTerm/` *in the following four files*
   `ptdef.pts`
   `ptdef.ptc`
   `ptdef.ptk`
   `ptdef.ptp`
3. Close PowerTerm.
4. Copy the four configuration files via network or USB stick and make them available to Scout Enterprise Console.
   Or:
   Transfer the files from the client to the Scout Enterprise Console remotely by using **Request diagnostic files** with an individual template. For further information, see Configuring diagnostic files.

The configuration files for the actual PowerTerm configuration are provided. The second step may be carried out.

Defining a PowerTerm InterConnect application for all clients

1. In the Scout Enterprise Console, add a new application for the desired OU.
2. On the **Emulation** tab, in the **Emulation type** list, select `PowerTerm`.
3. Edit the following fields:

Option	Description
Name of application	Enter an appropriate name without using blanks.

Option	Description
Parameters	Optional starting parameters for the PowerTerm application: `-fullscreen` full screen `-maximize` maximized window `-no-menu-bar` no menu bar `-no-tool-bar` no toolbar `[myName].pts` name of an individual PowerTerm configuration file of the client Example 1: `-fullscreen -no-menu-bar -no-tool-bar` Example 2: `-fullscreen ptconfig001.pts`
Terminal setup file	Select the relevant `.pts` file of the reference client from the file system.
Communication file	Select the relevant `.ptc` file of the reference client from the file system.
Keyboard file	Select the relevant `.ptk` file of the reference client from the file system.
Power PAD file	Select the relevant `.ptp` file of the reference client from the file system.
x button	Delete previously selected configuration file from the Scout Enterprise database if required. To delete the file physically from the client you need to perform a factory reset.

4. Confirm with **Apply** and **OK**.

PowerTerm InterConnect is available to all clients of the relevant OU on the next restart.

7.9. SAP GUI

If you want to use the **SAP GUI** feature , the software packages **SAP R/3 client PlatinGUI** (**sap-platingui**) and **IBMJAVA2** must be installed.

eLux supports the SAP/R3 client with eLux RP. However, this feature is not available for all hardware platforms. Please check in the relevant eLux container on www.myelux.com whether a SAP R/3 client is available.

Minimum system requirements:

- 96 MB free hard drive space
- 128 MB RAM

7.9.1. Defining a SAP GUI application

1. Add a new application and click the **SAP GUI** tab.
2. In the **Name** field, enter a descriptive name for the application in the console, and in the **Display name**[1] field , enter a name that is shown on the client.
3. Select the **Classical user interface** option , if you want to use the classic SAP design.
4. Confirm with **Apply** and **OK**.

There are two ways to configure the SAP client:

Locally on the client	SAP GUI can be configured directly on the Thin Client when the user starts the SAP client for the first time.
Configuration via administrator	The administrator can transfer a SAP configuration file or message server list to the relevant devices. The SAP client configuration file is `/setup/sapgui/platin.ini`. For further information about how to transfer files, see Advanced settings > Files.

Note
For further information on SAP GUI configuration, see the SAP documentation.

[1] for Scout Enterprise Management Suite 14.7 and later versions

8.1. Troubleshooting

Error / problem	Reason	Solution
Missing firmware	The required software is not installed on the Thin Client	Install the software on the Thin Client. For further information, see Creating an IDF in the ELIAS guide and Firmware update.
Doubled names	Two applications have the same name. This causes conflicts because applications are identified by their names.	Use unique names.
Hidden application cannot be executed	Applications are invisible for the user when they run in hidden mode. This option is available for applications of the **custom** type .	Enable the option **Start automatically** or **application restart** to start hidden applications on start or run them non-stop, respectively.

Error / problem	Reason	Solution

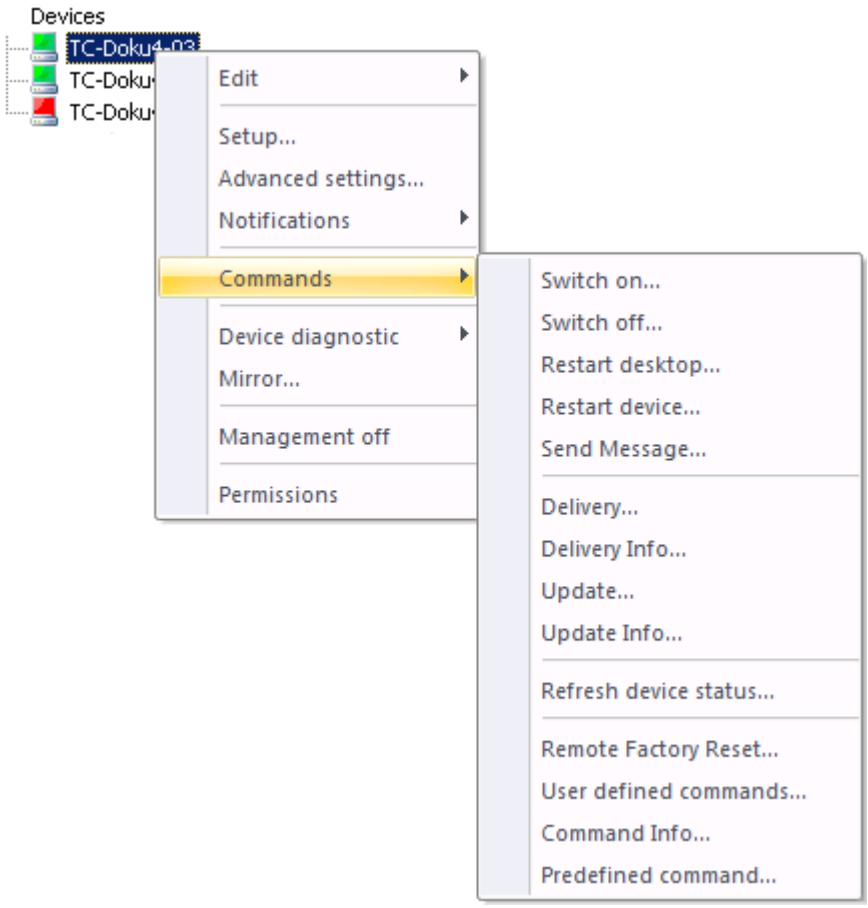
Problems with certificates in combination with VMware View Server	Server problem occurred:
	VMware View Server (>4.5) after successful installation is using a so-called "self-signed" certificate. If a Thin Client is configured correctly, it won't accept. The reason is that the **FQDN** (fully qualified domain name) is mandatory for server certificates, but is missing in the **CM**.
		Create a server certificate in the **Windows-CA** with **FQDN**.
		Create server certificate using **mmc**: Certificates (Local computer). The key must be exportable. The following steps depend on the server version:
		1. For VMware View Server 5.x and later versions:
		The display name of the server must be **vdm**. The certificate store `Local computer / Personal` must contain only one certificate with exactly this name.
		2. For VMware View Server < 5.x :
		Export the certificate including the private key as `<name>.pfx` and create a <*password*>. Save the file to `C:\Programs\VMware\VMwareView\Server\sslgateway\conf`. In the same directory, edit the file `locked.properties` and add the following lines:
		`keyfile=<name>.pfx`
		`keypass=<password>`
		Restart the VMware View Connection server.
		The correct certificate is used now.

9. Client remote management by commands

By using the Scout Enterprise commands the administrator can change the status of the devices, perform updates and send messages. The commands can be executed immediately or can be scheduled to be run once or periodically.

You can apply the commands on individual devices, on OUs and on Dynamic Client Groups.

In addition, the context menu of an individual device provides the commands for device diagnostics and for mirroring.



9.1. Available commands

The context menu of a device, OU or Dynamic Client Group provides the following **Command** options resulting in the **Execute/Schedule command** dialog for further configuration:

Command	Description
Switch on...	Switches on the device/devices
Switch off...	Switches off the device/devices
Restart device...	Restarts the device/devices
Restart desktop...	Restarts the eLux interface.

Command	Description
Send message...	Sends a message to the device/devices The message text can be formatted by using HTML-tags. The message title can be modified.
Delivery...	Delivers software for a firmware update
Update...	Performs a firmware update
Refresh device status...	Requests the current device status and refreshes the status of the device/devices in the tree view
Remote factory reset...	Sets the device back to initial state The configuration is deleted, the IDF remains. Both, the Scout Enterprise Server address and the licenses remain on the client unless you select the options • Delete Scout Enterprise Server address on the client (as is for remote factory reset on the client) • Delete client-side stored licenses (for example due to resale)
User-defined commands...	Sends a user-defined command to the device/devices such as a script for a BIOS update **Note** After having executed an user-defined command, after a time span of 30 seconds, you can run the next user-defined command or update command.
Pre-defined command...	Provides user-defined commands that have been pre-defined globally. For further information, see Pre-defined commands.
Cofiguration run...	Prepares the configuration data for an OU or Dynamic Client Group. For further information, see Configuration run. This command is not available for an individual device.

The following options open the relevant log file:

Command	Description
Delivery Info...	Opens the log file of the latest software delivery
Update Info...	Opens the log file of the latest firmware update
Command Info...	Opens the log file of the latest user-defined command

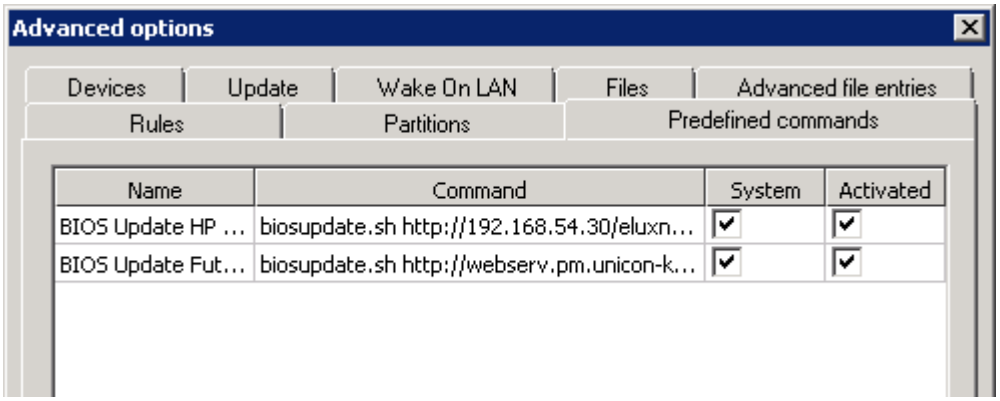
9.2. Pre-defined commands

User-defined commands can be pre-defined and provided globally. For example, you can pre-define scripts for the BIOS update of particular hardware that subsequently are listed as commands in the **Commands > Pre-defined Command...** list-field.

Defining pre-defined commands

1. On the Scout Enterprise menu, click **Options > Advanced options> Pre-defined commands**.
2. Click **Add**.
3. Edit the new entry by clicking on the fields **Name** and **Command**.

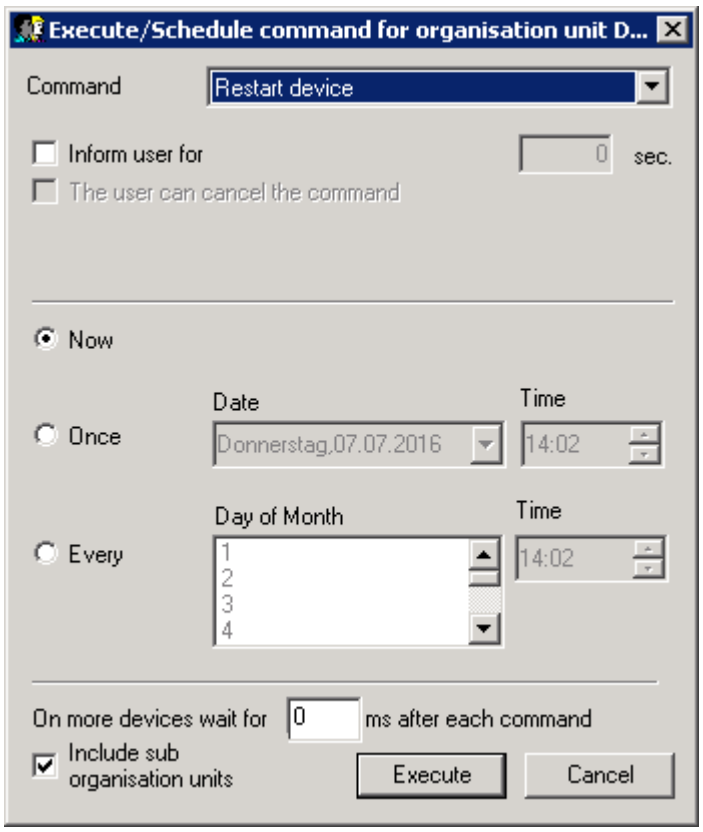
   *The command name specified in the **Name** field will be shown to the users in the **Commands** dialog, while the command itself will not be shown.*
4. To run the command with system rights, leave the **System** option selected.
5. To show the command in the listfeld of pre-defined commands, leave the **Activated** option selected.
6. Confirm with **Apply** and **OK**.



*All activated pre-defined commands are provided in **Commands > Pre-defined command...** in the relevant list-field and can be applied on individual devices, on OUs and on Dynamic Client Groups.*

9.3. Scheduling and executing commands

1. For the relevant device, OU or Dynamic Client Group, open the context menu and click **Commands**.
2. On the sub-menu, click the desired command.



