

Scout Enterprise Management Suite

Administrator's Guide

How to manage a client infrastructure through Scout Console 15

Last edited: 2021-12-22

0. Legal information	5
1. Representation	6
2. Overview	7
2.1. Features of the Scout Enterprise Management Suite	7
2.2. Communication between Thin Client and Scout Server	9
2.3. Installation	9
2.4. Keyboard shortcuts	10
3. Interface of the Scout Console	11
3.1. Organizational structure	11
3.2. Icons in the tree view	12
3.3. Windows	12
3.4. Status bar	17
3.5. View settings	17
3.6. Changing language	18
3.7. Searching for devices, OUs or applications	18
3.8. Moving and copying elements	21
3.9. Switching OU to top-level	22
4. Device management	23
4.1. Self-registration of devices	23
4.2. DHCP configuration	25
4.3. Searching for devices (Discovery)	29
4.4. Reserving device profiles	31

4.5. Device names	31
4.6. Secure device management with Scout Enterprise	33
4.7. OU filter	34
4.8. Dynamic Client Groups	41
4.9. Client relocation between Scout Servers	46
5. Device configuration	53
5.1. Concept	53
5.2. Configuration method	60
5.3. Evaluating configuration data	62
5.4. FollowMe Desktop	63
5.5. General tab	67
5.6. Network tab	69
5.7. Desktop tab	84
5.8. Display tab	92
5.9. Mouse/Keyboard tab	100
5.10. Firmware tab	103
5.11. Security tab	116
5.12. User authentication	119
5.13. Multimedia tab	130
5.14. Drives tab	132
5.15. Printer tab	134
5.16. Hardware tab	140
5.17. Diagnostics tab	146
5.18. Power management tab	146
5.19. Troubleshooting device configuration	153
6. Advanced device configuration and Advanced options	156
6.1. Devices	157
6.2. Update/Delivery	158
6.3. Management	158
6.4. Predefined commands	159
6.5. Predefined IDFs and containers	159
6.6. Wake On LAN	161
6.7. VPN	162
6.8. Files configured for transfer	165
6.9. Advanced file entries	168
6.10. Rules	170
6.11. Environment variables	172
6.12. TPM 2.0 support	172
7. Defining applications	176
7.1. General	176
7.2. Connecting to a Citrix farm	186
7.3. RDP	210

7.4. Virtual Desktop	215
7.5. Browser	218
7.6. Local and user-defined applications	226
7.7. Emulation	230
7.8. Applications in kiosk mode	232
7.9. Local web sites	246
7.10. Troubleshooting application definition	248
7.11. Third party software	250
8. Client remote management by commands	253
8.1. Available commands	253
8.2. Executing commands	255
8.3. Scheduling commands	256
8.4. Command results and update information	257
8.5. Command history	258
8.6. Factory reset command	260
8.7. Creating predefined commands	262
8.8. Defining templates for standard commands	264
8.9. eLux Command Scheduler	266
9. Remote maintenance	271
9.1. Device identifier for support	271
9.2. Mirroring	271
9.3. Device diagnostics	274
10. Firmware Update	280
10.1. Requirements	281
10.2. Access to applied images	281
10.3. Planning and performing firmware updates	284
10.4. User information before update	289
10.5. Delivering software in advance	291
10.6. Dynamic proxy client	294
10.7. Troubleshooting firmware update	297
11. Passwords	298
11.1. Local device password	298
11.2. Scout Console password	301
12. Managing administrators	302
12.1. Activating administrator policies	302
12.2. Adding administrators	302
12.3. Deleting administrators	303
12.4. Administrator policy	304
12.5. Viewing administrator activities	309
12.6. Pass-through authentication	310
12.7. Maintenance windows	311

13. Scout Statistics Service	313
13.1. Defining status messages (keep alive messages)	313
13.2. Examples of status messages	314
13.3. Dynamic asset details for statistical analysis	315
14. Console communication	316
14.1. Closing the console	316
14.2. Sending messages	316
14.3. Managing consoles	317
14.4. Managing commands	317
14.5. Managing reports for Scout Dashboard	318
15. Import/Export	319
15.1. Exporting	319
15.2. Importing	319
16. Log files and optimizing	320
16.1. Log files	320
16.2. Optimizing	325
17. Appendix	329
17.1. Program and file directories	329
17.2. eLux partitions	329
17.3. IP ports	331
17.4. SNMP	336

0. Legal information

© 2021 Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH

This document is copyrighted. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, without our express consent. Information in this document is subject to change without notice. We disclaim all liability regarding correctness, completeness and topicality of the information contained herein and any errors or damage resulting from the information provided.

eLux[®] and Scout Enterprise Management Suite[®] are registered trademarks of Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH in the European Union, GB and the United States.

ScoutaaS[®] is a registered trademark of Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH in the European Union, GB, the United States and Japan.

All other product names are registered trademarks of their relevant owners.

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

1. 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 <code>Courier New</code> . Also, file names and path names are displayed in <code>Courier New</code> .
STRG	Keys to be pressed are displayed in CAPITAL LETTERS.
<Placeholder>	Placeholders in instructions and user input are displayed in <i>italics</i> 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 <i>italics</i> .

Abbreviations and acronyms

Abbreviation	Description
AD	Active Directory , directory service of Microsoft Windows Server
EBKGUI	Interface of the eLux Builder Kit (component of Scout Enterprise)
EPM	eLux package module (. <code>epm</code> , software package)
FPM	Feature package module (. <code>fpm</code> , part of a software package)
FQDN	Fully qualified domain name
GB	Gigabyte
GHz	Gigahertz (processing speed)
HDD	Hard disk drive (flash memory)
IDF	Image Definition File (. <code>idf</code>)
IIS	Internet Information Services: Microsoft Web server
MB	Megabyte
OU	Organizational unit Unit or group within the organizational structure
VPN	Virtual Private Network

2. Overview

2.1. Features of the 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 devices can be managed by using basic Scout management features.

Scout Enterprise Management Suite consists of several components. Most of the components listed below are included in the standard installation but can be optionally excluded when choosing custom installation.

Component	Description	Installation
Scout Server	The service controls and manages eLux devices as well as Windows devices on which Scout Agent for Windows has been installed.	Scout Enterprise.exe
Scout Console	User interface for the management of eLux devices and for the management of Windows-based devices on which Scout Agent for Windows has been installed Server communication only via database Multiple consoles can be managed with one Scout database.	Scout Enterprise.exe
Recovery service	Customized TFTP service to realize a PXE recovery environment for eLux endpoints	Scout Enterprise.exe
ELIAS	Legacy dialog program eLux Image Administration Service (ELIAS) for creating individual image definition files (.idf) for modular firmware updates of the eLux devices. The legacy ELIAS will be replaced by ELIAS 18.	Scout Enterprise.exe ¹
ELIAS 18	New web-based platform-independent ELIAS application for creating individual image definition files (.idf)	separate (EliasInstaller.exe)
Scout Report Generator	Tool for creating freely definable reports across all currently existing devices, applications and OUs in the Scout Console	Scout Enterprise.exe
Scout Statistics Service	Service for the evaluation of device status information and dynamic asset details	Scout Enterprise.exe

¹for Scout Enterprise Management Suite Version 15.7 and later versions, the legacy ELIAS is no longer included in the standard installation. To install the feature, select **User-defined**.

Component	Description	Installation
Scout Dashboard	Web-based console for the management of eLux devices and for the management of Windows-based devices on which Scout Agent for Windows has been installed	Scout Enterprise.exe
Web API ¹	Application programming interface for the management of eLux devices and for the management of Windows-based devices on which Scout Agent for Windows has been installed	Scout Enterprise.exe
Scout Command Interface	Command line interface for Scout commands	Scout Enterprise.exe
Scout Database Connection Editor	Tool for modifying database connection settings of the Scout Server and Scout Console	Scout Enterprise.exe
Scout Cloud Gateway	Cloud gateway with VPN backend for convenient connection of devices from the Internet to a Scout infrastructure	separate
Scout Agent for Windows	Service providing an interface for Windows-based devices to be managed through Scout Enterprise Management Suite	separate

The features are described in the following guides:

- Scout Enterprise Management Suite:
Configuration, control and management of the client devices using the Scout Console
Scout Statistics Service
- ELIAS
- ELIAS 18
- Scout Report Generator
- Scout Command Interface
- Scout Dashboard
- Scout Cloud Gateway

Recovery procedures for eLux devices are described in the **eLux Recovery procedures** short guide.



Note

To compose and use your own image files, in addition to the Scout Enterprise Management Suite installation, you need an eLux container for the software packages.

For further information, see [Installing a container](#).

¹for Scout Enterprise Management Suite 15.0 and later versions

2.2. Communication between Thin Client and Scout Server



Note

The certificate-based management protocol ensures secure communication between Scout Server and clients.¹ For further information, see [Certificate-based management protocol](#) in the **Installation** guide.

During system start the client devices connect to their Scout 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 Server. The Scout Server has no updated configuration data. Client continues booting with its configuration.
- Client accesses the Scout Server. The Scout 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 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 Server and Thin Client. During shutdown, the client reports its current status to the Scout Server (except for VPN connections).

2.3. Installation

All contents relating to installation and setup are covered by the **Installation** guide. For further information, see [Installing Scout Enterprise Management Suite](#).

¹for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

2.4. Keyboard shortcuts

Keys	Selected element	Description
CTRL+SHIFT+INSERT	Individual OU	Opens the Advanced device configuration ¹ 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

¹formerly **Advanced settings**

3. Interface of the Scout Console

3.1. Organizational structure

The main window of the Scout 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](#).

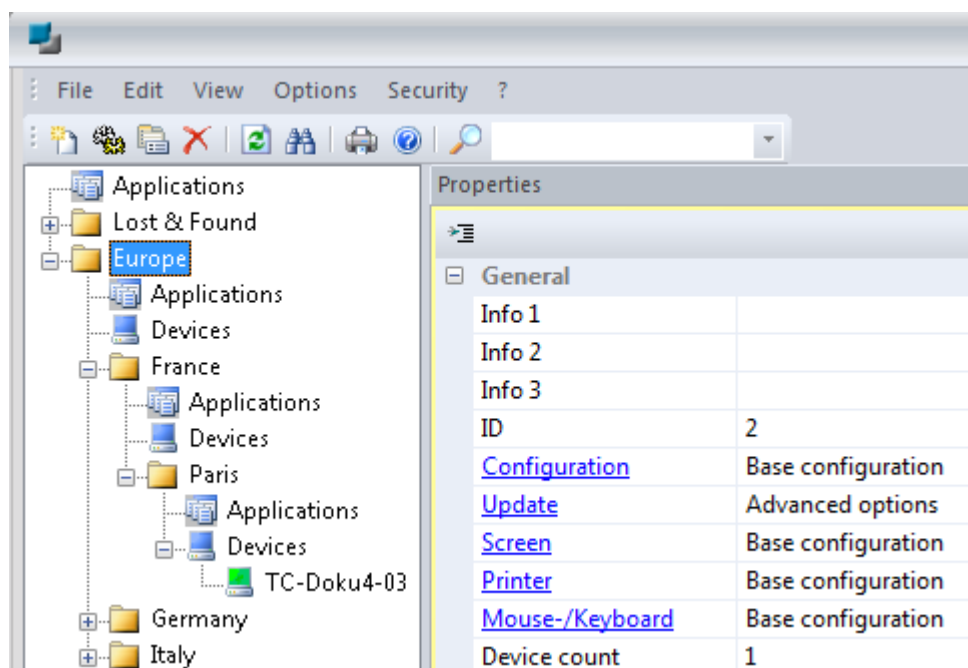
To each organizational unit - hereafter referred to as OU - you can add applications, devices and other OUs. Each OU can contain subordinate OUs, applications and devices.

By default, inheritance is active. Application definitions and device configuration data are inherited by subordinate OUs and devices.

If you add a new device to an OU, it will receive all application definitions and device 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 [Device configuration/Concept](#).



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

¹for Scout Enterprise Management Suite 15.0 and later versions









²for Scout Enterprise Management Suite 15.0 and later versions

Adding a new OU

1. For the relevant OU, on the context menu, click **Add > Organization unit...**
*The **Advanced device configuration**¹ 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 contains the folders  **Applications** and  **Devices**.

3.2. Icons in the tree view


Icon	Description
	Organization unit (OU)
	Applications
	Device, not connected to Scout Enterprise yet (Example: Device import)
	Device, running and ready for operation
	Device, switched off or not available
	Device, desktop is initializing or the log-on screen is shown
	Device, firmware update is running
	Device, missing management license

3.3. Windows

Click **View > Windows** to show further windows next to the organizational structure:

Window	Description
Properties	Properties of the selected application, OU or device For further information, see Properties .


¹formerly **Advanced settings**

Window	Description
Assets (only for devices)	<p>Hardware information of the selected device</p> <p>Is shown as a tab of the Properties window</p> <p>For further information, see Hardware information.</p>
Dynamic Client Groups	Shows the defined Dynamic Client Groups (list view)
Independent configurations ¹	<p>Shows OUs and devices that do not use the parent device configuration (list view)</p> <p>For further information, see Blocking inheritance - independent configuration</p>
Compare configurations ²	Shows differences in the device configuration between devices or OUs
OU devices/applications	<p>Devices or applications of an OU view without icons (list view)</p> <p>Double-clicking on a device shows the corresponding device in the tree view. This feature can be disabled, see below.</p>
All devices	<p>Shows all devices without icons (list view)</p> <p>The device data are only loaded from the Scout Enterprise database when you click the  Refresh button. This is meant to prevent unintentional loading of huge amounts of data.</p> <p>The context menu offers the same functions as in the tree structure. Several functions such as commands can be applied to multiple devices. To do so, select the devices by pressing CTRL or SHIFT</p> <p>Double-clicking on a device shows the corresponding device in the tree view. This feature can be disabled, see below.</p> <p>To search window content, use the Search field of the toolbar, 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.</p>

Sorting columns

- ▶ Click a column header to sort rows.

Showing/Hiding properties

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

¹formerly setups

²formerly setups

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
```

3.3.1. Properties

The properties of the selected application, OU or device are displayed.

Many properties come from the device configuration (devices and OUs) and application definition (applications) and are updated with each configuration update. For further information, see [Configuration method](#).

Some device properties come from the Scout Server and are updated dynamically.

Date and time fields are shown according to the international standard ISO 8601.



Note

By default, not all fields are displayed. To show or hide fields, click the  icon.

Device properties

Examples:

Option	Description
Name	Host name of the device
Configuration	Origin of the device configuration, mostly inherited from parent instance
Manager	IP address of the Scout Server the device is assigned to
Info1-3	The Info fields are shown on the device in the Configuration panel under Information and can be enabled for users for editing (user rights). They are already provided in the First Configuration Wizard.
OS version	Version of client operating system
Container	eLux container configured for the device in the firmware device configuration
Update time	Time stamp of the last firmware update
	For further information, see Command results and update information

Option	Description
Last contact	Time stamp of the last contact between server and device The field is not only updated on a device restart but also on each successful connection set-up from the server to the device.
Status	Example: <code>Switched on</code> The status of a device is triggered by the 'keep alive' mechanism and by active status messages of the device on start, shutdown, logoff, performing updates and more.
Status time	Time stamp of the last status refresh
Primary MAC address	Device address of the hardware (MAC=Media Access Control)
Simple device identifier	Temporary device identifier users may request for support cases
Client identifier ¹	Globally unique identifier for the device or eLux Portable USB stick
Partitions	The system, setup and update partitions are displayed with their respective sizes.

OU properties

Examples:

Option	Description
OU	Shows the ID of an OU In addition to the decimal value, you can show the hexadecimal value. This requires a new registry entry: Key: <code>HKEY_CURRENT_USER\Software\UniCon\Scout\Settings</code> Value name: <code>DisplayHexOUID</code> Value type: <code>DWORD: 32</code> Value data: <code>1</code>
Device count	Number of devices in the OU and the subordinate OUs

Quick links in the Properties window of devices and OUs

- ▶ Make use of the links shown in blue to quickly browse the relevant configuration and information in each context. Double-click the links:

Selected element	Option	Description
Device	Configuration	Opens the relevant Device configuration

¹for Scout Enterprise Management Suite 15.10 and later versions

Selected element	Option	Description
Device	Image	Opens ELIAS with the image configured for this device in the relevant container The connection to ELIAS is made with the data configured in the ELIAS settings of the Scout Console. For further information, see "Access to applied images" on page 281
Device	Update State	Double-click or ... opens the Update-Info for the device providing information on performed updates. For further information, see Command results and update information
OU	Configuration	Opens the relevant Device configuration
OU	Update	Opens the relevant Update settings in the Advanced device configuration or Advanced options .
OU	Screen, Printer, Mouse/Keyboard	Opens the relevant configuration (Device configuration or Advanced device configuration) for Screen, Printer or Mouse/Keyboard.

3.3.2. Hardware information

For the selected device, in the **Properties** window, on the **Assets** tab, device-specific hardware information is shown:

- Hardware information of the device
- Hardware information of connected devices such as USB devices and monitors



Note

By default, not all fields are displayed. To show or hide fields, click the  icon.

Hardware information of the device

Examples:

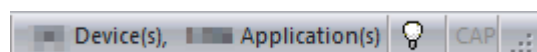
Option	Description
Device type	Product details provided by the hardware manufacturer (character string)
Main memory	Main memory size
Flash memory	Flash memory type
Flash size	Size of the flash memory

Hardware information of connected devices

Examples for a USB device:

Option	Description
Product	Type of USB device
Vendor	Vendor name
Serial number	Serial number of the USB device
Revision number ¹	Firmware version of the USB device

3.4. Status bar



On the right of the status bar, the total number of devices and applications are displayed. When you perform large operations such as importing, moving, exporting or deleting a large number of devices, they are also displayed on the status bar.²

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

3.5. View settings

Some preferences regarding the view can be set via the menu **View > Settings**:

Option	Description
Refresh display of devices	
In the tree view	Time span in seconds for periodically refreshing the display of devices, OUs and applications in the tree view
In the list view	Time span in seconds for periodically refreshing the display of devices, OUs and applications in the list view
Show new devices automatically in tree view ³	New devices after onboarding are automatically added to the tree view (disabled by default).
Status bar/ Refresh totals	Time span in seconds for periodically refreshing the number of all devices and applications across the infrastructure
On console start / Show recently used element	After the console is restarted, the last selected item in the tree view is highlighted.

¹from Scout Enterprise 15.8

²from Scout 15 2110

³from Scout Enterprise 15.8

Option	Description
Show confirmation messages / Before view is refreshed	After you press F5 or click View > Refresh , the system prompts you before refreshing the view.
Check independent configurations	When you modify a device configuration, all subordinate independent configurations are checked. You then receive a list of the relevant parameters and can conveniently determine whether and to which instances the modifications are to be transferred. For further information, see Blocking inheritance - independent device configuration .
Verbose level	For level 1, a confirmation message is shown before commands are executed, indicating the number of affected devices.

3.6. Changing language

The console is started with the display language you have chosen for the Scout Enterprise Management Suite installation. You can change the display language at any time: gewählt haben. The language setting refers to the display of interface elements and can be changed at any time:

1. Click **View > Select language** and choose your language.
2. Restart the Scout Console.

The console is started with the selected language.

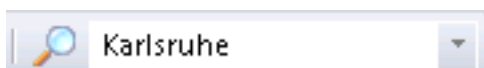
Important Individual window layouts will not be restored after the language change.

3.7. Searching for devices, OUs or applications

Quick search

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

If configured accordingly, 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.



Note

The search is performed using the search parameters set in the **Find** dialog.

Quick search in the All devices window

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

If configured accordingly, 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.



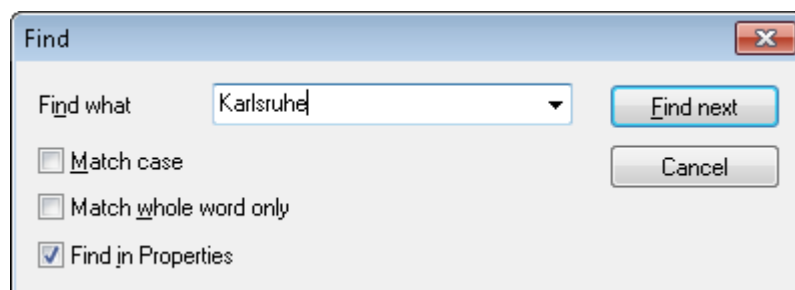
Note

You can also search the **All devices** window when it does not have focus: Press SHIFT+RETURN to start searching for the specified object. 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 accordingly, 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 the 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.

Advanced search view

The **Advanced search** window¹ provides further options that allow you to search for devices including multiple filter criteria and wildcard search. You can perform commands and notifications on search results.

1. Show the **Advanced search** window. To do so, click **View > Window > Advanced search**.

Some fields are shown as columns including a search field.

2. To show or hide fields as columns, click the  button.

*The **Adjust** dialog with all available fields opens. Configure which fields to show.*

Fields that cannot be used for a search contain the entry N/A.

3. To change the order of the columns, also use the **Adjust** dialog.

The column order is relevant if you want to define multiple filter criteria.

4. In the desired column, in the search field, enter a search term. To replace characters, you can use the wildcard character % at the beginning or end of the search term.
5. To start the search, click the filter icon.
6. To narrow the search, use additional filter criteria in allowed columns.

Use the context menu to perform commands and notifications on the search results.

¹for Scout Enterprise Management Suite 15.2 and later versions

3.8. 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, after you have moved a device or OU, it receives the properties of the new parent OU.

Moving devices, OUs or applications

1. In the tree view, show the source and target position of the relevant element.

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**.

Confirm your changes again and the element is moved to the target OU.

Moving devices to another OU via context menu

1. In the tree view, in the **OU devices** window or in the **All devices** window, for the relevant device, open the context menu.
2. Click **Edit > Move...**
3. In the dialog, expand the organizational structure and select the target OU.
4. Confirm with **OK**.

Confirm your changes again and 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 **Applications** 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](#).

3.9. Switching OU to top-level



Note

This feature can only be applied to an OU.

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

The relevant OU is moved to the highest level. It becomes one of the base-OUs. Device configuration and inheritance remain as defined. If inheritance is active, all settings are adopted from the base device configuration.

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 devices such as

- Self-registration of devices
- Discovery: Searching for devices

New devices must be assigned to an organizational unit (OU). You can configure whether 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 under **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 OUs.

4.1. Self-registration of devices

By default, the first time a Thin Client boots, it automatically searches for an available Scout Server. The client requires the IP address of the Scout 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 Server. You can also specify more than one Scout Server and a destination OU. For further information, see **DHCP configuration**.

or

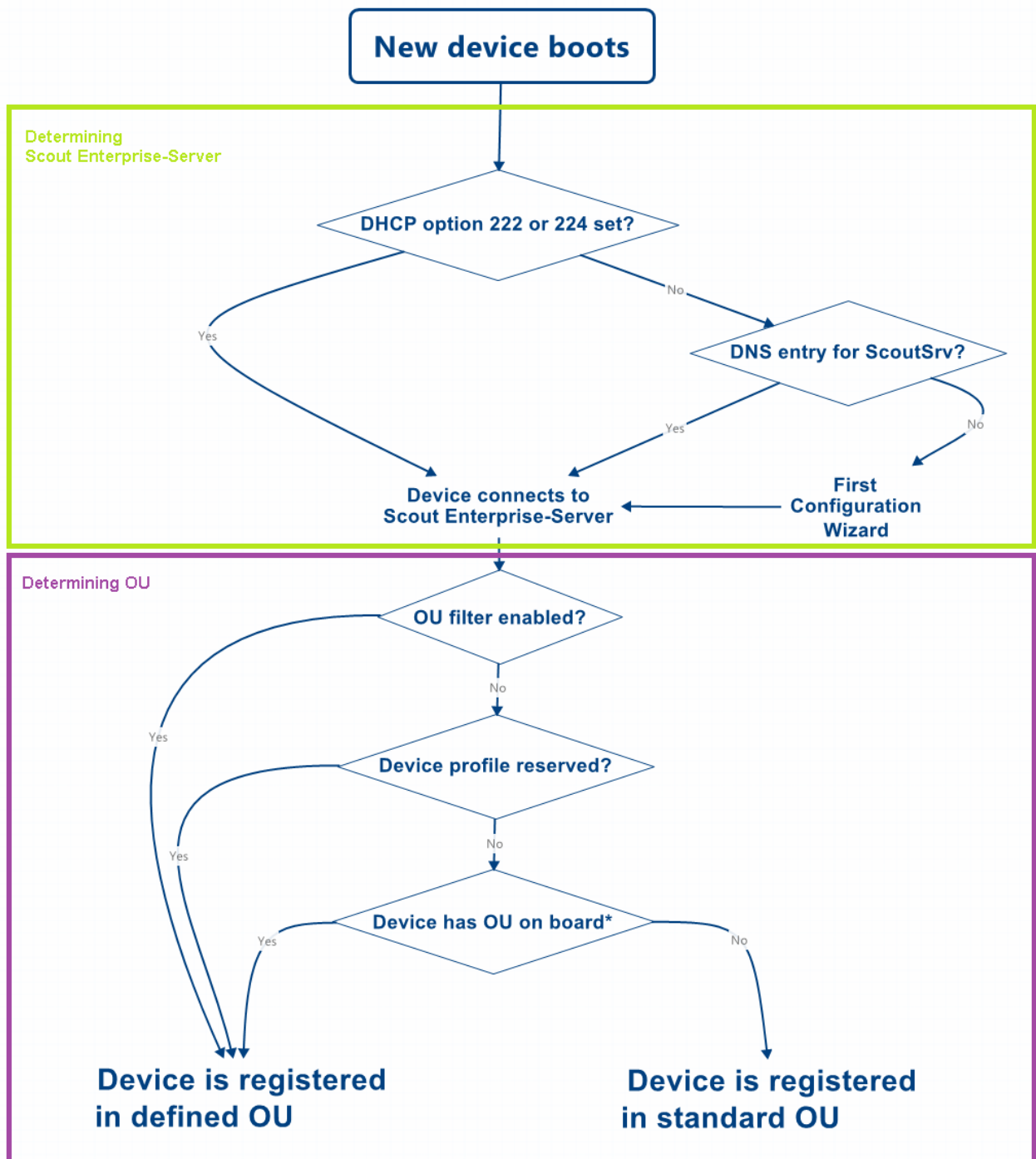
- DNS: The DNS server resolves the host name `ScoutSrv` (no case-sensitivity).

If the Scout 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 on the Thin Client.

If the requirements for self-registration are met, the device contacts the Scout 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 Server and to an OU. Details such as the **Accept only known devices** have not been considered.

4.2. DHCP configuration

- optional -



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 Server (option 222)
- List of Scout Servers (option 224)
- ID of the destination OU on the Scout Server (option 223)

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

In method 1 (recommended), you define a new vendor class, set the new options, and then 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 2012.

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 <i>The entry is automatically extended with the related hexadecimal number (45 4C 55 58 4E 47).</i>

4. Click **Action > Set Predefined Options....** Then, in the **Option class** list field, select **eLux NG**.
5. To define one Scout Server, click **Add...** and edit the new option as follows:

Option	Value
Name	Scout Server
Data type	String

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

6. To define more than one Scout Server, click **Add...** and edit the new option as follows:

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

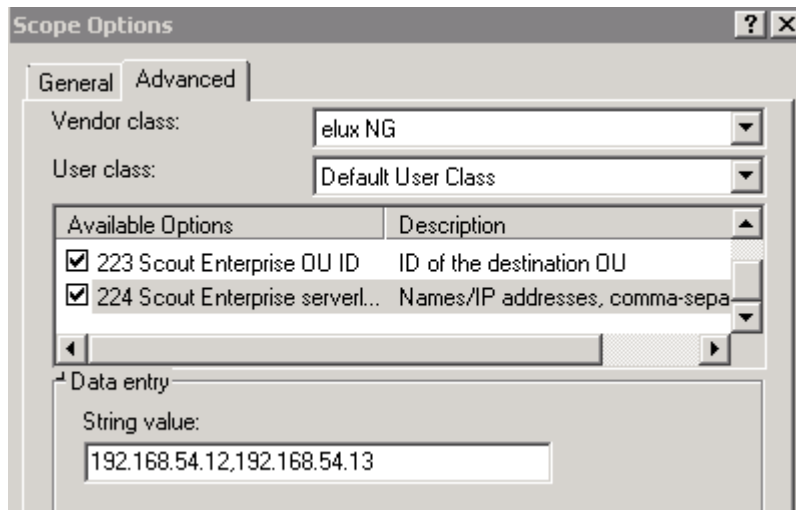
7. To define a specific OU that you can assign new devices to, click **Add...** and edit the new option as follows:

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**. Then click **Action > Configure Options... > Advanced**.

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

Option	Value
222 Scout Server	<Name or IP address of the Scout Server>
223 Scout Enterprise OU ID	<ID of the destination OU>
224 Scout Server list	<Names or IP addresses of the Scout 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 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**. Then click **Action > Configure Options... > General**.

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

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

Disabling DHCP option 12 as source for host names

If you have configured DHCP option 12 (host name), when connecting new devices, you can have the host names set via DHCP. To obtain the host name **not** via DHCP but from another source, such as the name template defined in the Scout Console, prevent the take-over from DHCP option 12. To do so, use a `terminal.ini` parameter:

File	/setup/terminal.ini	
Section	Network	
Entry	IgnoreDHCPHostname	
Value	true	By default, the value is false.

4.3. Searching for devices (Discovery)

Based on the IP address, you can search for devices throughout the entire network or within specific subnets. Any matching devices are automatically registered 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 device configuration/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**.

Discover devices

Start address: 192.168.54.42

Count: 1

End address: 192.168.54.42

Password: ••••

Destination group:

- [-] AT
- [+] DE
 - [-] DE_KA_Doku
 - [-] DE_MA
- [-] FR
- [-] IT
- [-] NL

When restarting device

☒ Inform user for 60 sec.

☒ The user can cancel the command

OK Cancel

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: <code>elux</code>) The password must match the password currently set on the individual clients.
Destination group	OU you want to assign the devices to Default is the predefined <code>Lost&Found</code> group with the base device 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 Server. The devices are assigned to their destination group and are restarted. The devices inherit the configuration of their new OU. Local non-protected device configuration is overridden. With immediate effect, on each restart, the clients connect to their Scout Server and, if available, are given the latest configuration and application definition data.

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

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



Note

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

4.4. Reserving device profiles

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

By creating devices manually in the Scout Console, you reserve a [MAC address](#) device profile. As soon as such a manually created device contacts its Scout Server for initial start-up, the 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
- DNS alias name `ScoutSrv`
- DHCP option 222 for the Scout Server



Note

If an OU filter is active, the OU filter is applied prior to the device profile reservation.

Reserving a device profile

1. Select the OU you want to assign the device to, and show its sub tree.
2. Open the  **Devices** context menu under the OU and select **Add...**
3. Enter the 12-digit MAC address of the device without hyphens.

*If the MAC address is valid, the **Device configuration** dialog opens. The **Use parent** option is selected by default.*

4. Confirm with **OK**.

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



Note

Importing devices also results in the reservation of device profiles within the OU structure. To create new devices in a greater number, we recommend using the **Import** feature. For further information, see [Import/Export](#).

4.5. Device names

The devices' host names can either be taken from the devices without modification or be set from the Scout Console. In addition, name templates are available that use, for example, the MAC address or the IP address of the devices. The settings for this can be found under **Advanced options > Devices**. For further information, see "Devices" on page 157.

Device names are subject to the following format rules:

- The first character must be a letter (a–z, A–Z) or a digit (0–9).
- The last character must not be a hyphen –.

4.6. Secure device management with Scout Enterprise

An enhanced security level is available for adding new clients to Scout Enterprise.

Clients that are registered with their **MAC addresses** in the Scout Enterprise database (**reserved device profile**) are accepted by the Scout Server and can be integrated into 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.

Accepting known clients only

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

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



Note

Only the requests of those clients are accepted whose MAC addresses have been 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). The assignment is based on predefined criteria. This is particularly helpful when registering new devices or relocating existing ones.

There are two options for configuring the OU filter:

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

You can only use one filter at a time. For each filter, you can define multiple filter rules and specify the sequence you want the rules to be applied in.

Once defined, the filter rules are retained unless deleted manually. Deactivate the filter rules that are currently not required but that you want to keep for future use.

The OU filter has precedence over

- OU assignment of devices via 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**.

For individual devices, you can ignore the OU filter (**Advanced device configuration¹ > Management**).



Note


OU filters are included when you export the data category **Advanced options**. For further information, see [Import/Export](#).

4.7.1. Setting up an OU filter as subnet filter

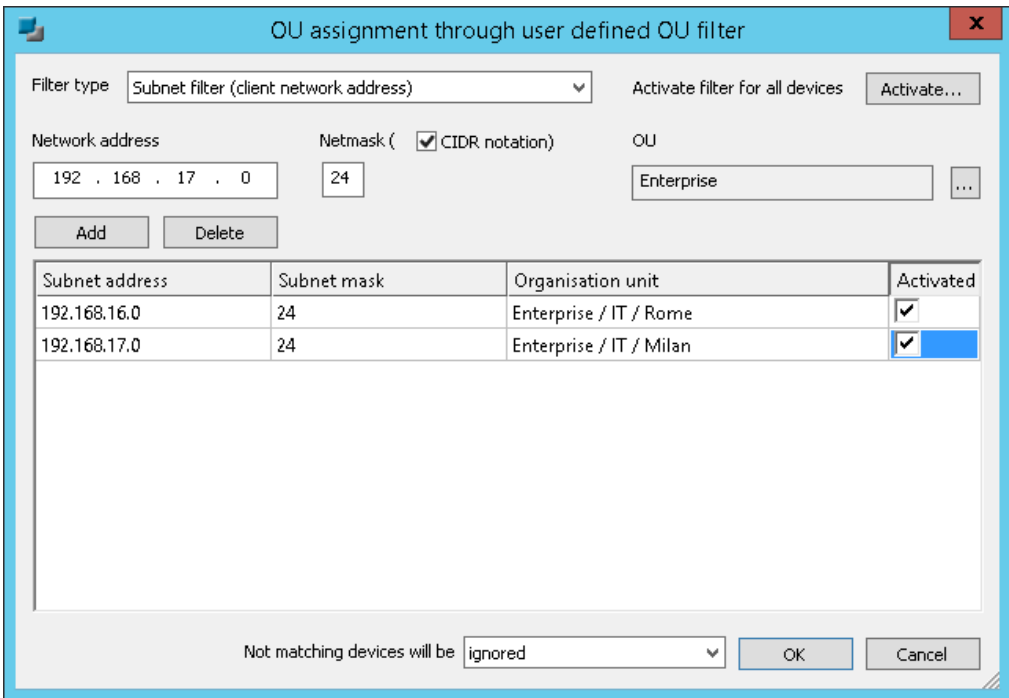
You can use the OU filter to filter on client network addresses and assign the matching devices to an OU.

1. Click **Options > Advanced options... > Devices**.
2. Under **New devices**, select the **Assign OU depending on the OU filter** option.
3. To open the **OU assignment** dialog, if required, click the ... button.

¹formerly **Advanced settings**

4. In the top section, from 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. Click the  button to browse the **OU** list. Select the OU you want to assign the devices to.
8. Click **Add**.

The filter rule is displayed in the field below.



OU assignment through user defined OU filter

Filter type: `Subnet filter (client network address)` Activate filter for all devices:

Network address: `192.168.17.0` Netmask (☒ CIDR notation): `24` OU: `Enterprise` ...

Subnet address	Subnet mask	Organisation unit	Activated
192.168.16.0	24	Enterprise / IT / Rome	<input checked="" type="checkbox"/>
192.168.17.0	24	Enterprise / IT / Milan	<input checked="" type="checkbox"/>

Not matching devices will be: `ignored` OK Cancel

9. If required, add more filter rules and configure them. For further information, see [Editing OU filter rules](#).
10. In the bottom section, from the list **Non-matching devices will be**, select where you want to keep the non-matching devices.

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. Any user-defined filter rules will not be taken into account.

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

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

eLux RP devices send an **OU filter text** field containing their device information to the Scout Server. You can use the **OU filter text** field in the Scout Enterprise Report Generator and for the user-defined OU filter. It includes the following information:

Host name, OS name, OS version, serial number, supplier, device type, BIOS, CPU speed, model, kernel version, flash type, flash size, RAM size, graphics, IDF name,¹ MAC address.²

1. Click **Options > Advanced options > Devices**.
2. Under **New devices**, select the option **Assign OU depending on the OU filter**.
3. To open the **OU assignment** dialog, if required, click the ... button.
4. In the top section, from 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 consists of three parts:

asset information string from OU filter text	logical operator =	value you want to filter by
---	--------------------	-----------------------------

Examples:

```
ELUX_HOSTNAME=Melissa;
ELUX_OSNAME=eLux RP;
ELUX_OSVERSION=6.1.0-3;
ELUX_SERIAL=72500422542;
ELUX_SUPPLIER=WYSE;
ELUX_DEVICETYPE=ZQ Class;
ELUX_BIOS=1.0J;
ELUX_CPU=1500;
ELUX_PRODUCT=ZQ Class;
ELUX_KERNEL=4.9.30;
ELUX_FLASH=16GB SATA Flash;
ELUX_FLASHSIZE=15272;
ELUX_MEMORY=4096;
ELUX_GRAPHICS=ATI AMD Radeon HD8330E;
ELUX_IDF=rec5608.idf;3
ELUX_MAC=7CD30A22D0AE4
```

Use the logical operators AND and OR to link multiple filter criteria. Use capital letters for the operators.

¹for eLux RP 5.7/eLux RP 6.2 and later versions

²for eLux RP 5.7/eLux RP 6.2 and later versions

³for eLux RP 5.7/eLux RP 6.2 and later versions


⁴for eLux RP 5.7/eLux RP 6.2 and later versions

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

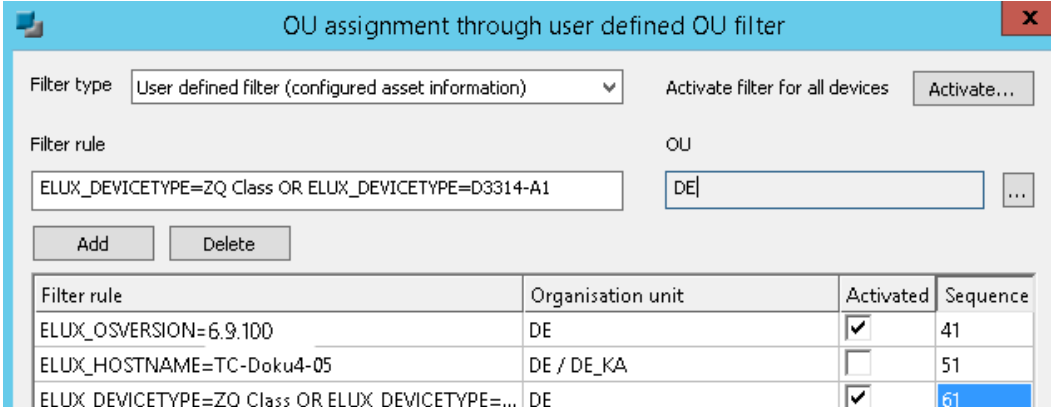
Examples for filter criteria:

Example 1: ELUX_OSNAME=eLux RP AND ELUX_OSVERSION=6.9.100

Example 2: ELUX_DEVICETYPE=D3314-A1 OR ELUX_DEVICETYPE=ZQ Class

6. In the **OU** list next to the **Filter rule** box, select the OU you want to assign the devices to. Click  to browse.
7. Click **Add**.

The filter rule is displayed in the field below.



Filter rule	Organisation unit	Activated	Sequence
ELUX_OSVERSION=6.9.100	DE	<input checked="" type="checkbox"/>	41
ELUX_HOSTNAME=TC-Doku4-05	DE / DE_KA	<input type="checkbox"/>	51
ELUX_DEVICETYPE=ZQ Class OR ELUX_DEVICETYPE=...	DE	<input checked="" type="checkbox"/>	61

8. If required, add more filter rules and configure them. For further information, see [Editing OU filter rules](#).
9. From the list **Non-matching devices will be**, select where you want to keep the non-matching devices.


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. Any user-defined subnet filter rules will not be taken into account.

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**, select the option **Assign OU depending on the OU filter**.
3. To open the **OU filter** dialog, click the  button.

4. In the top section, from the **Filter type** list, select the required filter option.
5. Use the following features:

Option	Action	Description
Add	Click button	<p>User-defined filter:</p> <p>The filter criteria of the Filter rule field and the destination OU selected in the OU field are added as a new filter rule to the list.</p> <p>Syntax for a filter criterion: <code><String from OU filter text>=<value></code></p> <p>You can combine two or more filter criteria by using one of the logical operators AND or OR. Use capital letters for the operators.</p> <p>For examples, see Setting up an OU filter as user-defined filter.</p> <p>Subnet filter:</p> <p>The data from the fields Network address, Netmask and OU are added as a new filter rule to the list.</p>
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 directly in the list.
Activate / Deactivate	Select/Clear Activated option	<p>Deactivated filter rules are not executed.</p> <p>Newly added filter rules are active by default.</p>
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.

6. From the list **Non-matching devices will be**, select where you want to keep the non-matching devices.

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.

7. Review all active filter rules thoroughly to avoid unintentional assignments.
8. 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 filter for individual devices

If the OU filter is enabled, all active filter rules are applied and the matching devices are assigned to the specified OU on their next restart. To exclude an individual device from the filter, deactivate the OU filter for that device.

1. For the relevant device, open **Advanced device configuration**¹ > **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.

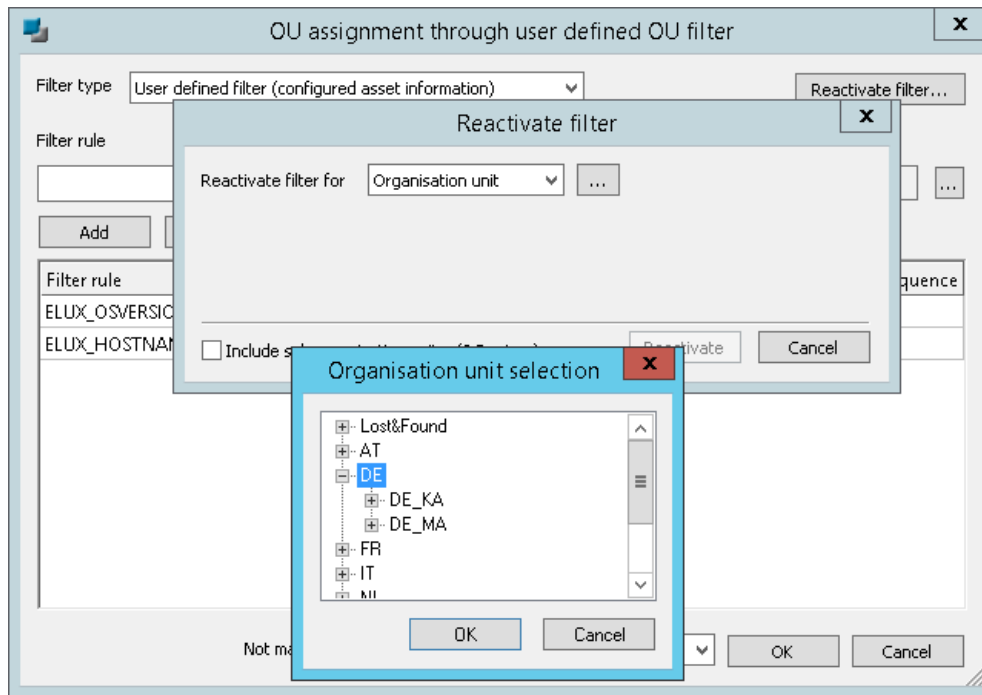
4.7.5. Re-activating OU filter


The OU filter can be deactivated for individual devices - either by applying the relevant option in the Scout Console or by moving devices by a drag-and-drop operation. To bring the relevant devices back to the OU filter, use the Scout Console option **Re-activate filter**.

1. Click **Options > Advanced options... > Devices**.
2. Under **New devices**, select the option **Assign OU depending on the OU filter**.
3. To open the **OU assignment** dialog, if required, click the  button.
4. In the upper right section, click **Reactivate filter...**²

¹formerly **Advanced settings**

²For Scout Enterprise Management Suite Version 15.1 and earlier versions, the **Activate...** button can be used to re-assign the OU filter to **all** devices. In later versions, you can also select a device group.



5. Select to re-activate the OU filter for all devices, for an individual organization unit (OU) or for a Dynamic Client Group.
6. To re-activate the OU filter for an OU or Dynamic Client Group, click the  button next to the list-field and select an OU or Dynamic Client Group.
To include subordinate OUs, select **Include sub organization units**.
7. Confirm with **Reactivate** and **OK**.

The OU filter is re-activated for the selected devices.

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 specific image throughout the whole organization. Or you can run a BIOS update on all devices with a specific BIOS version, across all OUs. Even client relocation to another Scout Server can be applied to a Dynamic Client Group. The following features can be applied:

- Commands
- Configuration run
- Notifications for software deliveries or firmware updates
- Notifications for relocation

Dynamic Client Groups are based on reports created in the Scout Report Generator. The reports are exported to the Scout Console once, and from that point onward, are displayed as a **Dynamic Client Group**. Commands applicable to OUs or to individual devices can also be applied to Dynamic Client Groups.



Note

The report layout must include the Client identifier¹ or the MAC address², respectively. The report type must be a list of **Devices** or **Assets**.

For further information on defining Dynamic Client Groups, see [Creating Dynamic Client Groups](#) in the Scout Report Generator guide.

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

User rights

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

By default, executing commands and other functions on a Dynamic Device Group is subject to the object rights configured for the relevant devices and OUs.³ This can result in a function not being executed because at least one device does not have the required object rights. To avoid this, disable the check for the underlying object rights under **Security > Manage administrators > DCG rights**.

4.8.1. Using Dynamic Client Groups

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

¹from Scout Enterprise 15.10

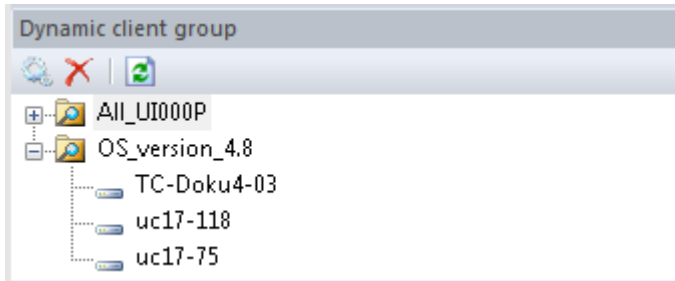
²up to Scout Enterprise 5.9

³for Enterprise 15.1 and later versions

For further information on defining and exporting DCGs, see [Creating Dynamic Client Groups](#) in the Scout Report Generator guide.

Displaying Dynamic Client Groups

- ▶ In the Scout 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 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 Console.

If a Dynamic Client Group is not needed any longer, use the button to delete it. 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 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 **Properties** window.
2. To update the Dynamic Client Group, click the  **Re-create** button. This way you ensure that exactly the currently matching devices are affected.
3. Open the context menu of the Dynamic Client Group and select a command or notification.

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

4.8.2. Special form of Dynamic Client Groups by import

To create a Dynamic Client Group, instead of using the Scout Report Generator, you can use the **Import** feature of the Scout Console and 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 only have to be registered in Scout Enterprise. Note that the **Import** feature is not used to import devices.

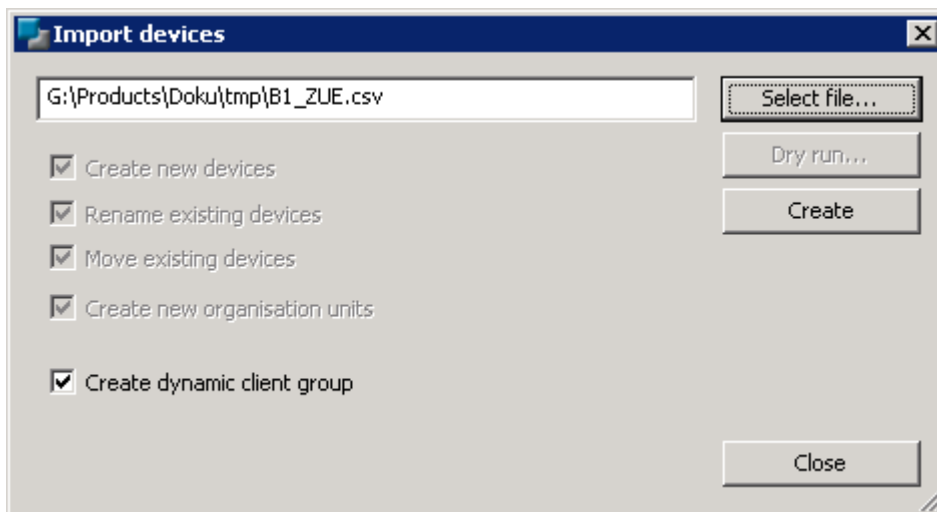
Creating Dynamic Client Groups by import



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 Console, click **File > Import > Devices....**



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

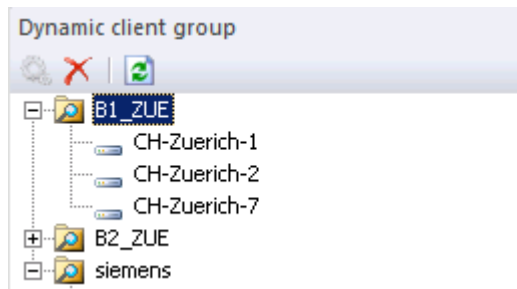
All options related to the device import are disabled.

3. Click **Select file...** and select the relevant `.csv` file from the file system.
4. Click **Create**.

The `.csv` file is evaluated. Scout Enterprise creates a new Dynamic Client Group. It contains all devices of the `csv` list whose MAC address is registered in Scout Enterprise. The dynamic device group adopts the name of the `.csv` file.

Displaying Dynamic Client Groups


- ▶ In the Scout 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 via the import feature cannot be updated with the  **Re-create** button. To update the Dynamic Client Group, after having modified the device list, save the *.csv file under the same name and perform a new import as described above.

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. Check the information shown in the **Properties** 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 Scout Servers

Relocating devices from one Scout Server to another can be very helpful in different scenarios of device migration, for example when relocating devices from a test/QA server to a production server, or consolidating several Scout Servers to a single server (server fusion).

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 time of relocation.

Example: External suppliers, in their environment, set up devices to be used in the customer's environment.

License information and local configuration can either be included in the transfer or left on the source server.



Note

You can use the client relocation procedure also in Service Provider mode. Here there is no need to carry license information.

4.9.1. Relocation procedure

The relocation procedure is initiated by the source server (device-releasing server) and, by default, completed by the target server (device-receiving server). The actual relocation procedure, however, is performed by the devices. They check the conditions and transfer the license information.

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

The devices then check whether the transmitted target server's address is available via the network. Provided, the target server's Scout version is valid,¹ the relocation process is started and the devices are deleted from the source server.

By default, the devices bring their management and application licenses as well as their proportional Subscription validity with them to the target server. The license and Subscription information is then deleted on the source server and added to the target server.

The new devices are assigned to the specified OU on the target server. If no destination OU has been specified, the default OU or the OU defined by OU filter rules is used (configured in **Advanced options > Devices > New devices**).

The relocation procedure is completed by an automatic device restart which activates the configuration of the target server. If configured, locally defined configuration is pertained. If the OU filter is used, an additional device restart is provoked by the system after assignment.

¹14.5.0 or later

Options

In contrast to the default procedure, the administrator can configure the following options in the notification:

- Offline relocation

The devices are removed from the source server without checking whether the target server is available. They move to the target server only when they can connect to it.

- Relocation without transfer of licenses

License and Subscription information is left on the source server so it can be used by other devices. This includes management licenses, application licenses assigned to the devices (if any), and the subscription portion of the relevant devices.

- Retain local configuration on new Scout Server¹

If on the source server is configured that users' local configurations in unlocked fields should not be overwritten by server-side configurations (**Advanced options > Devices**), then the local configurations are carried along. The relocated devices receive the target server's device configuration only where there are no local configurations.

Important Do not reserve device profiles by entering 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

The relocation procedure is initiated by the source server (device-releasing server) and completed by the relevant client devices. If you perform an offline relocation, the devices do not verify whether the target server (device-receiving server) is available and ready to accept the devices.

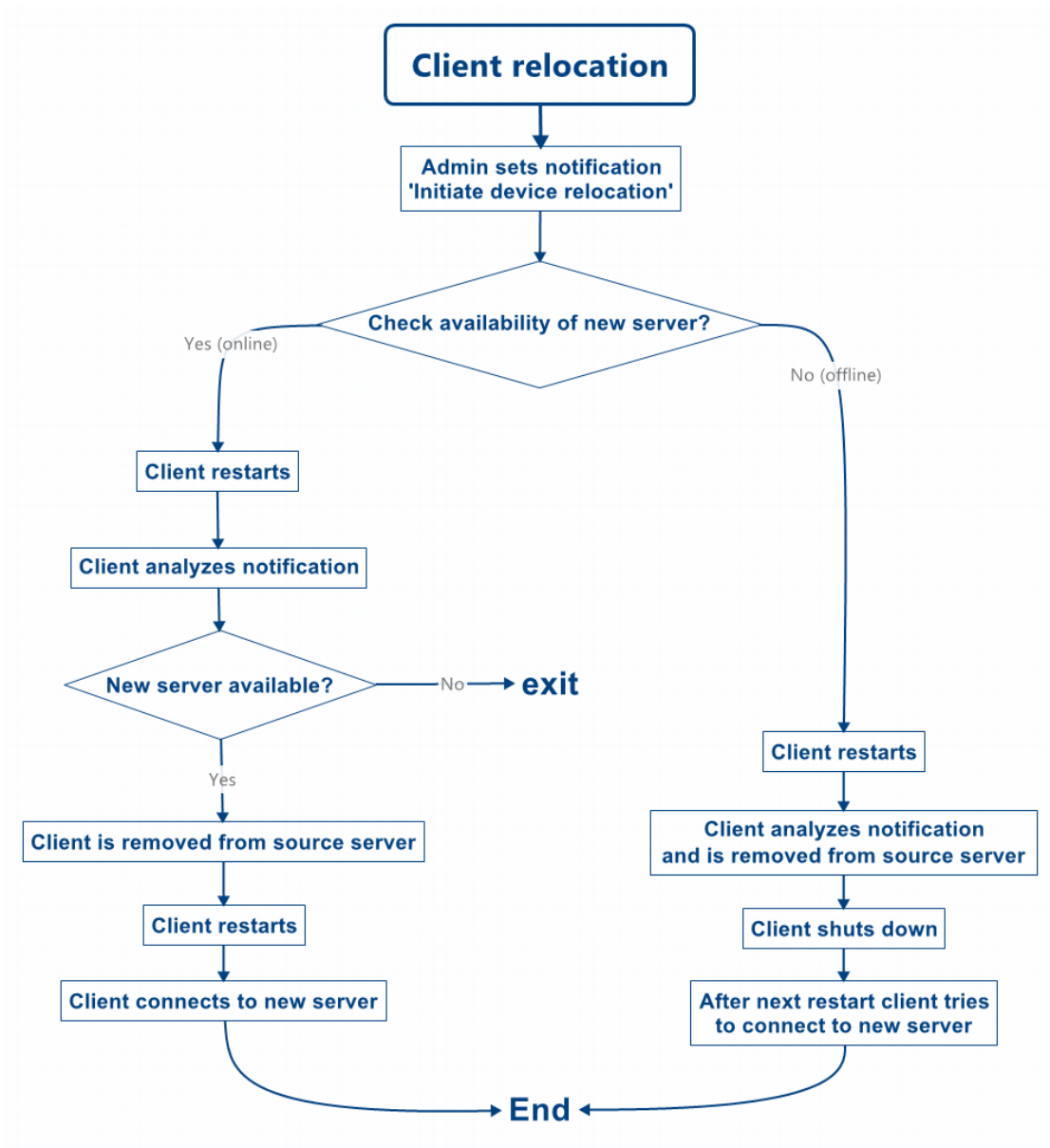
The administrator still triggers the relocation by setting a notification **Initiate client relocation** for the relevant devices in the Scout Console of the source server. The notification includes all required details. On the next device restart, the configuration is synchronized with the source server,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

The relevant devices are removed from the source server without further verification. On the next restart, the devices will try to connect to the target server.

License information and local configuration can either be included in the transfer or left on the source server.

¹from Scout 15 2110

4.9.3. Relocation flow chart

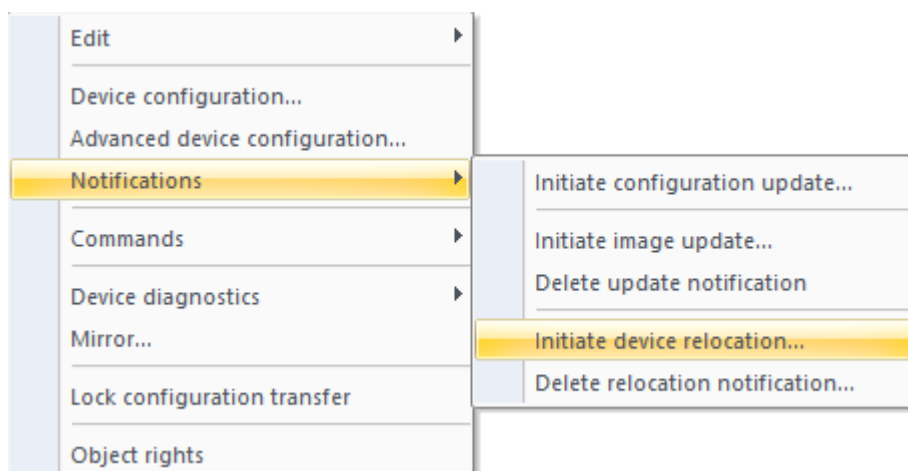


4.9.4. Initiating client relocation

U Requires

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

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....**



3. In the **Client relocation notification** dialog, in **New Scout Server**, type the name (FQDN) or the IP address of the target server.

U Note

To connect the devices via Scout Cloud Gateway to their target server, type the name or IP address of the SCG instance. The Scout Cloud Gateway must be fully configured.

4. Edit the following fields:

New OU-ID	ID of the 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 defined by the OU filter rules.
Relocation without transfer of licenses	The licenses of the relocating devices are left on the source server. The subscription portion for these devices also remains at the source server.
Check availability of new Scout Server	'online' relocation Relocation is only done when the devices can access the target server via the network. selected by default
Retain local configuration on new Scout Server ¹	User-defined values of the local device configuration in unlocked fields will be retained. This is relevant if the corresponding option in Advanced Options > Devices is used.
Include sub organization units	All devices located in lower-level OUs will also be moved.



Note

Notifications are always set or deleted for all selected devices regardless of whether they are only available for individual devices.

5. Confirm the notification and confirmation.

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

Relocation notification **Activated (doku4.unicon-ka.de / 192.168....**

¹from Scout 15 2110

U Note

To define which fields you want to show in the **Properties** window, click .

*For devices not involved in the relocation, the **Relocation notification** field remains empty.*

The devices evaluate the notifications after their next restart and then start the relocation process. Alternatively, trigger the relocation by command to control the time of relocation.

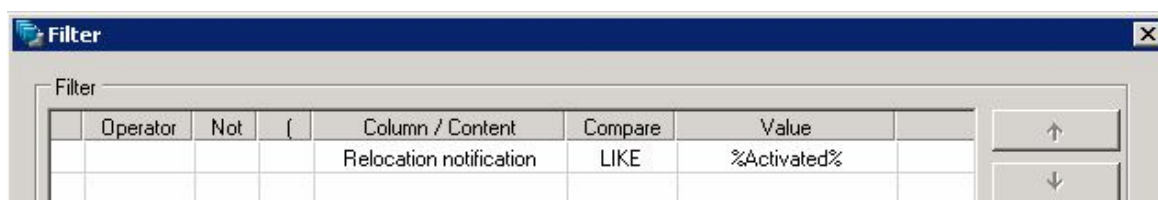
4.9.5. Scheduling relocation process

To carry out the client relocation outside working hours, for example, and to add a slight delay after each device is processed, proceed as follows.

U Requires

The relocation has been initiated and the relevant devices have their relocation notification.

1. In the Scout Report Generator, identify all devices with active relocation notification.

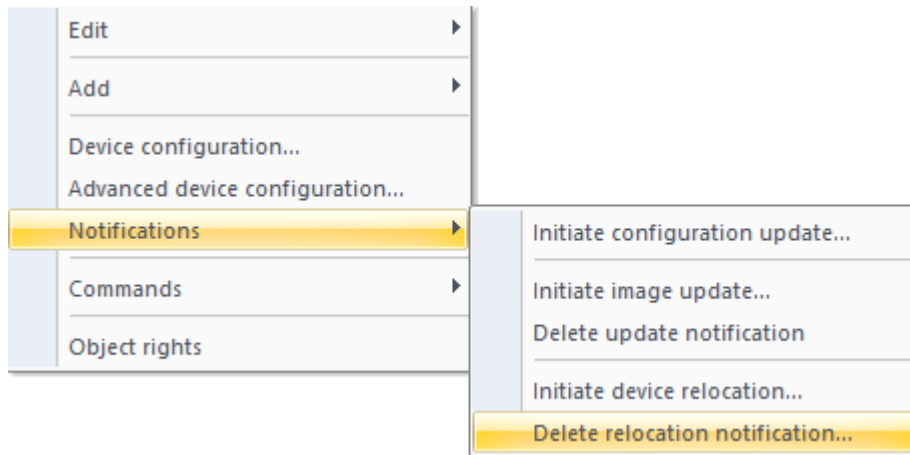


2. Export the identified devices to a Dynamic Client Group.
3. In the Scout Console, for your Dynamic Client Group, schedule a **Restart device** command:
 - In the Command dialog, choose date and time of the execution.
 - Specify a delay in milliseconds, that will be applied after the command execution of each device..

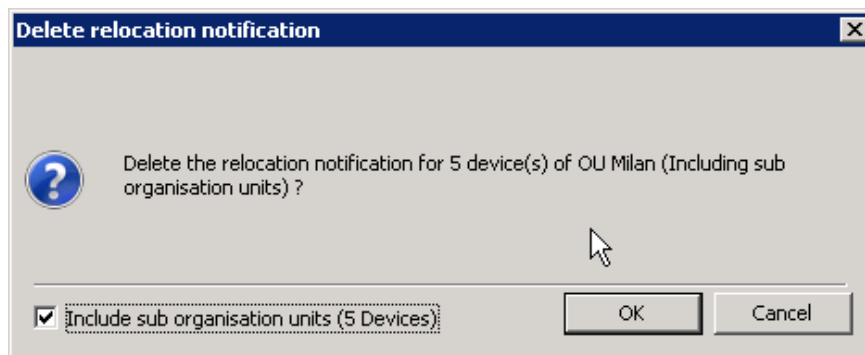
The relevant devices are restarted at defined time and then start the relocation process. They obtain their new configuration data from the target server. If you perform the relocation offline, the relevant devices will be removed from the source server, but will only connect to their new server when they can connect to it.

4.9.6. Deleting relocation notification

1. For the relevant OU, device or Dynamic Client Group, on the context menu, click **Notifications > Delete relocation notification...**



2. To include the devices of all subordinate OUs, in the **Delete relocation notification** message, select the option **Include sub organization units**.



The number of devices shown in brackets is updated dynamically.

3. Confirm with **OK**.

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



Note

Notifications are always set or deleted for all selected devices regardless of whether they are only available for individual devices.

5. Device configuration

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 takes this into account by using an inheritance approach. By default, the base device configuration defined at top level passes its properties on to the devices on lower instances. The concept of inheritance helps you keep your configuration consistent and efficient. To define any variations, simply modify the relevant settings. Scout Enterprise provides flexibility to override any settings on all levels.



Note

Changes to the device configuration take effect on the next restart of the relevant clients.

Important The device configuration of a client depends on the software packages installed on it.

5.1.1. Inheritance of configuration

The base device configuration and the configuration of OUs can be inherited by lower instances.

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

If the option **Use parent device configuration**¹ is active, the configuration of the superior element of the hierarchy is applied to the current instance. By default, the option **Use parent device configuration** is active, so a device inherits its configuration from the base device configuration.

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

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

On each level, you can inherit the device 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 device configuration.

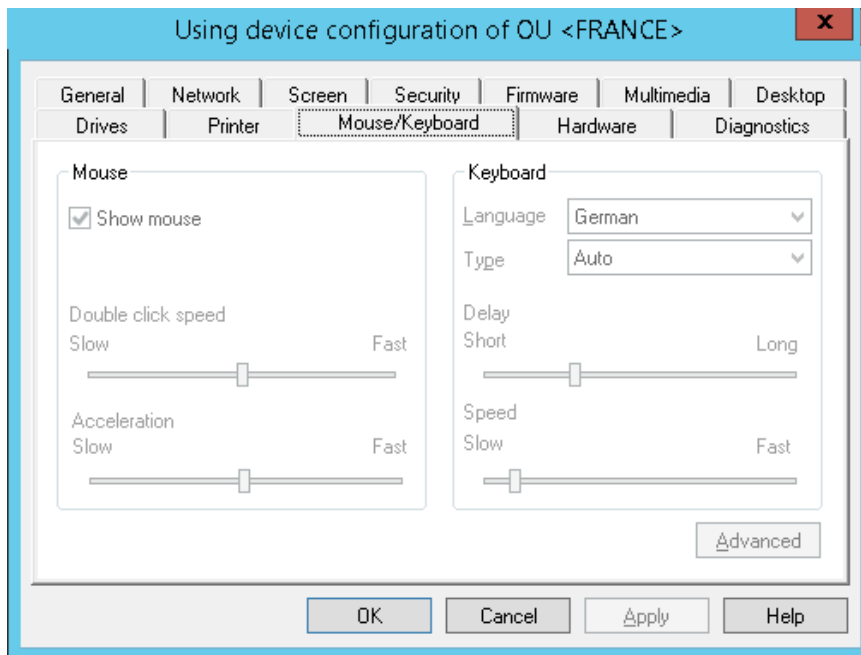


Note

Pay attention to the **Device configuration** dialog title. It indicates the location of the current

¹formerly Use parent

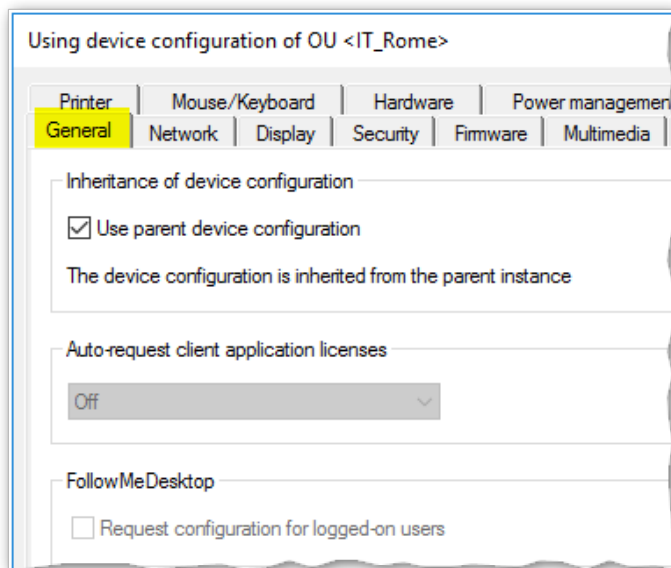
U configuration. This can be the base device configuration, or a superior OU, or the individual device.



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

5.1.2. Blocking inheritance - independent device configuration

If you want to define independent settings for an individual 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 **Device configuration...**¹.

*The **Device configuration** dialog opens and the title bar shows the currently active device configuration instance. This can be the base device configuration or a superior OU. For further information, see [Opening device configuration dialogs](#).*

2. On the **General** tab, clear the **Use parent device configuration**² 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 superior instances.



Note

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



Note

In **View > Settings...**, you can specify that when you modify a device configuration, all of its subordinate independent configurations are checked. You then receive a list of the relevant parameters and can conveniently determine whether and to which instances the modifications are to be transferred.

¹formerly Setup

²formerly Use parent

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 individual 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.

Retaining local device configuration

1. Click **Options > Advanced options... > Devices**.
2. Under **Field update**, select **Retain local configuration (unlocked fields)**.¹

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

Retaining local device configuration during factory reset

- from Scout Enterprise 15.7 and eLux RP 6.7 -

1. Select the option **Advanced options > Retain local configuration (unlocked fields)**, see above.
2. In the command dialog for the factory reset, select **Retain local configuration (unlocked fields)**.

The client is reset to its initial state and the device configuration of the locked fields is reset. However, the local user configurations in unlocked fields are retained.

For further information, see [Factory reset command](#).

Initiating a one-time update of all device configuration data

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

- ▶ In the Scout Console, for the relevant device, on the context menu, click **Notifications > Initiate configuration update...**

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

¹formerly: Only locked fields are updated

5.1.4. Accessing device configuration

Opening the base device configuration

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

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

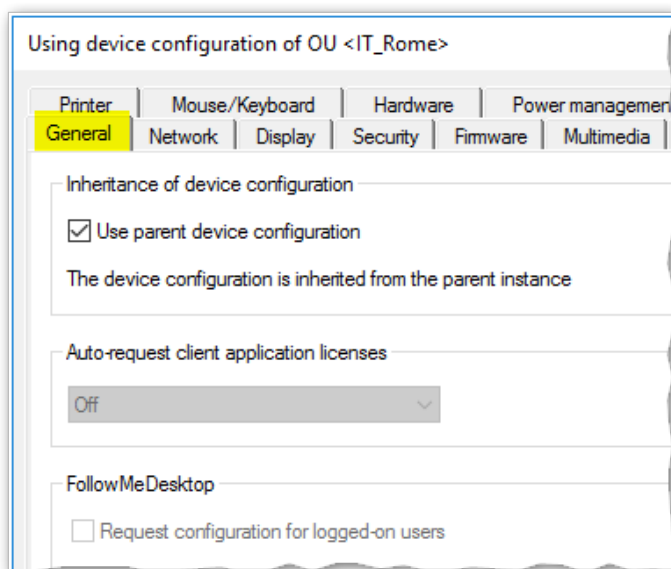
Opening Device configuration¹ dialog for OUs and devices

- ▶ Select an element in the tree view. Then click **Edit > Device configuration...**²

or

- ▶ For the relevant element, open the context menu. Then click **Device configuration...**

The **Device configuration** dialog of the selected element opens. Possibly, the options are disabled as the **Use parent device configuration**³ option is selected. In this case, the relevant OU or the base device configuration is specified in the dialog title.



The figure shows the device configuration of a device in the sub-tree of the OU *IT_Rome*. If the dialog has been opened as described above, all options on all tabs are disabled. Only **Use parent device configuration** can be modified.

¹formerly Setup

²formerly Setup

³formerly Use parent

Opening the relevant Device configuration dialog (preferred method)

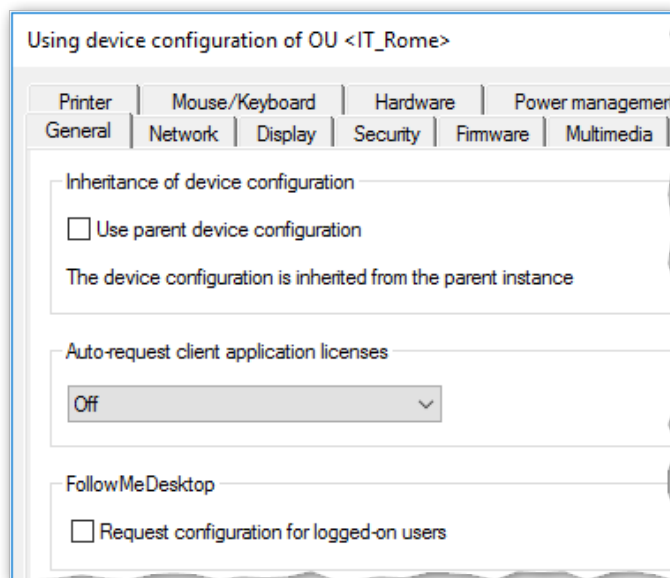
This method allows you to quickly and easily access the point where the device configuration is defined for the relevant devices.

1. In the tree view, select a device (or an OU).
2. To show the **Properties** window, click **View > Window > Properties**.

*In the **Properties** window, next to **Configuration**, the instance is displayed from where device configuration data are applied to the selected element.*

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

*The **Device configuration** dialog of the displayed instance opens. It contains the device configuration data applied to the selected instance. The options of all tabs can be edited as far as permitted by the user rights.*



*The figure shows the relevant device configuration for the same device. This is the configuration of the OU *IT_Rome*.*



Note

To save your changes, in Scout Enterprise Management Suite 15.4 and later versions, click **Apply**. In earlier versions, subsequently confirm with **OK** to make your changes persistent.

5.1.5. Comparing device configurations between OUs or devices

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

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

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

2. Drag two or more OUs or devices into the **Compare configuration** window by using a drag-and-drop operation.

Or:

On the context menu of the relevant OU or device, click **Edit > Add to configuration compare....**

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

The device configuration 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 configuration** window, click the **All** icon.

All properties are shown.



Note

To compare actual and target settings of individual devices, use a report. For further information, see [Evaluating configuration data](#).

5.1.6. Locking configuration transfer

- for Scout Enterprise Management Suite 15.0 and later versions¹ -

Individual devices can be excluded from the process of updating device configuration data.



Requires

Object right **Activate/Lock configuration transfer**

1. For the relevant device, open the context menu.
2. Click the option **Lock configuration transfer**.

The device is no longer provided with updated device configuration data but remains in the Scout Enterprise management.



Note

For newly added devices without management license, the configuration transfer is automatically locked.

¹replaces the **Management off** command of former Scout Enterprise Management Suite versions

5.2. Configuration method

During system start of the clients managed by the Scout Enterprise Management Suite, the clients connect to their Scout Server and check whether any updated configuration data are available, taking inheritance into account. There may be updates for the following data:

- Device configuration (formerly Setup)
- Application definition
- Files configured for transfer
- Advanced file entries

The Scout Server identifies the relevant configuration data at runtime. That means that all modifications made to configurations in the Scout Console until then are included.

5.2.1. Configuration run

If the system determines updated configuration data for a client, the relevant modified data are identified, compressed and saved to the database. They are then transferred to the client in one step.

When modifying the configuration of a large number of clients (e.g. when changing the application definitions due to a move to another back-end infrastructure), the administrator can initiate the process of identifying and compressing the relevant data in a data object in advance, for instance at night. To do so, the administrator uses the **Configuration run** command. With this command, the required configuration data can be prepared to be ready for transfer on the next restart of the clients, which might be on the next working day.

Performing a configuration run



Note

The configuration run command only prepares configuration data for clients with a configuration delta.

1. For the relevant OU or Dynamic Client Group, on the context menu, click **Commands**.

Execute/Schedule command for organisat...

Command: Configuration run

☐ Now

☒ Once

Date: Sonntag ,30.07.2017 Time: 12:00

☐ Every

Day of Month: 1, 2, 3, 4 Time: 15:15

2. On the sub-menu, click the **Configuration run...** command.
3. Specify a time for execution and confirm with **Schedule**.

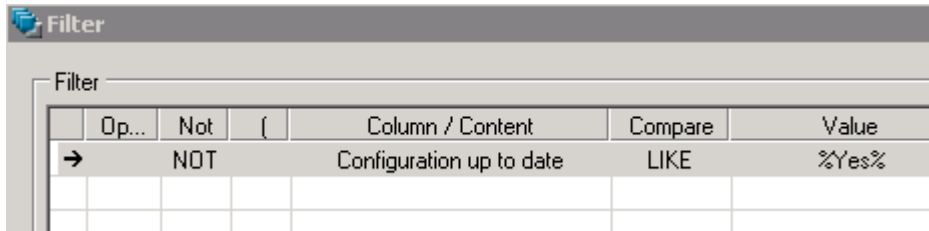
*The processing progress is shown in the **Command history**.*

5.3. Evaluating configuration data

The Scout Report Generator provides fields you can use to analyze configuration data:

Configuration ID	ID for a compressed data object holding configuration data Is created either as a result of a configuration run, or by synchronizing configuration data on the first client to server contact after the configuration settings have been modified
Configuration up-to-date	Yes - client has the configuration that is currently defined for it in the Scout Console No - client is running an earlier eLux version which cannot evaluate the field
Configuration transfer	The option Lock configuration transfer is active for the client For further information, see Locking configuration transfer .

Example:



5.4. FollowMe Desktop

- for Scout Enterprise 15.8 and later versions -



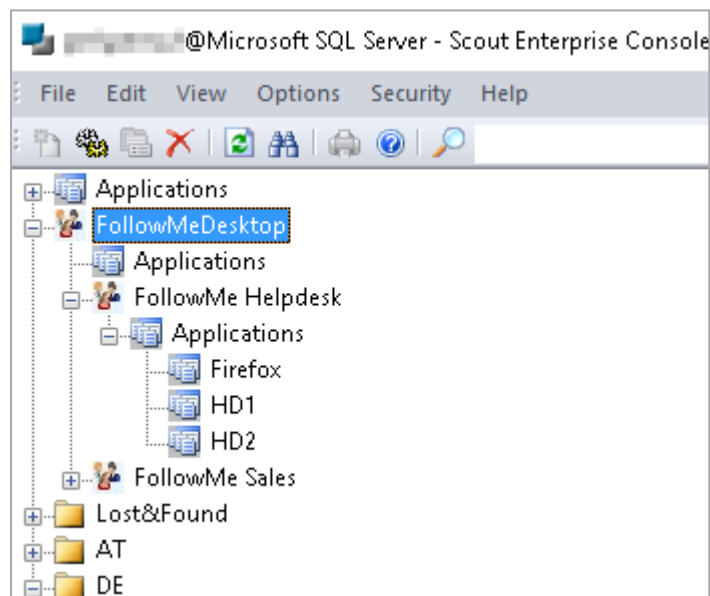
Note

To use this feature, you will need user authentication via Active Directory.

FollowMe Desktop allows you to make user-specific configuration settings that are valid across devices.

In addition to the device configuration option, which is bound to devices, the FollowMe Desktop feature allows users to take their configuration settings with them to any device. Users' configured desktop layout and configured applications "follow" them to any device they log on to.

FollowMe Desktop is configured in the tree structure node of the same name and is implemented as one of the top-level OUs. This FollowMe Desktop instance can be used right away or can act as a container for further FollowMe configurations, which are added as subordinate OUs. This is how a device-independent and cross-hierarchical structure of configurations is mapped, which might be motivated by users' subject-specific functions. For example, a **FollowMe Helpdesk** OU could contain all application definitions and the desktop layout for Helpdesk employees.



A FollowMe Desktop configuration may consist of application definitions and defined configuration values of the device configuration. For further information, see "Scope of configurable options" on page 65.

The FollowMe configurations are assigned to users via AD properties. The administrator applies filter definitions to the FollowMe Desktop instance and all subordinate OUs, which then filter for the relevant AD membership.

When an AD user logs on to a device that is enabled for FollowMe Desktop, the user's AD properties are matched against the filter definitions of the FollowMe OUs. If a FollowMe configuration with matching filter values is found, the desktop is loaded with the layout and applications defined in that FollowMe OU. When working with the FollowMe configuration, users can make changes to it, such as placing application icons freely on the desktop. These changes, however, will not be saved.

After the user closes his session and logs off, the original device configuration is reloaded.

FollowMe Desktop configurations can be exported and imported.

5.4.1. Configuring FollowMe Desktop

To use the FollowMe Desktop feature, make one or more FollowMe configurations available to certain AD users via filter definitions. Then define on which devices you want to allow the retrieval of a FollowMe configuration.

Creating FollowMe configurations



Requires

Administrator base right **Show FollowMe Desktop OU**

1. In the tree structure, below the **FollowMe Desktop** top-level OU, create further FollowMe OUs such as a **FollowMe Helpdesk** OU. To do so, from the context-menu, choose **Add > Organization unit**.
2. Edit the device configuration of the new FollowMe OUs (Desktop, Drives, USB options, Power management). Then add the relevant application definitions to the FollowMe OUs.



Note

New FollowMe Desktop OUs do not inherit configuration values from the base device configuration or base applications. Within the FollowMe Desktop structure, however, inheritance is active by default. Subordinate FollowMe OUs inherit the device configuration and applications from the parent FollowMe instance, unless you disable inheritance.

The configuration values of a FollowMe-OU overwrite the device configuration values valid on the device.

3. For each FollowMe OU, define a filter that filters for an AD membership. To do so, from the context-menu, choose **Set filter**.



Note

The filter definitions are independent of any inheritance. For each FollowMe OU, define a separate filter.

Filter rule	Organization unit	Activated	Sequence
GROUP=Helpdesk	FollowMeDesktop / FollowMe He...	<input checked="" type="checkbox"/>	60

In the filter rule, you can filter for the AD properties **User**, **Group** or **Domain**.

Syntax: USER | GROUP | DOMAIN=<Value>

Multiple filter rules are allowed.



Note

For devices with the FollowMe Desktop enabled, the user AD properties are written to the `eluxd.log` file (search for `FollowMeDesktop`).

All active filter rules are processed in the specified order. AD users matching this filter definition will have access to the applications and desktop properties configured in the FollowMe OU after logging on to devices for which FollowMe Desktop is enabled.

User-related FollowMe configurations are defined. In the next step, define for which OUs or devices these configurations may be retrieved.

Enabling devices for FollowMe Desktop

Specify the devices that shall have access to multiple configurations. In some cases, users may prefer the device configuration defined in the OU structure on their workstation device. On other devices, for example in the service area, they may prefer a FollowMe configuration.

In the device configuration of an OU / device (or in the base device configuration), you define whether a device should retrieve Follow-Me configurations when authorized AD users log on.

- ▶ In the device configuration of the relevant devices, under **General > FollowMe Desktop**, select **Request configuration for logged-on users**.

After AD users log on, their AD properties are evaluated. If the Scout Server finds a matching FollowMe OU, the configuration defined there is loaded.

5.4.2. Scope of configurable options

The following properties can be configured for FollowMe OUs:

- All application types with all application properties
- Software default settings for Firefox and Chromium (browser home directory)
- Device configuration with following options

Desktop	All options except date and time
Desktop > Advanced	Sort Configuration panel System bar Background picture
Drives	All options
Hardware	All USB options
Power management	All options

Configuration values of a FollowMe OU will overwrite the configuration values of the "normal" device configuration on this device. For options not listed, the values of the "normal" device configuration remain active.



Note

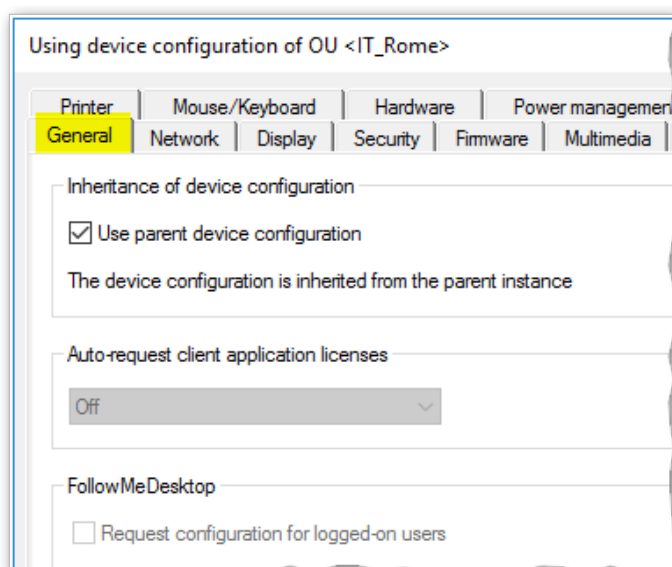
Within a FollowMe OU, only those applications will be available that have been defined for it.

The administrator can further limit the scope of the configurable options of FollowMe OUs for operational administrators (**Security > Manage administrators > Default object rights**).

5.5. General tab

Use parent

This option of the **General** tab is active by default and ensures that consistent device configurations are used. If **Use parent device configuration** is selected, all other fields of the dialog are disabled: For the relevant device or OU, the device configuration is used that is displayed in the title bar (in the figure IT_Rome). This is where an administrator will normally make any configuration changes.



Note

In some cases, it might be useful to disable the **Use parent device configuration** option temporarily.

For further information, see [Blocking inheritance](#).

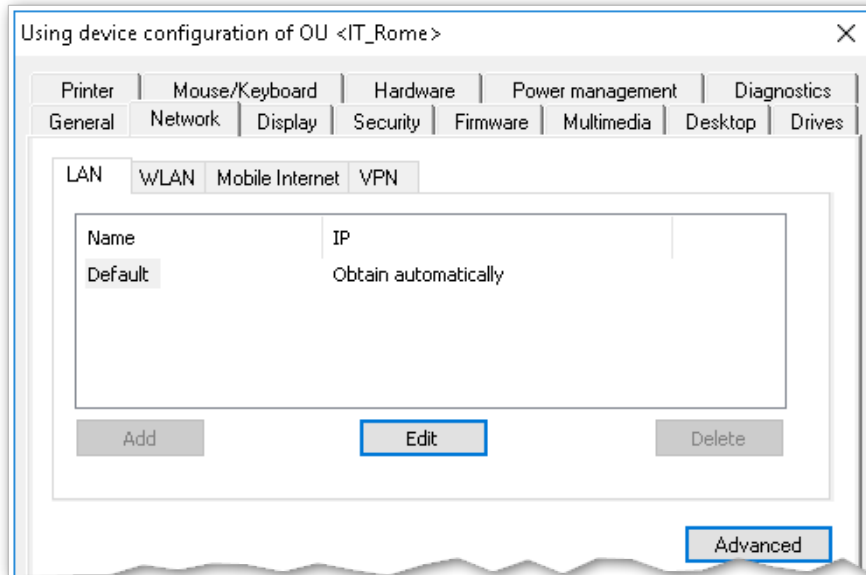
Additional options

Option	Description
Auto-request client application licenses	<p>Enables the device to automatically request application licenses when licensed applications are installed or used</p> <p>To do so, in the License information dialog, select Auto-assign. For further information, see Automatic assignment of application licenses in the License management short guide.</p>
FollowMe Desktop / Request configuration	<p>Allows authorized users to use multiple configurations on this device</p> <p>For further information, see Configuring FollowMe Desktop.</p>

Hardware information for individual devices is listed in the **Properties** window of the Scout Console. For further information, see [Properties window](#).

5.6. Network tab

Depending on the installed image and the hardware used, users can use different network connections. In the Scout Console, you define network profiles for different network types. The user can then choose from the defined network connections on the system bar.



The following network profiles are available:

- LAN (only one profile, cannot be deleted)
- Wireless LAN
- Mobile Internet (Wireless Wide Area Network)¹
- VPN²



Note

To create VPN network profiles, use the **Advanced device configuration** for individual devices. For further information, see "VPN" on page 162.

¹from Scout Enterprise Management Suite 15.5

²from Scout Enterprise Management Suite 15 2101 For earlier versions, see "VPN" on page 162 in the Advanced device configuration.

5.6.1. Defining a LAN profile

1. For the relevant device or OU, open **Device configuration > Network**.
2. Select the **LAN** tab. Then, for the **Default** connection, click **Edit**.
3. In the **Edit network profile** dialog, under **Ethernet**, edit the following fields:

Option	Description
Obtain an IP address automatically	<p>The IP address is obtained automatically via DHCP.</p> <p>Define a timeout period in seconds.</p> <p>Later on, under Advanced, specify the behavior for failing DHCP requests.</p>
Use following IP address	Alternatively, specify a fixed IP address and the corresponding options.



Note

If you do not use DHCP options for Scout Enterprise, we recommend that you select **Advanced > Ignore Scout Server DHCP options**.

4. To modify the network speed and Maximum Transmission Unit (MTU), edit the **Medium** tab.
5. Under **Advanced**, edit the following fields:

DHCP settings	Specify the behavior for failing DHCP requests.
Proxy ¹	<p>Define a system-wide proxy server for this network profile, see Proxy configuration.</p> <p>The proxy setting you define here is used by the <code>System proxy</code> option in the browser application definition.</p>

6. Under **IEEE 802.1X authentication**, edit the following fields:²

Activate	Enable IEEE 802.1X authentication in general.
Allow LAN connection without 802.1X if 802.1X fails ³	<p>Specify whether a connection may be set up if a timeout or authentication error for 802.1X occurs (for Ethernet connections only).</p> <p>If the option is cleared, users can only connect after successful 802.1X authentication.</p>

¹for Scout Enterprise 15.5 and later versions

²Up to Scout Enterprise Management Suite 15.8, use the **Advanced** tab to enable IEEE 802.1X

³for Scout Enterprise Management Suite 15.9 and later versions

Number of auto-connect retries ¹	Number of connection retries before aborting
Number of authentication retries ²	Number of authentication retries for a successful connection before the authentication is aborted
Timeout authentication	Time period in seconds before an authentication try is aborted



Note

The WPA encryption is performed using the WPA supplicant and the configuration file `wpa.conf`. For further information, see [WPA support](#).

7. Confirm with **OK** and **Apply**.

Use the **Internet connection test** option to check anytime whether web addresses are accessible via the Internet.³ For further information, see "Options for all network profiles" on page 80.

¹for Scout Enterprise Management Suite 15.9 and later versions

²for Scout Enterprise Management Suite 15.9 and later versions

³for Scout Enterprise Management Suite 15.9 and later versions

5.6.2. Advanced network settings

In **Device configuration**¹ > **Network** > **Advanced** you will find a host list as well as features that apply 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 Server in the specified time interval, provided the Scout Statistics Service is installed. 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 to do is 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 automatically transferred on the next restart.

¹formerly Setup

5.6.3. Defining a WLAN profile

The following configuration options are provided:

- A. In the Scout Console, in the device configuration, you can create a WLAN profile for a device, OU or for all devices, see below.
EAP authentication is not supported with this method.
- B. Users can create individual WLAN profiles locally on the device. Local profiles and profiles created in Scout Enterprise can be merged automatically. This way you can make them connect depending on the user's 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.
Users can additionally create individual WLAN profiles locally on the client. Configured WLAN networks can connect automatically depending on location and priority. For further information, see [WPA support](#).

Creating a WLAN profile in the Scout Enterprise device configuration

1. In the Scout Console, for the relevant OU, open **Device configuration**¹ > **Network**.
2. On the **Wireless LAN** tab, click **Add**.
3. Edit the following options:

Option	Description
Profile name	Freely selectable name for the WLAN profile
Connect automatically	Note: If the option is cleared, there is no automatic use of any existing Wifi connection. In this case, the user must start a WLAN manually from the live information on the system bar.
Internet connection test ²	For further information, see "Options for all network profiles" on page 80.
Medium > Network name/SSID	Wifi name / Service Set Identifier
Medium > Timeout	Time period in seconds waiting to connect
Medium > Channel	Selected automatically by default

¹formerly Setup

²from Scout Enterprise Management Suite 15.9

Option	Description
Medium > Encryption	<p>Authentication type</p> <ul style="list-style-type: none"> ■ None ■ WPA with pre-shared key (PSK) ■ WPA2 with pre-shared key (PSK) <p>To authenticate via EAP (Extensible Authentication Protocol), use a WPA configuration file. For further information, see WPA support.</p>
Medium > Hidden SSID ¹	<p>Select this option if a WLAN is hidden.</p> <p>Below, the access point MAC address (BSSID) is shown. If the network has multiple access points, the MAC addresses found are separated by semi-colons.</p> <p>BSSIDs are required for devices to automatically connect to a hidden WLAN.</p>
IP > Obtain an IP address automatically	<p>The IP address is obtained automatically via DHCP.</p> <p>Define a timeout value in seconds.</p>
IP > Use following IP address	<p>Alternatively, specify a fixed IP address and the corresponding options.</p>
Advanced > DHCP settings	<p>Specify the behavior for failing DHCP requests.</p>
<p>U Note</p> <p>If you do not use DHCP options for Scout Enterprise, we recommend that you select Ignore Scout Server DHCP options.</p>	
Advanced / Proxy ²	<p>Define a system-wide proxy server for this network profile, see Proxy configuration.</p> <p>The proxy setting you define here is used by the <code>System proxy</code> option in the browser application definition.</p>

4. Confirm with **OK**.

U Note

To create an individual WLAN profile locally on the client (B), apply the same steps in the eLux device configuration, provided you have the necessary user rights.

¹from Scout Enterprise Management Suite 15.10 and eLux RP 6.11

²for Scout Enterprise 15.5 and later versions



Note

To check the network activities on the client, use the **Diagnostics** feature (Enhanced log level) and the `systemd-journal.log` file.¹

5.6.4. WPA support

To secure your LAN and WLAN, you can use WPA encryption with 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 uses IEEE 802.1X and WPA2 uses IEEE 802.11i.

Authentication can be performed either with a pre-shared key (PSK) or, for IEEE 802.1X, via 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.

`wpa-supPLICant` is a free software application. For further information, see http://w1.fi/wpa_sup-PLICant/.

Providing WPA configuration file

1. Create a text file named `wpa.conf` by using the `wpa-supPLICant` program. See below for an example.
2. To transfer the `wpa.conf` file to the clients, use the Scout Enterprise feature **Files configured for transfer**. Use the following destination:

LAN	setup/scep/
WLAN	setup/wlan/

For further information, see [Files configured for transfer](#).

Example of a WPA configuration file with 802.1X (WLAN)