*The **Execute/Schedule command** dialog opens. The shown options can be slightly different depending on the selected command.*

*The **Command** list-field provides all available commands.*

3. To show the complete title, move the mouse pointer over the title bar.
4. Specify whether and how long the user should be informed, and if the user is allowed to cancel the command.
5. Specify when the command should be executed and if it should be repeated.
6. If more than one device is concerned, you can define a delay after each command.
7. If an OU is concerned, select **Include sub units**, if required.
8. Confirm with **Execute**.

The command is executed at the defined point in time. Depending on the command, you are asked to confirm.

9.4. Command results per device

Feedback on performed update, delivery and user-defined commands is available both for a particular device in the **Properties** window and independent of the device in the **Command history** window. All processes are recorded, even if they turn out to be obsolete and haven't been run or if they are aborted. If they have been completed successfully, they have a green symbol.

Viewing command results on a particular device

Note
The following instructions are related to update commands. Viewing results of a delivery or user-defined command is done accordingly.

1. Make sure to show the **Properties** window: **View > Window > Properties**.

   *The **Properties** window is shown permanently in the upper right. For the selected device some properties are shown. Properties can be shown or hidden by using the*  *icon.*

2. Select the relevant device in the tree view.

   *In the **Properties** window, in the Update section, the following fields are provided:*

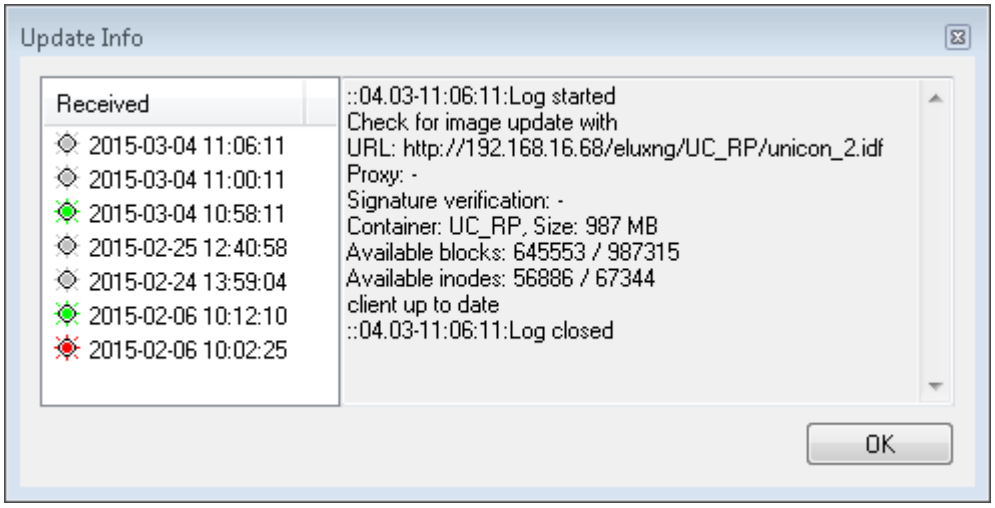
Image	Current image
Update time	Exact point in time of the latest update
Update status	Current status such as `Update in progress`, `Update successful` or `Update not necessary`
Update provider[1]	Origin of software packages (web server or proxy)
Update size	Size of the transferred packages in compressed format

3. Double-click the term **Update status** or click **...** at the end of the line.

   *The **Update Info** window is displayed. On the left side, you can see all updates that have been processed, aborted or not been processed because the IDF had been up-to-date. For a selected update you can view all logged data on the right side, among them the installed software pack-*

[1] For Scout Enterprise Management Suite 14.8 and later versions

ages.



Note
Information on the last update of the relevant device can also be viewed by using the context menu and **Commands > Update-Info...**.

Any performed commands are recorded and shown independently of the device in the **Command history** window. For further information, see Command history.

9.5. Command history

All of the executed **Update**, **Delivery**, and **User-defined** commands can be viewed in the command history. When calling the command history, the permissions of the administrator management are respected.

- Click **View > Command history...**

*The **Command history** window opens and displays one job (command for 1 to n devices) per line providing the following information:*

Option	Description
Type	Type of object the command is applied to. This can be an individual device, an OU with sub units (OU+), an OU without sub units (OU) or a Dynamic Client Group.
Name	Object name (name of device, OU or Dynamic Client Group)
Command	Executed command (Update, Delivery or User-defined command)
Devices	Number of devices concerned

Option	Description
Start	Date and time of sending command to the devices / starting time
End	Date and time of sending command to the devices / ending time The ending time of a job is reached when either the devices report back `Successful` or `Failed` or when the timeout of 5 minutes for feedback is passed. If the administrator terminates a job, the ending time is defined by the terminating time.
Successful	Number of devices that have successfully processed the command
Failed	Number of devices that have reported failure during command processing
Timeout	Number of devices that haven't reported feedback within the defined time period of 5 minutes
Progress %	Progress of command processing in percent, across all concerned devices
Administrator	Administrator who ran the command

Apply the following options to the job list:

Option	Action
Refresh	Press F5.
Sort table rows	Click the column title by which you want to sort. *A first click sorts the jobs ascending and the second one sorts descending. To reproduce the default sorting order click F5.*

Apply the following options to a selected job:

Option	Action
View details	Click **Details...**. *The **Command details** window displays all processing details of the concerned devices. Among with starting and ending times you can find the current status and the command processing result for each device.*
Search object in Scout Enterprise tree view	Right-click an object name, and then click **Find in tree view**. *The first result is selected in the tree view.*
Terminate running job	Select the running job, and then click **Terminate**. *A command terminating request is sent to the Scout Enterprise Server and the transmission of the command to the devices is stopped.*

10. Remote maintenance

For maintenance, user help-desk and troubleshooting purposes, the administrator can use different tools to access the client devices.

10.1. Mirroring

Note
This feature can only be applied to an individual device.

Mirroring (Shadowing) allows administrators to either view or take control of eLux user sessions. It can be very helpful in a variety of scenarios such as when administrators assist users or when administrators need to check correct functioning of client updates or newly installed software.

10.1.1. Requirements

- On the administrator's system, a VNC viewer must be installed. A VNC viewer is provided by
  - the Scout Enterprise Console or
  - the Scout Enterprise Mirror App
- On the target device, a VNC server must be installed.
  For eLux clients, a VNC server is installed with the **VNC Server extension** which is part of the **XOrg** package. This feature package module must be included in the client's IDF.
- For the target device, in **Setup > Security > Mirror settings**, mirroring must be enabled and configured. For further information, see Configuring Mirroring.

10.1.2. Mirroring from Scout Enterprise Console

Throughout a mirror session, the device user is given notice by a system message which pops up both on the client screen and on the administrator's screen. The system message remains permanently on top and allows the user to cancel the mirror session at any time by clicking the **Quit** button.

Launching a mirror session

Note

- If there are two monitors connected to the client, both monitors are mirrored. To get the best result, make sure to have connected two monitors with the same or higher resolution on the Scout Enterprise machine.
- Within the mirror session, the keyboard layout of the Scout Enterprise machine is used and not the one of the client.

1. For the relevant device, open the context menu and click **Mirror...**.

   *The **Mirroring** dialog opens.*

2. In the **Session type** field, choose if you want to mirror the desktop or a particular session:

Option	Description
Desktop	Mirror the eLux desktop (Display 0).
XDMCP 1	Mirror the first open XDMCP session (Display 1).
XDMCP 2	Mirror the second open XDMCP (Display 2).

3. Confirm with **OK**.
4. Depending on your configuration in **Setup > Security** a password is requested. For further information, see Configuring Mirroring.

   If configured, the user must confirm the mirror session.

The mirror session starts. On the user's screen, a system message is displayed that cannot be closed unless the mirror session is closed.

The user can set the following options:

Option	Description
Mirror enabled	If cleared, the terminal cannot be accessed anymore for mirroring.
Confirmation needed	Before mirroring, the user must confirm within 10 seconds. Otherwise, the connection is denied.
Read only	The administrator has only read-access on the mirrored device. Mouse and keyboard input are not transmitted into the mirror session.

The mirror session ends when the administrator closes the session window or when the user on the system message clicks the **Quit** button.

10.1.3. Mirroring with Scout Enterprise Mirror App

In order to avoid increased server load and to enhance the help-desk facilities, a separate mirroring tool is available that can be run standalone. The access rights defined in the Scout Enterprise administrator management are applied to the Scout Enterprise Mirror App.

Configuring mirroring by using the Scout Enterprise Mirror App

1. In Scout Enterprise, click **Options > Base configuration > Security > Mirroring settings > Advanced** and select the **Allow Scout Enterprise only** option.

   Or locally on the client:

   In the control panel, click **Setup > Security > Mirror server settings > Advanced** and select the **Allow Scout Enterprise only** option.

   Mirroring is allowed by using the Scout Enterprise Console and by using the Scout Enterprise Mirror App, but other VNC viewers are not allowed. This allows to apply the access rights defined in Scout Enterprise.

2. In Scout Enterprise, click **Security > Manage administrators > Default object rights**, and then set the required admin object rights:

   `Execute mirror` and
   `Visible`

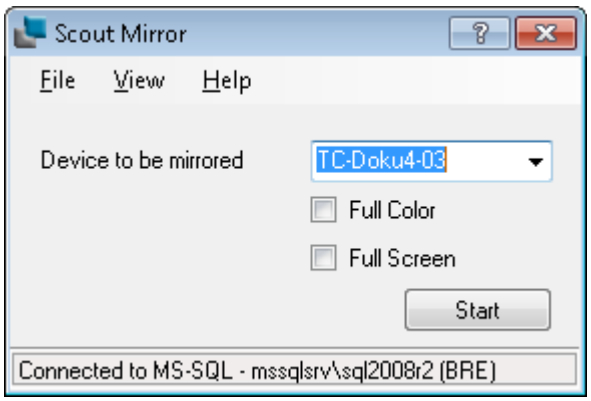
3. In Scout Enterprise, click **Security > Manage administrators > Edit base permissions** and ensure that the permission `Use of Scout Enterprise Mirror` is active.

4. Download and install the program **Scout Enterprise Mirror Application** from www.my-elux.com.

Note
The device to be mirrored can be accessed by entering its IP address, host name or MAC address.

Launching a Scout Enterprise Mirror App session

1. From the Windows start menu, open the Scout Enterprise Mirror App



2. Type the IP address, host name or MAC address of the device to be mirrored, and then click **Start**.

For further information on the procedure of mirroring, see Mirroring from Scout Enterprise console.

10.2. Device diagnostics

Note
This feature can only be applied to an individual device.

Device diagnostics helps you run predefined commands on the client and retrieve protocol and configuration files from the client to Scout Enterprise for diagnostic purposes. The requested client files support the administrator in error analysis and are required when opening a support ticket.

You can also use this feature to request any files that you have defined.

10.2.1. Requesting diagnostic files

Note
Before performing device diagnostics, temporarily enable enhanced debugging on the client to make sure to retrieve all data needed. After device diagnosis, disable enhanced debugging, otherwise you risk to exceed the flash memory capacity of the Thin Client.

1. For the relevant device open the context menu and click **Setup...**.
   On the **General** tab, clear the option **Use parent**.
   On the **Diagnosis** tab, set the **Debug level** option to `On`.
   Confirm and perform a restart of the client.

   Enhanced debugging on the client is enabled.

2. For the relevant device, open the context menu and click **Device diagnosis > Request files...**.

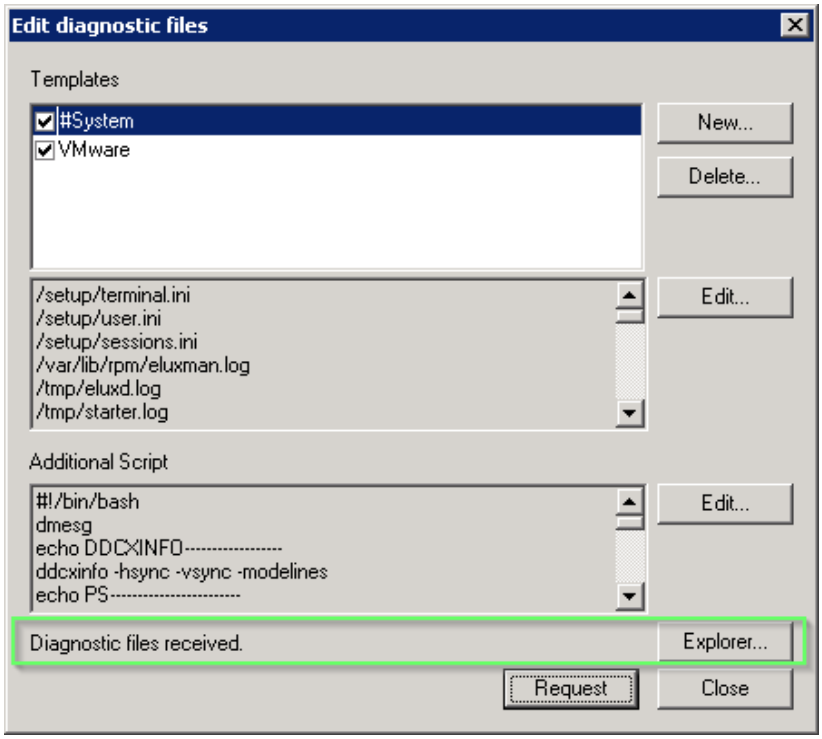
   *The **Edit diagnostic files** dialog opens. Under **Templates**, any already defined templates are shown. Templates can contain files and script. Only active templates (check mark) are processed. The predefined `#System` template is always active.*

3. If you are authorized, you can select or clear further templates of the list.

4. Click **Request**.

   All scripts defined in the active templates are executed on the client.
   All files defined in the active templates are retrieved from the client and saved as `.zip` file in the local user directory such as

   `<userprofile>\Documents\UniCon\Scout\Console\Diag`.



*Scout Enterprise gives feedback in the lower section of the dialog. When the diagnostic files have been received, the **Explorer...** button is displayed.*

5. Click **Explorer**.

   The Windows Explorer opens showing the target directory.
   The latest ZIP file contains the relevant diagnostic files.

6. For the relevant device open the context menu and click **Setup...**.
   On the **Diagnosis** tab set the **Debug level** option to `Off`.
   On the **General** tab check the option **Use parent**.

   After the next restart, enhanced debugging on the client is disabled and setup inheritance is restored.

Note
Whenever you wish to use this feature to transfer any files defined in an individual template, you do not need to carry out step 1 and 6.

10.2.2. Configuring diagnostic files

The **Diagnostic files** dialog provides a predefined template called `#System`. This template includes a file list containing relevant configuration and log files and , secondly, script code to be run on the client. Both of them cannot be edited .The `#System` template is used each time the device diagnosis is performed via **Request**.

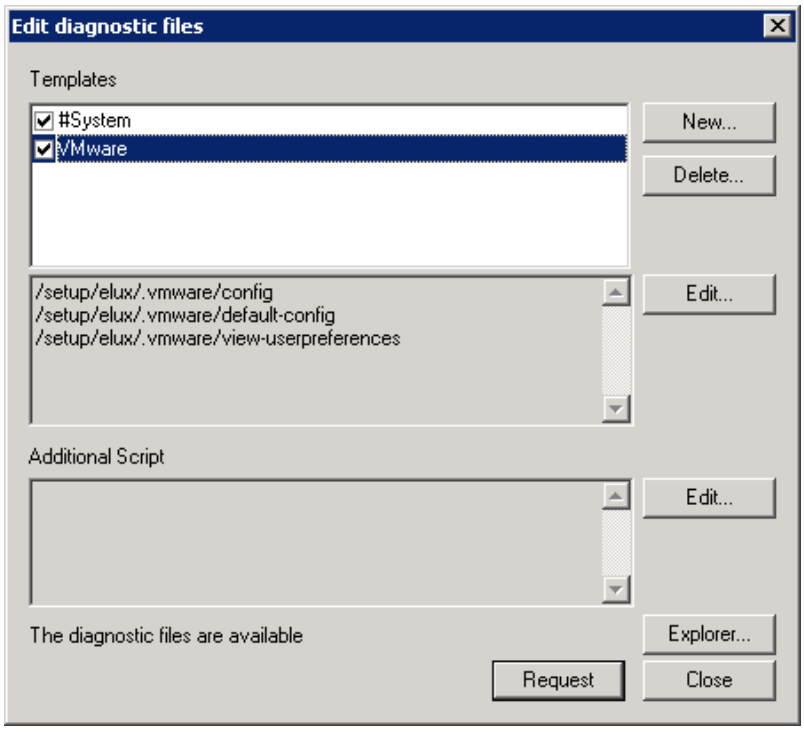
In addition you can define further templates containing file lists and script. The templates are available globally, no matter where you define them.

Defining a template for device diagnosis

1. Open the context menu of a device and click **Device diagnostics > Request files**.

   *The dialog Edit diagnostic files opens. Under **Templates**, the predefined `#System` template and , if defined, further templates are shown .*

2. Click **New...**, and then enter a name for your new template. Confirm with **OK**.
3. In the **Templates** list, select your new template, and then click **Edit** next to the file list.
4. In the text box, enter line by line the relevant file names including paths. Confirm with **Save**.



5. To enter script code you want to be performed on the client, click **Edit** next to **Additional script** and enter your code. Confirm with **Save**.

Note

When performing device diagnosis with **Request** all active templates are included. However, if all of the listed files of the `#System` template are written and transferred, depends on the selected debug level. For further information, see Setup > Diagnostics tab.

10.2.3. Comparing target and actual settings

Note
This feature can only be applied to an individual device.

The actual configuration settings of the client are compared to the target configuration settings defined on the Scout Enterprise Server.

- For the relevant device, open the context menu and click **Device diagnostic > Setup comparison**.
  Or:
  Select the desired device and press CTRL-E.

The configuration of the selected device is compared to the currently stored settings in the Scout Enterprise database. Differing properties are listed in a window.

Note
To compare the configuration between particular devices or OUs, show the **Compare setups** window. For further information, see Comparing configurations between OUs or devices.

11. Firmware Update

On delivery, the Thin Clients are already equipped with the operating system and the basic software components such as ICA client, RDP client, browser and emulations. This software called firmware is stored on the client flash drive. Whenever new software versions are available or demands change, software components need to be added or removed which requires a firmware update.

Basic steps:

- Download of the relevant software packages from myelux.com
- Modifying the IDF on the web server by using ELIAS.
- Checking the firmware configuration of the relevant Thin Clients
- Performing the update
  - Software deployment
  - Installing the new software on the client

Performing the update can be done in one step by using an **Update** command. In this case, the required software packages are delivered and, after that, automatically installed. Alternatively, the two actions can be uncoupled (for Scout Enterprise Management Suite version 14.6 and later): This means to deliver the software in a first step by using a command, before you start installation of the software by an **Update** command.

Note
To save bandwidth, you can use a proxy client for updates. For further information, see Update through proxy client.

Ways to initiate a firmware update

Updates can be performed immediately or initiated automatically at a defined point in time:

- Firmware updates can be executed or scheduled (once or periodically) by using the **Update command** feature.
- The devices can be configured to automatically check for new IDF versions on start or shutdown. If a later version is available, an update is started.
- Defining an **Update notification** results in the execution of a firmware update on the next client restart

If configured, the user can defer the execution of the update.

Updates are only performed, when the relevant IDF has been modified. All update activities are logged.

Relevant devices

Commands and notifications can be applied to the following devices and groups:

- Individual devices
- Multiple devices selected in the **All devices** windows (multiple selection by using CTRL and SHIFT allowed)
- OU
- Dynamische Gerätegruppe

The **Check for update** option is part of **Device configuration > Firmware** and can be applied to individual devices, OUs and all devices.

Recovery-Installation

If you want to reset your devices to initial state, you can perform a recovery installation. A recovery can also be required if critical feature packages of the Base OS have been changed, or if your operating system has not been updated for a long time. By performing a recovery installation, all data on the storage medium are destroyed (except license data) and the eLux software is installed. For further information, see Recovery procedures in the Recovery Short Guide.

11.1. Requirements

The following components are required to perform a firmware update:

- Scout Enterprise Server and Scout Enterprise Console to configure firmware updates for the clients
- ELIAS tool to create and modify Image Definition files (IDF) in the software container
- Web server (HTTP, HTTPS, FTP, FTPS) with container directory providing eLux software packages and Image Definition Files (`.idf`)
- eLux software packages to be installed

The Scout Enterprise Server and Console including the ELIAS tool can be downloaded from www.myelux.com. These components are part of the standard installation.

The current software bundle `eLux`*`version`*`_AllPackages.zip` and further software packages can also be downloaded from www.myelux.com.

The web server can be Microsoft IIS or any other web server such as Apache.
Make sure to have enabled the relevant web server role.

11.2. Update partition

The latest eLux versions create an update partition on clients provided with the required flash memory space. An update partition enables the following features:

- Software delivery before update
- Client can be used as Dynamic Proxy
- Signature check for eLux software packages

In the following cases eLux creates an update partition on the client:

eLux version (minimum)	Flash memory (minimum)	Update partition is created at
eLux RP 4.6.1	2 GB	• PXE recovery or • USB Recovery or • Firmware update including flash format before update
eLux RP 5.1	4 GB	
eLux RP 5.3	4 GB	System start – if there is no update partition yet next to the system partition (2 GB)

The size of the update partition complies with the storage space provided. For eLux RP 5.3 clients, the size varies between 2 GB and 14 GB.

11.3. Planning an update

Note
The following procedure includes firmware configuration of the clients. Once configured suitably, for periodic updates, use the **Check for update** option to perform firmware updates automatically by carrying out just the first two steps.

1. If the software container does not contain the relevant software, download and import the required packages. For further information, see Importing packages to a container in the ELIAS guide.
2. In ELIAS, modify the relevant IDF in order to provide the desired software features. For further information, see Create IDF in the ELIAS guide.
3. For the relevant OU or the relevant device, open the **Setup** dialog.
   If you want to perform the update for all clients, click **Options > Base configuration**.
4. On the **Firmware** tab, check if the fields are configured correctly, in particular the entries of the **Protocol**, **Server**, **Path** and **Image file** fields.

   *From these values, the URL shown below of the **Path** box is generated. The URL is relevant for the transfer of image file and eLux software packages.*

   The specified image file must be identical to the image file updated in ELIAS.
5. If you want to have updates performed automatically on start or shutdown of the clients, select the relevant option **Check for update** in the bottom area of the **Firmware** tab.

   As the update is initiated by the client, the locally saved firmware parameters on the client are used.

   For further information on the firmware update configuration, see Setup/Firmware.

   If you want to perform updates by using a proxy, see Update through proxy client.
6. Confirm with **OK**.

The firmware update is configured for the relevant clients.

Note
As soon as an updated IDF is available, and if one of the **Check for update** options is selected, the update is performed on the next client restart or shutdown, respectively.

Alternatively, you can initiate the update using one of the following procedures:

- Perform an update command
- Schedule an update command for a defined point in time, once or periodically
- Define an update notification

For further information, see Performing updates via command or Performing updates via notification.

11.4. Performing updates via command

Note
If you want to deliver the software packages in a separate step before performing the update, use the **Delivery** command.

1. For the relevant device, OU or Dynamic Client Group, on the context-menu, click **Commands > Update...**

   *The **Execute command** dialog opens.*

2. If you want to inform the user, select the **Inform user for** option.

   This option triggers a system message to be shown on the client and gives the user the chance to control the time of the update process.

   Note
   If you want to allow the users to defer an update, this must be configured for the relevant clients in **Firmware > Reminder settings**. This feature allows the users to determine the update time by themselves as soon as the administrator runs an **Update** command. For further information, see Update deferment by user.

   *If the **Number of allowed deferments** in the **Reminder settings** is set to `1` or more, the system message provides an option for the user to postpone the required firmware update.*

   - In the box next to **Inform user for**, enter the display duration of the system message in seconds.

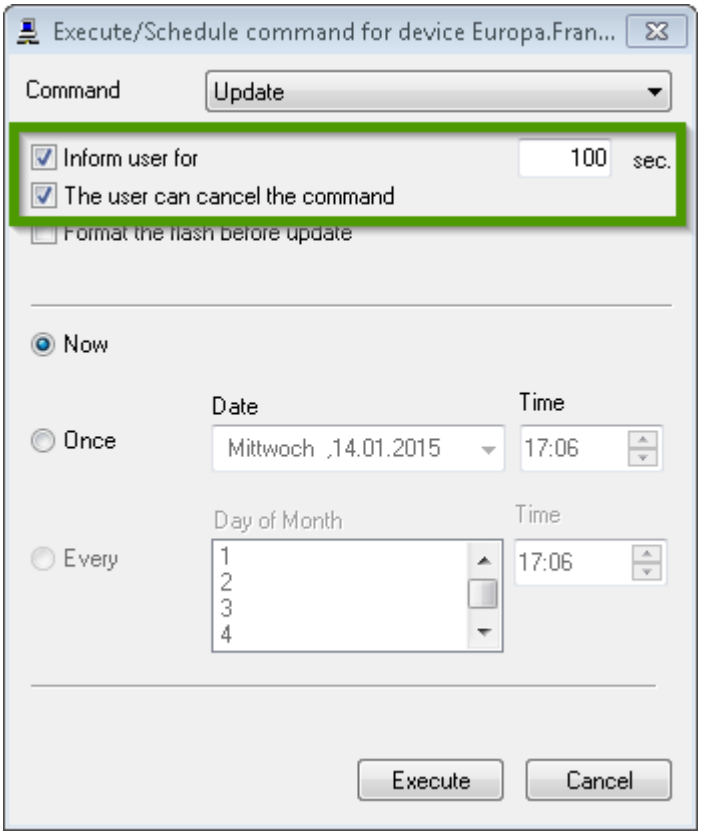
     *Within the defined time period the user is given the chance to close applications and to log off before the update is performed. In addition, the user is given the chance to defer the firmware update for a selectable interval (as defined in **Delays until next reminder**).*

     If you leave the display duration at `0`, the system message is shown until the user clicks one of the push buttons.