```
ctrl_interface=/var/run/wpa_supPLICant
ctrl_interface_group=0
ap_scan=1
network={
    ssid="<WLAN name>"
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=TLS
    identity="<Common Name as specified in certificate>"
    priority=6
    ca_cert="/setup/cacerts/root-ca.pem"
```

¹for eLux RP 6.4 and later versions

```
client_cert="/setup/cacerts/client.pem"
private_key="/setup/cacerts/client.key"
}
```



Note

Network profiles (LAN and WLAN) that are transferred to the device via a `wpa.conf` file cannot be edited locally on the device.

For further information on WPA configuration and on using variables, see [Configuring WPA supplicant](#) in the short guide **IEEE 802.1X authentication**.

5.6.5. Corporate WLAN

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

After having set up your WPA configuration file, you can deploy it wherever required. For further information, see [WPA support](#).

With a corporate WLAN, you can allow users to create their own WLAN profiles in parallel. 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.

For eLux RP 5, for a corporate WLAN, an additional dummy WLAN profile must be configured in the device configuration. For eLux RP 6, due to the new network stack, the steps described below are no longer required.

Configuring corporate WLAN with dummy profile

- for eLux RP 5 only -

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

Option	Wert	Beschreibung
Name	#DUMMY#	Using this name and SSID ensures that the WLAN profile on the client is invisible to the user. The name is mandatory.
Connect automatically	selected	mandatory
SSID	#DUMMY#	
Timeout		Use the default value.
Channel		Use the default value.

Option	Wert	Beschreibung
Encryption	WPA (PSK)	
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 via a WPA configuration file.

To define a higher priority than the manually created WLAN profiles (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

- for eLux RP 5 only; for eLux RP 6 see [Adding a WLAN profile](#) in the **eLux** guide -

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

If no network connection is available, the WLAN profile editor is displayed.

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.

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

5.6.6. Defining a Mobile Internet profile (WWAN)

- for Scout Enterprise Management Suite 15.5 and later versions -

For mobile devices equipped with an appropriate SIM card, define profiles that allow users to connect to cellular data networks such as LTE or UMTS.

1. In the Scout Console, for the relevant OU, open **Device configuration**¹ > **Network**.
2. On the **Mobile Internet** tab, click **Add**.
3. In the **Edit network profile** dialog, edit the following options:

Option	Description
Profile name	Name of the new profile
Connect automatically	If the signal strength is sufficient, the client automatically attempts to connect to the cellular network.
APN	Access Point Name: Address used by the client to connect to the Internet when the cellular data connection is used
PIN	PIN of the SIM card (if used)
Username	Username for the mobile account
Password	Password for the mobile account
Roaming	The cellular data connection remains intact when the device is outside the mobile operator's network.

4. Confirm with **OK**.

Unlock blocked SIM card via command

If, for example, a SIM card has been blocked due to incorrect PIN entries, use the PUK to create a new PIN.

1. For the relevant device, open the context menu and click **Commands > User-defined command**.
2. Enter the following command:

```
mmcli -i 0 --puk=<PUK code> --pin=<PIN code>
```
3. Select **Run with system rights**.
4. Click **Execute**.

5.6.7. Defining a VPN profile

- from Scout Enterprise Management Suite 15 2101 -



Note

To create VPN network profiles in earlier versions, use the **Advanced device configuration** for individual devices. For further information, see "VPN" on page 162.

You can define one or more VPN profiles for entire OUs.

¹formerly Setup

1. In the Scout Console, for the relevant OU, open **Device configuration > Network**.
2. On the **VPN** tab, click **Add**.
3. In the **Edit network profile** dialog, edit the following options:

Option	Description
Profile name	Name for the new VPN profile
Connect automatically	The VPN client starts automatically and sets up a connection.
VPN client type	Choose between OpenVPN, CiscoAnyconnect or a user-defined VPN client. If you use a user-defined VPN client, specify its ID number.
Configuration (only OpenVPN)	Name of the OpenVPN configuration file without file name extension The specified configuration file must be available on the devices.

4. Confirm with **OK**.

For further information on creating OpenVPN and Cisco AnyConnect profiles, see "VPN" on page 162.

5.6.8. Options for all network profiles

Option	Description						
Name	Name for the network profile (can be defined freely)						
Connect automatically	(except for LAN)						
Internet connection test ¹	<p>Each time a connection is set up, the system checks whether addresses on the Internet can be reached via the current network profile (LAN and WLAN). If a connection to the Internet cannot be set up, the system checks for the existence of a captive portal and, if available, redirects to it.</p> <hr/> <table> <tr> <td>Auto (default)</td><td>A connection test is automatically performed for WLAN profiles, provided that no central system proxy is defined.</td></tr> <tr> <td>On</td><td>For LAN and WLAN network profiles, the Internet connection is automatically tested.</td></tr> <tr> <td>Off</td><td>No automatic connection test is performed. The device does not display any content in the browser and does not attempt to connect to external services or websites.</td></tr> </table> <hr/> <p>The option is protected by a dedicated object right (Device configuration > Network > Handling of network profiles > Internet connection test) and by a dedicated user right.²</p>	Auto (default)	A connection test is automatically performed for WLAN profiles, provided that no central system proxy is defined.	On	For LAN and WLAN network profiles, the Internet connection is automatically tested.	Off	No automatic connection test is performed. The device does not display any content in the browser and does not attempt to connect to external services or websites.
Auto (default)	A connection test is automatically performed for WLAN profiles, provided that no central system proxy is defined.						
On	For LAN and WLAN network profiles, the Internet connection is automatically tested.						
Off	No automatic connection test is performed. The device does not display any content in the browser and does not attempt to connect to external services or websites.						

¹from Scout Enterprise Management Suite 15.9

²from Scout Enterprise Management Suite 15 2101

5.6.9. Proxy configuration

For each network profile, you can define a proxy server that is used by web clients or browsers. The proxy server can be configured manually or automatically.

If you define the proxy server centrally in the device configuration, it can be accessed from all application definitions (browsers). This central **system proxy**¹ contains the proxy setting which can either be a fixed server setting, automatically determined, or simply `No Proxy`.

Using an automatic WPAD configuration, all web clients of an organization can then be configured easily to the same proxy server or servers.

For the **system proxy** setting, in the network profiles, you will find the options described below.

- Scout Console: **Network > Advanced**
- eLux RP 6: **Network configuration > Advanced > Use proxy > Proxy settings**

Option	Description
No proxy	No proxy server is used
Manual (Proxy:Port)	Specify fixed proxy server with port number Example: <code>proxy.sampletec-01.com:3800</code> To define destinations that you do not want to access via proxy, in the Proxy exception list , enter the relevant network addresses separated by semicolons.
Auto (URL)	Proxy auto-config (PAC): Determines the appropriate proxy for each URL Examples: <code>http://proxy.sampletec-01.com/proxy.pac</code> <code>http://wpad.sampletec-01.com/wpad.dat</code>
Pass-through logon for proxy (with AD user authentication) ²	If a central system proxy is configured with AD authentication, the AD logon data are used for authentication. Proxy authentication may be required if you use browser content redirection under Citrix.
Proxy username ³	Username for authentication on the system proxy
Proxy password ⁴	Password for authentication on the system proxy



Note

When you define a browser application, the default proxy setting is `Use system proxy`. The proxy setting defined in the relevant network profile is now active. For further information, see [Defining a browser application](#).

¹for Scout Enterprise Management Suite 15.5 and later versions

²from Scout Enterprise Management Suite 15.8 and eLux RP 6.7

³from Scout Enterprise Management Suite 15.8 and eLux RP 6.7

⁴from Scout Enterprise Management Suite 15.8 and eLux RP 6.7

5.6.10. Internet Protocol version 6 (IPv6)

In addition to full support of Internet Protocol Version 4 (**IPv4**), **IPv6** is used by default for local applications including automatic network configuration (DHCP, DNS, NTP).¹

- ▶ To disable IPv6, in the Scout Console, for the relevant clients, configure the following Advanced file entry:

File	/setup/terminal.ini
Section	Network
Entry	DisableIPv6
Value	true (default = false)

For further information, see [Advanced file entries](#).

5.6.11. Firewall for eLux devices

- for eLux RP 6.8 and later versions -

To secure your eLux devices with a firewall, for example to allow exactly one more connection besides the connection to the Scout Server, use the eLux **Firewall support** package, which allows you to define appropriate rules.

By default, **nftables** are used. Alternatively, the **iptables** syntax can be used.

Once the eLux **Firewall support** package is installed, the firewall rules are applied on system start. By default, only data packets that are required for communication with the Scout Server are allowed to pass. To allow further connections, define filtering rules and transfer them to the devices in a file.

If the **Firewall support** package has been installed on the device without filtering rules, the firewall will only start if the feature package **Strict firewall policy** is installed. Then communication between the Scout Server and the device is established via the management protocol (port 22125) and no other communication is allowed.

Configuring firewall rules (nftables)



Note

The eLux package **Firewall support** and the included feature packages **eLux firewall plugin** and **firewall nftables programs and libraries** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

¹for eLux RP 6.6 and later versions

1. Create the `nftables.conf` file according to the following example:

```
table ip filter {
    chain input {
        tcp dport 22 accept
        tcp sport 80 accept
    }
    chain output {
        tcp sport 22 accept
        tcp dport 80 accept
    }
}
```

In the example, outgoing `http` and incoming `ssh` connections are accepted.

2. Transfer the files to the devices to `/setup/firewall/nftables.conf`. To do so, use the Scout feature **Files configured for transfer**.
For further information, see [Files configured for transfer](#) in the **Scout Enterprise** guide.

Configuring firewall rules (iptables)



Note

The eLux package **Firewall support** and the included feature packages **eLux firewall plugin** and **Firewall iptables compatibility programs and libraries** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

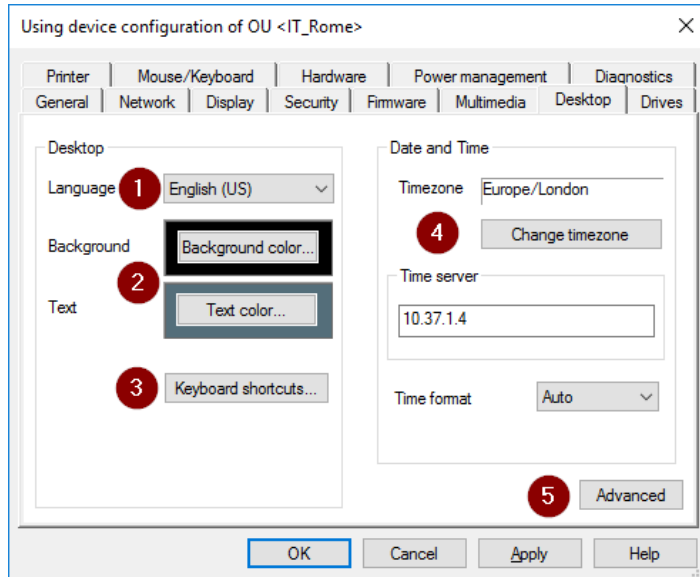
1. Create the file `rules.v4` for IPV4 or `rules.v6` for IPV6. Use the **iptables** syntax for the rules.
2. Transfer the files to the devices to `/setup/firewall/rules.v4` or `/setup/firewall/rules.v6`, respectively. To do so, use the Scout feature **Files configured for transfer**.
For further information, see [Files configured for transfer](#) in the **Scout Enterprise** guide.

All rule files are included in the **Diagnostics** feature and are part of the `System` template.¹

¹for Scout Enterprise 15.8 and later versions

5.7. Desktop tab

On the **Desktop** tab, you can modify the eLux desktop layout.



- 1 Display language
- 2 Background and text colors
- 3 Keyboard shortcuts
- 4 Date and time settings
- 5 Advanced settings

5.7.1. Configuring language and colors

1. For the relevant device or OU, open **Device configuration**¹ > **Desktop**.
2. In the **Language** list, click the preferred desktop and application language.

The following languages are supported: English, German, French² and Spanish³



Note

The language setting refers to the display of desktop elements. It does not affect text services and input. For a smooth performance, ensure that the applications support the selected language.

3. Click the **Background color** button to select a desktop background color.
4. Click the **Text color** button to select a text color for the application icons.⁴ Make sure there is sufficient contrast to the background color.

For further configuration options of the eLux RP 6 desktop, see "eLux RP 6 User Interface" on page 90.

5.7.2. Keyboard shortcuts

For switching applications and locking the screen, keyboard shortcuts are already predefined and you are free to customize them. To define keyboard shortcuts freely, follow the syntax rules given.

¹formerly Setup

²for eLux RP 6.9 and later versions

³for eLux RP 6.9 and later versions

⁴from Scout Enterprise 15.4

Defining Keyboard shortcuts

1. Open **Device configuration** > **Desktop** > **Keyboard shortcuts**.
2. You may select keyboard shortcuts for the following actions:

Option	Description	How to define
Switch applications	Switch between open applications or sessions The default shortcut ALT+CTRL ↑ helps avoid conflicts with the shortcut ALT+TAB which is used to switch between the tasks within a Windows session.	Select an option from the list-field.
Log off ¹	Log off currently logged-on user (AD users) The logon dialog is then displayed.	Specify the desired key combination as free-text, see below.
Lock screen ²	Activate password-protected screen saver (AD users) Default: <Ctrl><Alt>End	Specify the desired key combination as free-text, see below. Otherwise, the default key combination is active.

Furthermore, you can define a key combination for multi-monitor environments that allows users to quickly switch between clone mode and extended desktop.³ For further information, see "Multiple monitors" on page 93.

Rules for specifying key combinations

- Key combinations consist of a combination of one or more modifier keys and a single non-modifier key
- For the non-modifier key, you can choose from the following keys:
Letter keys, number keys, function keys, Windows logo keys, Esc key, position and numpad keys as specified
- Key combinations must be specified in the following format:

```
<modifier key><modifier key (optional)><modifier key (optional)>additional key
```

No spaces or other characters may be placed between the keys.

- The spelling of the key names must follow the specification, see examples. To receive a complete list of allowed key names and their spelling, use the following command in an eLux shell:

Modifier key names: `xmodmap -pm`

Non-modifier key names: `xmodmap -pk`

¹from Scout Enterprise 15.8 and eLux RP 6.9

²from Scout Enterprise 15.8 and eLux RP 6.9

³from Scout Enterprise 15 2101 and eLux RP 6 2101

Examples

Option	Description
<Ctrl><Alt>Escape	
<Shift><Ctrl>1	
<Mod4><Alt>F1	Mod4 corresponds to the Windows logo key
<Ctrl><Mod4><Alt>End	
<Mod4>Super_R (= right Windows button if used as key)	Super_R corresponds to the Windows logo key on the right if used as a key
<Mod5>KP_End	Mod5 corresponds to ALT GR KP_End corresponds to the END key of the numpad

Important If you define a key combination for eLux that is already defined within an application/session, this key combination will only work for eLux. Avoid using the same key combinations in different environments.

Behavior of the CAPS LOCK key

In most environments, pressing the (CAPS LOCK) key in combination with letter keys results in the display of uppercase letters, while the number keys above the letter block output numbers despite the CAPS LOCK key. To display the special characters of the number keys, the SHIFT key must be pressed.

- ▶ To let users write special characters with the CAPS LOCK key, for the relevant devices, configure the following Advanced file entry:¹

Datei	/setup/terminal.ini	
Abschnitt	Keyboard	
Eintrag	ForceShiftLock	
Wert	true	Default: false

For further information, see [Advanced file entries](#).

The CAPS LOCK key then behaves like the SHIFT key.

5.7.3. Date and time

Option	Description
Time zone	Click Change time zone and select the required time zone from the list..

¹from eLux RP 6 2107

Option	Description
Time server	<p>Under Time server, specify the relevant server name or IP address.</p> <p>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.</p> <p>The service runs on port 123 and uses the UDP protocol.</p> <p>For further information on the Windows Time Service, see the Microsoft documentation. For further information on NTP, see http://www.ntp.org.</p>
Time format ¹	<p>The time can be displayed in 24 hour or 12 hour time format.</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Auto (default) The displayed time format depends on the configured display language (see same dialog). <input type="radio"/> 12 hour <input type="radio"/> 24 hour

5.7.4. Advanced desktop settings

System bar

Option	Description
Show system bar	The system bar will be displayed on the devices. Below, select its behavior and the icons you want to show on the system bar. (selected by default)
Always on top	The system bar is always visible, even when applications are running in full-screen mode.
Hide automatically	The system bar is hidden by default. As soon as users point the mouse to the bottom of the screen, the system bar is displayed.
Show Desktop icon	Users click this icon to minimize all open windows and show the desktop. (selected by default)
Show live information icons ²	These icons allow users to view current status information such as plugged USB devices. for eLux RP 6.8 and later versions via right-click (selected by default)

¹from Scout Enterprise 15 2101

²from Scout Enterprise 15.7 and eLux RP 6.7

Option	Description
Show time	Shows the current time When users point the mouse to the time, the current date is shown. (selected by default)
Show Config panel icon ¹	Allows users to open the device configuration (Configuration panel) (selected by default).

Important Only when the Configuration panel is displayed, can the administrator unlock the configuration via device password locally on the device.

Quick Config:² Quick access to Config Panel dialogs via system bar

All options are selected by default.

Option	Description
Volume	Volume control for input and output devices
Keyboard	Keyboard language and key speed
Display	Screen settings
Peripherals	Settings for peripherals such as USB and Bluetooth devices, and COM ports
Network	Network information and setup, disconnect/connect
Device information	Information on the device
Date and time	Date and time settings

Background

Different background images can be defined for primary/secondary monitors and for the time before/after the AD logon.³

- ▶ Select a background image from the list-field. Then configure it via the buttons.

Option	Description
Background picture	Desktop wallpaper (default) If further pictures are defined, this one will be used only for the primary monitor and after AD logon. ⁴
Additional picture	Desktop wallpaper for secondary monitors

¹from Scout Enterprise 15.4 and eLux RP 6.8

²for eLux RP 6.8 and later versions

³from Scout Enterprise 15.8

⁴from Scout Enterprise 15.8

Option	Description
Background picture AD	Desktop wallpaper until AD logon (primary monitor)
Additional picture AD	Desktop wallpaper until AD logon (second and more monitors)
Load	<p>Browse the file system and select a picture file. The picture file will be imported into the database.</p> <ul style="list-style-type: none"> The following file formats are supported: .svg, .png, .jpg¹ Maximum file size 500 KB
Delete	Remove the current background image from the database.
Set URL ²	As an alternative to a picture file from the file system, specify a web address for loading pictures.



Note

Make sure you have enough flash memory on the devices. The background image is stored in the `/setup` directory of the flash card.

Further options

Option	Description
Sort Configuration panel	The Configuration panel dialogs are displayed in alphabetical order (default from version 15.9)
Timer for shutdown confirmation ³	<p>Before the device is shut down, a message is displayed for the specified time period (in seconds). This allows users to prevent the shutdown by clicking the Cancel button or pressing the ESC key. (deselected by default)</p> <p>This option has its own user right and object right (for administrators). Both rights are enabled by default.</p>
Desktop sort order ⁴	<p>Sort order of the desktop icons</p> <p>The administrator can specify the sort order for users without the user right Sorting desktop icons. Users who have this user right can freely place desktop icons on the desktop.⁵</p>

¹.jpg cannot be previewed

²from Scout Enterprise 15.8

³from Scout Enterprise 15 2103 and eLux RP 6 2103

⁴from Scout Enterprise 15.10

⁵from eLux RP 6.9

5.7.5. eLux RP 6 User Interface



Requires

eLux RP 6.0 or a later version

eLux RP 6 clients come with a new desktop interface that can be customized to your needs and that provides a personal desktop view. For further information, see [eLux RP 6 User Interface](#) in the **eLux** guide.

Customizing the layout of the eLux RP 6 User Interface

1. For the relevant OU, use the [Advanced file entries](#) feature of the Scout Console to modify the client file `/setup/terminal.ini` in the **Layout** section. Add the following new entries and specify the relevant values:

Entry	Value range	Description
DesktopLogo	<i>Path and name of the picture file</i> none	Option 1 replaces the eLux Logo in the lower right section by the specified picture file. Example: <code>setup/public/myPic.png</code> Option 2 removes the eLux Logo in the lower right section. ¹



Note

To show an individual picture file, transfer the picture to the clients. For further information, see [Files configured for transfer](#).

DesktopTextColor	<code>#<rgb></code>	Text color of application icons
DesktopHighlightedTextColor	<code>#<rgb></code>	Text color of application icons when the mouse pointer is moved over them
DesktopTitleTextColor	<code>#<rgb></code>	Color of the folder/tab title (All Applications, StoreFront store name)
DesktopSearchTextColor	<code>#<rgb></code>	Text color in the search field
DesktopSearchBackgroundColor	<code>#<rgb></code>	Background color of the search field
DesktopSearchIconColor	<code>#<rgb></code>	Color of search icon (magnifier)
DesktopSortIconColor	<code>#<rgb></code>	Color of sort icon (A-Z)

2. To display a background image, configure the relevant picture file in the **Advanced** desktop settings of the device configuration. For further information, see [Advanced desktop settings](#).

For multiple monitors, the image will be used as a background image on each monitor.

¹for eLux RP 6.5 and later versions



Note

The background image overrides the **Background** color defined on the **Desktop** tab.

3. To set a solid background color for the desktop, use the **Background** option on the **Desktop** tab.

To set a gradient background color, use the RGB values R 102, G 138, B 185.

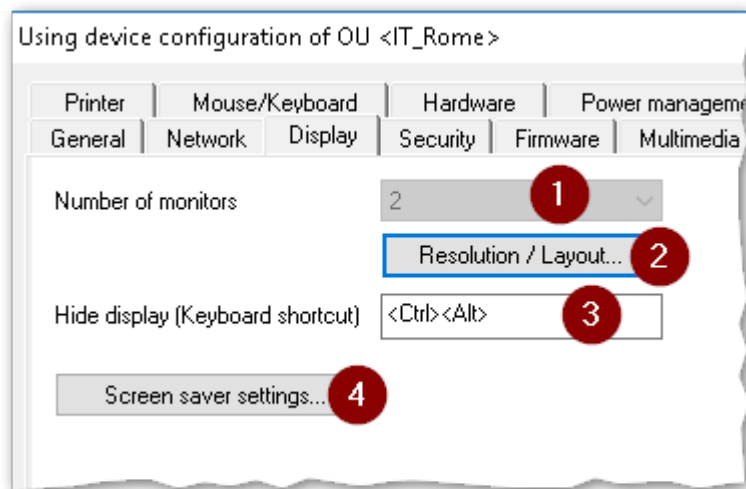
4. To configure the position of the system bar,¹ define the following entry in the `/setup/terminal.ini` file in the **Layout** section:

Entry	Value range	Description
SystembarPosition	0 1	0: bottom of the screen 1: top of the screen

¹for eLux RP 6.8 and later versions

5.8. Display tab

On the **Display** tab, you can choose between display settings and screen saver settings. To define display settings for one or more monitors, open the **Resolution/Layout** dialog.



1 Define the number of monitors together with further display options in the **Resolution/Layout** dialog.

2 Configure the display:

- ☒ Display options per monitor
- ☒ multiple monitors

3 Keyboard shortcut to hide/show the content of a monitor

4 Select and configure a screen saver

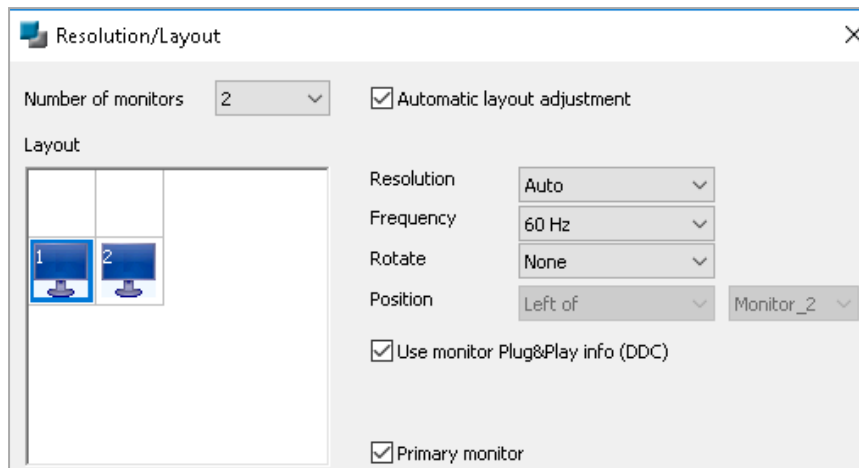


Note

For Scout Enterprise Management Suite 15.3 and later versions, you will find the power saving options on the **Power management** tab.

5.8.1. Configuring the display

1. If you have defined more than one monitor, in the **Resolution/Layout** dialog, select a blue monitor icon.



2. For the selected monitor, use the list fields on the right to specify the screen resolution, frequency, and rotation.

Resolution Screen resolutions that are not listed may be added to the database table `dbo.Resolution`. After modifying the table, restart the Scout Console.

Frequency Refresh rate

Rotation The screen display can be rotated 270° (left), 180° (inverted) and 90°(right).

Position Only for multiple monitors

3. To have the values supported by the monitor processed by the client, select **Use monitor Plug&Play Info (DDC)**.

Clear the option to activate the **Monitor class** field.

U Note

If you decide to use adapters or the analog VGA port to connect monitors to Thin Clients, warranty for the operation of these clients will be excluded. These types of combinations are not part of functional acceptance tests.

4. To define the selected monitor as the primary one, select **Primary monitor**.
5. Confirm with **OK** and **Apply**.

Important If your monitors do not support the settings you have defined, you may have to perform a factory reset of the device and modify the desired screen settings.

5.8.2. Multiple monitors

Up to eight monitors can be configured.

Defining multiple monitors

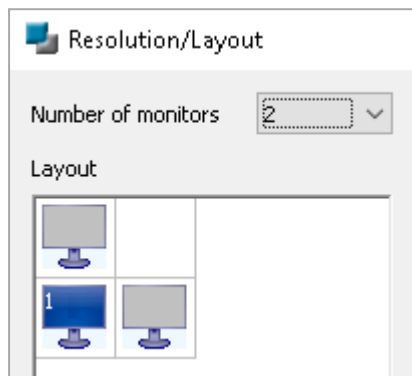
1. In **Device configuration > Display**, click **Resolution/Layout** to open the dialog of the same name.

The field **Number of monitors** specifies one monitor by default. In the field below, this monitor is represented by a blue monitor icon with the number 1. By default, the first monitor is defined as the primary monitor (see option in the lower section).

For a different setting, 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, their possible positions (horizontal and vertical) are shown as gray monitor icons.



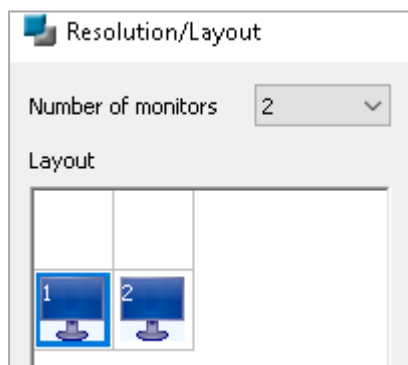
3. Double-click the gray monitor icon that shows the position of the second monitor.

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



Note

Alternatively, right-click a monitor position to assign a monitor to it.



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 a blue monitor icon with its number.

5. To automatically adjust the layout after one of the monitors is removed, select the option **Automatic layout adjustment**.¹

If the option is not active, the current layout is retained regardless of the actual situation.

¹from Scout Enterprise Management Suite 15.9



Note

A four-monitor configuration is supported on the following devices: Dell Z50QQ, Hewlett-Packard t620 Plus and Hewlett-Packard t730.



Note

A five-monitor configuration is supported on the following devices: Fujitsu FUTRO S940 and Fujitsu FUTRO S9010.

Defining positions of all monitors freely

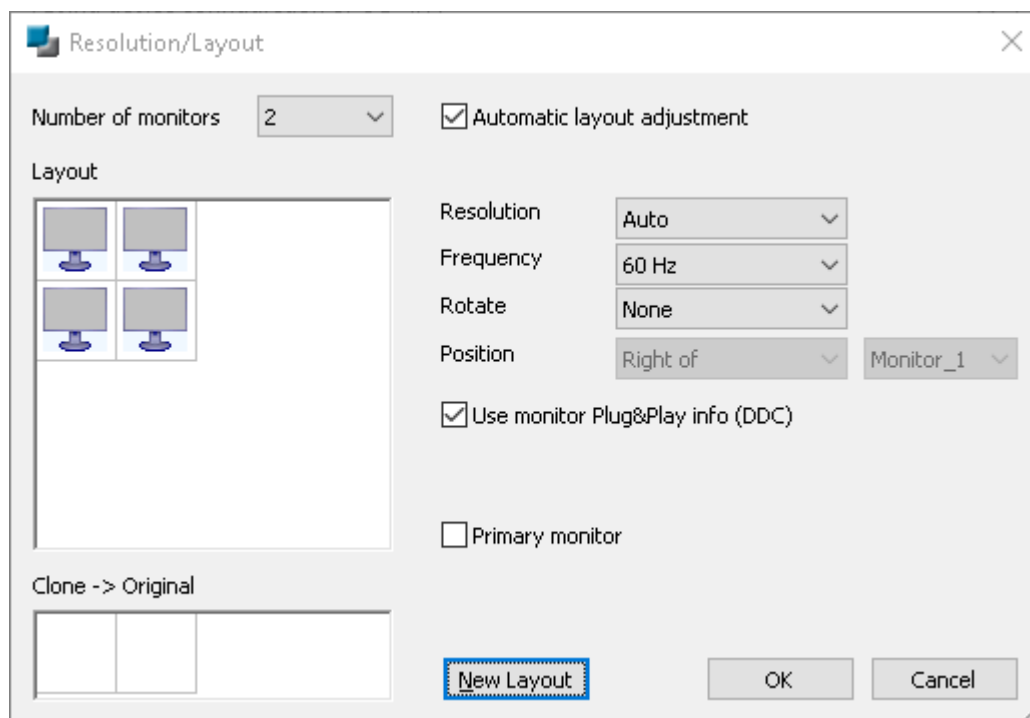
To define the position of the first monitor, use a new layout.

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 a blue monitor icon. For each additional monitor, their possible positions (horizontal and vertical) are shown as gray monitor icons.

2. Click **New layout**.

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

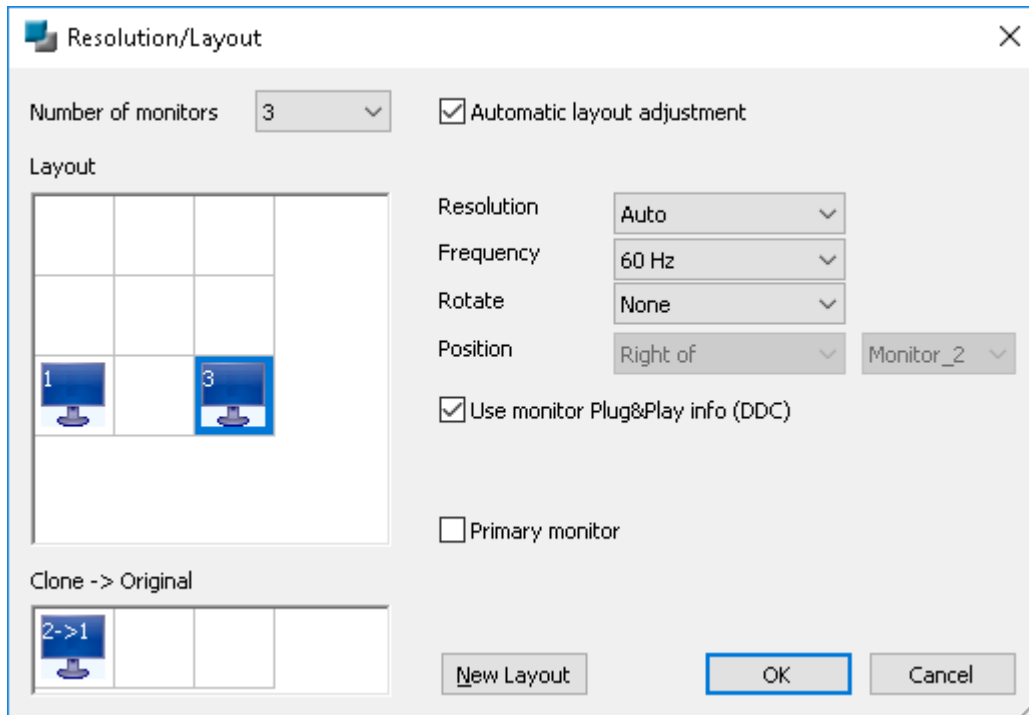


3. Double-click the desired monitor position for the first monitor. Then, double-click the desired monitor positions of the remaining monitors.

Cloning monitors (Clone mode)

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

- ▶ Right-click the last defined blue monitor icon, and on the context menu, click **Clone of x**.



To deactivate the Clone mode, use the **New Layout** feature (see above).

Key combination for switching between clone mode and extended desktop

- from Scout Enterprise 15 2101 und eLux RP 6 2101 -

- ▶ To allow users to quickly switch between the two modes, define the following Advanced file entry for the relevant devices:

File	/setup/terminal.ini		
Section	Hotkeys		
Entry	CloneDisplays		
Value	<Mod4>p	<Mod4> corresponds to the Windows logo key	

For further information, see [Advanced file entries](#) in the **Scout Enterprise** guide.

5.8.3. Screen saver

Configuring the screen saver

1. Under **Display > Screen saver settings**, choose between a black screen, a specific screen saver or multiple screen savers.
2. Depending on the option chosen, select one or more screen savers from the list. To select multiple entries, press SHIFT or CTRL



Note

The **HTML** option allows you to choose a website.¹

3. To configure each screen saver, use the settings on the right.

Enabling the screen saver

- ▶ On the **Power management** tab, for each profile, select **Enable screen saver after** and specify a waiting time in minutes.²

Locking the screen on the device

If the screen saver is enabled, eLux users can lock the screen before the configured waiting time with the following key combination:

- ▶ Press CTRL+ALT+END

Password-protected screen saver



Note

When user authentication is enabled, password protection of the screen saver becomes active and cannot be turned off.³

The password is set to \$ELUXPASSWORD. For further information, see [Where to apply user variables](#).

The screen saver becomes active after the defined time period and the system is locked. By pressing a key or moving the mouse, a dialog is displayed for unlocking. It provides the following options to users:

Option	Button	Description
The logged-on user unlocks the screen by entering his/her password / smart card	Unlock	Default

¹for Scout Enterprise 15.8 and later versions

²for earlier versions **Screen > Screen saver**

³for eLux RP 6.3 and later versions

Option	Button	Description
Another person leaves a message for the logged-on user	Message	<p>The screen remains locked. The logged-on user receives a notification with the message when he or she unlocks the screen.</p> <p>This function is enabled by default and can be disabled by the following Advanced file entry:¹ File: <code>/setup/terminal.ini</code>, section: <code>xscreensaver_dialog</code>, entry: <code>MessageEnabled</code>, value: <code>false</code></p>
Another user authenticates to log off the previous user (and to log on), restart or shut down the device. ²	Log off	<p>Useful if devices are used by multiple users: Allows users to reuse devices that have been left without logging off and therefore are blocked</p> <p>Once the new user has authenticated, the Restart, Shut down and Log off buttons become active. In any case, the previously logged-on user is logged off.</p> <p>This function is disabled by default and can be enabled by the following Advanced file entry: File: <code>/setup/terminal.ini</code>, section: <code>xscreensaver_dialog</code>, entry: <code>ShowSysCommandButtons</code>, value: <code>true</code></p>

Important Data loss may occur if the **Log off** option is used followed by restart, shutdown, or logoff. The user currently logged on is logged off regardless of whether the documents or data last edited have been saved.

Download of picture files for screen saver

- for eLux RP 6.5 and later versions -

The Scout Enterprise administrator can optionally configure the direct download of picture files to the device into the screen saver's picture directory. To do so, use the **FileFetch** tool, which downloads graphic files via **wget**.



Requires

- The eLux package **FileFetch** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.
- The picture files must be located in the specified directory and have the file extension `.gif`, `.jpg` or `.png`. The filename must be numeric. Examples: `0001.jpg`, `0002.jpg`, `0003.png`, `0004.gif`

¹for eLux RP 6.8 and later versions

²for eLux RP 6.8 and later versions

- ▶ For the relevant clients, configure the web server and the directory of the picture files. To do so, choose the **Advanced file entries** feature of the Scout Console:

File	/setup/terminal.ini
Section	FileFetch
Entry	URL
Value	<URL of the web server including path> Example: http://webserver.sampletec-01.com/eluxng/pictures

For further information, see [Files configured for transfer](#).

*The **FileFetch** tool checks on each device restart whether new picture files are available on the web server for download.*

5.8.4. Hide display

- from Scout Enterprise 15 2103 -

Users can temporarily hide the content of a monitor using a predefined key combination. This can be helpful when multiple monitors are used and certain information should not be visible to others present.

The following options are provided:

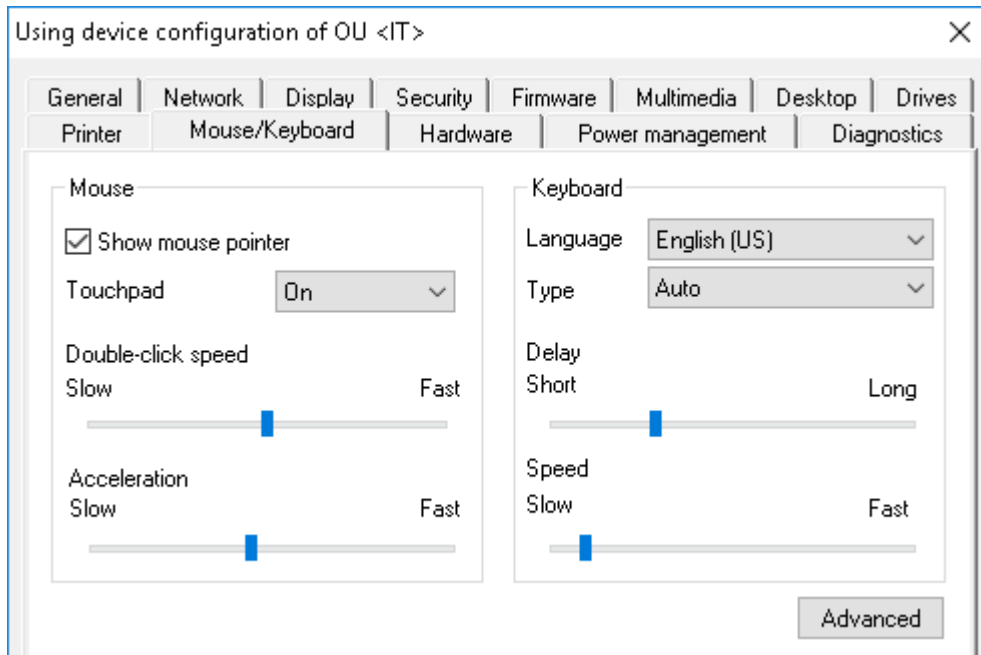
Option	Default keyboard shortcut
1 Hide display of primary monitor	<Ctrl><Alt>1
2 Hide display of second and all other monitors	<Ctrl><Alt>2

The digits **1** and **2** are fixed. The modifier keys <Ctrl><Alt> may be defined differently by you.

Defining alternative modifier keys

- ▶ Next to **Hide display (Keyboard shortcut)**, enter the desired modifier keys. For further information on how to spell the key names, see "Keyboard shortcuts" on page 84.

5.9. Mouse/Keyboard tab



5.9.1. Configuring mouse

- ▶ On the **Mouse/Keyboard** tab, under **Mouse**, edit the following fields:

Option	Description
Show mouse pointer	To hide the mouse pointer, clear the option. The mouse type is automatically identified.
Touchpad ¹ (for mobile devices)	<div>On Enables touchpad (default)</div> <div>Off Disables touchpad</div> <div>Auto Disables touchpad when a mouse is plugged in</div>
Double-click speed	Double-click speed defines the time interval between the two clicks of a double-click.
Acceleration	The faster the mouse pointer, the smoother the movements.

¹from Scout Enterprise Management Suite 15.9 and eLux RP 6.9.0

5.9.2. Configuring keyboard

- ▶ On the **Mouse/Keyboard** tab, under **Keyboard**, edit the following fields:

Option	Description
Language	Keyboard layout
Type	If the value is set to <code>Auto</code> (default), the keyboard type is identified automatically by the system.
Delay	The delay controls how long a key needs to be pressed until the letter is retyped.
Speed	The speed controls how fast a letter is retyped when a key is pressed.

5.9.3. Advanced mouse and keyboard settings

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

Option	Description	
Left-handed	Switches primary and secondary 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 they need to be pressed before you press a character key (` + A => à). Note: Some hardware platforms and some applications do not support this option.	
Console switch	Users can use key combinations to switch between consoles. If the option is not selected, console 1 (eLux desktop) is always shown. For further information, see Shortcuts in the eLux guide.	
Extended keys	Enables multimedia keys and other keys with special functions on the keyboard.	
Num Lock	On	Enables the numeric keypad of the client keyboard on device start (default)
	Off	Disables the numeric keypad of the client keyboard on device start
	Auto 1	Enables the numeric keypad on mobile devices and disables it on other devices

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

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

¹for Scout Enterprise Management Suite 15.3 and later versions

5.10. Firmware tab

The **Firmware** tab provides the relevant information required to perform a firmware update (software update) of the devices via network.

- 1 Network protocol for software package transfer from the web server to the devices
- 2 Name or IP address of the web server providing the eLux software packages and the image files
- 3 Optional: alternative web server for devices connected via VPN¹
- 4 Directory path of eLux software packages on the web server (container path)
- 5 Image file on the web server, also called image definition file or IDF, defines the software packages to be installed on the devices
The image is created with the ELIAS application and then made available on the web server.
- 6 Optional: UEFI file in eLux container with assignment of device types and UEFI firmware to be installed²
- 7 From 1-4 a URL is generated, which is used by the devices to update the firmware.
- 8 If a UEFI file is specified, the system generates a URL which is used by the devices to update the UEFI system.



Note

The image file and the container path can be parametrized if required.

¹from Scout 15 2107

²from Scout 15 2107


5.10.1. Configuring firmware updates



Note

The fields **Protocol**, **Server**, **Path** and **Image file** are used to build a URL used by the devices for firmware updates. The URL address is displayed below the **Path** field.

1. For the relevant device or OU, in the Scout Console, open **Device configuration > Firmware**.

Option	Description
Protocol	Network protocol of the web server for software package transfer to the clients (HTTP, HTTPS, FTP, FTPS)
Server	<p>Name (FQDN) or IP address of the web server containing the eLux software packages and the image definition file</p> <p>Optional: click  to specify an alternative web server for devices connected via VPN.¹ Enter its FQDN or IP address. The system displays a message if the name cannot be resolved or the IP syntax is incorrect.</p>
Proxy (optional)	<p>IP address and port number (3128) of the proxy server</p> <p>Format: IP address:port</p> <p>Example: 192.168.10.100:3128</p> <p>For Scout Enterprise Management Suite 15.3 and later versions, you can set a role for the static proxy² or choose <i>Dynamic</i>.</p>
User and Password (optional)	Username and password (if required) to access to the eLux software container of the FTP server
Path	<p>Directory path of eLux software packages on the web server</p> <p>Use slashes / to separate directories.</p> <p>Example: Use <code>eluxng/UC_RP6</code> to refer to the IIS web server directory</p> <p><code>W:\inetpub\wwwroot\eluxng\UC_RP6\</code></p> <p>If you use ELIAS 18, specify the path name defined during the ELIAS 18 installation.</p> <p>Example: <code>elias/UC_PR6_X64</code></p> <p>To distinguish by installed eLux major versions, use the container macro.</p>
Image file	<p>Name of the image definition file (IDF) on the web server which is used for firmware updates</p> <p>Depending on the object rights, an IDF name can be entered or an IDF is selected from the list-field. For further information, see Protecting firmware configuration.</p> <p>To define an alternative image for specific hardware models, use the Release macro.</p>

¹from Scout 15 2107 and eLux RP 6 2110.1

²supported up to eLux RP 6.8

Option	Description
Check for new version on start / shutdown	The device checks during start or shutdown whether any firmware updates are available and necessary. To allow users to decline an update, select User must confirm update .
Elias... button	Starts the ELIAS tool and opens the image definition file indicated in the Image file field
Security... button	The Security settings allow you to define a signature check before update through the client. Signature checks can be performed for the image definition files and/or eLux software packages.
Reminder... button	The Reminder Settings allow you to define whether 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 .

- Edit the following fields:
- Test the **Firmware** settings on a client. To do so, on the eLux RP 6 device, on the **Command panel**, click **Update**. For further information, see [Updating the firmware](#) in the eLux guide.

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

5.10.2. Protecting firmware configuration

Image definition files (IDF) are provided on the web server in an eLux container. They must be specified in the device configuration under **Firmware** in order for the devices to access the intended image in the event of an update request. Depending on the object rights defined, in the **Firmware** configuration, administrators are allowed to enter individual IDF names as free text or need to select one of the predefined IDFs from the list-field. The same applies to the software container (**Path** field) in the **Firmware** configuration.

To protect such critical firmware configuration parameters, the IDFs and the container paths to be selected or configured for a firmware update can be defined in advance. In combination with the relevant object rights, operational administrators can then only choose between predefined values.

For Scout 15 2107 and later versions, the firmware of UEFI systems¹ can be updated via the same mechanism as the software (firmware update). Therefore, an **UEFI file** field can be found in the same dialog that behaves accordingly.

Setting object rights for firmware configuration fields

The object rights for the **Image file**, **Path**, and **UEFI file** fields are each divided into **predefined** and **user-defined**. If you grant an administrator both rights, he can add new entries as free text as an

¹from eLux RP 6 2107

alternative to selecting a predefined entry from the list-field.



Requires

Administrator policies are enabled.

1. For the relevant OU, on the context menu, click **Object rights...**
2. Select the relevant administrator /administrator group and click **Edit object rights...**
3. For **Device configuration**¹ > **Firmware**, change the object rights as required by double-clicking or pressing the SPACE bar:

Image file (pre-defined)	<p>The administrator can only select one of the IDF s provided in the Image file list-field on the Firmware tab.</p> <p>The list-field contains predefined IDF s (see below). If predefined IDF s are missing, the list-field shows the recently used IDF s.</p>
Image file (user-defined)	The administrator is allowed to enter any IDF name into the text field.
Path (pre-defined)	<p>The administrator can only select one of the paths provided in the Path list-field.</p> <p>The list-field contains predefined paths (see below). If predefined paths are missing, the list-field shows the recently used paths.</p>
Path (user-defined)	<p>The administrator is allowed to enter any path into the text field.</p> <p>The path must correspond to a software container on the web server.</p>
UEFI file (pre-defined)	<p>The administrator can only select one of the files provided in the UEFI file list-field.</p> <p>The list-field contains predefined UEFI files (see below). If predefined files are missing, the list-field shows the recently used UEFI files.</p>
UEFI file (user-defined)	The administrator is allowed to enter any UEFI file name into the text field.

4. Confirm with **OK**.

For further information, see [Administrator policy](#).

Predefining Firmware configuration values

1. On the menu, click **Options > Advanced options > Predefined IDF s**.
2. To add additional IDF names, click the **Add** button and edit the new entry. Note that the spelling must match the actual names.

¹formerly Setup

3. For all entries you want to share in the firmware configuration, select the **Valid** option.
4. Confirm with **Apply** and **OK**.

*All valid IDFs, container paths and UEFI files are provided in the device configuration under **Firmware** and can be used by authorized administrators.*



Note

Scout Enterprise does not check the physical existence of files or container paths on the web server.

For further information, see [Predefined IDFs and containers](#).

5.10.3. Different hardware models

- from eLux RP 6 2103 -

To update the firmware of devices with an alternative image depending on the hardware model, the release macro is available. For example, you can update newer model types to a CR version, while older models remain on their previous (LTSR) image. If there are no changes to the previous image, as in the LTSR image example, all devices whose type is not whitelisted are unaffected by the update command.

For the release macro, in the firmware configuration, an `__RM__` string is inserted into the image file name.

Path: Image file:
 https://websrv.sampletec-01.com/eluxng/UC_RP6_X64/ITaa__RM__.idf

Before an update is executed, an appropriately configured device resolves the macro using a whitelist:

- If the model type of the device is part of the whitelist, the `__RM__` parameter is replaced by a string you define. So the device will pull the alternative image with the newly created name.
- If the model type of the device is **not** part of the whitelist or the whitelist cannot be loaded, the `__RM__` parameter is removed from the image name. This leaves the device on the previous image (image name as in the firmware configuration, but without the `__RM__` string).

Creating a whitelist



Requires

The web server must support the file extension `.mee` in the MIME type settings.

1. Create a text file named `elux.mee`. Then, enter the section name `[__RM__]`.



Note

Make sure you use the correct spelling for the section name: Two underscores followed by RM (uppercase) followed by two more underscores.

2. Begin the second line with `ReplaceWith=` and then define a short string.

This string must be included in the image name for the alternative image, see below. If you do not specify anything, the string CR is set by default.

3. Begin the third line with the string `Product=`. Then, enter all model types you want to receive the alternative image in the same line.

Separate the model types by white spaces.

Enter type names that contain white spaces without the white spaces.