   - If desired, select the **User can cancel the command** option.

     *The system message on the client will contain a **Cancel** button enabling the user to abort*

the firmware update definitely. There is no self-acting retry of the update process.



3. To format the flash memory before writing, select the **Format flash before update** option.
4. Define the point in time for the update. For further information, see Scheduling and executing commands.
5. Click **Execute**.

*The update process is released at the defined time. The update status is displayed for each device in its **Properties** window. For further information, see* Update log.

Note that updates are only performed, when the relevant IDF has been modified. If an update fails, no efforts will be made to retry.

Note

When executing an **Update** command, the core information is the URL that is transferred to the client. The URL is created by using the values set in **Setup > Firmware** at the time when the command is run. Note that if the client initiates the update, the local **Firmware** configuration is concerned.

11.5. Performing updates via notification

Clients can be configured to check for new image versions on each shutdown or restart.[1] As soon as the IDF referenced in their **Firmware** configuration has been modified, the clients will be updated to that IDF.

However, by using update notification, you can send an explicit one-time update request to selected clients to be evaluated with the next connection to the clients. The clients then are updated to the IDF configured in the Scout Enterprise firmware configuration.

1. Select a device, an OU, a Dynamic Client Group or devices within the **All devices** window.
2. On the context menu, click **Notifications > Initiate image update...**

   *The **Image update notification** dialog is shown.*
3. Specify whether and how long you want to inform the user, and if the user is allowed to cancel the command.
   For further information, see Performing updates via command.
4. To format the system partition before the update is performed, select the relevant option.
5. Confirm the notification and confirmation.

   The notifications for firmware update are defined.

   *For the relevant devices, in the **Properties** window, the **Image update notification** field shows the value* `Activated`.

   > **Note**
   > If the **Firmware update notification** field in the **Properties** window is hidden, click  to define which fields you want to show.
6. If you want to delete the update notification for one or more devices, use the context menu option **Notifications > Delete update notification**.

For the relevant clients, a firmware update notification is set. As soon as a device restarts and reconnects to Scout Enterprise, it receives an update request and the firmware update notification is automatically deleted.

*Depending on how you have configured the notification and the device configuration in **Firmware > Reminder settings**, the update is performed immediately or the user receives a system message including deferment options. For further information, see Impact of the user deferment option.*

*The update status is displayed for each device in its **Properties** window. For further information, see Update log.*

Note that updates are only performed, if the relevant IDF has been modified. If an update fails, no efforts will be made to retry.

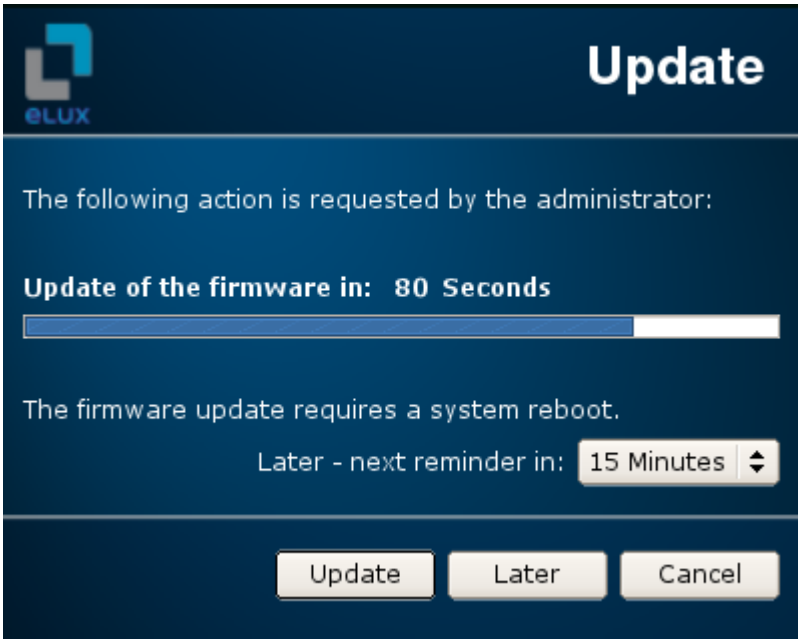
[1] **Firmware > Check for Update**

For devices without update partition, an update request might be shown although an update is not required. When the user clicks the **Update** button, the window is closed, no update is initiated.

Note
In the Scout Enterprise Report Generator, you can filter devices by the field **Firmware update notification**.

11.6. Impact of the user deferment option

Any **Update** command run with the **Inform user** option selected, provokes a system message on the client including the defined user options. If configured in **Firmware > Reminder settings**, the user is provided with buttons to be used for deferment or aborting.



Option	Description
Later - next reminder in	Select list containing the time intervals for the next reminder of the firmware update, defined in **Delays until next reminder**. Is displayed only, if the **Number of allowed deferments** is set to `1` or higher, and if at least one more deferment is possible.
Update button	Perform firmware update immediately.
Later button	Postpone firmware update by the time period selected. If the client is shut down before timeout, the update is performed during shutdown. Is displayed only, if the **Number of allowed deferments** is set to `1` or higher, and if at least one more deferment is possible.
Cancel button	Abort update process definitively. Is displayed only, if the option **User can cancel the command** is checked.

11.7. Delivering software in advance

Before performing a firmware update, you can deliver the required software packages in a separate step. Only after the software deployment has been reported successful on all relevant devices, you start the installation by using an **Update** command.

Requires

The following instructions require the firmware settings of the relevant clients to be configured correctly. For further information, see Planning an update.
Moreover, note the following requirements:

- Scout Enterprise version 14.6 and later
- eLux RP 5.2 and later
- Clients are provided with an update partition

1. For the relevant device or OU, open the context menu and click **Commands > Delivery...**
2. In the **Execute command** dialog, specify whether and how long the user should be informed, and if the user is allowed to cancel the command.
3. If you want to clean the update partition of the clients before writing, select the **Clean update partition before delivery** option.
4. Specify the point in time for the delivery.
   For further information, see Scheduling and executing commands.
5. Click **Execute**.

Delivery is triggered at the defined point in time. If there is an updated IDF, and if the required software packages do not exist on the update partition of the relevant clients, the delivery of the software packages is started. The system only downloads those packages that are not yet available. If there is less than 30 MB storage space available on the update partition, old packages are deleted before new packages are transferred.

*During delivery, on the client, a green arrow icon is shown in the systray. If the administrator has selected the option **Allow user to cancel the command**, the user can click the **Cancel** button in the popup dialog*

*In the Scout Enterprise Console, for each device, the delivery status is shown in the **Properties** window. For further information, see* Command results per device.

Note

To install the software packages and update the IDF, perform an **Update** command.

11.8. Static proxy client

If you want to update narrow-band connected clients, you might wish to use a proxy client to forward the firmware update. Proxy clients download the required software packages and distribute them to other devices.

For the static proxy client, Squid is used as the proxy server software.

Note

- Using a Thin Client as a proxy requires 1 GB RAM or more main memory, since the packages are provided locally in the RAM of the proxy client. Depending on the overall size of the packages defined by the IDF you might need even more RAM.
- Squid does not support `HTTPS` as the caching mechanism does not work with `HTTPS`. To make the update process more secure, use signatures. For further information, see Firmware security through signature.

Configuration in Scout Enterprise includes three basic steps:

- Creating an application definition for Squid
- Setting up the proxy client
- Configuring the relevant devices for the proxy update

Creating application definition for Squid

1. Create a new OU which will be configured particularly for the proxy client.
2. In this OU, define a new local application, see Adding applications.
3. On the **Local** tab, edit the following fields:

Option	Value
Name of application	`Squid`
Local application	`Custom`
Parameter	`squid`
Hidden	On
Start automatically after 0 seconds	On

4. Move the proxy client into the OU and restart the client.

The client receives the Squid application definition.

Setting up the proxy client

1. Provide the proxy client with a firmware update containing the Squid software package. For this, modify the IDF by using ELIAS. For further information, see Planning an update.

   After restarting, the Squid software is installed on the proxy client.

2. For the OU of the proxy client, open **Setup > General** and clear the **Use parent** option.

   Inheritance is disabled and the proxy OU can be configured independently.

3. In **Setup > Firmware**, if you use the `HTTP` protocol, leave the **User** and **Password** fields empty.

4. For the proxy client, select **Setup > Network > LAN**, and then select the first entry and click **Edit**.
   In the **Edit network profile** dialog, select the option **Use following IP address**.
   Leave the **Domain** box empty and confirm with **OK**.

   The last obtained IP address is used as static IP address by the proxy client.

Configuring devices for the proxy update

1. For the OU or the device that you want to update through the proxy client, open the **Setup** dialog. If you want to define the proxy for all clients, select **Options > Base configuration**.

2. On the **Firmware** tab, edit the following fields:

Protocol	`HTTP`
Proxy	*<IP address of proxy client>*:3128
User and Password	*<no entry>*

3. Edit the further fields as usual, see Setup/Firmware.

Once the modifications have become active, the relevant clients receive their firmware updates from the proxy client.

11.9. Dynamic proxy client

You can use dynamic proxy clients for the software package distribution to all devices in the same subnet. A dynamic proxy client is an automatically selected device in a subnet that downloads the relevant software packages from the configured web server, and then provides them to all other clients in the subnet.

The solution is based on the device roles **Provider** and **Consumer**.

The fully automated provisioning (provider) and discovering (consumers) of the proxy service within subnets is realized in eLux RP by using the zero-configuration networking implementation Avahi.

11.9.1. Requirements

To be able to perform updates by using a dynamic proxy client, next to the eLux operating system, the following eLux packages must be installed on the devices of the relevant subnet:

- dynamicproxy-*xxx*.UC_RP-*x*
- avahi-*xxx*.UC_RP-*x*
- squid-*xxx*.UC_RP-*x*

11.9.2. Frame conditions and roles

The dynamic proxy client concept bases on the following roles:

Provider

The provider is the device that acts as Dynamic Proxy client. All devices with an update partition can be selected for the provider role. Once a provider is selected, the device remains in the provider role for the upcoming updates. In case the provider is not available at the required point in time, another device with an update partition takes over the provider role. The provider is selected automatically and dynamically.

To exclude devices from the provider role, modify the local file `/setup/terminal.ini`.

- Use the **Advanced file entries** feature of the Scout Enterprise Console to edit the `ini` file. For further information, see Defining individual file entries.

Option	Value
File	`/setup/terminal.ini`
Section	`DynamicProxy`
Key	`UseProvider`
Value	`false`

Consumer

All clients of a subnet that are not selected for the provider role are consumers. The consumers perform their update through the provider of the subnet and need not download any software packages from the web server.

To exclude devices from the consumer role, modify the local file `/setup/terminal.ini`.

- Use the **Advanced file entries** feature of the Scout Enterprise Console to edit the `ini` file. For further information, see Defining individual file entries.

Option	Value
File	`/setup/terminal.ini`
Section	`DynamicProxy`
Key	`UseConsumer`
Value	`false`

Note
In the **Firmware** configuration, if `HTTP` is used, the **User** and **Password** fields must remain empty.

11.9.3. Update procedure

Update check

In the case of an update request coming either from the Scout Enterprise Server or from the local **Firmware** configuration (**Update on boot / shutdown**), the consumers download the latest IDF file from the web server and check if they need to perform an update.

Discover proxy service

If software packages are required, the consumers try to discover the proxy service in the subnet. If there is no provider existing in the subnet so far, one of the devices with update partition automatically takes over the provider role and provides the proxy service.

Download software packages

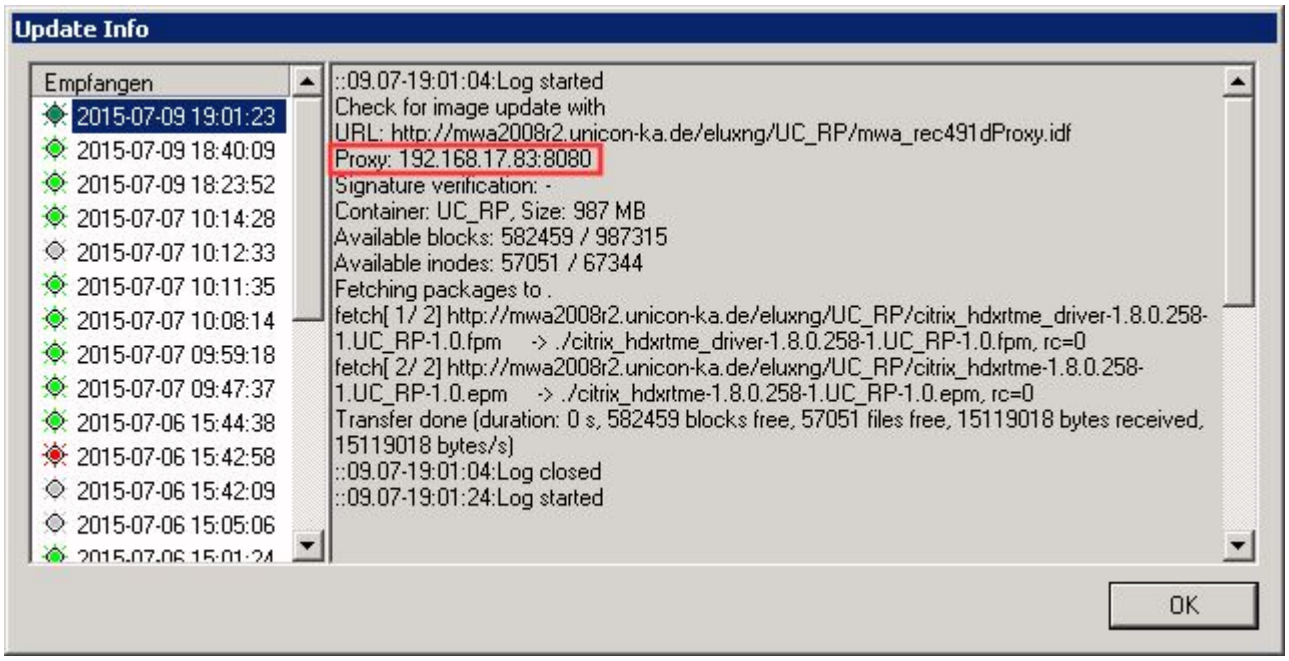
The provider checks the availability of the requested software packages on its update partition and downloads missing packages from the web server specified by the consumers.

Deploy and install software packages

The software packages are transferred from the provider to the consumers, and the consumers install the packages. Devices without update partition use the rhythm 'fetch one package - install one package', while devices with update partition fetch all required packages in one step and install them subsequently. Only after the last consumer was provided with the relevant software packages, the provider updates its own system, if needed.

Update information is recorded for both the consumers and the provider:

- For each updated device, the **Update Info** including the provider which has offered the proxy service can be viewed by double-clickling **Update Status** in the **Properties** window.
  For further information, see Update log.



- The provider has a local file `/tmp/dynamic-proxy.log` containing the consumers that have been provided with software packages.

11.10. Troubleshooting

Error messages

Error message	Reason	Solution
Bad container	Containers are hardware-specific.	Check if the container matches your Thin Client specifications.
Bad flash size	IDF size exceeds flash size	Verify if the image size defined by the IDF matches with the actual flash size of the Thin Client.
Bad authorization	Wrong device password	Correct the entry in **Setup > Security**.
Client needs recovery information	If critical feature packages (`.fpm`) are updated in the baseOS, the Thin Client requires a recovery installation before it can be updated.	For further information see Installing eLux RP in the **eLux Live-Stick**-Guide.

Update options

If the update is still faulty, try to modify update settings. For further information, see Advanced setup > Update options.

12. Passwords

12.1. Local device password

The device password affects only the local device. All clients managed by a particular Scout Enterprise Server receive the same device password.

The device password is required to verify the access rights for the clients. Scout Enterprise requests the device password for management tasks like discovery.

The device password can only be changed in the base configuration of Scout Enterprise. The initial password is set to `elux`.

Usually, the access rights do not allow users to modify their local security configuration. However, if the administrator changes the device password locally in the control panel of a client, this device cannot be managed by Scout Enterprise any longer.

Note
We recommend to change the password at once in order to avoid unauthorized configuration caused by local users.

For further information, see client password in the eLux guide.

12.1.1. Changing local device password via Scout Enterprise Console

Important
By using this feature, you change the device password of **all** clients managed by this Scout Enterprise Server.

1. In the Scout Enterprise Console, on the **Options** menu, click **Base Configuration... > Security**.
2. Under **Local security**, click **Edit**.
3. In the **Password** box, enter a new password and repeat it in the **Password confirmation** box.
4. Confirm with **OK**.

The new device password is assigned to the clients on the next restart.

Note
To activate the new password at once, perform the Scout Enterprise **Restart** command for the relevant devices (now or scheduled). For further information, see Scheduling and executing commands.

12.1.2. Changing local device password on the client

1. On the eLux control panel, click **Setup > Security**.
2. Under **Local security**, click **Edit**.
3. In the **Password** box, enter a new password and repeat it in the **Password confirmation** box.
4. Confirm with **OK**.

Important

The client cannot be managed by Scout Enterprise any longer.

12.2. Scout Enterprise Console password

The default account `Administrator` with console password is only active, if the **Activate Administrator Policies...** option is disabled.

In initial state,the Administrator policies are disabled and the console password is set to `elux` (all lowercase).

Note
We strongly recommend to change the password at once to prevent unauthorized access.

- To change the console password, log in to Scout Enterprise as administrator and click **Options > Change console password...**

  or

- Enable the Administrator policies.

  As soon as the administrator policies are enabled, the default account and console password are disabled.

We recommend to enable the Administrator policies and to use and modify your AD accounts for Scout Enterprise.

13. Managing administrators

13.1. Activating administrator policies

Managing more than one Scout Enterprise administrators requires enabling the **Administrator policies** feature. Scout Enterprise administrator accounts are based on AD accounts which must be defined before. Scout Enterprise administrator accounts can be configured in many ways.

By default, the administrator policies are disabled.

Note
Enabling the administrator policies requires being logged in as a full-access administrator. The initial account is `Administrator` with the password set to `elux`.

1. In the Scout Enterprise Console, click **Security > Activate administrator policies**.
2. Confirm with **OK**.

You are logged out and, from now on, you can only log in by using your Windows AD account.
*The **Security** menu options become active. For example, you can enable* pass-through authentication *now.*

*The `Administrator` default account is not available any longer and the **Change console password...** option is disabled.*

13.2. Adding administrators

You can define any AD users and groups as Scout Enterprise administrators.

1. In the Scout Enterprise Console, click **Security > Manage administrators...**
2. In the **Administrator permissions** dialog, click **Add Administrators...**

   The **Initial administrator profile** *dialog opens.*
3. Select the access range for the new admin and confirm with **OK**.

   The Windows **Permissions for Administrators** *dialog opens.*
4. Below of the **Group or user names field**, click **Add...**

   The Windows **Select Users or Groups** *dialog opens.*
5. Enter the relevant AD user name or AD group name, and then click **Check Names**.
   Or:
   Search for the AD user or AD group by using the **Advanced...** button.
6. Confirm with **OK**.

The new user or group is added to the list of administrators. You can assign the appropriate permissions to the user or group now. For further information, see Administrator policy*.*

New administrators can log on by using their Windows account information.

Note

If you use only AD groups, and if a user is member of more than one group, the access rights of the groups are not consolidated, but the rights of the first group that is found apply.
If users are authorized with their AD users and if they are authorized with one or more AD groups at the same time, the access rights are not consolidated but the rights of the AD user apply.

13.3. Deleting administrators

1. In the Scout Enterprise Console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Delete administrator**.

The selected administrator is deleted from the Scout Enterprise administrators list without an 'Are you sure?' verification.

13.4. Administrator policy

For all Scout Enterprise administrators there are three different kinds of permissions:

Base permissions	Main access permissions (total control)
Menu permissions	Access permissions for specific menu commands
Object permissions	Access permissions for OUs and/or individual devices

In the relevant **Administrator rights** dialog the provided rights are displayed with a green or red symbol:

Access granted	
Access denied	

By double-clicking or pressing the space key, the rights can be turned on and off.

If you click the **Full access** or **No access** buttons, all of the displayed rights are

set to green or red, respectively.

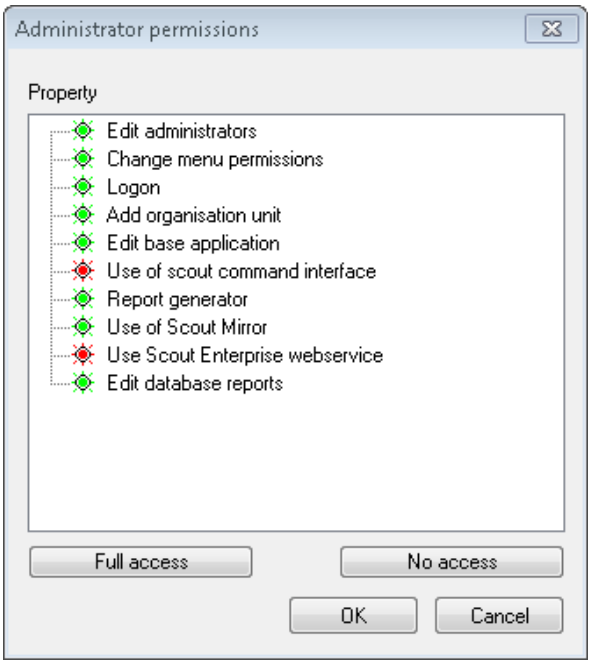
Important

For all kinds of permissions the following applies: If a permission is turned off, the relevant administrator has no longer access . For the last or the only administrator existing you cannot turn off access rights. This is to prevent being locked out of the Scout Enterprise Console.

13.4.1. Changing base permissions

1. In the Scout Enterprise Console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Base permissions...**.

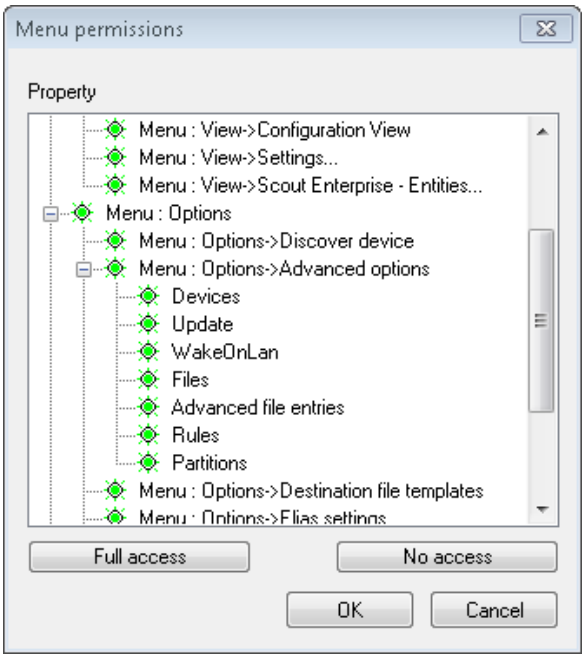
   *The **Administrator permissions > Base permissions** dialog opens.*
4. Change the relevant permissions by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.



13.4.2. Changing menu permissions

1. In the Scout Enterprise Console, click **Security > Menu permissions...**.
2. In the **Menu permissions** dialog, select the relevant administrator.
3. Click **Menu permissions...**.

   *The **Menu permissions** dialog opens.*
4. Change the relevant permissions by doubleclicking or by pressing the SPACE bar.
5. Confirm with **OK**.

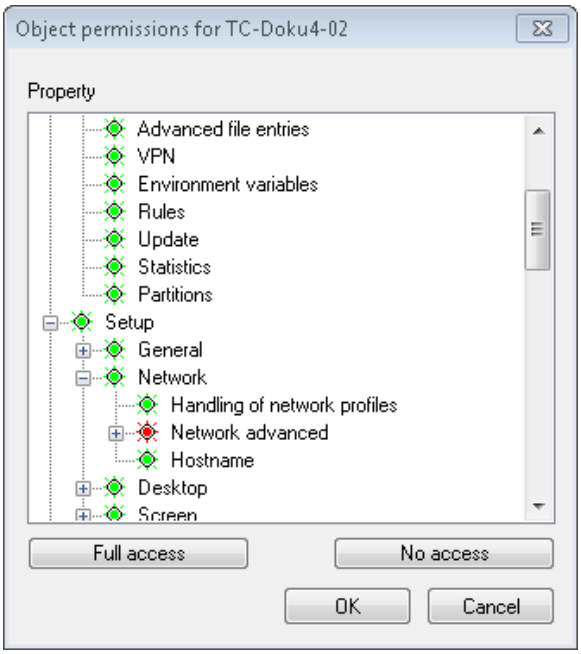


13.4.3. Changing object permissions

1. In the Scout Enterprise Console, select an OU or device.

1. Click **Security > Object permissions...**.
2. In the **Object permissions** dialog, select the relevant administrator.
3. Click **Object permissions...**.

   *The **Object permissions for ...** dialog opens.*
4. Change the relevant permissions by doubleclicking or by pressing the SPACE bar.
5. Confirm with **OK**.



13.4.4. Changing default object permissions

Default object permissions apply to all objects for which there are no specific rules defined .

1. In the Scout Enterprise Console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Default object permissions...**.

   *The **Default object permissions** dialog opens.*
4. Change the relevant permissions by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.

13.4.5. Defining a Start OU

This feature lets you deterrmine that an administrator is allowed to see only a particular start OU including its subordinate OUs.

1. In the Scout Enterprise Console, click **Security > Managing administrators**.
2. In the **Administrator permissions** dialog, select the relevant administrator.
3. Click **Set root OU ...**.

   *The **Root organisation unit** dialog opens.*
4. Check the **Use the following root organisation unit** option .
5. Select the relevant root OU.
6. Confirm with **OK**.

13.5. Pass-through Authentication

The pass-through authentication enables Single-Sign-On. Your Windows account information is used to automatically log you on to Scout Enterprise. The **Scout Enterprise log-on** window is not shown any longer.

14. Scout Enterprise Statistics Service

The Scout Enterprise Statistics Service is included in Scout Enterprise Management Suite 13.5.0 or later versions. The statistics service enables configurable status messages (keep alive messages) from the clients: Within a defined time interval the configured clients send status messages to the Scout Enterprise Statistics Service. These status messages allow to refresh the status of the relevant clients in the Scout Enterprise Console.

Note

In Scout Enterprise Management Suite version 14.4.0, the Scout Enterprise Statistics Service is not included. If, during installation, a statistics service of an earlier version is found, it will be uninstalled.

An enhanced statistics service using HTTP instead of UDP protocol is included in Scout Enterprise Management Suite 14.5.0. To use the new statistics service, update to version 14.5.0, then run the Scout Enterprise 14.5.0 installation routine once again (setup.exe), and install the **Scout Statistic service** feature by choosing **Change program**.

To use the status (keep alive) messages of the clients with the new statistics service, eLux RP version 4.9.0 is required for the clients. The UDP protocol for keep alive messages must not be active on the clients via **Advanced file entries**.
For further information, see Defining status messages.

Enhanced functionality of the Scout Enterprise Statistics Service with Scout Enterprise Management Suite version 14.5.0 and later

In addition to configurable status messages of the clients (keep alive messages) the Scout Enterprise Statistics Service also processes dynamic asset details for statistical analysis, if configured. The statistical data are stored in a separate SQL database. In the Scout Enterprise Console, you can configure if and which asset data of the devices are transferred. Analysis and display of the statistical data is done in Scout Enterprise Dashboard.

14.1. Requirements

Compatibility

See below for compatibility between different server and client versions:

- Scout Enterprise version 13.5.0 to 14.3.0 / clients running eLux RP 4.4.0 to 4.8.0 ⇒ no modification required for 'keep alive' messages
- Scout Enterprise version 13.5.0 to 14.3.0 / clients running eLux RP 4.9.0 or later ⇒ **Legacy Mode** for 'keep alive' needs to be activated*
- Scout Enterprise version 14.4.0 ⇒ 'keep alive' messages and statistics service not available
- Scout Enterprise version 14.5.0 or later / clients running eLux RP 4.4.0 to 4.8.0 ⇒ Update to eLux RP 4.9.0 required
- Scout Enterprise version 14.5.0 or later / clients running eLux RP 4.9.0 or later ⇒ no modification required
  The 'keep alive' messages and the statistical device data are transferred via HTTPS.

*To activate the **Legacy Mode** for the 'keep alive' messages, use the **Advanced file entries** feature of the Scout Enterprise Console:

File	`/setup/terminal.ini`
Section	`Statistics`
Entry	`KeepAliveLegacy`
Value	`true`

For further information, see Advanced file entries.

Hardware requirements

For a maximum number of 200.000 devices, we recommend

- 8 GB RAM
- 4 CPUs

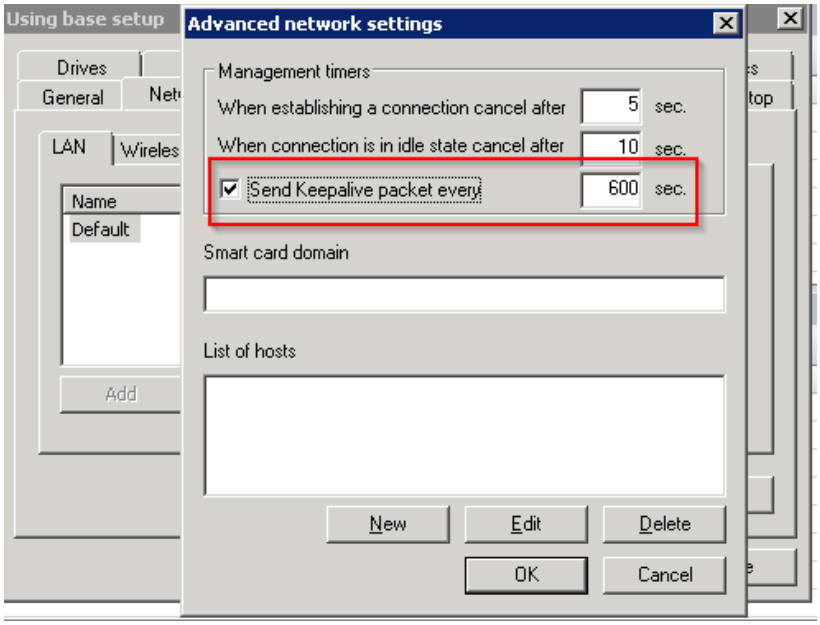
For 200.000 up to 400.000 devices, we recommend

- 16 GB RAM
- 8 CPUs or more

14.2. Defining status messages (keep alive messages)

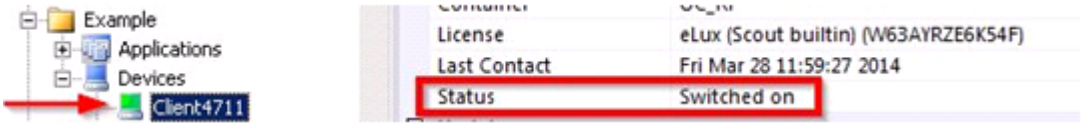
The Scout Enterprise Statistics Service helps you configure automatic updating of the status messages (keep alive messages).

1. In the Scout Enterprise Console, select **Options > Base configuration > Network > Advanced** or open, for the relevant device or OU, the **Configuration > Network > Advanced** dialog.

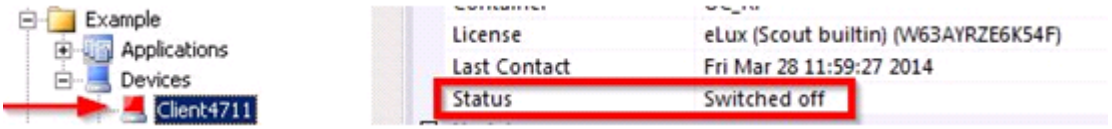


2. Select the **Send keepalive packet** option.
3. Enter a time interval in seconds.
4. Confirm with **OK**.

Within the defined time interval, the configured clients send their status messages to the statistics service. The status messages result in a refresh of the client icons in the tree view and of the relevant property:



If, however, a status message within the defined interval is missing, the device status in the Scout Enterprise Console is set to `Switched off`*:*



Note

To use the 'keep alive messages' consider the dependencies of the different Scout Enterprise and eLux versions. For further information, see Requirements.

14.3. Examples of status messages

The color of the client icons in the tree view indicates the status of the devices:

- 

  The client is properly working. Status messages are forwarded to the Scout Enterprise Statistics Service.

- 

  The client is without network connection or is switched off. Status messages cannot be forwarded to the Scout Enterprise Statistics Service.

- 

  The client is reconnected to the network. Status messages are forwarded to the Scout Enterprise Statistics Service.

For further information on client icons, see Scout Enterprise interface/Icons.

14.4. Dynamic asset details for statistical analysis

Use the **Advanced file entries** feature of the Scout Enterprise Console to configure how to transfer asset data for statistical analysis. For further information, see Advanced file entries.

File	`/setup/terminal.ini`
Section	`Statistics`
Entry	`Supervise`
Value	`usb,pci`

If you specify `usb` and/or `pci` as value, the asset data of the relevant OU are sent to the Scout Enterprise Statistics Service via HTTPS and they are saved to the Statistics database. This feature requires the Scout Enterprise Statistics Service being installed within the Scout Enterprise installation routine stating a certificate for server authentication. For further information, see Installing Scout Enterprise.

The analysis and display of the statistical data is done in the Scout Enterprise Dashboard. The Scout Enterprise Dashboard is installed with the Scout Enterprise Management Suite specifying the relevant databases (Scout Enterprise, Statistics and Dashboard).

14.5. Certificate for Scout Enterprise Statistics Service

As the eLux clients and the Scout Enterprise Statistics Service communicate via HTTPS, the installation of the Scout Enterprise Statistics Service includes the binding of an SSL certificate for server authentication to port 22124 (default).

As soon as a certificate becomes invalid, a new certificate must be bound to the port to keep the Scout Enterprise Statistics Service working. Use the `netsh.exe` tool of the Windows command-line interface of the system the Statistics Service is running on.

Note
If the computer has more than one network adapter, the certificate must be bound to all IP addresses.

Viewing the current SSL certificate bindings

1. Launch the command-line interface.
2. Use the following command:
   `netsh.exe http show sslcert`

All ports with certificate bindings are shown including the relevant information.

Deleting an SSL certificate from a port

1. Launch the command-line interface.
2. Use the `netsh.exe` tool as shown in the following example:
   ```
   netsh.exe http delete sslcert ipport=192.168.10.1:22124
   ```

   The `ipport` parameter specifies the IP address and port number.

Binding a new SSL certificate to a port

1. Launch the command-line interface.
2. Use the `netsh.exe` tool as shown in the following example:
   ```
   netsh.exe http add sslcert ipport=192.168.10.1:22124 cer-
   thash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={957ba029-e2a1-
   4a13-b426-645a5e3802e2}
   ```

   The `ipport` parameter specifies the IP address and port.

   The `certhash` parameter specifies the thumbprint of the certificate.

   The `appid` parameter is the ID of the Scout Enterprise Statistics Service and has the value shown in the example.

Viewing the thumbprints of certificates

1. Launch the Powershell. Note that the command is not supported by the normal command-line interface (cmd).
2. Use the following command depending on the certificate store:
   ```
   dir cert:\LocalMachine\My
   ```

For all certificates available in the Microsoft Management Console under Local Computer\Personal (with and without binding) the thumbprints are shown.

15. Console communication

15.1. Closing the console

1. In the Scout Enterprise Console, click **File > Console Management > Close console**.

   *The **Close console** dialog opens.*
2. Click **Refresh** to receive an up-to-date list showing all active consoles.
3. Choose **Find** to filter the list.
4. If you want the user to receive a message, check the **Inform user for** option and enter the seconds as desired.
5. If you want to give the user the chance to cancel the command, check the **Command can be canceled by the user** option .
6. Select the relevant consoles in the list.
7. Click **Close selected consoles** or **Close all consoles**, respectively.

The command is communicated to the consoles. Closing the consoles might take several minutes. The dialog waits up to 5 minutes for receiving the confirmation of all consoles. The list of all active consoles is updated continuously within the time period.

15.2. Sending messages

With the aid of this function you can send messages to other console instances. Every console instance shows a message only once. If the console instances have not been started within the whole period of validity, the message is not shown. If a user starts within the period of validity a console instance which was not yet involved in the database, the message will only be shown in the case the option **To all consoles** was activated.

1. Choose **Receiver** and which console should receive the message.
2. Choose in **time period** how long the message should be displayed.
3. Enter in **Message** the text.
4. The option **inform user...** closes the message located in the receiver console automatically after expiration of the time period stated.
5. The option **Command can be canceled by the user** allows the user to close the message in the receiver console without confirming the receipt of the message. In this case this particular message will be displayed again after a reboot of the console executed within the time of validity. If the time of validity is expired and the user selected no button the message can be seen as received.
6. Choose **Send**.
   The message will be sent to the consoles selected.

15.3. Managing consoles

As soon as a console is opened by an administrator it is registered to the Scout Enterprise database. The registered consoles are displayed in the **Manage consoles** dialog.

- Click **File > Console management > Manage consoles**.

For every console available, the logged-in user, the name of the computer as well as the log-on domain is shown. The active console is hidden. If a user has opened various console instances on its computer, the consoles are numbered serially. For example is `mfr #2` the second console instance of the user `mfr`.

You can deactivate console instances by clearing the option for the relevant instance. This console instance is no longer displayed in any of the console communication dialogs.

If you delete a console instance, all commands concerning this console are deleted and you lose part of the command history. Possibly, commands which are not yet processed are deleted. The **Delete** command is needed for deleting consoles from the memory that are not used anymore. There is no affect of this procedure concerning currently opened and active consoles.

You can check if all users are registered in the Active Directory. Unknown users can be selected and can possibly be deleted or added to the Active Directory.

By using the **Search** command you can search in each column of the list. The place holders `*` and `?` are accepted within the search text and text searches are case-insensitve. By clicking the button **X** the search field is closed.

15.4. Managing commands

Any console commands that have been run such as **Close console...** and **Send message...** can be viewed. Moreover, in the bottom list, the receiving consoles can be viewed and filtered.

Displaying commands

1. If you want to filter the commands, use one of the options: **All**, **Active**, **Inactive**, **Older than** and **Younger than**.
2. If you want to display a search field for one of the columns, click **Find**.

Changing validity of commands

- Select a command and modify date and time under **Valid until**.

Deleting commands

1. If you want to delete all commands, click **Delete all**.
2. If you want to delete a particular command, select the command and click **Delete**.

15.5. Managing reports for Scout Enterprise Dashboard

Reports that have been saved to the database are globally available and can be used by all authorized Scout Enterprise administrators (base permission: **Report Generator**) in the Scout Enterprise Report Generator. Additionally, all reports stored in the database can be used in Scout Enterprise Dashboard.

The availability of reports in Scout Enterprise Dashboard can be restricted by means of the report management in the Scout Enterprise Console: Here, you can assign reports to AD users or AD groups, or vice versa.

Requires

- The administrator policies are activated (**Security > Activate administrator policies**).
- You are provided with the menu permission for **File > Console management > Dashboard > Manage reports...**

Assigning administrators to a report

1. Click **File > Console management > Dashboard > Manage reports...**
2. Make sure that the reports are shown on the left. If required, click **Change view...**
3. In the **Reports** list, select a report, and then, under the **Administrators** list, click **Add...**

   All Scout Enterprise administrators are displayed.
4. Select one or more administrators or groups and confirm with **OK**.

   For the selected report, the authorized administrators are displayed.
5. Select the option **Use report assignment for Dashboard**.

The authorized administrators can use the selected report in Scout Enterprise Dashboard.

Assigning reports to an administrator or administrator group

1. Click **File > Console management > Dashboard > Manage reports...**
2. Make sure that the administrators are shown on the left. If required, click **Change view...**
3. In the **Administrators** list, select a user or group, and then, under the **Reports** list, click **Add...**

   All reports stored in the Scout Enterprise database are displayed.
4. Select one or more reports and confirm with **OK**.

   For the selected administrator/group, the allowed reports are displayed.
5. Select the option **Use report assignment for Dashboard**.

The selected administrator or administrator group can use the assigned reports in Scout Enterprise Dashboard.

Important

If the option **Use report assignment for Dashboard** is not selected, all reports saved to the database are available for all administrators.

16. Import/Export

All functions can either be applied via Scout Enterprise Console or SCMD-Interface. Further information to SCMD can be found at the SCMD documentation.

The export files are saved in XML format. The filename extension depends on the data category.

Data category for export/import	Filename extension
Configuration of OUs	.oustp
Configuration of devices	.devstp
Properties of OUs	.oupro
Properties of devices	.devpro
Properties of applications	.apppro
Device list	.csv
OU tree	.outree

These files can be edited by using Scout Enterprise Configuration Editor. For further information, see Scout Enterprise Configuration Editor.

16.1. Exporting

1. Select the OU you want to export data from.
2. Click **File > Export** and what you want to export.
3. Select a folder to save and apply with **OK**.

16.2. Importing

You can import device configuration data, device properties and application properties. In addition, you can import device lists and OU trees. The import file must have the relevant file name extension.

1. Select the OU you want to import data into.
2. Click **File > Import** and the data category you want to import.
3. Apply with **OK**.

17. Log files and optimizing

17.1. Log files

Scout Enterprise provides three logging options which are saved as log files on the Scout Enterprise Server.

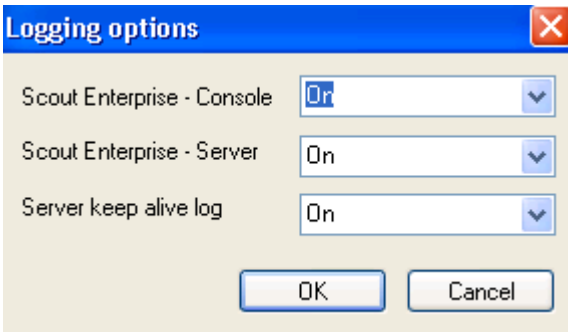
Option	Log file	Description
Scout Enterprise Console	`scout.log`	Required for debugging Path: *%USERPROFILE%*\Documents\UniCon\Scout\Console In Scout Enterprise, open the log file by clicking **View > System diagnostics > Console log**.
Scout Enterprise-Server	`eluxd.log`	Log file of the Scout Enterprise service, required for support calls Default path: *%PUBLIC%*\Documents\UniCon\Scout\Server Previous versions are renamed in `elux.-log.1...elux.log.3` etc. In the Scout Enterprise Console, open the log file by clicking **View > System diagnostic > Server log** (only if the Scout Enterprise Console is installed on the same machine as the Scout Enterprise Server).
Server keep alive log	`keepAlive.log`	Log file for keep alive-entries of the Scout Enterprise Server created every 10 minutes Default path: *%PUBLIC%*\Documents\UniCon\Scout\Server

For further information about file paths, see Paths.

Note
Click **View > System diagnostic > Server files** to open the `Unicon` server files directory in the Windows Explorer (if console and server are installed on the same machine). The `Unicon` directory contains all configuration and log files organized in their application directories.

17.1.1. Enabling logging

1. In the Scout Enterprise Console, click **Options > Logging options.**
2. For the desired options, in the list field, select `On`.



The selected log files are created by the system as described.

17.1.2. Configuring Scout Enterprise Server log

For the Scout Enterprise Server log file `eluxd.log` the Scout Enterprise Server creates more than one backup. Once a new `eluxd.log` is created, the previous version is saved to the file `eluxd.log.1`, while the old `eluxd.log.1` is saved to `eluxd.log.2` and so on.

Beginning with Scout Enterprise version 14.5, the log files continue recording when the server is restarted. Instead of a server restart, creating a new log file is triggered by the following parameters:

- log file size
- maximum number of log files

Modifying size and number of backups for the server log file

1. In the file system, in `%PUBLIC%\Documents\UniCon\Scout\Server`, open the `eluxd.ini` file for editing.
2. Add the following entries:

Section	Entry	Default	Description
[ELUXD]	`MaxLogFileSizeMB`	`100`	Maximum size of the log file in MB
[ELUXD]	`MaxLogFiles`	`10`	Maximum number of log files (`eluxd.log` plus backups)

Note
Scout Enterprise version 14.4 and earlier versions create up to three backups triggered by the server restart.

By default, the server log file and the keep alive log file are written to `%PUBLIC%\Documents\UniCon\Scout\Server`. With Scout Enterprise 14.8 and later versions, you can specify any local directory excluding network directories.

Modifying server log path

Important

Specify only a local directory that can be accessed by the Scout Enterprise Server. Do not use the UNC (Uniform Naming Convention) format.

1. In the file system, in `%PUBLIC%\Documents\UniCon\Scout\Server`, open the `eluxd.ini` file for editing.
2. Add the following entry:

Section	Entry	Example	Description
[ELUXD]	`LogFileLocation`	`c:\log`	Local directory to be used for the log files `eluxd.log` and `keepAlive.log`

When the Scout Enterprise service is restarted the log files are written to the specified directory. If the Scout Enterprise service cannot access the directory, it cannot start, and it generates an entry in the Windows Event Viewer. If the Scout Enterprise service is running and cannot write the log file, it generates an entry in the alert messages of the Scout Enterprise Console.

17.2. Optimizing

To optimize the performance and deal with high network loads you can use the following options:

- Configuring handshake options for a device, OU or all devices
- ManagerLoadBalancing to configure load distribution if you use a SQL database
- Configuring the number of ODBC connections if you use a SQL database

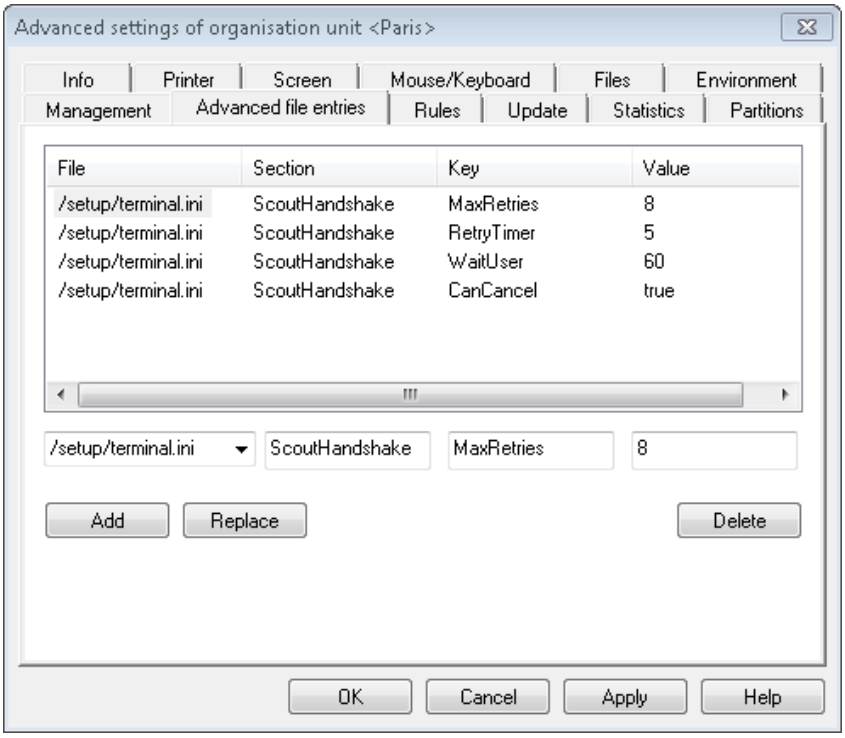
17.2.1. Optimizing with handshake

During each start-up the Thin Clients contact their Scout Enterprise Server and check for new configuration data and application definition data. If they can't access the Scout Enterprise Server, they retry to connect and synchronize according to their handshake configuration.

Activating new configuration data might require a restart of the client. Then the user is informed and has the chance to suppress restarting.

Handshake parameters can be set in the `terminal.ini` file of the client by using the **Advanced file entries** feature. For further information, see Advanced file entries.

Handshake can be configured for the entire organization or for a particular OU or device.



The values shown in the figure above are examples and can be modified. By default, handshake is not configured.

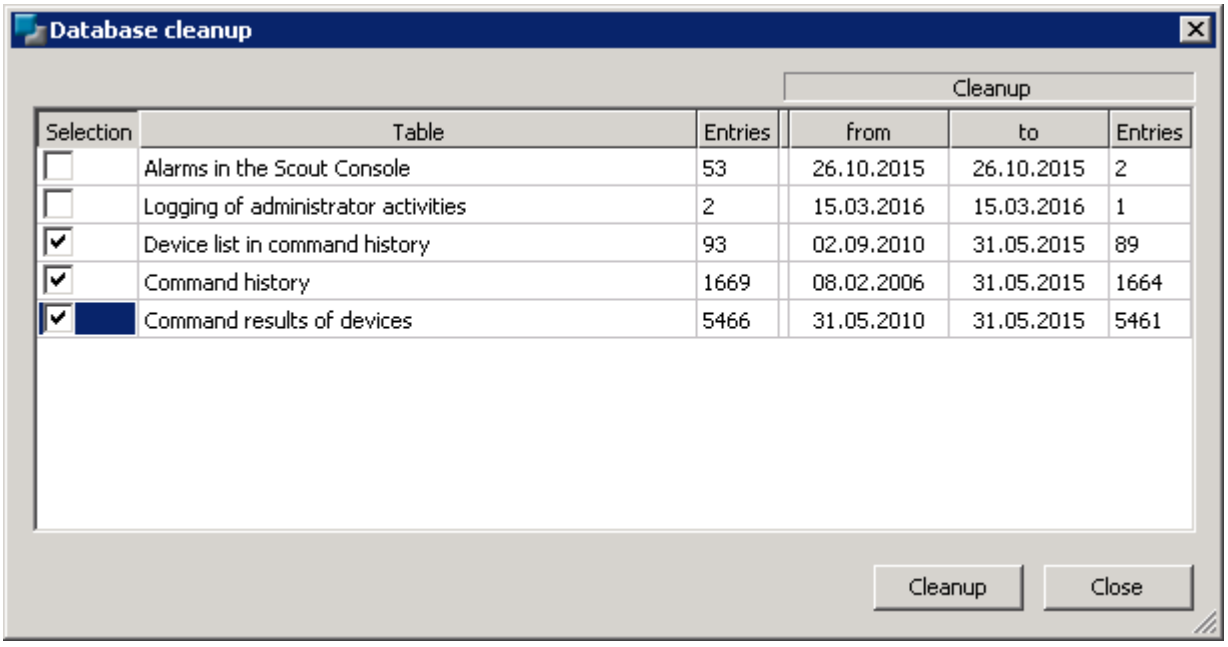
The section `ScoutHandshake` provides the following configurable parameters:

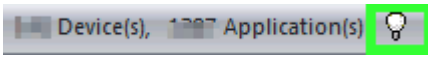
Parameter	Description
MaxRetries	Number of connection attempts The value `0` deactivates handshake.
RetryTimer	Period of time in seconds until next connection attempt (start value) After each attempt the interval is doubled (+/- random value). Example: Having defined `8` connection retries and a **RetryTimer** start value of `5` seconds, the 8. connection attempt is carried out after about 21 minutes.
WaitUser	Waiting time before client restarts to give the user the chance to close applications or log off.
CanCancel	Defines, if the user is allowed to suppress a client restart (`true` | `false`).

17.2.2. Database cleanup

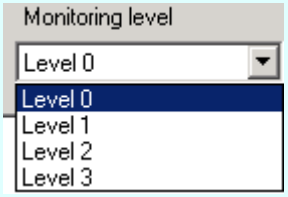
Scout Enterprise stores huge amounts of data concerning various processes such as any performed update commands. To purge the Scout Enterprise database tables, authorized administrators can delete database entries from particular tables for a specified period of time[1].

The relevant tables are listed in the **Database cleanup** dialog, each table providing the total number of entries and the creation date of the first entry. The administrator can modify only the fields **Selection** and **to**.



Alerts in the Scout Enterprise Console	Alert messages (Error, Warning, Info), can be viewed by double-clicking the lamp icon on the Scout Enterprise status bar	

[1] For LocalDB, this feature is available with Scout Enterprise 14.9 and later versions

Logging of administrator activities	Log file entries about the activities performed by an administrator according to the monitor level configured in **Security > Manage administrators...** (Table `Monitor` of the Scout Enterprise database) 
Device list in command history	History data of commands shown in **View > Command history...** of the Scout Enterprise Console (entries for particular devices)
Command history	History data of commands shown in **View > Command history...** of the Scout Enterprise Console (entries for OUs)
Command results of devices	Result reporting of commands performed on the devices (Update, Delivery, user-defined command). The log data can be viewed in the Scout Enterprise Console in the **Properties** window or by using the context menu of a device **Commands > Update/Delivery/Command**.For further information, see Update and delivery log.

Performing a database cleanup

1. Select **View > System diagnostics > Database cleanup...**
2. In the **Database cleanup** dialog, for the relevant table, in the **to** field, specify a date, that indicates the end point of the time span for the entries to be deleted (all entries up to and including this date are deleted).

   *The **Entries** column at the right shows the number of entries to be deleted.*
3. Click into the field of the `Selection` column at the left to activate this table for cleanup.

   A check mark indicates that entries from this table are intended for cleanup.
4. Click **Cleanup**.

   A message shows the total of all entries in all tables which are intended for cleanup.
5. Confirm with **Yes**.

From the selected tables, all entries up to the specified dates are deleted.

Note
Before you can delete command history entries, you are required to delete the according device list entries.

18. Appendix

18.1. Time server

To synchronize computer clocks and provide accurate time throughout the network, we recommend to use a time server. The user then can synchronize time online in the eLux control panel.

The time server must comply with the Network Time Protocol (RFC 1305) or the Simple Network Time Protocol, a simplified form of NTP. Microsoft Windows operating systems include the **W32Time** service which communicates via SNTP in older versions such as Windows 2000, and uses NTP in later versions. The time service is started automatically.

The service runs on port 123 using the UDP protocol.

For further information on the Windows Time Service, see the Microsoft documentation.

For further information on NTP, see http://www.ntp.org.

18.2. IP ports

eLux

Port	Type	Description	How to deactivate	In/Out
	ESP	VPN (data transfer)	Uninstall package `VPN System`	Incoming
	ESP	VPN (data transfer)	Uninstall package `VPN System`	Outgoing
123	UDP	Windows Time server (NTP)	Do not configure a time server (**Setup > Desktop**)	Incoming
123	UDP	Windows Time server (NTP)	Do not configure a time server (**Setup > Desktop**)	Outgoing
21	TCP	Update via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	3270, 5250, 97801 emulations and telnet sessions		Outgoing
53	TCP	DNS server (Windows)		Outgoing
53	UDP	DNS server		Outgoing
67	UDP	DHCP server	Configure a local IP address (**Setup > network**)	Outgoing
68	UDP	DHCP client (or: BootP client)	Configure a local IP address (**Setup > network**)	Incoming

Port	Type	Description	How to deactivate	In/Out
69	UDP	TFTP server (only used during PXE recovery)		Outgoing
80	TCP	Firmware update by using HTTP (and proxy port, if used)		Outgoing
111	UDP	Port mapper – drive access on NFS servers Works with NFSD drive access (port 2049) and mountd (random)	Uninstall FPM `Automount` in `Network Drive Share` package	Outgoing
111	TCP	Port mapper – RPC internal use only Works with lockd (random)	Uninstall FPM `Automount` in `Network Drive Share` package	Incoming
139	TCP	SMB drive mapping, (NetBIOS) and SMB user authentication (CIFS)	Uninstall FPM `Automount` in `Network Drive Share` package and `User authorisation modules` package	Outgoing
139	UDP	SMB drive mapping (NetBIOS) and SMB user authentication (CIFS)	Uninstall FPM `Automount` in `Network Drive Share` package and `User authorisation modules` package	Outgoing
161	UDP	SNMP	Uninstall `SNMP Environment` package	Incoming
161	UDP	SNMP	Uninstall `SNMP Environment` package	Outgoing
162	UDP	SNMPTRAP	Uninstall `SNMP Environment` package	Outgoing
177	UDP	XCMCP protocol		Outgoing
389	TCP	LDAP user authentication and AD authentication with user variables		Outgoing
443	HTTPS	VPN (connecting)	Uninstall package `VPN System`	Incoming
443	HTTPS	VPN (connecting)	Uninstall package `VPN System`	Outgoing
443	HTTPS	Firmware update by using HTTPS		Outgoing
514	TCP	Shell, X11 applications		Outgoing
515	TCP	Printing via LPD	Uninstall package `Print environment (CUPS)`	Outgoing

Port	Type	Description	How to deactivate	In/Out
515	TCP	Printing via LPD	Uninstall package `Print environment (CUPS)`	Incoming
631	TCP	CUPS (IPP) print client	Uninstall package `Print environment (CUPS)`	Outgoing
631	UDP	CUPS (IPP) print client	Uninstall package `Print environment (CUPS)`	Outgoing
2049	UDP	NFSD drive access NFS	Uninstall FPM `NFS Support` in `Network Drive Share` package	Outgoing
5900	TCP	Mirroring eLux desktop	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Incoming
5901	TCP	Mirroring first XDMCP session	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Incoming
5902	TCP	Mirroring second XDMCP session	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Incoming
6000	TCP	Remote X11 application	In **Setup > Security**, clear **Allow remote X11 clients** option	Incoming
6001	TCP	first XDMCP session		Incoming
6002	TCP	second XDMCP session		Incoming
7100	TCP	Font server can be assigned in eLux control panel (**Setup > Screen > Advanced**		Outgoing
20000	UDP	Wake On LAN		Incoming
20000	UDP	Wake On LAN		Outgoing
22123	TCP	Scout Enterprise Manager (secure)		Incoming
22123	TCP	Scout Enterprise Manager (secure)		Outgoing
22124	UDP	Scout Enterprise Statistics		Outgoing

Port	Type	Description	How to deactivate	In/Out
9100	TCP	Printing directly to parallel port can be assigned in eLux control panel (**Setup > Printer**)	In **Setup > Printer**, clear the **TCP direct print** option	Incoming
9101	TCP	Printing directly to USB port can be assigned in eLux control panel (**Setup > Printer**	In **Setup > Printer**, clear the **TCP direct print** option	Outgoing

Scout Enterprise Server

Port	Type	Description	In/Out
1433	TCP	MS SQL Server	Incoming
1433	TCP	MS SQL Server	Outgoing
1434	UDP	MS SQL Server (Browser service)	Incoming
1434	UDP	MS SQL Server (Browser service)	Outgoing
22123	TCP	Scout Enterprise Manager (secure)	Incoming
22123	TCP	Scout Enterprise Manager (secure)	Outgoing
22124	UDP	Scout Enterprise Statistics	Incoming

Scout Enterprise Console

Port	Type	Description	How to deactivate	In/Out
1433	TCP	MS SQL Server		Outgoing
1434	UDP	MS SQL Server (Browser service)		Outgoing
5900	TCP	Mirroring the eLux desktop	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Outgoing
5901	TCP	Mirroring of the first XDMCP session	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Outgoing

Port	Type	Description	How to deactivate	In/Out
5902	TCP	Mirroring of the second XDMCP session	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Outgoing

Scout Enterprise Dashboard

Scout Enterprise Dashboard can be installed with HTTP or HTTPS. For both protocols, a port other than the default port can be specified.

Port	Typ	Description	How to deactivate	In/Out
80	HTTP	Dashboard-service / web server		Incoming
443	HTTPS	Dashboard-service / web server		Incoming
1433	TCP	MS SQL Server		Outgoing
1434	UDP	MS SQL Server (Browser service)		Outgoing
5901	TCP	Mirroring the eLux desktop	In **Setup > Security**, clear **Enable mirroring** option or uninstall package `Mirror eLux Desktop`	Outgoing

18.3. SNMP

SNMP (Simple Network Management Protocol) is a network protocol which allows querying status information and other management data and which allows defining configuration parameters.

The configuration of

- SNMPv2 for eLux RP4 is based on the software package: `snmp-5.6.1.1-2`
- SNMPv3 for eLux RP5 is based on the software package: `snmp-5.5.2.1-1`

1. Download from **www.myelux.com eLux Software Packages > eLux RP Container > Released Packages > Add-On > snmp-5.x.x.x-x**.

   Note
   The command line program **snmpget** is not integrated in the software package. For the query of SNMP status information, please use a software provided by a third party supplier..

2. Choose from two configuration methods:

   A) Transfer the configuration file `snmpd.conf` to

   `/setup/snmpd.conf` for eLux RP4 bzw.
   `/setup/snmp/snmpd.conf` for eLux RP5
   by using the Scout Enterprise feature Files

   Or:

   B) Use the Advanced file entries feature of Scout Enterprise

   Example:

File	`/setup/terminal.ini`
Section	`SNMPD`
Entry	`rocommunity`
Value	`secret`

   Note
   If the file `/setup/snmpd.conf` or `/setup/snmp/snmpd.conf`, respectively, does exist, configuration method A is preferred.
   If the file does not exist, the section [`snmpd`] of the `terminal.ini` file is evaluated.
   For eLux RP4 only: If the [`snmpd`] section does not exist, the read only community `public` is created. Use the local shell (XTERM) for testing:
   `snmpget -v 2c -c public <ip-address> SNMPv2-MIB::sysName.`

3. In the section [SNMPD], you can enter more of the so called SNMPD Configuration Directives, for example `syscontact` or `syslocation` in order to modify the configuration.
   The Configuration Directives control:
   - the access rights to the SNMP agent.
   - the information that is supplied by the SNMP agent.
   - the active monitoring of the local system.
   - the extension of the SNMP agent's functionality.
4. For debugging purposes, you can specify further commands in the [`SNMP`] section . These commands are called SNMP Configuration Directives. Again, by using the **Advanced file entries**, you can, for example, set the entry `doDebugging` in the section [`SNMP`] of the file `terminal.ini` to the value `1`.

18.4. SNMPD and SNMP Configuration Directives

The following table refers to the software package **snmp-5.6.1.1-2** for eLux.
For further information on using SNMP with eLux, see SNMP.

For further information on SNMP commands, see http://www.net-snmp.org.

Application	Command
authtrapenable	1 | 2 (1 = enable, 2 = disable)
trapsink	host [community] [port]
trap2sink	host [community] [port]
informsink	host [community] [port]
trapsess	[snmpcmdargs] host
trapcommunity	community-string
agentuser	agentuser
agentgroup	groupid
agentaddress	SNMP bind address
syslocation	location
syscontact	contact-name
sysservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1|v2c|usm security
access	name context model level prefx read write notify
view	name type subtree [mask]
rwcommunity	community [default|hostname|network/bits] [oid]
rocommunity	community [default|hostname|network/bits] [oid]
rwuser	user [noauth|auth|priv] [oid]
rouser	user [noauth|auth|priv] [oid]
swap	min-avail
proc	process-name [max-num] [min-num]
procfix	process-name program [arguments...]
pass	miboid command

Application	Command
pass_persist	miboid program
disk	path [minspace | minpercent%]
load	max1 [max5] [max15]
exec	[miboid] name program arguments
sh	[miboid] name program-or-script arguments
execfix	exec-or-sh-name program [arguments...]
file	file [maxsize]
dlmod	module-name module-path
proxy	[snmpcmd args] host oid [remoteoid]
createUser	username (MD5|SHA) passphrase [DES] [passphrase]
master	pecify 'agentx' for AgentX support
engineID	string
engineIDType	num
engineIDNic	string

SNMP Configuration Directives

Application	Command
doDebugging	(1|0)
debugTokens	token[,token...]
logTimestamp	(1|yes|true|0|no|false)
mibdirs	[mib-dirs|+mib-dirs]
mibs	[mib-tokens|+mib-tokens]
mibfile	mibfile-to-read
showMibErrors	(1|yes|true|0|no|false)
strictCommentTerm	(1|yes|true|0|no|false)
mibAllowUnderline	(1|yes|true|0|no|false)
mibWarningLevel	integerValue
mibReplaceWithLatest	(1|yes|true|0|no|false)
printNumericEnums	1|yes|true|0|no|false)
printNumericOids	1|yes|true|0|no|false)
escapeQuotes	(1|yes|true|0|no|false)

Application	Command
dontBreakdownOids	(1|yes|true|0|no|false)
quickPrinting	(1|yes|true|0|no|false)
numericTimeticks	(1|yes|true|0|no|false)
suffixPrinting	integerValue
extendedIndex	(1|yes|true|0|no|false)
printHexText	(1|yes|true|0|no|false)
dumpPacket	(1|yes|true|0|no|false)
reverseEncodeBER	(1|yes|true|0|no|false)
defaultPort	integerValue
defCommunity	string
noTokenWarnings	(1|yes|true|0|no|false)
noRangeCheck	(1|yes|true|0|no|false)
defSecurityName	string
defContext	string
defPassphrase	string
defAuthPassphrase	string
defPrivPassphrase	string
defVersion	1|2c|3
defAuthType	MD5|SHA
defPrivType	DES (currently the only possible value)
defSecurityLevel	noAuthNoPriv|authNoPriv|authPriv