```
1 [__RM__]
2 ReplaceWith=CR
3 Product=D3544-A1 17e2 D3313-G1
```

You can retrieve the model type of a device from the Scout Console. It is shown in the **Properties** window in **Asset > Hardware information > Type**. On the devices, the model type can be found in the `terminal.ini` under `HWInfo.Product`.

4. Copy the `elux.mee` file into your `UC_RP6_X64` container on the web server.

Preparing the software container on the web server (ELIAS)

1. Leave the existing image as you want the devices outside the whitelist to receive it.

Example: `recovery.idf`

2. In ELIAS, create an alternative image that you want the devices in the whitelist to receive.

For example, to be able to update newer models to a CR version, create an image containing the eLux packages of the latest CR version.

3. Assign the same name to the alternate image, but include the string defined in the whitelist under `ReplaceWith=`

Example: `recoveryCR.idf`

The software container now contains two images whose names differ only by the defined string, and the whitelist `elux.mee`

Modifying device configuration

1. For your OU, open the device configuration under **Firmware**.
2. Under **Image file**, insert the `__RM__` string into the file name, see screenshot above. The file extension `.idf` must be kept.

Example: revover__RM__.idf



Note

Make sure you use the correct spelling: Two underscores followed by **RM** (uppercase) followed by two more underscores.

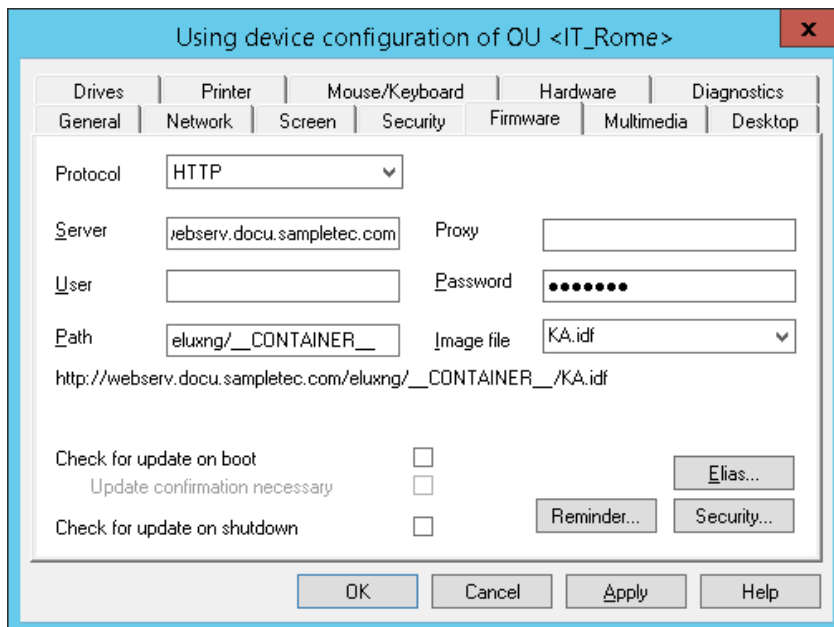
3. Confirm with **Apply** and **OK**.

The next update command on your OU will apply the alternative image to the whitelisted devices.

5.10.4. Different eLux versions

The `__CONTAINER__` parameter is useful if you have more than one major eLux version in use and you want to update the firmware of multiple devices regardless of their major version. All updated devices remain within their respective major version.

The parameter replaces the container path in the URL



The `__CONTAINER__` parameter is part of the directory path and parametrizes the relevant software container (directory) on your web or FTP server. When the administrator sends an update command to a device configured with container parameter, the parameter is resolved by a macro according to the installed eLux main version.

Example:

If you run devices with both, eLux RP 5 and eLux RP 6, the eLux RP 5 devices require the `UC_RP5` container, while the eLux RP 6 devices require the `UC_RP6_X64` container. To provide all devices with their appropriate software, in **Device configuration > Firmware > Path** of all devices, use the `__CONTAINER__` macro parameter. The devices then resolve the container parameter according to their installed major version to `UC_RP5` or `UC_RP6_X64`, respectively. The advantage is that an image file with the same name can be used for both platforms. So, in ELIAS, you would create an image with the same name for eLux RP 5 and for eLux RP 6.



Note

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

ELIAS 18 containers

To use the container parameter with ELIAS 18, choose the following names for your containers:

UC_RP5	eLux RP 5
UC_RP6	eLux RP 6.1 and eLux RP 6.2 (32-bit)
UC_RP6_X64	eLux RP 6.3 and later versions (64-bit)

For further information, see [Creating a container](#) in the **ELIAS 18** guide.

Spelling of the container parameter

When replacing a fixed container name by the container parameter, make sure you use the correct spelling:

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



Note

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

5.10.5. Different BIOS systems (UEFI)

- For eLux RP 6.2 and earlier versions -



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`). For eLux RP 6.3 and later versions, the 64-bit kernel is used and the system automatically identifies whether it is UEFI or non-UEFI.

To update UEFI devices and devices with a traditional BIOS in one step, use the Base System parameter¹ `__BM__`. It is meant for shared firmware configuration. The macro string is inserted into the IDF name. Whenever an update command is run, the device resolves the Base System parameter due to its BIOS system (device with UEFI | device without UEFI). Devices running eLux RP 6.3 or later versions ignore the Base System macro in the image name.

¹formerly: BIOS macro

Configuring firmware updates for mixed environments

1. In ELIAS, create an image for the UEFI devices. Make sure you include the 64 bit kernel package. The image file name must contain the string `EFI`.

Example: `kaEFIrc.idf`

2. In ELIAS, create a second image for the devices without UEFI. The image name must correspond to the one for UEFI devices but without 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` parameter then evaluates the relevant container.

3. In the Scout Console, for the relevant OU, open **Device configuration**¹ > **Firmware**.
4. In the **Image file** field, enter the file name of your IDF. Instead of the `EFI` string within the file name, insert the string `__BM__` for the Base System macro. The file name extension `.idf` and the rest of the file name must be maintained.

Using base device configuration

Drives	Printer	Mouse/Keyboard	Hardware	Diagnostics
General	Network	Screen	Security	Firmware

Protocol:

Server: Proxy:

User: Password:

Path: Image file:

http://webserv.docu.sampletec.com/eluxng/__CONTAINER__/ka__BM__rc.idf

Check for update on boot ☐

Update confirmation necessary ☐

Check for update on shutdown ☐

Elias... Reminder... Security...

OK Cancel Apply Help

The image file specified in the figure above requires the existence of the image `karc.idf` for devices without UEFI and of the image `kaEFIrc.idf` for UEFI devices.

5. Edit the other fields of the **Firmware** tab. For further information, see [Configuring firmware update](#).

When an update command is run, the relevant devices evaluate the Base System parameter due to their BIOS system and convert the parameter either to `EFI` or to an empty string. In the example shown above, the following URLs are generated:

¹formerly Setup

UEFI devices (x64)	<code>http://webserv.docu.sampletec.com/eluxng/UC_RP6/kaEFIrc.idf</code>
Non-UEFI devices (x86)	<code>http://webserv.docu.sampletec.com/eluxng/UC_RP6/karc.idf</code>
Devices running eLux RP 6.3 or later	<code>http://webserv.docu.sampletec.com/eluxng/UC_RP6/karc.idf</code>

The system automatically identifies whether it is UEFI or non-UEFI.

Special option for HP t630

The HP t630 device can use a 64-bit kernel without UEFI.¹ The HP t630 resolves the `__BM__` parameter to the value `x64`. For the example above, the following URL is generated:

HP t630 non-UEFI (x64)	<code>http://webserv.docu.sampletec.com/eluxng/UC_RP6/kax64rc.idf</code>
------------------------	--



Note

The HP t630 is only supported for the 64-bit Linux kernel, UEFI (x64) or non-UEFI (x64).

Spelling of the Base System 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 Base System macro in the firmware configuration or in the recovery settings **Options > Recovery settings...**

5.10.6. Firmware security through signature

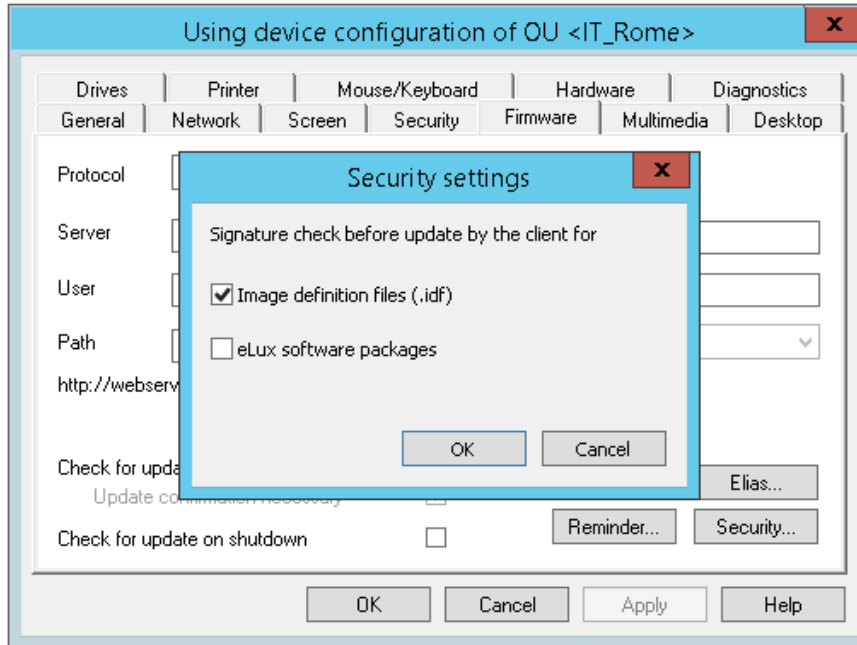
You can configure the firmware configuration in the Scout Console or on the client to have the client check signatures each time before an update is performed. An update is then only performed if the signature of the image definition file (IDF) and/or the signature of the eLux software packages have been successfully verified. The update cannot be run, however, if the IDF or one of the eLux software packages to be installed does not have a valid or verifiable signature.

Important A signature check of eLux software packages requires an update partition on the client computer. On devices without an update partition, signatures can only be checked for image definition files but not for eLux software packages. For further information on update partitions, see [eLux partitions](#).

¹for eLux RP 5.7/6.2 and later versions

Activating signature check

1. In the Scout Console, under **Device configuration**¹ > **Firmware**, click **Security...**.
On the eLux RP 6 client, select **Configuration panel** > **Firmware** > **Check signatures before update**.



2. Under **Signature check before update**, select the **Image definition file** option and/or the **eLux software packages** option.
3. Confirm with **OK** and **Apply**.

U Note

In eLux, both options are provided on the **Firmware** tab or in the **Firmware** dialog.

*The signature verification results are documented in the update log file on the client. After an update has been performed, the update log file is sent to the Scout Server. To view it for the selected device, in the **Properties** window, double-click the **Update status** field.*

Certificates

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. To do so, use the Scout Enterprise feature **Files configured for transfer**. For eLux packages provided by Unicon, all required certificates are included in the BaseOS.

For further information on how to create IDF signatures, see [Signing an image](#) in the **ELIAS** guide.

¹formerly Setup

5.10.7. Update deferment by users

- applies to firmware updates (software) and UEFI updates¹ -

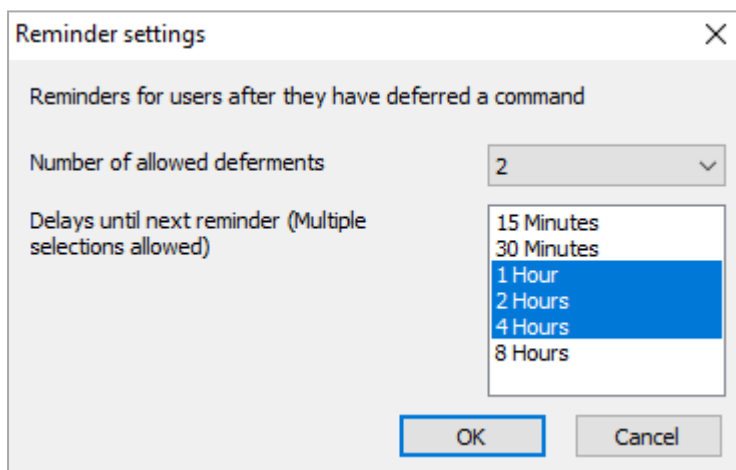
This feature allows users to determine the update time as soon as the administrator runs an **Update** command. This allows users to avoid firmware updates while using the device.

The client reports the current update process status to the Scout Server. The status can be viewed in the Scout Console in the **Update State/UEFI 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 users

1. For the relevant devices, open **Device configuration > Firmware > Reminder...**
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 users can choose when they receive the next reminder.

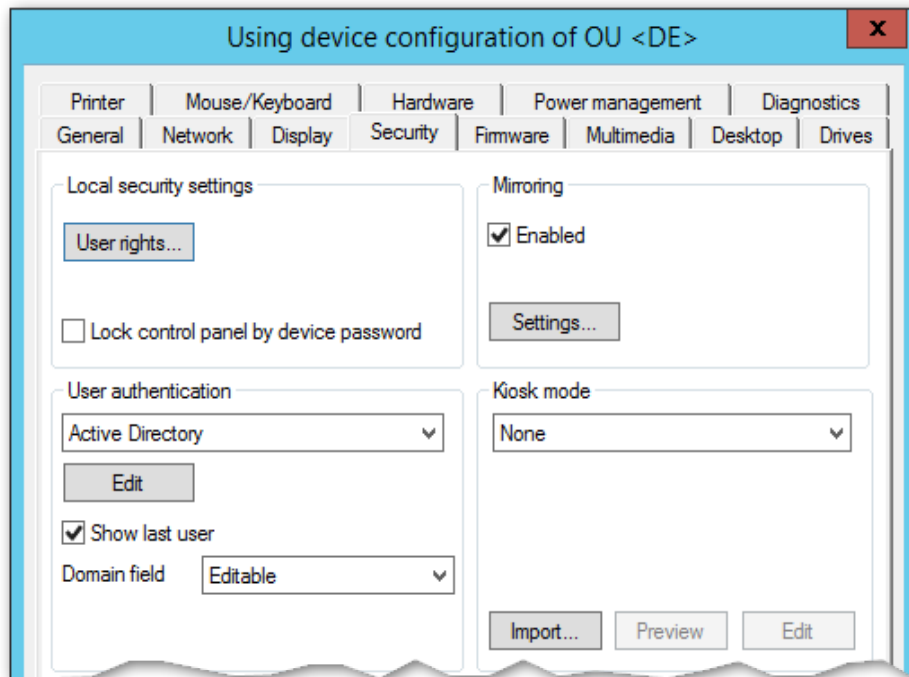


*The ability for users to defer updates is enabled. If the admin performs an Update command with the **Inform user** option, the user will receive a system message including deferment options. For further information, see [User information before update](#).*

Important Update deferment must be configured once on the **Firmware** tab and additionally activated for each **Update** command you run in the **Command** dialog via the **Inform user** option. For further information, see [Performing updates via command](#).

¹from eLux RP 6 2107

5.11. Security tab



5.11.1. User rights

To prevent users from configuring defective or unwanted settings locally on the client, you can disable user rights for individual features.

Functions that you disable via the user rights are not displayed on the device.

User rights can be configured for OUs and for individual devices, even for individual fields. For example, for security reasons, you might want to disable all tabs, but enable specific options such as some screen settings.



Note

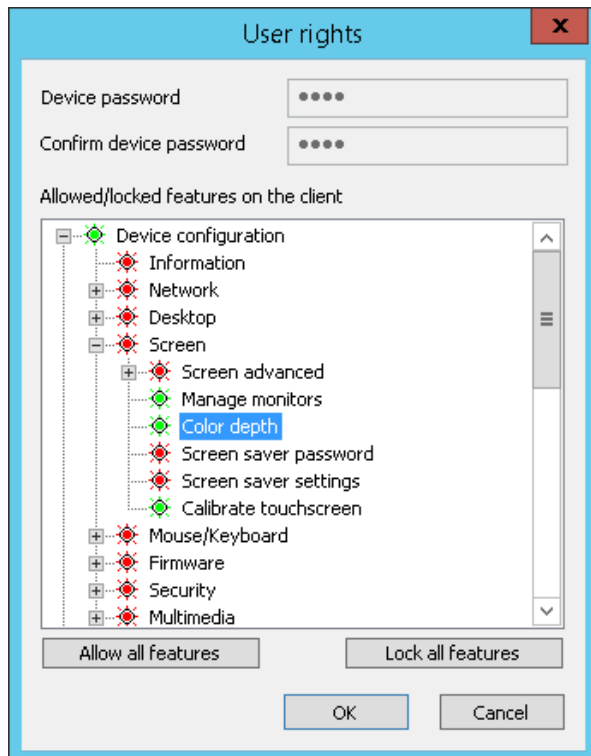
If you allow local device configuration for some features, you can prevent the relevant fields and sections from being overridden by updating Scout Enterprise configuration data. For further information, see [Supporting local device configuration](#).

User rights are available for the following functions:

- Device configuration
- Application definition
- General functions such as **Log off**

Modifying user rights for device configuration

1. On the **Security** tab, under **Local Security**, click **User rights**.



The **Device configuration** node refers to the devices' device configuration and its structure corresponds to the Configuration panel dialogs of eLux RP 6.

In addition, among the user rights under **Security > Scout settings**,¹ you will find options for the fields **Info1**, **Info2** and **Info3** shown in the Scout Console in the **Properties** window of a device. On the devices, they are displayed in the **Configuration panel** under **Information**.²

2. Expand the **Device configuration** node and navigate to the desired function.
3. To modify the status of a function, double-click it or press the SPACE key.

Allowed functions 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. In the **User rights** dialog, expand the **Application definition**³ node.
2. To allow or block users from creating, editing, or deleting application definitions, change the function's status. To do so, double-click it or press the SPACE key.

Allowed functions are displayed in green, locked features are displayed in red.

¹for eLux RP 6 under Security > Info 1-3

²For eLux RP 6.5 and later versions, only one user right is used for all tree Info fields (Security > Info1-3).

³up to eLux RP 6.2 and Scout Enterprise 15.3: Configuration

If you lock the **Application definition** node, on the device, the **Applications** tab of the Configuration panel (Lux RP 6) is disabled and users will not be able to view the application definitions.



Note

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

Modified user rights become active on the next restart of the devices.

5.11.2. Local security settings

Protecting control panel by device password

- for eLux RP 5 devices only -

As an administrator you can secure the opening of the control panel by requesting the device password.



On the **Security** tab, under **Local security settings**, select **Lock control panel by device password**.



Note

You can also hide the icon that opens the control panel. For further information, see the **System bar** settings under **Advanced desktop settings**.

5.11.3. Configuring mirroring

1. On the **Security** tab, under **Mirroring**, select **Enable**.



Note

After you enable mirroring, the device needs two restarts to be able to start the VNC server.

2. Click **Settings...** for configuration:

Option	Description
Password (optional)	<p>If you define a mirror password, the password will be requested before a mirror session can be started.</p> <p>The password must have 6 characters minimum and 8 characters maximum.</p>
Read-only access	<p>Allows read access only</p> <p>If not selected, in the mirroring session, the user may still select the Read only option so that the administrator has read-only access.</p>
User must confirm within	<p>Before the mirror session can be started, the user must confirm.</p> <p>Specify how many seconds you want to display the request before the connection is aborted.</p>
Log mirror session	For each mirror session, a log file is created and saved to a sub-directory of the Scout Server files directory.
Encrypt data transmission	Uses encrypted transmission
Allow from Scout Enterprise only	Mirroring is only allowed if the Scout Console is used.
Log off on disconnection	Automatic logoff as soon as the connection is aborted

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

For further information, see [Mirroring](#).



Note

The user can cancel a mirror session at any time.

5.12. User authentication

User logon and authentication can take place directly on the eLux device after device start-up or on the back-end server to which the device connects.

eLux supports user authentication with Active Directory. This can be done via username and password or via smart card. Both eLux methods are configured on the **Security** tab of the device configuration as described below. Additionally, authentication via Evidian is supported.¹

Note that for authentication under eLux, the appropriate eLux software packages must be installed on the devices. For smart card check, in addition to the eLux functions, appropriate middleware and hardware drivers for the smart card readers are required.

¹from Scout Enterprise 15.11

5.12.1. Configuring user authentication



Note

The eLux package **User authentication modules** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

1. In the device configuration, under **Security > User authentication**, choose from the following authentication methods.

None	Disables user authentication
Active Directory	Active Directory (Microsoft directory service)
AD + smart card	Smart card with Active Directory
Evidian ¹	Identity and access management via RFID or smart card

On the eLux RP 6 client, under **Security > User authentication**, enable user authentication. Then under **Authentication type**, choose the method.

2. Click **Edit**.
3. On the **AD directory** tab, specify the server, server list or domains to which users may log on. Define multiple entries, if you want to create a selection for users when they log on.
For Evidian, on the **Evidian server** tab, specify a server or server list.
4. To help users log on quickly, select the **Show last user** option.
5. Only for AD: In the **Domain field** list, choose whether you want to show users the specified domain so they can edit it, or whether you want to hide it.
6. Confirm with **OK**.

After you have enabled user authentication, the users will be prompted for their username and password after the next device restart.

The screen saver is automatically protected by password.



Note

To devices that are not managed by Scout, administrators may log on with the username `LocalLogin` and device password to correct any settings, if required.

¹from Scout Enterprise 15.11

Active Directory (AD)

Define multiple domains that can be displayed with friendly names. In the client logon dialog, users can then choose between default and alternative domains.



Note

To enable users to log on to different domains, the following software packages must be installed on the devices: **User authentication modules** and **Security libraries**.

AD directory tab

- ▶ Click **Add** to create one or more entries. Then edit the entry (F2 or double-click).

Option	Description
Name (optional)	Display name of the domain
Server, server list or domain	<p>IP address or name of the domain controller</p> <p>To specify more than one domain/server, separate them by spaces.</p> <p>Example: <code>int.sampletec-01.com dev.sampletec-01.com</code></p> <p>If the server is not located in the same subnet as the client, enter the fully qualified domain name (FQDN).</p> <p>If you define more than one domain, users will be able to choose a domain from a list. The domains are shown with their display name. The first entry of the list is the default domain in the AD logon dialog on the client. You can specify applications that are shown in only one of the domains.</p>



Note

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

User variables tab

Based on LDAP attributes, you can define local variables and use them in the device configuration and application definition. For further information, see [User variables](#).

Automated logon tab

- from Scout Enterprise 15.9 -

By using predefined logon data, terminals can, for example, run in kiosk mode under an AD service account.

Username, password and domain can be set as variables.

Active Directory + Smart card

To enable users to use smart card readers, install the relevant middleware on the devices. **sc/interface** by Cryptovision is a smart card middleware that integrates smart cards and other smart tokens into IT environments. sc/interface supports more than 90 different smart card profiles. For further information, see the Cryptovision web page.



Note

For smart card authentication, eLux packages for middleware (such as **Cryptovision sc/interface**) and for the hardware drivers (such as **PCSC Lite**) must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

Smart card tab

Option	Description
Behaviour of smart card on removal	If you choose <code>Lock screen</code> , in the Screen saver settings, Password protected will be selected. ¹
Allow logon with user-name+password	Smart card application allows user/password logon via the User-name & Password link.
Show Username+password dialog by default ²	Logon via username + password can be forced despite smart card configuration. To use this option, enable Allow logon with username+password .

Certificate tab

Certificate-based logon 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 device.

User variables tab

Based on LDAP attributes, you can define local variables and use them in the device configuration and application definition. For further information, see [User variables](#).

For the **AD directory** and **Automated logon** tabs, see [Active Directory \(AD\)](#).

¹for eLux RP 6.3 and later versions

²from Scout Enterprise Management Suite 15.5 and eLux RP 6.6

Enhanced logging for smart card authentication

When using **PCSC Lite**, you can have an additional log file `/tmp/PCSCDlog.txt` created. To do so, temporarily enable enhanced logging via **Device configuration > Diagnostics > Enhanced logging for smart card support**¹. After diagnosis, we recommend that you disable the enhanced logging function in order to avoid unnecessary strain on the flash memory capacity of the device.

Evidian



Note

The eLux package **Evidian** must be installed on the clients. For smart card authentication, eLux packages for the middleware (such as **Cryptovision sc/interface**) and for the hardware drivers (such as **PCSC Lite**) must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

With Evidian access management, you can connect via RFID or smart card. Evidian uses the SOAP network protocol.

- ▶ On the **Evidian server** tab, create an entry and edit the following fields:

Option	Description
Name (optional)	Display name of the Evidian server
Server or server list	Specify your Evidian server depending on whether you use HTTP or HTTPS in the following format: <code>http://<FQDN or IP address>:9764/soap</code> <code>https://<FQDN or IP address>:9765/soap</code> To specify more than one server, separate them by spaces.
Use smart card	Enables authentication via smart card
Allow logon with user-name+password	Users may alternatively log on with username and password.
Secret	Copy the secret from the registry entry of the Enterprise Access Management server <code>HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\Framework\Authentication</code> from the key <code>ExternalRoamingSessionSecret</code> . Do not encrypt.

You can configure to show users the system bar during logon. This allows them to access the Configuration Panel and Command Panel. For further information, see "Starting Configuration panel from logon dialog" on page 125.

¹from Scout Enterprise 15.10 and 15.9.1000 for eLux RP 6.8 and later versions

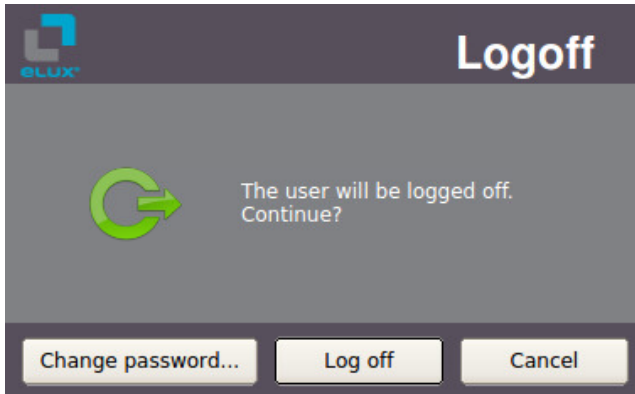
5.12.2. Additional options for AD users

If Active Directory is used for user authentication, users log on with their AD domain account and password on their device. Pass-through logon is supported by applications which provide access to back-end systems (Citrix, RDP, VMware).

On the device, in the Configuration panel under **Information**, the user logged on is shown.¹

Change password

To change the password, users choose the eLux command **Logoff** and then click **Change password**:



Password-protected screen saver



Note

When user authentication is enabled, password protection of the screen saver becomes active and cannot be turned off.²

The password is set to `$ELUXPASSWORD`. For further information, see [Where to apply user variables](#).

The screen saver becomes active after the defined time period and the system is locked. By pressing a key or moving the mouse, a dialog is displayed for unlocking. It provides the following options to users:

Option	Button	Description
The logged-on user unlocks the screen by entering his/her password / smart card	Unlock	Default

¹for eLux RP 6.4 and later versions

²for eLux RP 6.3 and later versions

Option	Button	Description
Another person leaves a message for the logged-on user	Message	<p>The screen remains locked. The logged-on user receives a notification with the message when he or she unlocks the screen.</p> <p>This function is enabled by default and can be disabled by the following Advanced file entry:¹ File: <code>/setup/terminal.ini</code>, section: <code>xscreensaver_dialog</code>, entry: <code>MessageEnabled</code>, value: <code>false</code></p>
Another user authenticates to log off the previous user (and to log on), restart or shut down the device. ²	Log off	<p>Useful if devices are used by multiple users: Allows users to reuse devices that have been left without logging off and therefore are blocked</p> <p>Once the new user has authenticated, the Restart, Shut down and Log off buttons become active. In any case, the previously logged-on user is logged off.</p> <p>This function is disabled by default and can be enabled by the following Advanced file entry: File: <code>/setup/terminal.ini</code>, section: <code>xscreensaver_dialog</code>, entry: <code>ShowSysCommandButtons</code>, value: <code>true</code></p>

Important Data loss may occur if the **Log off** option is used followed by restart, shutdown, or logoff. The user currently logged on is logged off regardless of whether the documents or data last edited have been saved.

Service app

- for eLux RP 6.4 and later versions -

You can enable AD users to start eLux in service mode. To do so, define a service app that can be started from the logon dialog using the **Service** button. For further information, see [Defining a service app](#).

Starting Configuration panel from logon dialog

- for eLux RP 6.5 and later versions -

You can enable AD users to access the Configuration panel before they log on. This allows them to connect to a WLAN or VPN or to change the language before logging on.

You can show the system bar for users authenticating via Evidian before they log on. This allows them to access the Configuration panel and Command panel.

- ▶ For the relevant devices, under **Security > User rights** on the bottom, enable the user right **Start Config panel from logon dialog**.

¹for eLux RP 6.8 and later versions

²for eLux RP 6.8 and later versions



AD: On the next restart, the logon dialog shows the button for opening the Configuration panel, so AD users can access the options you allow them to.

*Evidian: While the Evidian authentication manager is displayed, users may open the Configuration Panel dialogs and access commands such as **Shut down** and **Restart** in the Command Panel.*



Note

By default, the user right **Start Config panel from logon dialog** is disabled.

5.12.3. User variables



Note

If you want to use user variables, the **User authentication modules** and **Open LDAP** packages must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

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

Predefined user variables are

\$ELUXUSER

\$ELUXDOMAIN

\$ELUXPASSWORD

The variables are used when users log on and [user authentication](#) is active.

Where to apply user variables



Note

To use this feature, user authentication via Active Directory is required.

When they are applied, user variables must have a leading \$. User variables can be applied in the following fields:

Device configuration

	Field	User variable
Drives	Username	\$ELUXUSER
	Password	\$ELUXPASSWORD
	Directory, Server, Share	Any \$ELUX variable
	Browser home directory	Any \$ELUX variable
Power management ¹	Enable screen saver (also manual activation)	\$ELUXPASSWORD

¹for Scout Enterprise 15.2 and earlier versions: Screen tab

Application definition

	Field	User variable
Citrix	Server	Any \$ELUXvariable
RDP	Username	\$ELUXUSER
VMwareView	Password	\$ELUXPASSWORD
	Domain	\$ELUXDOMAIN
Browser	Proxy type, Proxy port	Any \$ELUXvariable
Tarantella	Server	Any \$ELUXvariable
Local / Custom application	Parameter for all programs run from the command line Example: eluxrdp /vint.sampletec-01.com.de /u:\$ELUXUSER /p:\$ELUXPASSWORD	Any \$ELUXvariable

Defining new user variables



Note

To use this feature, user authentication via Active Directory is required.

You can define your own user variables as local variables based on LDAP attributes. The variable definition has the form `Local variable = LDAP variable`

1. On the **Security** tab, under **User authentication**,¹ select `Active Directory (AD)` or `Active Directory + Smartcard`.
2. Click **Edit**.

¹formerly Access authorization

- Under **User authentication > User variables**, edit the following fields:

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

- Confirm with **OK** and **Apply**.



Note

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

5.13. 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** option separately.

By default, the priority is defined: USB - Analog - Digital.

- ▶ To change priority, move the list entries by using drag-and-drop operations.

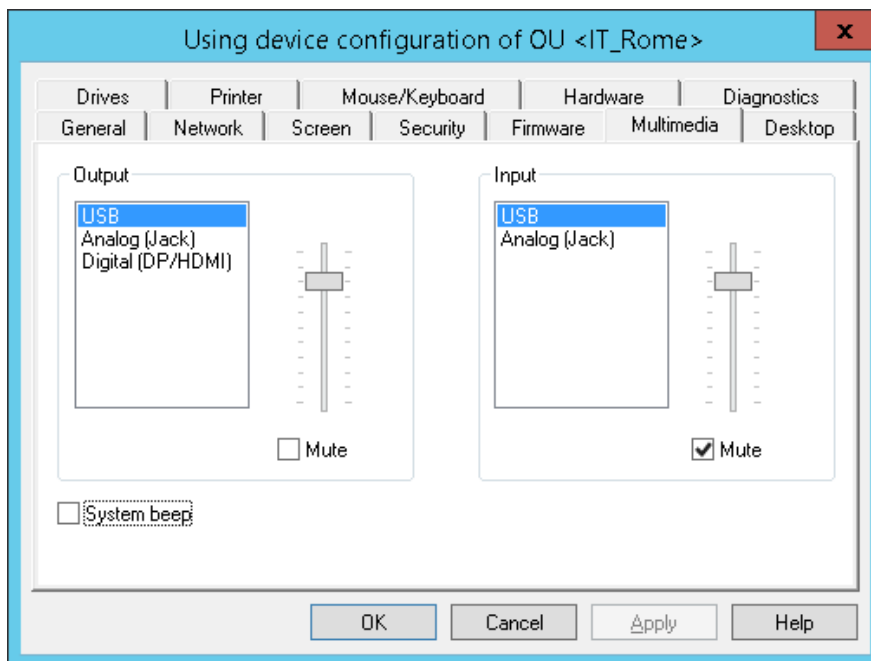
The audio **input** devices are grouped in classes depending on their connector:

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

For each device class, you can control the sensitivity and **Mute** option 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
System beep	Acoustic feedback signal when switching off the client
Priority of device classes	By using drag-and-drop operations, you can change the priority of the device classes for input and output. The top entry has the highest priority.

5.14. 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.

5.14.1. Defining a network drive

1. In **Device configuration > 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
Username and password	Windows username 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 logon data are used to access the directory. The fields Username 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, 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 via ELIAS.

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

The directory path `/smb/` is automatically inserted before the directory name. The data are provided on the local flash drive under `/smb/<Directory name>`.

Example: `/smb/share`

Note
Here, you may apply LDAP user variables. For further information, see [Where to apply user variables](#).

To make browser settings such as bookmarks permanently available, define a network drive as the browser home directory. For further information, see [Browser home directory](#).

5.14.2. 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, mount points are assigned chronologically: The first device is assigned /media/usbdisk, the second one media/usbdisk0, etc.

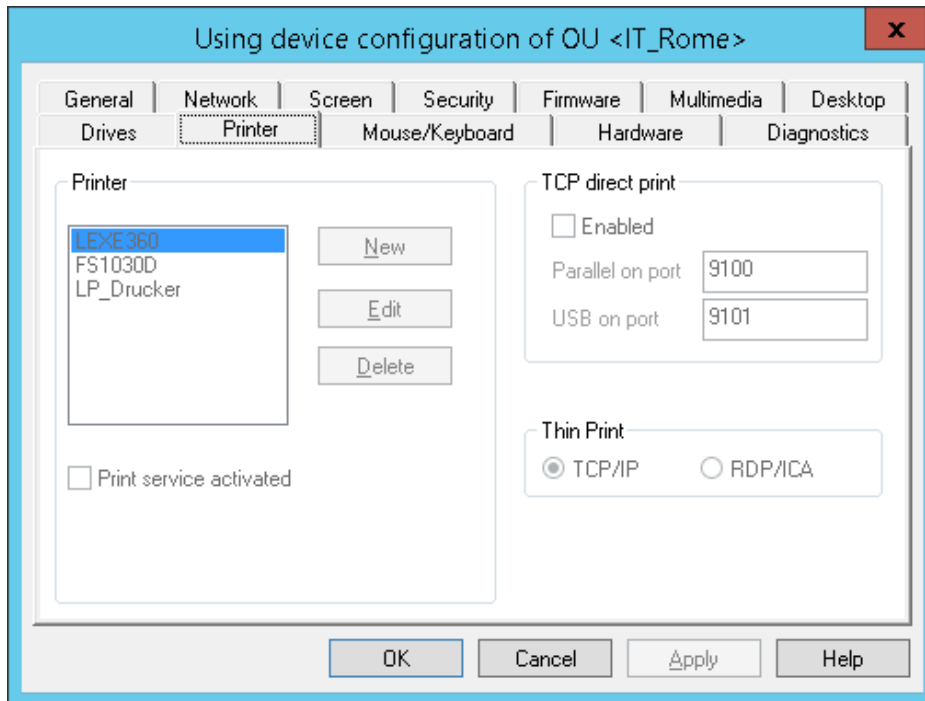
Mounted devices are shown as live information icons. For managed devices, the administrator can suppress the display of live information icons.

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

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

5.15. Printer tab

eLux supports printing from local applications both to locally connected printers and to network printers. In addition, other systems or servers within the network can use a locally installed printer on a Thin Client running eLux. Next to the protocols LPR and TCP direct printing, proprietary protocols are also available.



In the Scout Console, in **Device configuration > Printer > New**, you can define and configure local printers with logic names.

5.15.1. Defining a locally connected printer

1. In the device configuration, on the **Printer** tab, click **New**.
2. In the **Define printer** dialog, type a name for the printer.
3. In the **Connection type** list, choose how the printer is connected to the client.
4. In the **Filter** list, choose whether to use a filter. To print via a Linux Shell, select the `text` filter. For further information on the filters, see [Defining a network printer](#).
5. Confirm with **Apply** and **OK**.

5.15.2. Defining a network printer

1. In the device configuration, on the **Printer** tab, click **New**.

2. In the **Define printer** dialog, type a name for the network printer.
3. In the **Connection type** list, select **Network**.
4. In the **Filter** list, select one of the following options:

Option	Description
None	The printing data from the session are forwarded to the printer in an unfiltered format.
Text	Enables printing from a local shell
PCL2	Enables printing to non-postscript printers in PCL format If the users do not print from a Citrix session, the connected printer must support one of the following languages: PCL2 , PS(Postscript) or PDF .

5. In the **Printer address** field, enter the IP address of the server.
6. In the **Printer queue** field, enter the share name of the printer.
7. In the **Driver name** field, enter the printer's driver name. The driver is used for printing from a Windows session.

Important Make sure that the printer driver name is spelled in the same way as the name of the installed driver on the server. The name is case-sensitive and sensitive to white spaces. If the names do not match, the server cannot identify the driver.

For further information, see [Citrix auto-created printers](#).

8. Confirm with **OK** and **Apply**.

For further information, see your printer's manual.

5.15.3. Sharing printers

All printers defined in **Device configuration**¹ > **Printer** can be shared with other systems via LPD within the network.

1. In **Device configuration** > **Printer**, select the **Print service activated** option.
2. Activate the Windows LPD service (Line Printer Demon).

This option ensures that the print service is started at the client. All printers defined in the list can be used to print jobs from network devices.

The printers are controlled by the CUPS server.

5.15.4. Selecting a default printer

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

The list provides all defined printers for this element.

¹formerly Setup

²formerly **Advanced settings**

5.15.5. CUPS

The CUPS server is installed by default on the clients (**Print Environment (CUPS)** package) and allows printing from local applications and the use of locally attached printers.

The Common UNIX Printing System™ (CUPS™) is a free-of-charge software from Easy Software Products. It provides a common printing interface within local networks and dynamic printer detection and grouping. For further information, see www.cups.org.

The CUPS server can print to serial and parallel ports, USB and the network (LPD).

The CUPS printing system 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 such as **PostScript to PCL** on the CUPS server.

CUPS web interface for print management



Note

The eLux package **Print Environment (CUPS)** and the included feature package **Web administration service** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

To manage print jobs, the user can access the CUPS web interface in a local browser with the following URL:

```
http://localhost:631
```

The web interface can also be used by the administrator to configure the CUPS server. To do this, you must enter the credentials for the local administrator account (`LocalLogin` and device password).

5.15.6. Citrix auto-created printers

Citrix XenApp provides automatic configuration of printers (**autocreated printers** or **dynamic printer mapping**). When the user logs on through a Citrix connection, an automatic printer definition is created on the Citrix server. The printer definition can only be used by the logged-on user and is deleted when the user logs off.

Citrix uses either the specified printer driver or, if not available, the universal Citrix printer driver, which is not tied to any specific device.

Configuring local printer for auto-creating on the client:

1. In **Device configuration > Printer**, specify one or more printers.
2. In the **Define Printer** dialog, in the **Name** box, enter the Microsoft Windows printer's name precisely as listed in the drivers list of the server. The name is case-sensitive.

When the user connects to the Citrix server, the automatically created client printers are shown in the printer settings.

If the specific driver is not installed on the application server or the name is not identical, the client printer can not be created and the universal Citrix printer is used.

Citrix Universal Printing

The universal Citrix printer and various printer settings can be configured on the Citrix server, administrator rights provided.

For further information, see the **Citrix Product Documentation**.

5.15.7. TCP direct print

The print data can be received directly via TCP/IP and sent to the parallel port or USB port to the printer. The data are not modified before printing and there is no spooling of print jobs. TCP/IP handles the flow control.

Configuring TCP direct print

1. In **Setup> Printer**, under **TCP direct print**, select the option **Enabled**.
2. Specify the relevant port number for the communication.
The default port numbers are:
9101 for USB printers
9100 for parallel port printers



Note

Note that the specified ports are opened on the client.

To print from a Windows session, for the printer port, choose a standard TCP/IP port. Specify the client IP address and the TCP/IP port selected in the previous step. Select `Raw` for the protocol in Windows.

5.15.8. ThinPrint

ThinPrint software from ThinPrint GmbH allows optimized network printing across various platforms. ThinPrint is a print protocol that, unlike TCP direct print, LPR or CUPS, allows bandwidth limitation. It is therefore recommended for networks with low bandwidth (WAN).

The software consists of a server component and a client component. The ThinPrint server processes the print data for the target printer and sends them to the client in compressed form. The ThinPrint client receives the print jobs from the server, decompresses and forwards them to the selected printer.

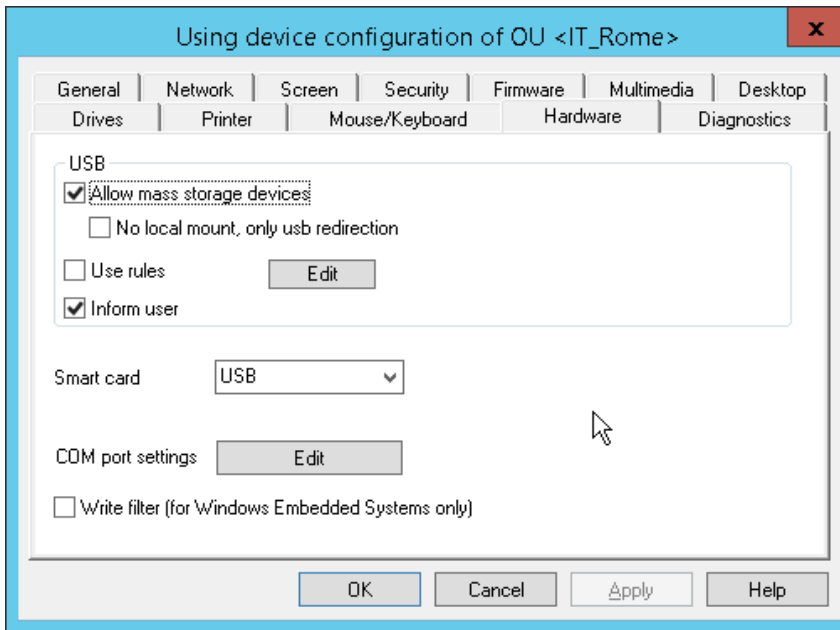
ThinPrint server and client are connected via TCP/IP.

Configuring ThinPrint

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

¹formerly Setup

5.16. Hardware tab



5.16.1. USB mass storage devices and card readers

Option	Description
Allow mass stor- age devices	Allows using connected USB mass storage devices If the local use of USB devices via mountpoints is allowed, connected USB devices are shown on the system bar in the systray (eLux RP 5) or live information (eLux RP 6). ¹
No local use, only USB redirection	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 such as smart card readers.
Edit	Opens the USB rules dialog: Define rules to explicitly allow or deny individual device models.

¹for eLux RP 6.4 and later versions

Option	Description
Inform user on changes	When a USB mass storage device is connected or disconnected, a live information message ¹ is displayed.
Card reader	Enables card readers on the selected port
Power line frequency ²	Allows to set the refresh rate of webcams to 50 Hz or 60 Hz
COM port settings	Set particular COM port settings such as speed, parity, stop bits
Write filter (only Windows Embedded)	The user is not allowed to store local data on their Windows Embedded client.



Note

To enable users to use smart card readers, ensure to install the relevant middleware on the clients. **sc/interface** by Cryptovision is smart card middleware that integrates smart cards and other smart tokens into IT environments. **sc/interface** supports more than 90 different smart card profiles. For further information, see the Cryptovision web page.

To use **sc/interface**, the eLux package **Cryptovision sc/interface PKCS11** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

¹for eLux RP 6.4 and later versions

²from Scout Enterprise 15.10 and eLux RP 6 2103

5.16.2. Defining rules for using USB devices

1. For the relevant OU or device, open **Device configuration**¹ > **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 on the device in the Config panel under **Peripherals** > **USB** > **Information**):

Peripherals	
USB	^
Settings	▼
Information	^
Optical Mouse	▼
USB Keyboard	▼
JetFlash	^
Product name JetFlash	
Vendor name Transcend Information, Inc.	
Serial number DA43E690	
Product ID 1000	
Vendor ID 8564	
Type Mass storage	
Mountpoints Free space /media/usbdisk 7.27 GB of 7.27 GB	

5. Confirm with **OK**.

¹formerly Setup

Example rules

Rule	Code
Allow a specific USB mass storage device model only	<pre>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.</pre>
Deny a specific smart card model only	<pre>DENY: VID=18a5 PID=0302 # Deny particular smart card model (Example: Omnikey CardMan 3821) ALLOW: CLASS=0B # Allow all devices of the class SMARTCARD</pre>
Deny all printers, mass storage devices, smart card readers.	<pre>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</pre>
Deny all devices	<pre>DENY: # Deny all devices.</pre>

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

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

5.16.3. Defining rules for USB redirection

For Citrix Receiver 13.x and later versions and VMware Horizon 4.1 and later versions, you can define USB filtering rules for USB redirection of connected USB devices from eLux.

1. Type the required USB filtering rules into the appropriate configuration file:

Application	Configuration file	Examples
Citrix	/setup/ica/usb.conf	<pre>ALLOW: VID=0781 PID=5151 DENY: CLASS=08</pre>
VMware	/setup/elux/.vmware/default-config	<pre>viewusb.ExcludeFamily = "storage" viewusb.IncludeVidPid = "vid-0781_ pid-5151"</pre>

2. To transfer the configuration files to the clients, use the Scout Enterprise feature **Files configured for transfer**. For further information, see [Files configured for transfer](#).

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

5.16.4. 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.

Users on their device can right-click the USB icon (live information icon) on the system bar¹ and then click **Remove safely**.

Defining a key combination for safe removal of all USB devices

In the Scout Console, you can define a key combination that allows the users to remove all connected USB mass storage devices safely in one step. The following instructions use the key combination ALT+WINDOWS+S as an example:

1. In the Scout Console, for the relevant clients, open **Advanced device configuration > Advanced file entries**.
2. Define the following entry

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

For further information, see [Advanced file entries](#).

5.16.5. Enabling Bluetooth audio devices

- for eLux RP 6.6 and later versions -

You can allow the use of Bluetooth audio devices centrally from the console. Users can then search for devices in the eLux Config panel and connect.

- ▶ In the Scout Console, for the relevant clients, configure the following Advanced file entry:

File	/setup/terminal.ini
Section	Bluetooth
Entry	Enabled
Value	true

For further information, see [Advanced file entries](#) in the **Scout Enterprise** guide.

For further information, see also [Connecting Bluetooth audio devices](#) in the **eLux** guide.

¹for eLux RP 6.4 and later versions

5.16.6. Webcams

Webcams on devices are listed under **USB > Information** even if they are built in. To allow users to preview a webcam image, specify an app that can be used to display it.¹ The app supports multiple cameras, both built-in and USB-connected cameras.

Defining an app for camera preview

- from eLux RP 6 2107 -



Note

In the **eLux Desktop Extensions** package, the feature package **Web camera preview** must be installed on the devices. This may require modifications of the image definition file on the web server via ELIAS.

1. Add a new application and, in the **Application properties**, select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name for the application
Application	Custom
Parameter	<code>bash cameraPreview</code>

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

When users launch the app, they select one of the connected cameras to get a preview of the camera image. If only one camera is available, the preview window is displayed when the app is started.

¹from eLux RP 6 2107

5.17. Diagnostics tab

The **Diagnostics** tab allows you to configure the **Device diagnostics** feature that you can use to request diagnostic files from a client:

Option	Description
Debug level	<p>If the Debug level is set to On (Enhanced debugging), by using the Device diagnostics feature you run predefined commands on the client and retrieve a set of configuration and log files to a greater extent than without enhanced debugging.</p> <p>If you require technical support from Unicon, switch on enhanced debugging before you perform Device diagnostics.</p>



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.

Send files to	Destination for the files requested from the client
Enhanced logging for smart card support ¹	Creates an additional log file <code>/tmp/PCSCDlog.txt</code> when PCSC Lite is used

Device diagnostics is performed by using an online command. For further information, see [Device diagnostics](#).

5.18. Power management tab

- for Scout Enterprise Management Suite 15.3 and later versions -

Especially when using mobile devices, you will need options for power management. By using profiles, on the **Power management** tab, you can pre-define power management settings for your computer. These settings become active when you or the system enable the relevant profile:

- High performance: Favors performance, but may use more energy
- Power saver: Saves energy by reducing computer performance and screen brightness

You can either explicitly activate one of the power management profiles or, for mobile devices, you can let the system choose by selecting the **Auto** option: If the device is plugged in, the profile **High performance** will be active. If the device is on battery power, the profile **Power saver** is activated.

For both profiles, you can additionally distinguish between working and non-working hours.² You can further optimize energy consumption by making more rigorous use of energy saving options outside working hours. To do so, you are required to specify your working hours first. Once you have defined working hours, based on these, the system automatically switches between the **Working hours** profile

¹from Scout Enterprise 15.10 and 15.9.1000

²for Scout Enterprise 15.8 and later versions

and the **Default** (Non-working hours) profile. Important: If you choose not to define working hours, the system will use the **Default** profile settings, regardless of the day of the week and time.

Setting a power management profile

- ▶ On the **Power management** tab, from the **Active power management profile** list, select a profile or the **Auto** option.

The settings defined in the profile become active.

*The **Auto** option activates the **High performance** profile if the device is plugged in, and the **Power saver** profile if the device is on battery power.*

Profile-independent options

Option	Description
Low battery notification	For devices without power supply: Battery status in percent, from which the user is notified
Log off user before going to sleep mode ¹	Users must log on after the computer wakes from sleep mode.

5.18.1. Configuring power management profile

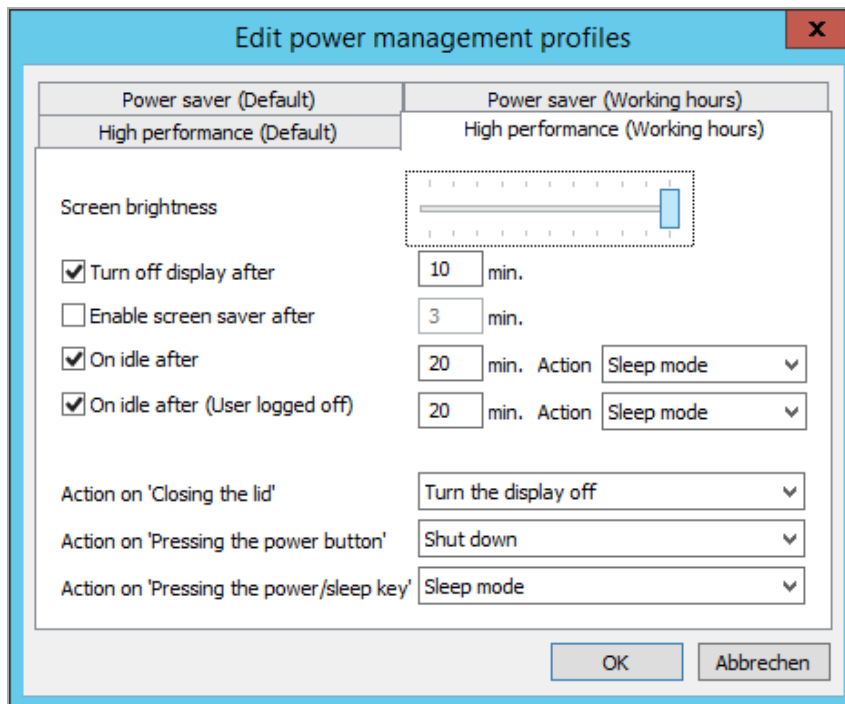


Note

If you define your working hours, you can also specify which energy-saving options you want to apply outside of working hours.² As long as you do not define working hours, the energy-saving options apply non-stop (24/7).

¹for Scout Enterprise 15.8 and later versions

²from Scout Enterprise Management Suite 15.8



1. Next to **Power management profiles**, click **Edit** and then select the tab for the required profile.¹
To define profiles for non-working hours, first define the working hours.²

¹from Scout Enterprise Management Suite 15.8, formerly: from the **Power management profile** list, first select a profile, then click **Edit**.

²from Scout Enterprise Management Suite 15.8

2. For each profile you want to use, edit the following fields:

Option	Description
Screen brightness	Screen brightness in percent for the selected profile Move mouse pointer over the slider to display the percentage.
Turn the display off after	Determines whether, after a specified number of minutes, the display is turned off when the user is not using the device (idle state)
Enable screen saver after	Determines whether, after a specified number of minutes, the screen saver is enabled when the user is not using the device (idle state)
On idle after - Action	Determines whether, after a specified number of minutes, the selected action is performed when the user is not using the device (idle state): ¹ Shut down Sleep mode Restart ² Log off ³
On idle - Action (User logged off) ⁴	When the user is logged off: Determines whether, after a specified number of minutes, the selected action is performed when the user is not using the device (idle state). ⁵
Action on 'Closing the lid'	Action that is performed when the user is closing the lid: No action Turn the display off Shut down Sleep mode
Action on 'Pressing the power button'	Action that is performed when the user presses the power button: No action Turn the display off Shut down Sleep mode

¹from Scout Enterprise Management Suite 15.9: Default is sleep mode after 20 minutes (for High performance profiles)

²from Scout Enterprise Management Suite 15 2101

³from Scout Enterprise Management Suite 15 2101

⁴from Scout Enterprise Management Suite 15.10

⁵from Scout Enterprise Management Suite 15.9: Default is sleep mode after 20 minutes (for High performance profiles)

Option	Description
Action on 'Pressing the Power-/Sleep key' ¹	Action that is performed when the user is pressing the Power/Sleep key on their keyboard (requires a suitable keyboard): ²
	No action
	Shut down
	Sleep mode ³

3. Confirm with **OK**.



Note

The sleep mode corresponds to **Suspend to RAM (S3)**. For further information, see [Sleep mode \(Suspend\)](#).

5.18.2. Defining working hours

- for Scout Enterprise Management Suite 15.8 and later versions -



Requires

User right **Define working hours**

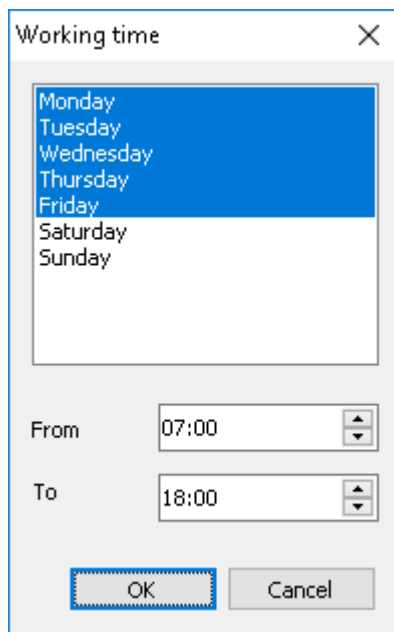
1. On the **Power management** tab, next to **Working hours** click **Edit**.
2. Select all weekdays that are working days and that are relevant to working times. To select multiple entries, press SHIFT or CTRL.
3. Select the earliest time for the start of work (**From**). This time refers to all defined working days.
4. Select the latest time for the end of work (**To**). This time refers to all defined working days.

¹from Scout Enterprise Management Suite 15.5

²If this key is not available, the configuration has no effect.

³Default

5. Confirm with OK.

A dialog box titled "Working time" with a close button (X) in the top right corner. It contains a list of days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. The days from Monday to Friday are highlighted in blue. Below the list, there are two time input fields: "From" with the value "07:00" and "To" with the value "18:00". At the bottom, there are two buttons: "OK" and "Cancel".

Working time

Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

From 07:00

To 18:00

OK Cancel

Once you have defined working hours, the **High performance** and **Power saver** profiles are divided into sub-profiles for **Working hours** and **Default** (non-working hours). Switching between the two sub-profiles is based on the working times you have defined.

5.18.3. Sleep mode (Suspend)

- from Scout Enterprise Management Suite 15.3 and eLux RP 6.3 -

The sleep mode corresponds to **Suspend to RAM (S3)**.

To put their device into sleep mode, users click a button in the extended Command panel. The sleep mode can also be activated by the system if the power management options are configured accordingly.

When the device goes into sleep mode, the eLux user remains logged on by default. After reactivating the device, users can continue working right away. This assumes that the backend is configured accordingly: When an application is disconnected, the user must not be logged off automatically.

If you want users to log on and authenticate again after the device wakes from sleep mode, select **Log off user before sleep mode** in the **Device configuration > Power management**.¹ The user is then logged off and when the device wakes from sleep mode is given the eLux logon dialog.



Note

In the Scout Console, the **Properties** window shows the status of a suspended device as `Switched off (Suspended)`.

¹from Scout Enterprise 15.8 and eLux RP 6.7

5.19. Troubleshooting device configuration

The solutions provided below refer to the Scout Console in the first place.

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.	<p>Prevent the registration as input devices by defining a <code>terminal.ini</code> entry.</p> <p>The basic functionality of the operating elements is not affected.</p> <p>For further information, see Preventing registration of USB multimedia components.</p>								
Multimedia USB devices, connected via DisplayPort to eLux RP 5 devices with an AMD processor , do not play back sound.	Sound reproduction via DisplayPort is disabled.	<p>Enable sound reproduction by defining a <code>terminal.ini</code> entry. To do so, use the Scout Enterprise feature Advanced file entries:</p> <table><tr><td>File</td><td><code>/setup/terminal.ini</code></td></tr><tr><td>Section</td><td><code>Screen</code></td></tr><tr><td>Entry</td><td><code>Radeon.Audio</code></td></tr><tr><td>Value</td><td><code>true</code></td></tr></table> <p>Alternatively, use a separate audio cable.</p>	File	<code>/setup/terminal.ini</code>	Section	<code>Screen</code>	Entry	<code>Radeon.Audio</code>	Value	<code>true</code>
File	<code>/setup/terminal.ini</code>									
Section	<code>Screen</code>									
Entry	<code>Radeon.Audio</code>									
Value	<code>true</code>									
Monitor via DisplayPort with AMD GPU: After changing to lower resolution the monitor brings an Out of range error message.	The resolution on this monitor interferes with the configured sound reproduction via DisplayPort.	<p>Disable sound reproduction via DisplayPort. This will fix the monitor error. To do so, use the Scout Enterprise feature Advanced file entries:</p> <table><tr><td>File</td><td><code>/setup/terminal.ini</code></td></tr><tr><td>Section</td><td><code>Screen</code></td></tr><tr><td>Entry</td><td><code>Radeon.Audio</code></td></tr><tr><td>Value</td><td><code>false</code></td></tr></table>	File	<code>/setup/terminal.ini</code>	Section	<code>Screen</code>	Entry	<code>Radeon.Audio</code>	Value	<code>false</code>
File	<code>/setup/terminal.ini</code>									
Section	<code>Screen</code>									
Entry	<code>Radeon.Audio</code>									
Value	<code>false</code>									
When you use a touch screen , the location of a fingertip touch is not recognized precisely.	The monitor has not been calibrated precisely enough.	<p>To calibrate the monitor, configure a custom application by using the parameter <code>calibrator</code>. Then start the application.</p>								

Error / problem	Reason	Solution
Only eLux RP 5.7.x: In dual monitor mode , if the second monitor is configured to vertical , the desktop icons are not displayed (correctly).	For some resolutions, the desktop icons on the primary monitor cannot be displayed when the second monitor is vertically aligned and the lower screen area is referenced.	For eLux RP 5.7.3000 and later versions: Use a new parameter to configure the vertical alignment to the upper screen area (<code>top</code>). To do so, use the Scout Enterprise feature Advanced file entries : <div> <div>File</div> <div>/setup/terminal.ini</div> <div>Section</div> <div>Screen</div> <div>Entry</div> <div>VerticalAlignment</div> <div>Value</div> <div>top</div> </div> The default value is <code>bottom</code> .
Display/general graphics issues	<p>The feature package for hardware acceleration HwVideoAccDrivers is not installed.</p> <p>Hardware acceleration (installed with the HwVideoAccDrivers FPM) is not supported by the device and causes problems.</p>	<p>Activate the HwVideoAccDrivers FPM within the XOrg package in the IDF.</p> <p>To exclude individual device types from hardware acceleration, create a blacklist that is transferred and locally saved to the clients by using the Scout Enterprise feature Files:</p> <div> <div>/setup/hwaccBlacklist</div> <div> <p>In the text file <code>hwaccBlacklist</code>, 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 Console, in the Properties window under Asset > Hardware information > Type.</p> <p>Example:</p> <pre>FUTRO S920 D3314-B1 HP t620 Dual Core TC</pre> <p>For all device types listed in the blacklist, hardware acceleration is disabled.</p> </div> </div>
AD logon to eLux RP 6.x does not work.	Port 389 is configured for the authentication server.	Do not define a particular port for the authentication server.



Note

After the `terminal.ini` file has been updated on the client, another client restart might be required to enable the new setting.

5.19.1. Preventing registration of USB multimedia components

The registration of USB devices as input devices can be prevented by defining a `terminal.ini` entry. To do so, use the **Advanced file entries** feature of the Scout Console.

1. In the Scout Console, for the relevant clients, open **Advanced options > Advanced file entries**.
2. Define the following entry

File	/setup/terminal.ini
Section	Xorg
Entry	IgnoreUsbInput
Value (VendorID) or	VendorID_1:ProdID_1,VendorID_2:ProdID_2 Example: 0b0e:034c,047f:c01e Important: Only use lowercase letters for hexadecimal values! You can replace individual characters by the wildcard character ?. Example: 0b0e:???? filters all products of a specific vendor.
Value (VendorName)	Alternatively, you can filter by vendor name: Example: Jabra,Netcom <ul style="list-style-type: none"> ■ White spaces or slashes in the vendor name must be replaced by an underscore _. ■ The vendor name can be entered as a sub-string. Exxample: Netcom finds GN Netcom and GN Netcom A/S. ■ Vendor names can be OR-linked: Example: Jabra Sennheiser <p>Note: To identify vendor names or IDs, use the follwing command: udevadm info --export-db grep -Ew "(NAME ID_ VENDOR) "</p>

For further information, see [Advanced file entries](#).



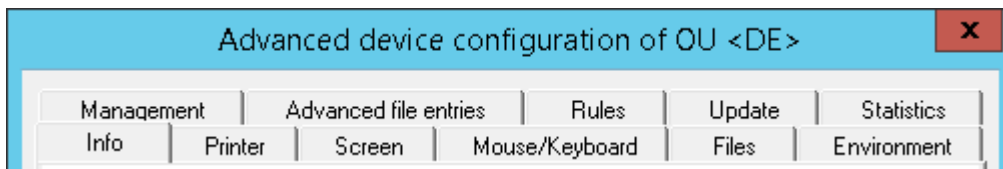
Note

After the `terminal.ini` file has been updated on the client, another client restart might be required to enable the new setting.

6. Advanced device configuration and Advanced options

The device configuration defined globally in **Options > Base device configuration** or for individual OUs or devices in their **Device configuration** can be extended as follows:

- Override applied options and add further options for individual devices or OUs by using the **Advanced device configuration**¹



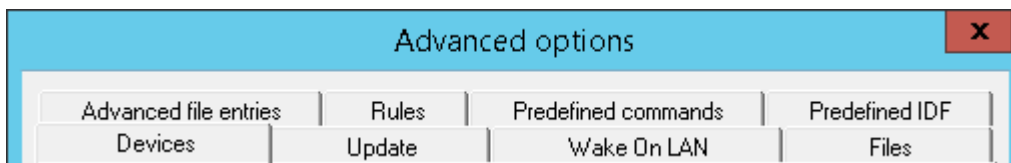
The **Advanced device configuration** is applied on OU or device level.

- ▶ Open the relevant context menu and click **Advanced device configuration...**

U Note

Inheritance is used for Advanced device configuration, either. By default, the option **Use parent of Advanced device configuration**² is selected. You can, however, clear this option on some of the tabs.

- Apply further options to all devices by using the **Advanced options**



The **Advanced options** are applied to all devices.

- ▶ On the Scout Console menu, click **Options > Advanced options**.

Some functions such as **Files** (configured for transfer), **Advanced file entries** and **Update** options can be found in both dialogs. Use **Advanced device configuration** to apply the function to individual devices. Use **Advanced options** to apply the function to all devices.

¹formerly **Advanced settings**

²formerly **Use parent advanced settings**

6.1. Devices

- only globally available for all devices (**Options > Advanced options**) -

Discover devices

Option	Description
Maximum ping-time (milliseconds)	Maximum response time in milliseconds by which clients should respond to a <code>ping</code> command.
Maximum discover time (seconds)	Total time for searching devices for Discovery. After the indicated time has expired, Discovery is stopped.

Field update

Retain local configuration (unlocked fields) ¹	<p>Editable fields of the local device configuration are free for individual user configuration and will not be overridden by Scout Enterprise. During synchronization of configuration data from the Scout Server to the device, only the values of the locked fields will be overridden.</p> <p>Which options are allowed to the user for editing (unlocked fields) is determined by the administrator under Device configuration > Security > User rights.</p> <p>The local user configuration values of unlocked fields can additionally be retained during a factory reset of the device.²</p> <p>For further information, see Supporting local configuration.</p>
---	---



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 Console to reload all configuration data. For further information, see [Supporting local configuration](#).

New devices

Default OU	OU new devices are assigned to, by default
Assign OU depending on OU filter	<p>Activates the OU filter for new devices</p> <p>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.</p>

¹formerly: Only locked fields are updated on the client

²from Scout Enterprise 15.7 and eLux RP 6.7

Lock config transfer for new devices	Newly added devices are not synchronized with the server's device configuration
Allow dynamic change of OUs	Allows dynamic assignment of devices via DHCP
Accept only known devices	The Scout Server accepts only devices with known MAC addresses. For further information, see Reserving device profiles .

Device name

Use the host name of the device	The device name is the client host name and cannot be changed in the Scout Console permanently.
To avoid duplicate names, change name of existing entry	When a new device with an 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 devices Can be overridden for particular OUs (Advanced device configuration > Management)
Apply name template only on new devices	Name templates are not applied when you move or relocate devices.

For further information, see "Device names" on page 31.

6.2. Update/Delivery

- not available for individual devices -

Option	Description
Maximum number of parallel updates or software deliveries	Restriction for performance reasons
Maximum time to connect	Time for setting up the connection before the next device is accessed



Note

The optimum values depend on the system.

6.3. Management

- only available for individual devices and OUs -

Option	Description
Note	Free text field for internal comments Can be shown in the Properties window
Visibility - only for OUs -	The visibility refers to the list of OUs that new clients request when they initially connect to the Scout Server to select an OU. Hidden OUs are not shown in the list. Visible OUs can be selected in the list but can be protected by password.
New devices - only for OUs -	When new devices register automatically, they can be subject to a predefined name template. Device names are configured globally in the Advanced options on the Devices tab. For further information, see Devices .
Ignore OU filter - only for individual devices -	If the OU filter is active (Advanced options > Devices), new devices are assigned to OUs due to the defined criteria. Individual devices can be excluded from the OU filter. By moving devices within the tree structure by a drag-and-drop operation, for the relevant devices, the option is selected automatically.

6.4. Predefined commands

- only globally available for all devices (**Options > Advanced options**) -

User-defined commands can be centrally predefined and provided as ready-to-use commands for operative administrators managing their clients remotely.

Active predefined commands are shown in **Commands > Predefined command** in the relevant list-field.

In addition, you can set preferences for standard commands used by administrators.

For further information, see [Creating predefined commands](#).

6.5. Predefined IDFs and containers

- only globally available for all devices (**Options > Advanced options**) -

By predefined certain configuration parameters of the **Device Configuration > Firmware**, you specify values to be used by operational administrators. For example, you can restrict the selection of valid image files.



Note

To use these functions effectively, configure the relevant object rights in the administrator policies. For further information, see [Protecting firmware configuration](#).

- ▶ To create a new list entry, click **Add** and then edit the new entry. The spelling of your entry must correspond to the existing file and path names. Note the following:
 - File and paths names are case-sensitive.
 - Do not use spaces.
 - File names must be specified with their extensions such as `.idf`

Section	Option	Description
Predefined IDFs	Image name	<p>Name of an image file (IDF) that if marked as valid can be selected in the firm- ware configuration under Image file</p> <p>Example: <code>myImage.idf</code></p> <p>Used shows the number of devices using the image Assigned shows the number of devices to which the image has been assigned</p>
Predefined paths	Path name	<p>Container path for software packages and images, which can be selected in the firmware configuration under Path if marked as valid</p> <p>Example: <code>eluxng/UC_RC6_X64</code></p>
Predefined UEFI files ¹	UEFI file	<p>Name of an <code>.udf</code> file that if marked as valid can be selected in the firmware configuration under UEFI file</p> <p>The UEFI file is needed to update a device's UEFI firmware with the appro- priate binary data.²</p> <p>Example: <code>myUEFI.udf</code></p>

¹from Scout 15 2107

²from eLux RP 6 2107

6.6. Wake On LAN

- only globally available for all devices (**Options > Advanced options**) -

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



Requires

Wake On LAN is supported by the thin client and is configured in the device BIOS.

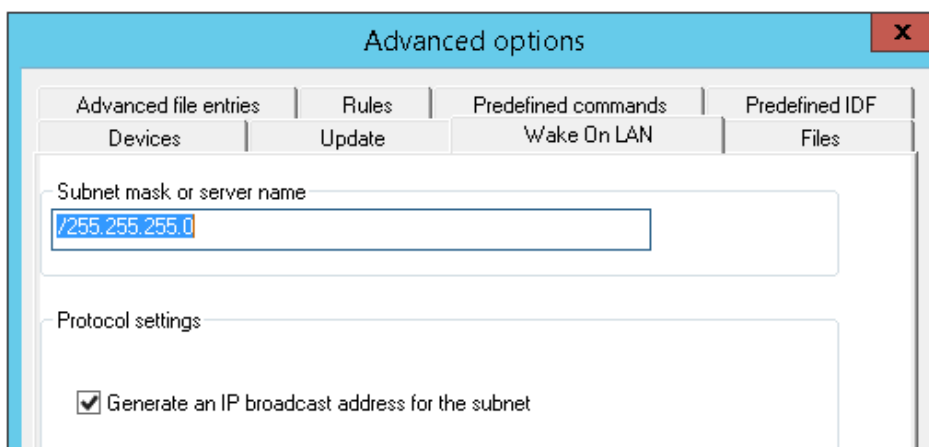
The Scout Server sends a so-called magic packet that is identified by the network adapter of the turned-off devices. The thin clients are woken via port 67.

The magic packet for Wake On LAN is sent as a broadcast (UDP, eLux port 20000 incoming/outgoing) within the current network subnet and cannot operate across the entire network. To wake up thin clients in remote subnets, subnet directed broadcasts are required.

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 from 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.

An IP broadcast address for the subnet must be configured once in the 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 device configuration ¹)

¹formerly **Advanced settings**

Option	Description
Generate an IP broadcast address for the subnet (only globally available in Advanced options)	<p>The packet is sent to the relevant subnet (dedicated subnet). Requires a subnet address in the Server name field using the format <code>/255.255.255.0</code> (Note the leading slash).</p> <p>Example: To wake up a device with IP address <code>192.168.10.44</code>, enter <code>/255.255.255.0</code> in the Server name field. This causes Scout Enterprise to generate the IP broadcast address <code>192.168.10.255</code> for the subnet.</p> <p>By default, this option is disabled.</p>

6.7. VPN

- only available for individual devices -



Note

One or more VPN profiles can be defined for entire OUs in **Device configuration > Network**.¹

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

- Cisco AnyConnect
- 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](#).

6.7.1. Configuring Cisco AnyConnect



Note

For versions up to eLux RP 6.5, the eLux package **VPN System** and the included feature package **Cisco AnyConnect** must be installed on the clients.

From eLux RP 6.6, the eLux package **Cisco AnyConnect** must be installed on the clients.

This may require modifications of the image definition file on the web server via ELIAS.

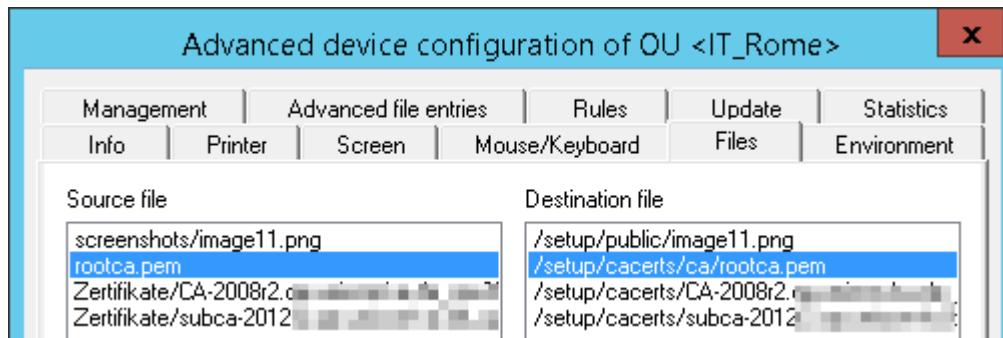
1. Transfer the root certificate to the clients to `/setup/cacerts/ca`. If you use the Scout Enterprise feature [Files configured for transfer](#), specify the destination file with destination path `/setup/cacerts/ca`.



Note

Cisco AnyConnect only accepts certificate files in `.pem` format.

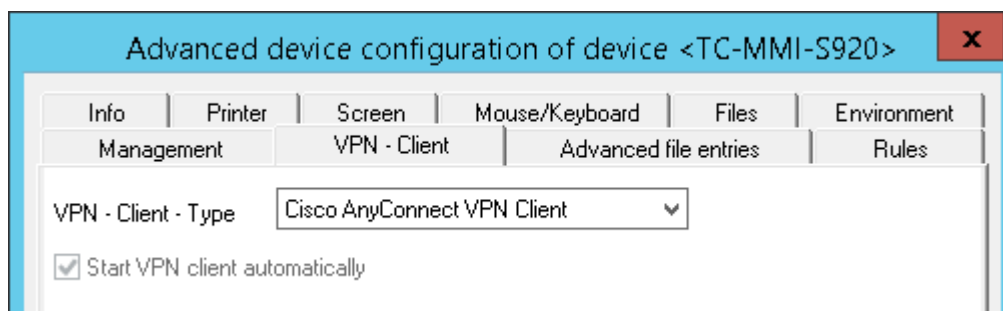
¹from Scout Enterprise Management Suite 15 2101



Note

The certificates that are transferred from the VPN server are stored in `/setup/cacerts/client`.

2. In the Scout Console, for the relevant device, open **Advanced device configuration > VPN client**. Then, in the list-field, select `Cisco AnyConnect VPN Client`.



3. Restart the client. The client might require one more restart to activate the VPN configuration data locally.

Configuration file

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/.cisco/profile/1` via the Scout Enterprise feature **Files configured for transfer**. In the configuration file, you can specify your back-end server address.

¹from eLux RP 6.4. For earlier versions: `/setup/elux/.anyconnect`

6.7.2. Configuring OpenVPN

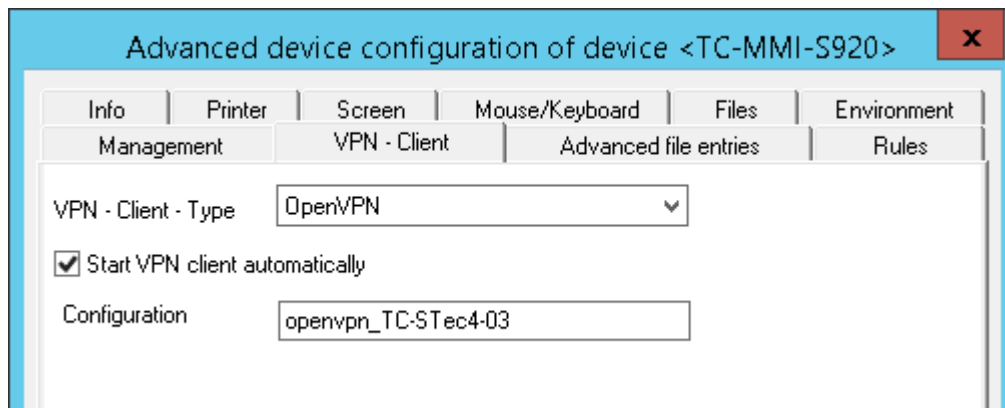


Note

For versions up to eLux RP 6.5, the eLux package **VPN System** and the included feature package **OpenVPN** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

From eLux RP 6.6, **OpenVPN** is an integral part of the eLux operating system.

1. Transfer the `.ovpn` configuration file and certificates to the clients to `/setup/openvpn`. If you use the Scout Enterprise feature **Files configured for transfer**, specify the source and destination file **with** file name extension and the destination path `/setup/openvpn`. If you use a USB stick, unzip the `.zip` file to the client directory `/setup/openvpn`.
2. In the Scout Console, for the relevant device, open **Advanced device configuration > VPN client**. Then, in the list-field, select `OpenVPN Client`.



3. Select the option **Start VPN client automatically**.
4. In the **Configuration** field, enter the name of the OpenVPN configuration file **without** the file name extension `.ovpn`.

On the next restart of the device, the VPN configuration file is transferred to the device and activated with another restart. The OpenVPN logon dialog is displayed and the user can connect.



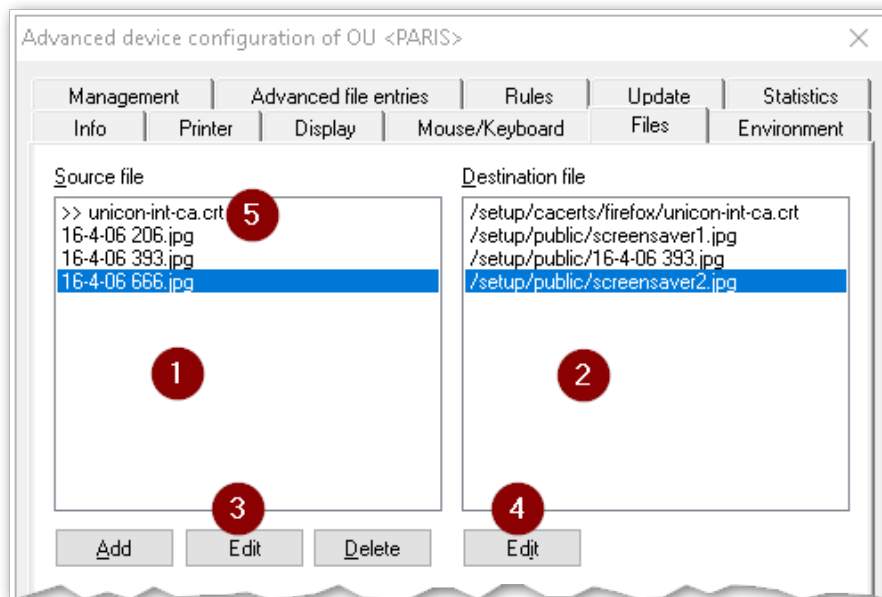
Note

The OpenVPN client can only be used with a valid `.ovpn` configuration file under eLux. Ensure that the configuration entries are correct. eLux does not accept the setting of an additional default route via the `.ovpn` configuration file. Some firewall vendors offer different configuration files for different operating systems, with and without a default route. For example, the Sophos configuration file for Android/iOS does not include this default route and can be used for eLux.

6.8. Files configured for transfer

This feature helps you transfer files to the devices. The defined files are transferred on the next device restart. You can apply a file transfer to all devices, to individual devices or to OUs.

The source files are imported to the Scout Enterprise database and therefore are included in an SQL database backup.



Example: Picture files are copied to the clients as screen savers.

Legend to numbers

- 1 The source files are selected from the file system via **Add**.
- 2 For each source file, a destination file on the device is created:
Specify the relevant destination directory and optionally a different file name.
- 3 Source files of the current level can be edited.
- 4 For entries of the current level, you can edit the destination file properties.
- 5 Entries from a parent OU or the global file list are identified by a **>>**.¹

You cannot edit these source files. With the corresponding object right, however, you can view them,² see below.

¹from Scout Enterprise Management Suite 15.4

²from Scout Enterprise 15 2101

Defining files for transfer


1. To configure a file transfer to all devices (global file list), click **Options > Advanced Options....** On top level, you can also define destination file templates for subordinate levels.

To configure a file transfer to the devices of an individual OU or to an individual device (individual file list), on the context menu of the relevant OU or device, click **Advanced device configuration...**



Note

Individual file lists have precedence over global file lists.

2. On the **Files** tab, click **Add**.
3. In the **Add file entry** dialog, to select the source file from the file system, click the  button and then select a file.
*A new entry for the **Source file** and **Destination file** lists is created.*
4. Under **Destination file**, if required, modify the directory and file name of the destination file on the device.
The destination file name may differ from the one of the source file.
If configured, alternatively use a destination file template from the **Template** list field.
The path and name of a destination file from a template cannot be changed later on.
5. Confirm with **OK**

Source and destination are defined. The files are transferred on the next restart of the devices. The files will not be reloaded unless you modify the file configuration.

Re-using imported source files

You can re-use source files that you have imported for one OU for the file transfer in other OUs.

1. In the Advanced device configuration of the source OU, on the **Files** tab, right-click the relevant entry in the **Source file** list.
2. To copy the entry to the Clipboard, on the context menu, click **Copy**.
3. Open the Advanced device configuration of the target OU.
4. On the **Files** tab, right-click the **Source file** list. On the context menu, click **Paste**.

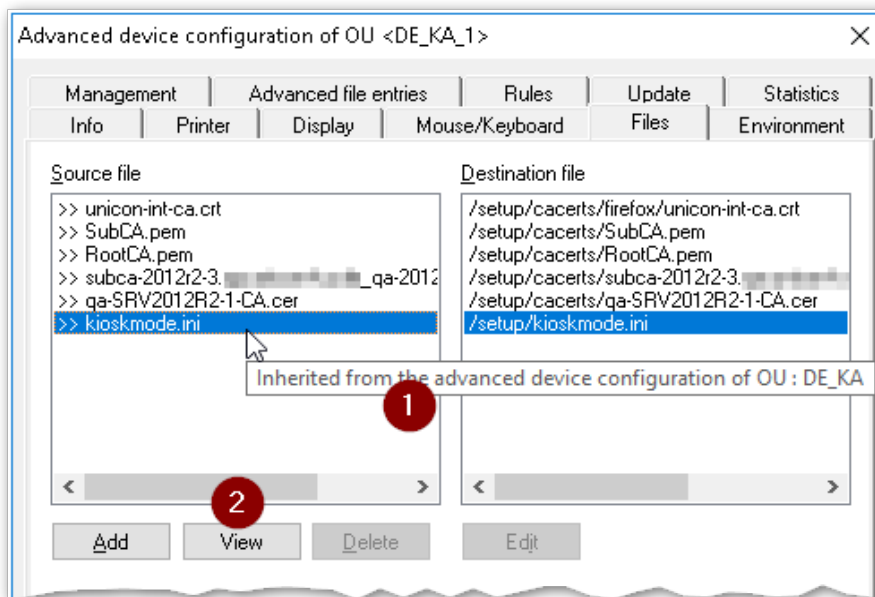
Removing transferred files

Once you have transferred files to a client they cannot be removed by using the feature **Files configured for transfer**.

- ▶ To remove all transferred files from a device, perform a factory reset.

Source files from parent OUs or the top level

The **Files** dialog also displays entries from parent OUs or the global file list. These inherited source files are identified by a >>¹ character and are protected from access by default.



Legend to numbers

- 1 To show the origin of a parent entry, move the mouse pointer over the entry.
- 2 You cannot edit source files of parent entries.

But, If the file privacy object right has been disabled, you can view the content of a source file.²

- ▶ To disable the object right, for the required OU and for the required administrator, open the object rights, and then navigate to **Edit properties > Files > Inherited file privacy**.

For further information, see "Changing object rights" on page 308.

¹from Scout Enterprise Management Suite 15.4

²from Scout Enterprise 15 2101

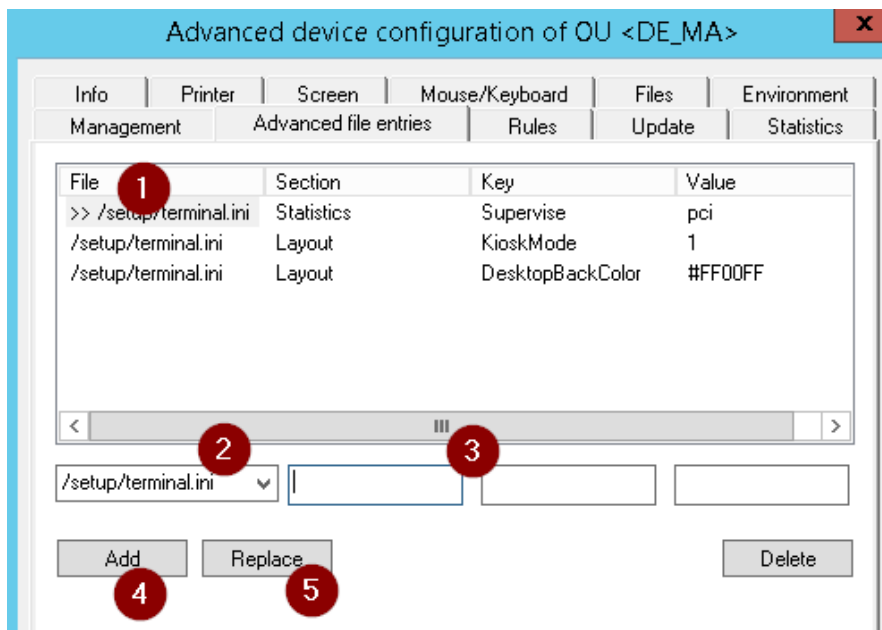
6.9. Advanced file entries

The **Advanced file entries** tab allows you to set parameters in `.ini` files that cannot be set by using the graphical user interface. For example, you can define additional layout parameters.

The following applies to the `.ini` files:

- `.ini` files contain at least one section. Each section contains zero or more keywords. The keywords contain zero or more values.
- Each section is headed by a symbolic name enclosed in square brackets.
- Each keyword and its value are in one line. Keyword and value are separated by an equal sign (=).
A 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.

6.9.1. Adding individual file entries



Legend to numbers

- 1 Entries from a parent OU or the global **Advanced options** are shown with a `>>`.¹
To show the origin, move the mouse pointer over the relevant entry.
- 2 For a new entry, first select the relevant file or enter the path and filename.
- 3 For the new entry, then specify the section, key and value.

¹for Scout Enterprise Management Suite 15.4 and later versions

Legend to numbers

- 4 Click **Add** to add the new entry.
- 5 Click **Replace** to replace the selected entry in the list by the new entry.

1. In the Scout Console, click **Options > Advanced Options**.
Or:
For the relevant OU, open the context menu and click **Advanced device configuration...**¹
2. Click the **Advanced file entries** tab.
3. Below the list, edit the following fields:

Option	Description
File	Enter the full path including file name or select from the list: Terminal: <code>/setup/terminal.ini</code> Citrix ICA: <code>/setup/ica/wfclient.ini</code> and <code>/setup/ica/appsrv.ini</code> Cisco VPN: <code>/setup/ciscovpn/sample.pcf</code>
Section	Section heading without brackets
Key	Keyword
Value	Value you want to assign to the keyword Blanks, hyphens and multiple values are allowed. Example: <code>valueA,valueB,valueC;comment</code>

4. Click **Add**.
5. Confirm with **Apply** and **OK**

The new entry is written to the .ini file on the next restart of the client.

6.9.2. Changing values of individual file entries

1. In the **Advanced device configuration**² > **Advanced file entries**, select the entry whose value you want to change.
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 restart of the client.

¹formerly **Advanced settings**

²formerly **Advanced settings**

6.9.3. Deleting individual file entries

1. In **Advanced device configuration > Advanced file entries**, define a new entry: Enter **File**, **Section** and **Key** 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 restart.



Note

If you use the **Delete** button to delete a selected row from the list, then Scout Enterprise will no longer update the respective entry.

6.9.4. Deleting complete sections

1. In the **Advanced device configuration¹ > Advanced file entries**, define a new entry: Enter **File** and **Section** of the relevant file entry, but leave the **Key** and **Value** boxes empty.
2. Click **Add**.

The 'empty' section overrides previous instructions. The section is deleted from the file on the next restart even if it contains file entries.

6.10. Rules

Using this feature helps you define rules which can be executed when closing the last application or using Scout Enterprise for the first time.

Option	Description
After terminating the last application execute the following action	Choose between the options of the list-field For OUs and devices, the <code>Use parent action</code> option is set by default to enable the rules defined for a higher OU level.
Display a message on the device for <x> seconds	Enter a time period in seconds to inform the user
After first management contact execute the following action	Select <code>Update the device</code> to ensure that the new devices are all up-to-date.

Special case kiosk mode

If you use the browser in kiosk mode to access Citrix applications, the option **After terminating the last application execute the following action** does not work. In this case, you can set an entry in the `terminal.ini` file to determine an action that is performed after the last Citrix application is closed.

¹formerly **Advanced settings**

- Define the following entry by using the Scout Enterprise feature [Advanced file entries](#):

File	/setup/terminal.ini	
Section	Global	
Entry	ActionAfterLastWfica	
Value	0	Use parent action
	1	Restart
	2	Shutdown
	4	Logoff
	8	Lock
	16	VPN disconnected

6.11. Environment variables

- only available for individual devices and OUs -

Environment variables can be used locally on the client. They contain strings.

Defining environment variables

1. In the **Advanced device configuration**,¹ click the **Environment** tab.
Previously defined variables are shown in the list. Entries from a parent OU are shown with a >>.²
2. Click **New**.
3. Enter the required variable using the format:
`Variable name=value`
and confirm with **OK**.
The new variable is shown in the list.
4. To encrypt the value of the variable, right-click the variable. Then on the context menu, click **Encrypt value**.



Note

When you apply variables, the variable names must begin with a dollar sign: `$<Variable name>`

6.12. TPM 2.0 support

- for eLux RP 6.7 and later versions -

A TPM 2.0 chip built into the thin client can be used for basic security functions:

- Encryption of the setup partition³ and system partition⁴

The setup partition on the thin client's flash memory contains the device configuration, application definitions, and certificate store. The system partition holds the software packages of the firmware.

In order to protect the system from manipulation, in addition to encryption, the disk is sealed with security measurements.⁵

- Store the private key of a SCEP client certificate inside the TPM 2.0 module

¹formerly **Advanced settings**

²for Scout Enterprise Management Suite 15.4 and later versions

³from eLux RP 6.7

⁴from eLux RP 6.10

⁵from eLux RP 6.10

To store the key inside the TPM 2.0 module, a `scep.ini` entry is required. For further information, see [Certificates for SCEP](#) in the **SCEP** guide.

Requirements for disk encryption

- The devices are provided with a TPM 2.0 module.
- The devices are started in UEFI mode.

Disk encryption via TPM 2.0

- from eLux RP 6.10 -

If the device-side requirements are met, encryption can be enabled using two different mechanisms:

- Via the configuration parameter **DiskEncryption**
- Via the feature package **Partition encryption** installed with the image

If the BaseOS package for eLux RP 6.10 or later is installed on the devices with the feature package **Partition encryption** enabled, the system is automatically encrypted. The parameter **DiskEncryption** is then ignored.

The feature package **Partition encryption** is enabled by default.

To encrypt the disk, the partitions must first be formatted. Therefore - as soon as the encryption is activated - a firmware update with previous formatting for the relevant devices is forced.

Encrypting the disk via parameter

- from eLux RP 6.10 -

1. In the Scout Console, for the relevant devices, open **Advanced device configuration**¹ > **Advanced file entries**.
2. Define the following entry:

File	/setup/terminal.ini		
Section	Security		
Entry	DiskEncryption		
Value	true	By default, the value is false.	

For further information, see [Advanced file entries](#).

For the relevant devices a firmware update is forced with previous disk formatting.

The configuration parameter has no effect on thin clients without TPM 2.0.

¹formerly **Advanced settings**



Note

You can find information on whether the disk of the device is encrypted in the **Properties** window.¹

When new clients with TPM 2.0 chip are added to the Scout Enterprise infrastructure (onboarding) and the destination OU is configured with `DiskEncryption`, it is ensured that the configuration data stored in the Scout Console is only saved locally on the thin client after the setup partition has been encrypted.

Update from earlier versions to eLux RP 6.10

Updates with disk encryption can only be performed from eLux RP 6.x. Upgrades from eLux RP 5 are not supported.

If you enable encryption when updating to eLux RP 6.10, another update may be required on the next device restart. This is due to the partition formatting that is required for encryption.

The **DiskEncryption** parameter replaces the **CryptSetupPartition** parameter of previous versions,² but is maintained for backward compatibility. From eLux RP 6.10, **CryptSetupPartition** has the same function as **DiskEncryption** and therefore encrypts setup and system partition.

Error handling

If a device fulfills the above-mentioned requirements for encryption and disk encryption still fails during the update, the setup partition will be partially cleaned like it is for a factory reset without deleting the Scout Enterprise-Server address. The device status in the Scout Console is then displayed with a yellow icon (initialization).

Resetting the disk encryption



Requires

The feature package **Partition encryption** must be uninstalled on the relevant devices. This requires modifying the image definition file on the web server via ELIAS.

- ▶ Set the advanced file entry `DiskEncryption`³ to the value `false`.
- or
- ▶ Perform a factory reset for the devices. To do so, use the **Remote factory reset** command with the option **Delete Scout Server address on the device**.

During the restart of the relevant devices, the disk is decrypted. That is why the start up process takes longer.

¹for Scout Enterprise 15.8 and later versions

²eLux RP 6.7 to eLux RP 6.9

³alternatively `CryptSetupPartition`

Downgrade to earlier versions < eLux RP 6.10

Devices with encrypted disk cannot be downgraded to eLux RP 6.9.100. If a downgrade is necessary, the disk must be decrypted first.

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 image](#) in the **ELIAS 18** 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




Note

You can define actions to be performed after the last application has been closed. For further information, see [Rules](#).

Additionally note that application definitions can be

- copied from one OU to another
- exported from one OU and imported to another OU (context menu > **Edit**).

7.1.1. Adding applications

1. In the tree view, right-click 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 Console

Important Applications are identified by their name. Make sure to use a unique name for them.

Display name (optional)	Name of the application shown on the client (control panel, start menu)
Sorting ID ¹	Specifies the sorting order for applications pinned to the system bar 1 sorts alphabetically (default)
Server	Name of the server the application connects to
Login	The user is automatically logged on to the terminal server by using predefined credentials (username, password, domain).
Pass-through login	The values of the local user variables <code>\$ELUXUSER</code> , <code>\$ELUXPASSWORD</code> and <code>\$ELUXDOMAIN</code> are used to log on to the authentication server. This allows to use the AD logon data of the eLux desktop for automatic logon 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 starts automatically after eLux has been started. Optionally, you can delay the auto-start process by defining 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

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. Depending on the application, different properties can be configured.*



Note

Properties of the selected application can be displayed in the **Properties** windows of the Scout Console. They cannot be modified there.

For each administrator, you can control the object rights for individual application types.² Object rights for the advanced settings and free parameters can be assigned separately.

¹from Scout Enterprise 15.10 and eLux RP 6.10

²for Scout Enterprise Management Suite 15.5 and later versions

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.

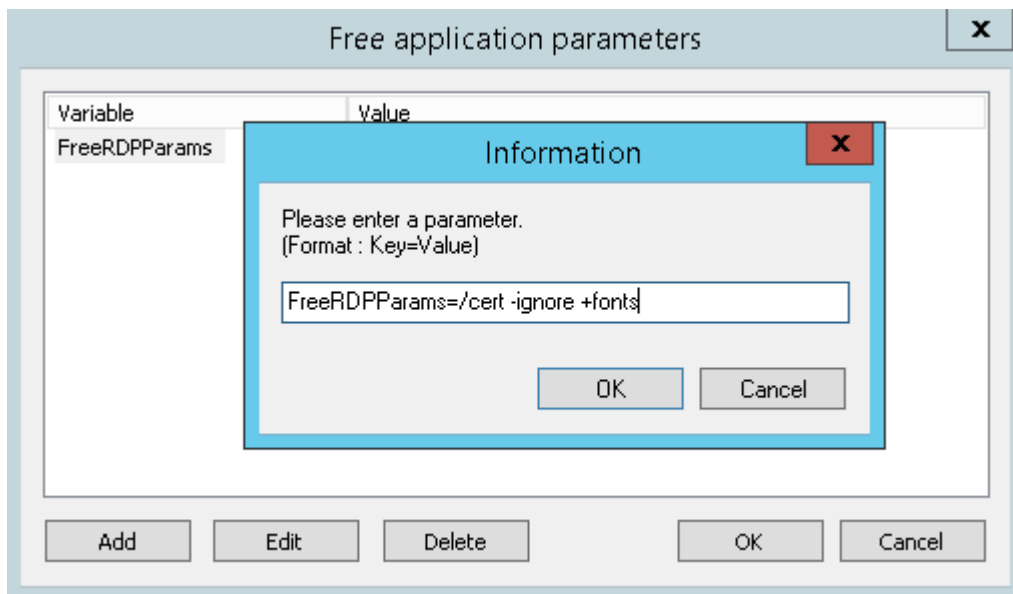
1. Open the **Application properties** of the relevant application.
2. Click **Free Parameters**.
3. Click **Add** and enter one or more parameters in the following format:

`FreeRDPPParams=<Parameter> <Parameter> <Parameter>...`

Separate multiple parameters by spaces.

4. Confirm twice with **OK**.

The defined parameters are saved with the application definition. They will be inserted for the relevant application into the file `\setup\sessions.ini`.



Note

Access to the free parameters can be restricted via the object rights.¹

For information on which parameters are available, refer to the description of the respective application definition.

The following parameters can be used across applications:

Parameter	Values	Description
pinned ²	true	The application is pinned on the system bar.

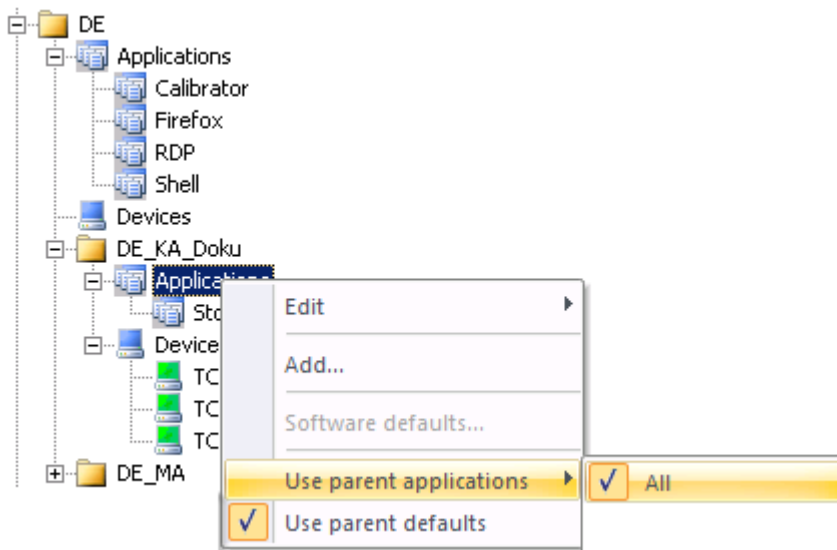
¹for Scout Enterprise Management Suite 15.5 and later versions

²for eLux RP 6.8 and later versions

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 this individual OU (and subordinate OUs).



Disabling inheritance 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 sub-menu **Use parent applications**, under **All**, select the application you want to inherit from above.

The selected application, on the sub-menu, receives a check mark, and its definition is provided on the next restart of the clients for that OU.




Note

Inherited properties of the selected applications will be lost if you move the respective OU to

U another parent OU. For moved OUs, the system automatically enables **Use parent applications > All**.¹

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 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*.*

OU devices/applications			
☰			
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.

U Note To also apply the default settings of the parent applications, on the **Applications** context menu, select the **Use parent defaults** option.

7.1.5. Defining application templates

- for Scout Enterprise 15.7 and later versions -

As an administrator, you can create a template for each application type, for example, a browser template: In the template, you specify values that users will find filled out when they create a browser application. If you create a browser template and specify the browser type **Firefox** and **System proxy** as proxy, as a result users at all levels will see Firefox and system proxy as predefined values when they create a new browser application.

Note that the values can be overwritten. However, if you disable the object rights for the advanced options or free parameters of an application type, these values remain because the relevant users do not have access to them in the application definition.

Application templates are defined at the top level. You can define exactly one template for each application type.


¹from Scout Enterprise 15 2101

Creating a application template



Requires

Administrators' base right: **Edit base application**


1. In the tree view, on the top level, right-click the **Applications**  icon.
2. On the context menu, click **Define application templates...**

*The **Definition of application templates** dialog opens. Each tab contains the application properties of an application type.*

3. Switch to the tab that contains the required application type.
4. Edit any options you want to predefine.
5. Confirm with **Apply** and **OK**.

For each new application definition of this application type, the predefined values will be set.

Modifying or resetting application templates

1. In the tree view, on the top level, right-click the **Applications**  icon and select **Define application templates...**

*The **Definition of application templates** dialog contains for each application type a tab with its application properties. Non-empty fields contain values that are used when new applications of this type are created.*

2. For the relevant application type, edit the options you want to change.
3. To reset all values that you have predefined for an application type, click **Reset**.

7.1.6. 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 Workspace app)¹ and for [browsers](#).²

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**.

¹formerly Citrix Receiver

²for Scout Enterprise Management Suite 15.0 and later versions

7.1.7. 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 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 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.

7.1.8. Defining application icons

You can define custom icons for applications to be displayed on the client desktop. For the icon files, in Scout Enterprise Management Suite 15.2 and later versions, the high-resolution formats `.svg` und `.png` are supported. These file types replace the bitmap formats `.xpm`, `.ico` and `.gif` which can be used in Scout Enterprise Management Suite and earlier versions.

1. In the tree view, for the top-level  **Applications**, on the context menu, click **Define application icons...**
2. Click **Add** and select the relevant file from the file system.
3. Confirm with **Open** and **OK**.

The application icon is shown in the dialog. The icon is defined but has not been assigned yet.

7.1.9. 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, on the context menu, 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.

7.1.10. Defining a service app

- for eLux RP 6.4 and later versions -



Note

To use this feature, user authentication via Active Directory is required.

If you use AD, you can allow users to start eLux in service mode without logging on. To do so, define one or more service apps. The AD logon dialog then provides an additional **Service** button that starts eLux in a protected mode (service mode). In service mode, eLux only offers the defined service apps on the desktop. In the Configuration panel, only the **Information** dialog is shown.

1. To define a service app, open the **Application properties** of the relevant application.
2. Click **Free Parameters** and add the following parameter:
`ServiceApp=true`
3. Confirm with **OK**.

*After the parameter is transferred to the client, the AD logon dialog contains a **Service** button.*



7.1.11. Limiting applications to one logon domain

- for eLux RP 6.4 and later versions -



Note

To use this feature, user authentication via Active Directory is required.

If users have configured multiple AD domains for log-on, you can limit the display of an application to one of the configured domains. This option is defined via a free parameter in the application definition.

1. Open the **Application properties** of the relevant application.
2. Click **Free Parameters** and add the following parameter:

```
ShowInDomain=<AD logon domain>
```

The AD logon domain must match with one of the domains specified in the device configuration under **Security > User authentication > AD directory**.

Example:

```
int.sampletec-01.com
```

3. Confirm with **OK**.

After the parameter is transferred to the client, the relevant application is only shown if users log on to the specified AD domain.

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 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 Web Interface server
- by a [PNAgent application](#) to a StoreFront server (XenApp Services Support must be enabled on the Citrix farm) or Web Interface server
- by an [ICA application](#) to a virtual desktop or published applications



Note

Access via the **ICA** application type is deprecated and only supported by Citrix up to XenApp version 6.x.

Requirements

- The eLux package **Citrix Workspace app for Linux** or **Citrix Receiver for Linux** must be installed on the clients.
- To connect via HTTPS, for the application types **Storefront**, **Self Service** and **PNAgent**, the relevant root and intermediate certificates 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](#) in the **Installation** guide.

- To connect via HTTPS, for the application type **Browser**, the relevant root and intermediate certificates 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 Citrix StoreFront server. Virtual desktops and published applications are aggregated and provided through stores. The Citrix products mainly used are XenApp and Citrix XenDesktop. StoreFront sites can be accessed via HTTP or HTTPS.

The StoreFront application 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 eLux RP 6 User Interface. For further information, see [eLux RP 6 User Interface](#).

Defining a StoreFront application



Note

HTTPS connections require the relevant [SSL certificates](#) on the device.

1. [Add a new application](#) and select the application type **StoreFront**.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Console
Use Provisioning File (.cr) ¹	<p>Enter the Citrix store provisioning file name without the file name extension. The Provisioning file must be located on the client in the directory <code>/setup/ica/</code>. For further information, see StoreFront / Store provisioning file.</p> <p>This option excludes the specification of Store URLs (next option).</p>
Stores	<p>Specify the URL of one or more stores</p> <p>▶ Click Add and replace the automatically created default value by your individual value (double-click or F2)</p> <p>Example: (<code>https://CtrXd76.sampletec-01.com/Citrix/Store33/discovery</code>)</p> <p>This option excludes the use of a Provisioning file (previous option).</p>
Logon	The user is automatically logged on to the store by using the specified credentials (username, password, domain).
Pass-through logon	<p>The user is logged on to the store via single sign-on. The AD user credentials are used.</p> <p>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.</p>

¹for Scout Enterprise Management Suite 15.5 and later versions



Note

If you want to use predefined credentials or pass-through authentication, the eLux package **Citrix Receiver Extensions** and the included feature package **Dialog Extension** must be installed on the clients.

For further information, see "StoreFront / Authentication" on page 190.

Show last user	The user credentials (except for password) of the last logon are displayed in the XenApp logon dialog. This option has no effect if you specify fix user credentials for automatic logon under Logon .
Autostart	Specify the names of those StoreFront applications you want to have started automatically. Make sure to spell the names exactly as in StoreFront. Separate multiple application names by semicolon. Example: MyApp1 ; MyApp2 If only one resource is defined for a store, alternatively use the free parameter <code>AutostartUniqueResource=true</code> ¹
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters .

- To delete an entry from the **Stores** list, select the entry and click **Delete**.
- 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.

¹for eLux RP 6.4 and later versions (Citrix Workspace app)

Option	Description
Application reconnection	<p>Determine the actions to be done on a reconnect to the StoreFront server</p> <p>Do not reconnect: The connection to the desktop or the published applications is not restored (default).</p> <p>Disconnected sessions only: The connection to a disconnected session is restored.</p> <p>Active and disconnected sessions: The connection to a disconnected or active session is restored.</p>
Manual logoff	<p>Determine the actions to be carried out upon logoff from the StoreFront server</p> <p>Logoff only server: Logoff is performed only from the StoreFront server</p> <p>Logoff server and applications: Logoff is performed from the StoreFront server and from the virtual desktop or published applications.</p> <p>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.</p>



Note

Access to the advanced settings can be defined via the object rights.¹

5. Confirm with **Apply** and **OK**.

*After users have logged on to a StoreFront server or Web Interface server, they can show all provided resources by double-clicking the **StoreFront** icon on the eLux desktop.*

7.2.2. StoreFront / Store provisioning file

- for eLux RP 6.3 and later versions -

A Citrix store provisioning file can be created by the Citrix back-end and contains all relevant connection information. Using this file allows to switch automatically from Citrix StoreFront connection data to Citrix Access Gateway connection data if StoreFront is not reachable (scenario of switching between company office and home office).

To use a store provisioning file for your eLux clients, note the following:

- The file must be located on the clients in the directory `/setup/ica/`
Transfer the `.cr` file by using the Scout Enterprise feature **Files configured for transfer**. For further information, see [Files configured for transfer](#).

¹for Scout Enterprise Management Suite 15.5 and later versions

- For Scout Enterprise Management Suite 15.4 and earlier, add two free parameters to the Citrix StoreFront application definition:

```
UseCrFile=true
CrFile=<filename>.cr
```

Leave the **Stores** field empty.

7.2.3. StoreFront / Authentication

If on the client, smart card packages are installed and the Citrix Workspace app for Linux identifies smart card middleware on the client, smart card logon has precedence by default. In order to still authenticate via username and password for certain clients, define the authentication method via a parameter:

Controlling the authentication method via eLux

The logon method can be changed to username and password regardless of the smart card packages installed.

- ▶ Define the following entry by using the Scout Enterprise feature [Advanced file entries](#):

File	/setup/sessions.ini
Section	ICADefaults
Entry	StoreFrontLogOnWithPassword
Value	true false (Default: false)

Configuring smart card behavior

If you use smart card authentication for StoreFront, you can configure the behavior of the smart card when it is removed.

U 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.

- ▶ 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)

Further parameters for authentication¹

To define further parameters for authentication, use the configuration file `/setup/ica/AuthManConfig.xml.template`. This file is transferred to the clients during installation. Using the **Diagnosis** and **Files configured for transfer** features, you can retrieve the file, edit it and transfer it back to the relevant clients. For further information, see [Advanced device configuration > Files](#).

For the function to become active on the client, a restart is necessary for the transfer to the client and another restart to activate the new parameters.

¹for eLux RP 6.8 and later versions

7.2.4. Self-Service user interface

The Self-Service user interface (UI) replaces the configuration manager **wfcmgr** and allows access to Citrix services providing published resources. After users are set up with an account, they can subscribe to desktops and applications, and then start them.

Defining Citrix Self-Service as local application



Note

The eLux package **Citrix Workspace app for Linux**¹ 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 via ELIAS.

1. Add a new application and select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select <code>Custom</code> .
Parameter (mandatory)	Enter the following program name to start the application: <code>selfservice</code>

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



Note

The `selfservice` application cannot be configured individually. To use configuration options, alternatively use the **Self-Service UI with extensions** (`ucselfservice`) for eLux RP 5 clients. For eLux RP 6.2 and later versions, you can use the see **Citrix Self-Service UI in kiosk mode**.

¹formerly Citrix Receiver for Linux

7.2.5. Self-Service user interface with extensions

The Citrix Self-Service user interface (UI) can also be used in an extended version with further functionality¹

- Configuration of the stores
- Logoff and reconnect options
- Dialog and window layout

Defining Citrix Self-Service UI with extensions

- Steps for eLux RP 5 / for eLux RP 6.2 and later versions, see [Citrix Self-Service UI in kiosk mode](#) -



Note

The eLux package **Citrix Workspace app for Linux** or **Citrix Receiver for Linux 13.x** must be installed on the clients.

The eLux package **Citrix Extensions 2.x**² or later and the included feature package **Self-service wrapper** must be installed on the clients.

For modifications on the Citrix dialog design, further feature packages must be installed on the clients:

Dialog Extension and Self-service dialog themes

This may require modifications of the image definition file on the web server via ELIAS.

1. [Add a new application](#) and select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select <code>Custom</code> .
Parameter (mandatory)	Enter the following program name to start the application: <code>ucselfservice</code>

¹for eLux RP 5.6 CR and later versions

²formerly Citrix Receiver Extensions

Option	Description
Free parameters	<p>Define StoreFront URLs for all stores you want to provide as Free application parameters as shown below:</p> <pre>StoreUrl1=<URL to store1> StoreUrl2=<URL to store2> StoreUrl3=<URL to store3></pre> <p>Alternatively, you can provide the users with a range of predefined stores to choose from.¹ For further information, see Self-Service user interface with multistore option.</p>

- Optionally, define further parameters and values for window properties and connection options. For further information, see [Parameters for the Self-Service extension \(ucselfservice\)](#).
- Confirm with **Apply** and **OK**.
- To change the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries**. For further information, see [Parameters for the Self-Service extension \(ucselfservice\)](#).

7.2.6. Self-Service user interface with MultiStore option

The Citrix Self-Service user interface with extensions can also be used with a different option allowing to provide users with a range of predefined stores. The users can then select one of the provided stores to connect to when they log in.²

Defining Citrix Self-Service UI with extensions and MultiStore option

- Steps for eLux RP 5 / for eLux RP 6.2 and later versions, see [Citrix Self-Service UI in kiosk mode](#) -



Note

The eLux package **Citrix Workspace app for Linux** or **Citrix Receiver for Linux 13.x** must be installed on the clients.

The eLux package **Citrix Extensions 2.x**³ or later and the included feature package **Self-service wrapper** must be installed on the clients.

For modifications on the Citrix dialog design, further feature packages must be installed on the clients:

Dialog Extension and Self-service dialog themes

This may require modifications of the image definition file on the web server via ELIAS.

¹for eLux RP 5.5.1000 LTSR CU and later versions

²for eLux RP 5.5.1000 LTSR CU and later versions

³formerly Citrix Receiver Extensions

1. Add a new application and select the application type **Local**.
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: <code>ucselfservice</code>
Free parameters	<p>Configure access to the stores you want the users to choose from. Use the Free application parameters as shown below:</p> <pre> Stores=<number of store entries> Store1=<store display name>,<store url> Store2=<store display name>,<store url> ... Domains=<number of domain entries> Domain1=<domain display name>,<domain> Domain2=<domain display name>,<domain> ... ShowLastUser=<0 1> </pre> <p>Note: You can predefine multiple stores and multiple domains using the format shown above.</p>

3. Optionally, define further parameters and values for window properties and connection options. For further information, see [Parameters for the Self-Service extension \(ucselfservice\)](#).
4. Confirm with **Apply** and **OK**.
5. To change the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries**. For further information, see [Parameters for the Self-Service extension \(ucselfservice\)](#).

7.2.7. Parameters for the Self-Service extension (ucselfservice)

Parameters for window properties and connection options

- ▶ In the application properties, define the following options as free parameters (Steps for eLux RP 5):

Parameter	Description	Origin
SharedUserMode=<true/false>	Shared User Mode allows you 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
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=<0 1>	1 Logoff timer is started with logon 0 Logoff timer is started when the last Citrix app is closed.	Unicon

Parameter	Description	Origin
LogoffInfoTimeout=<seconds>	During logoff (selfservice restart), an info dialog can be shown to the user for some seconds.	Unicon

For further information, see [Defining free application parameters](#).

Important To provide stores to the users, you can either predefine them as fixed values or predefine a range of stores the user can choose from in a pre-logon dialog.¹ For further information, see [Self-Service user interface with extensions](#) or [Self-Service user interface with MultiStore option](#).

Parameters for the design of the Citrix dialogs

- ▶ To modify the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries** and 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, another client restart might be required to enable the new setting.

¹for eLux RP 5.5.1000 LTSR CU and later versions

7.2.8. Custom design for Citrix Workspace app

- for eLux RP 6.4 and later versions -



Note

The eLux package **Citrix Workspace app** 18.08 or a later version must be installed on the clients.

To customize the layout of your Citrix session, transfer the relevant layout files to the clients into the Citrix directory structure. The files then are merged with the Citrix layout files.

To transfer the files, use the Scout Enterprise feature **Files configured for transfer**. For further information, see [Files configured for transfer](#).

As destination specify the provided Citrix directories. Example:

Default	/setup/ica/site_custom
If Shared User Mode is used	/setup/ica/site_custom/sum_screen

The Citrix directory structure must be retained. The original structure can be found under /opt/Citrix/ICAClient/site_orig.

7.2.9. 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 via ELIAS.



Note

HTTPS connections require the relevant [SSL certificates](#) on the client.

1. Add a new application and select the application type **Browser**.
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: <code>https://<Servername>/Citrix/StoreWeb</code> <code>https://<Servername>/Citrix/XenApp</code>

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 published applications, desktops and contents available are shown in the browser window.

7.2.10. 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 the published programs, the application 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 select the application type **PNAgent**.
2. Edit the following fields:

Option	Description
Name	Name of the application
Server	<p>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.</p> <p>Examples: <code>https://CtrXd.sampletec-01.com/Citrix/PNAgent/config.xml</code> <code>https://192.168.10.11:81</code></p>
Login	The user is automatically logged on to the Web Interface server by using the specified credentials (username, password, domain).
Pass-through logon	<p>The user is logged on to the store via single sign-on. The AD user credentials are used.</p> <p>Note: Kerberos authentication is no longer supported with Citrix Receiver for Linux 13.x and later versions.</p>
Autostart application/folder	<p>Specify the names of those applications you want to have started automatically.</p> <p>Alternatively, you can specify an autostart folder containing the relevant published applications. The folder must have already been created on the Web Interface server.</p>
Show last user	<p>The user credentials (except for password) of the last logon are displayed in the PNAgent logon dialog.</p> <p>This option has no effect if you specify fixed user credentials for automatic logon under Logon.</p>
Allow cancel	Allows the user to close the PNAgent logon dialog.
Application restart	See Adding applications
Start automatically	
Desktop icon	

Option	Description
Free parameters (optional)	<p>Individual parameters for application start</p> <p>Example: <code>PNATimeout=60</code> brings Citrix Workspace app¹ to try for 60 seconds to enumerate the published applications and desktops.</p> <p>To configure dual-monitor mode, you can also use the Free parameters, see below.</p> <p>For further information, see Defining free application parameters.</p>

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	<p>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.</p> <p>Alternatively, automatic logoff can be configured to be performed after the last PNAgent application has been closed.</p>
Application reconnection	<p>Determine the actions to be done on a reconnect to the Web Interface server</p> <p>Do not reconnect: The connection to the desktop or the published applications is not restored (default).</p> <p>Disconnected sessions only: The connection to a disconnected session is restored.</p> <p>Active and disconnected sessions: The connection to a disconnected or active session is restored.</p>
Manual logoff	<p>Determine the actions to be carried out upon logoff from the Web Interface server</p> <p>Logoff only server: Logoff is performed only from the Web Interface server</p> <p>Logoff server and applications: Logoff is performed from the Web Interface server and from the virtual desktop or published applications.</p> <p>Logoff server and disconnect session: Logoff is performed from the Web Interface server but the virtual desktop session is only disconnected. This enables users to reconnect later on.</p>

¹formerly Citrix Receiver



Note

Access to the advanced settings can be defined via the object rights.¹

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	Username
\$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 a domain.

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 are requested by a Citrix Web Interface logon 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.sampletec-01.com`.

Settings for dual monitor mode

For PNAgent sessions, you can configure a 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.

¹for Scout Enterprise Management Suite 15.5 and later versions

Method 1:

- ▶ Use the **Advanced file entries** feature of the Scout 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 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

7.2.11. Defining an ICA application**Note**

Access via the ICA application type is deprecated and only supported by Citrix up to XenApp version 6.x.

For elux RP 6, the local application definition does not support the ICA type.

1. [Add a new application](#) and select the application type ICA.
2. Edit the following fields:

Option	Description
Name	Name of 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)

Option	Description
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 no longer supported.
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 (username, password, domain).
Pass-through logon	The user is logged on to a 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 and later versions.
Smart card logon	The client uses a smart card for logon.
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters .
Connection options	Opens the Citrix configuration dialog (<code>wfcmgr</code>) Edit the relevant options.
Advanced (eLux)	The Citrix Workspace app ¹ configuration is saved to the file <code>/setup/ica/wfclient.ini</code> on the Thin Client and can be viewed from the Scout Console via 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.

¹formerly Citrix Receiver

7.2.12. Citrix software defaults

For all Citrix applications, in the Scout Console, you can define Citrix Workspace app¹ 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](#).



Note

To define parameters in individual configuration files, use the [Advanced file entries](#) feature. All parameters defined by using the **Advanced ini entries** override the software defaults.

Some of the Citrix default options are described below. For further information, see the Citrix documentation.

General tab

Option	Description
TW2StopwatchMinimum	<p>Scrolling speed for remote applications (such as Adobe Acrobat Reader, Microsoft Excel)</p> <p>The higher the value, the slower the speed when scrolling</p> <p>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.</p> <p>Default = 25</p>
Client name template	<p>Definition of the client name in the Citrix session</p> <p>Note: You can use the Program Neighborhood variables <code>\$ICANAME</code> and <code>\$ICADOMAIN</code> to set a unique client session name. This is required for Citrix Roaming and some XenApp programs. For further information, see PNAgent application.</p>

¹formerly Citrix Receiver

Drive Mapping tab

Option	Description
A-Z	<p>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.</p> <p>Enter the mount point relating to the local access path of the resource. The mount points are provided by eLux: <code>/media/usbdisk</code> or <code>/media/cdrom</code></p>
Attributes E / R / W	<p>Type of access right</p> <ul style="list-style-type: none"> <input type="checkbox"/> E = enable <input type="checkbox"/> R = read <input type="checkbox"/> 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
<code>/dev/ttyS0</code>	COM1
<code>/dev/ttyS1</code>	COM2

The availability of COM ports depends on the hardware platform.



Note

The client ports must be mapped on the Citrix resource (such as desktops) accordingly. To do so, use a `net use` command.

Example: `net use com1: \\Client\COM2: /persistent:yes`

7.2.13. Citrix Connection Center

By means of the Citrix Connection Center, users can see all current server connections and can log off, disconnect or close them without operating the application. In addition, the connection transport statistics can be viewed which might be helpful for slowing connections.

The Connection Center is provided as a desktop application.¹

Defining the Citrix Connection Center



Note

If you use **Citrix Receiver for Linux**, the eLux package **Citrix Receiver Extensions** and the included feature package **Connection Center** must be installed on the clients. If you use the later **Citrix Workspace app**, the included feature package **Utilities and tools** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

1. Add a new [application](#) and select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name for the application
Local application	Select <code>Citrix Connection Center</code> .
Parameter (optional)	Command-line parameters for program start

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

7.2.14. Logging for Citrix Workspace app

For the Citrix Workspace app, you can enable and configure logging via a configuration parameter.

Configuring the log level

1. In the Scout Console, for the relevant devices, open **Advanced device configuration > Advanced file entries**.

¹formerly as a systray icon on the taskbar

2. Define the following entry

File	/setup/ica/module.ini		
Section	WFClient		
Entry	SyslogThreshold		
Value	0 3 7	0 Logging disabled (default) 3 Only errors are logged 7 Logs for all levels are generated	

For further information, see [Advanced file entries](#).

As soon as the new configuration is active, logs are written to /var/log/messages.

Enabling detailed logging for Microsoft Teams



Note

The eLux package **Citrix Workspace app for Linux** version 21.9.0.25-5 (available with eLux RP 6 2110) or later and the included feature package **Microsoft Teams Optimization** must be installed on the devices.

1. Create a configuration file named `config.json` and enter the following:

```
{
  "WebrtcLogLevel" : 0,
  "WebrpcLogLevel" : 0
}
```

2. Transfer the `config.json` file to the devices to `/setup/ica/hdx_rtc_engine`

For further information, see [Files configured for transfer](#).

When Microsoft Teams (in VDI) is used on the devices, the relevant log files are written.

- ▶ To access the log files, use the diagnostics function. To do so, create a diagnostic template that contains the following entries:

```
/tmp/hdxrtcengine/*/*
/tmp/webrpc/*/*
```

For further information, see "Configuring diagnostic files" on page 277.

After retrieving the diagnostic files, you can find the log files in the `hdxrtcengine` and `webrpc` directories.

7.2.15. Updating Citrix Workspace app

- ▶ To install later versions of the Citrix Workspace app on the devices, perform a firmware update.

**Note**

The existing `/setup/ica/AuthManConfig.xml` template will be overwritten with the template of the new version. Individual entries must then be set again.

7.3. RDP

The **RDP** application type uses 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 options 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.

7.3.1. Defining an RDP Windows desktop session

1. [Add a new application](#) and select the application type **RDP**.
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 (username, password, domain).
Pass-through login	The user is logged on via single sign-on. The AD user credentials are used.
Free parameters	<p>Allows to define any parameters supported by eluxRDP in the format:</p> <pre>FreeRDPParams=<Parameter> <Parameter> <Parameter>...</pre> <p>Separate multiple parameters by spaces.</p> <p>Examples:</p> <pre>FreeRDPParams=/microphone:sys:pulse +fonts /cert-ignore</pre> <p>To view the allowed parameters, enter the eluxrdp command in a shell.</p> <p>For further information, see Defining free application parameters.</p>

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 back-end. The user starts `rdpconnect` from the shell and, subsequently, specifies the server to be connected to. This feature requires the eLux software package **RDPConnect**.

7.3.2. 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 select the application type **RDP**.
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. Examples: <code>c:\Program Files\Microsoft Office\Office\EXCEL.EXE</code> <code>%SystemRoot%\system32\notepad.exe</code>
Working directory (optional)	Working directory of the Windows application
Logon	The user is automatically logged on to the server by using the specified credentials (username, 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.

7.3.3. Advanced application settings / RDP and VMware

The settings described below apply to the following applications:

- RDP applications
- VMware applications

If you select a protocol other than RDP, some options are not available.

Accessing advanced application settings

U Note Access to the advanced settings can be restricted via the object rights.¹

- ▶ Scout Enterprise: In the **Application properties** dialog of an RDP or VMware application, click the **Advanced** button.
- ▶ eLux RP 6: In the **Application properties** dialog of an RDP or VMware application, under **Properties**, expand the relevant section.

View tab

Option	Description
Window size	Full-screen or a specific resolution
Full-screen on monitor	If you have selected the window size <code>Full-screen</code> , select if you want to display on one specific or all monitors. Up to eight monitors are supported. ²
Colors	Color depth for the session (8-32 Bit)

U Note If you use multiple monitors but wish to display content on only one of them, under **Device configuration**³ > **Desktop** > **Advanced** > **Windowmanager**, the **Maximize/fullscreen to single monitor** option must be selected.

Local Resources tab

U Note - for terminal servers supporting RDP protocol version 5.2 or later -
The settings take effect only if, on the **Advanced** tab, the value of the **Protocol** field is not set to RDP V4.

¹for Scout Enterprise Management Suite 15.5 and later versions

²for Scout Enterprise Management Suite 15.0 and later versions

³formerly Setup

Option	Description
Drive mapping	<p>Select drive, mount point and drive letter that you want to show in the RDP/VMware session.</p> <p>The mount points correspond to the local access paths of the resources and are provided by eLux.</p> <p>For USB devices the mount points are <code>/media/usbdisk</code> <code>/media/usbdisk0</code> and so on.</p> <p>For further information, see Mount points.</p>
Connect printer	<p>Up to four printer definitions can be created automatically for a session. The printers must be configured on the Printer tab in the eLux device configuration and 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, choose Set as default in the eLux printer configuration.</p>
Sound	<p>Play local reproduces the sound locally on the client. Play remote causes playback on the remote server.</p>
Connect ports	Makes the defined port connections accessible in the session
Enable smartcard	Smart cards based on a certificate can be used for login.

Advanced tab

Option	Description
Protocol (only RDP)	<p>Enables you to set the RDP protocol to version 4 or 5</p> <p>Normally, the protocol is recognized automatically.</p>
Keyboard language	<p>Defines the keyboard layout within a session</p> <p>The default is Auto which corresponds to the keyboard setting of the eLux device configuration.</p>

Important If you define a specific language, it must be identical to the keyboard language defined in the eLux device configuration, in the **Keyboard** dialog.

Deactivate Window-Manager Decorations	The frames of the eLux windows are hidden.
Deactivate encrypting	<p>The server does not accept encrypted sessions. You can use this option to increase performance.</p> <p>By default, the option is disabled.</p>
Deactivate mouse move events	<p>Mouse position data are not transferred to the server constantly, but with every mouse click. This increases system performance and is especially helpful for connections with small bandwidth.</p> <p>By default, the option is disabled.</p>

Show connection bar on full screen	Shows connection list in full-screen mode
Bandwidth	Choose between standard, modem, broadband or LAN.

7.3.4. Configuring RemoteFX

Microsoft RemoteFX™ offers comprehensive functionality for Virtual Desktop Infrastructure (VDI) by providing a virtual 3D adapter, intelligent codecs and the ability to redirect USB devices to virtual machines.



Note

RemoteFX only works if the server supports RemoteFX and is configured in the right way. The only parameter to be configured on the client is bandwidth.

1. For your **RDP** application, open the **Application properties** dialog and click **Advanced**.
2. On the **Advanced** tab, in the **Bandwidth** field, select **LAN**.
3. Confirm with **Apply** and **OK**.

7.4. Virtual Desktop



Note

For eLux RP 6, instead of **Virtual Desktop**, the application type **VMware Horizon** is available.

The **Virtual Desktop** tab helps you define Citrix or VMware connections with with a VD broker.¹ For Citrix XenDesktop, the logon data are defined according to an ICA connection.

7.4.1. Defining a virtual desktop

1. [Add a new application](#) and select the application type **Virtual Desktop**.
2. Edit the following fields:

Option	Description
Name	Name for the application
VD Broker	Select a virtual desktop application from the list.
Server	Enter the server IP address (or name)
Logon Pass-through logon	See Adding applications
Protocol (VMware Hori- zon only)	Choose between the following values: RDP PCoIP VMware Blast ²

3. To configure further settings for XenDesktop or VMware Horizon, click **Advanced**. For further information, depending on the broker selected, see
 - [Advanced application settings / RDP and VMware](#) (for VMware Horizon)
 - [Advanced XenDesktop settings](#) or
4. Confirm with **Apply** and **OK**.

7.4.2. VMware Horizon



Note

This application type is available only on the eLux RP 6 device. In the Scout Console, choose the **Virtual desktop** application type and, under **VD broker**, select **VMware View**.

¹From Scout Enterprise Management Suite 15.8, only VMware Horizon is supported.

²for Scout Enterprise Management Suite 15.2 and later versions

Application type
VMware Horizon

Name

Auto start
☐

Desktop icon
☒

Properties

VD Broker
VMware Horizon

Server

Pass-through login
☒

Use SSL
☐

Show last user
☒

Protocol
RDP

Display

Local resources

Advanced

Option	Description
Name	Name for the application
Auto-start	The application starts automatically after eLux has been started.
Desktop icon	Provides a desktop shortcut on your personal desktop
VD broker	VMware Horizon
Server	IP address or name of the server
Pass-through logon	The user is logged on via single sign-on. The AD user credentials are used.

Option	Description
Username, Password, Domain	The user is automatically logged on to the server by using the specified credentials.
Use SSL	Forces the connection via HTTPS Note that HTTPS connections require the relevant SSL certificates on the client.
Show last user	The user credentials (except for password) of the last logon are displayed in the logon dialog
Protocol	Choose between the following protocols: RDP PCoIP VMware Blast ¹

For information on **Display**, **Local resources** and **Advanced** settings, see [Advanced application settings](#).

You can configure the VMware Horizon client by using the application definition in the Scout Console or locally on the client. To set additional parameters that are not included in the interface, use a configuration file:

- ▶ With the help of VMware documentation,² create the file `view-userpreferences`. Transfer the file via the Scout feature [Files configured for transfer](#) to the clients to `/setup/elux/.vmware/view-userpreferences`



Note

The configuration on the Scout or eLux interface has precedence over the configuration file and will overwrite values of the configuration file.

¹for Scout Enterprise Management Suite 15.2 and later versions

²Installation guide for VMware Horizon Client for Linux

7.5. Browser

Supported browsers are Mozilla Firefox and Google Chromium.

In addition, the Builtin Browser is available as a slimmed-down browser.¹ The Builtin Browser is based on the WebKit2 engine which is part of the **Desktop environment**² package. By default, the Builtin Browser is run without address and navigation bar. These and some more features can be configured for the kiosk mode.



Note

If you use Chromium, we recommend that you equip your Thin Clients with 2 GB of RAM.

For eLux RP 6 and later versions, the Java browser plugin is no longer supported.

7.5.1. Defining a browser application

1. Add a new application and select the application type **Browser**.
2. Edit the following fields:

Option	Description
Name	Name of the browser shown in the Scout Console
Browser type	Select <code>Firefox</code> , <code>Chromium</code> or <code>Builtin Browser</code> . ³
Start page	Web page (URL) that opens when you click Home
Called page	Web page (URL) that opens after starting the browser
Proxy type	<ul style="list-style-type: none"> ■ <code>No proxy</code>: No proxy server is used ■ <code>Manual (Proxy:Port)</code>: Specify a proxy server and port number ■ <code>Auto (URL)</code>: Use a proxy configuration file ■ <code>Use system proxy (default)</code>:⁴ 'System-wide' proxy setting defined in the device configuration under Network > Advanced per network profile <p>Note that the setting behind <code>System proxy</code> can also be <code>No proxy</code>).</p>

For further information, see [Proxy configuration](#).

¹for Scout Enterprise Management Suite 15.4 / eLux RP 6.5 and later versions

²formerly MATE Desktop

³for Scout Enterprise Management Suite 15.4 / eLux RP 6.5 and later versions

⁴for Scout Enterprise Management Suite 15.5 and later versions



Note

For the Builtin Browser, the setting must be left on `Use system proxy`.

Application restart
Start automatically
Desktop icon

See [Adding applications](#)

Free parameters (optional)

Individual parameters for application start
see [Defining free application parameters](#)

3. To enable the **Kiosk** mode for Firefox, see [Configuring kiosk mode](#).
4. 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 that you 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	<code>/setup/cacerts/firefox</code> for eLux RP 6.4 and earlier versions <code>/setup/cacerts/browser</code> for eLux RP 6.5/Firefox 60.5 and later versions ¹
-----------------	--

Google Chromium	<code>/setup/cacerts/browser</code>
-----------------	-------------------------------------

For further information, see [Files configured for transfer](#).

Note that a second restart 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.

¹The certificates can be located in either directory.

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 [Files configured for transfer](#).

7.5.3. Preferences Firefox

For version 60 ESR and later versions, Firefox supports enterprise policies that are deployed via .json files and are cross-platform compatible.¹ Starting with RP 6.5 and later versions, Firefox is installed with enterprise policies enabled that block access to `about:config` and other configuration options by default.

Setting preferences with .json files (policies)

- for eLux RP 6.5 / Firefox 60 ESR and later versions -

You can use all options that are listed in the [README on the Mozilla GitHub repository](#).²

One or more options are transferred in a .json file to the client by using the Scout Enterprise feature **Files configured for transfer**.



Note

By default, access to the Firefox configuration is blocked.

1. Create a .json file (any file name) and insert one or more options separated by commas.

Example:

```
{
  "BlockAboutConfig": false,
  "DisableBuiltinPDFViewer": true
}
```

2. In the Scout Console, for the relevant clients, open **Advanced device configuration**³ > **Files**.

Define your .json file as source file. For the destination folder, use
/setup/firefox/policies/.

Example: /setup/firefox/policies/custom_A.json

For further information, see [Files configured for transfer](#).

On the next client restart, the files are transferred and evaluated.

¹This method will not work if Firefox is already being managed by using Windows group policies.

²Note that the current Firefox version may differ from that of the eLux version you are using.

³formerly **Advanced settings**



Note

You can deploy multiple `.json` files to the client to `/setup/firefox/policies/`. The files are merged in alphabetical order: For identical options, values from files with descending names have precedence (B overrides A).

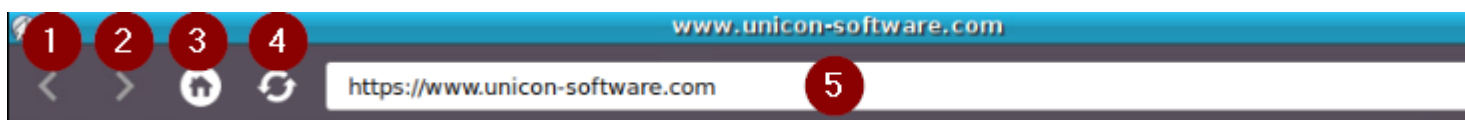
7.5.4. Preferences Builtin Browser

Display options

By default, the Builtin browser opens with only the title bar, but no navigation bar.

- ▶ To display the navigation bar with additional functions, open the properties of your browser application and click **Advanced**.¹

With which functions the navigation bar is displayed, you also define in the **Advanced browser settings**:



- 1 Back
- 2 Forward
- 3 Home button to open home page
- 4 Refresh
- 5 Address bar
- 6 Print

The title bar is always shown.

User Agent-String

With each page request, the Builtin browser transmits a 'User Agent' string, which is predefined by the WebKit2 engine. It contains information like Mozilla compatibility and operating system.

To transmit individual information, define an Advanced file entry:²

1. In the Scout Console, for the relevant devices, open **Advanced device configuration > Advanced file entries**.
2. Define the following entry:

```
File      /setup/sessions.ini
Section  [BuiltinBrowserDefaults]
```

¹from 15 2101 und eLux RP 6 2103

²from eLux RP 6.8.2

Entry	UserAgentString
Value	<i><name/version> <individual string></i> Example: Mozilla/5.0 (X11; Linux x86_64)

For further information, see [Advanced file entries](#).



Note

Name and version must be included in the User Agent string.

DNS cache

- from eLux RP 6 2104 -

The DNS cache of the Builtin browser is set to 120 seconds by default. To configure the timeout value individually, define an environment variable in the Advanced device configuration:

1. In the Scout Console, for the relevant devices, open **Advanced device configuration > Environment**.
2. To define a new variable, click **New**.
3. Enter the variable using the format:

WEBKIT_DNS_CACHE_EXPIRE_TIMEOUT=*<number of seconds>*
and confirm with **OK**.

The new variable is shown in the list.

For further information, see "Environment variables" on page 172.

7.5.5. Browser home directory

By default, the browser settings are temporarily saved to the flash memory. However, they are deleted with each client 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**).

Example: `/smb/share`

For further information, see [Defining a network drive](#).

Defining browser home directory



Note

The following information refers to Scout Enterprise Management Suite 15.0 and later versions. Documentation for earlier versions can be found in the **Archive** section of the [PDF downloads](#) page.

1. In the tree view, for the relevant level, open the **Applications** context menu and click **Software defaults...**
For further information, see [Defining software defaults](#).
2. In the list-field, select the relevant browser and click **Edit**.
3. In the **Browser home directory** field, enter the name of one of the defined drives in **Device configuration**¹ > **Drives**. The name must correspond to the name on the list.
Example: `/smb/share`
4. Confirm with **OK**.

The browser settings are saved to the specified Windows directory.

¹formerly Setup

7.5.6. Kiosk mode for Firefox

- for Firefox up to version ESR 52.8 ¹ and from version 71.0 -



Note

For eLux RP 6.5 and later versions, you can use the Builtin Browser in kiosk mode. For further information, see [Builtin Browser in kiosk mode](#).

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.

By default, the browser window is displayed without address bar and navigation buttons. So users are forced to stay on the predefined web page and cannot exit.

Kiosk mode is suitable if the users are supposed to see only one website and not use further applications on the Thin Client. For correct use of the kiosk mode, we recommend that you disable related functions of the Thin Client such as restarting the device and opening the control panel. For further information, see [Device configuration > Security](#).

Configuring kiosk mode



Note

Firefox supports kiosk mode again starting with version 71.0, but without configuration options. With Scout 15 2110, the Firefox application definition is adapted and offers only the option **Enable 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	Activates the kiosk mode
Display navigation bar ²	Allows using browser tabs despite kiosk mode Users can view multiple web pages of the defined web site concurrently
Add print button ³	Allows using browser tabs and provides a Print feature despite kiosk mode
Add address bar ⁴	Allows using browser tabs and provides the address bar including navigation buttons despite kiosk mode

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

¹included in eLux RP 6.4

²up to Scout 15 2107

³up to Scout 15 2107

⁴up to Scout 15 2107

On the next restart, the Firefox 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 an application is missing, you can define your own application or command via 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 first running the command within an XTerm session for testing purposes.

7.6.1. Defining predefined local applications

1. [Add a new application](#) and select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout 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 select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Console
Local application	Select <code>Custom</code> .

Option	Description
Parameter (mandatory)	Enter the program name required to start the application. If required, add start parameters. Example: <code>calibrator</code> calls the Calibrator tool <code>squid</code> calls the Squid application <code>squid /tmp/mycache</code> 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 screenshot shows the 'Application properties' dialog box for the 'Calibrator' application. The 'Local' tab is selected. The 'Name of application' field contains 'Calibrator'. The 'Display name' field contains 'Calibration'. The 'Sorting ID' field contains '1'. The 'Local application' dropdown menu is set to 'Custom'. The 'Parameter' field contains 'calibrator'. At the bottom, there are checkboxes for 'Hidden' (unchecked), 'Restart application' (unchecked), 'Start automatically after' (set to '0 s'), and 'Desktop icon' (checked). There are also buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

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 via the control panel, start menu, or desktop icon (provided that the **Calibrator** tool is included in the image).

7.6.3. Defining Zoom for Linux

The native Zoom client for Linux is a Video Conferencing and Web Conferencing service and offers high-quality video, audio, and screen-sharing experience.

The video and audio devices are configured via the application interface.

1. Add a new application and, in the **Application properties**, select the application type **Local**.
2. Edit the following fields:

Option	Description
Name	Name for the application
Application	Custom
Parameter	zoom

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

7.6.4. Defining Ekiga SIP Softphone

Ekiga is a free software application for audio and video telephony (VoIP) that supports the SIP protocol. Configuration is based on a SIP account.

1. Add a new application and, in the **Application properties**, select the application type **Local**.
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 username>
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. Emulation

From Scout 15 2110, the following emulations are supported:¹

- PowerTerm InterConnect

Licensed emulation suite that allows you to connect to IBM mainframes, IBM AS/400, Unix, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000, Data General and more

- 5250 terminal emulation

7.7.1. Configuring PowerTerm InterConnect



Note

The use of **PowerTerm InterConnect** requires the relevant application licenses.

The configuration of PowerTerm InterConnect is carried out in two steps:

- Define a PowerTerm application on a reference device and transfer the created configuration files
- Define a PowerTerm application for all devices by using the configuration files created on the reference device

Defining a PowerTerm InterConnect application for a reference device



Note

The **PowerTerm** software package must be installed on the device. This may require modifications of the image definition file on the web server via ELIAS.

1. On the reference device or in the Scout Console, define a PowerTerm application containing only the application name (for details see below).
2. Start the PowerTerm application on the reference device 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 the PowerTerm application.
4. Copy the four configuration files via network or USB stick and make them available to Scout Console.
Or:

¹Applications of the `Emulation` type can only be defined in the Scout Console but not locally on eLux RP 6 devices.

Transfer the files from the device to the Scout Console remotely by using **Request diagnostic files** with an individual template. For further information, see [Configuring diagnostic files](#).

The configuration files for the PowerTerm configuration are provided. The second step may be carried out.

Defining a PowerTerm InterConnect application for all devices

1. In the Scout Console, add a new application for the relevant 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 white spaces.										
Parameters	<p>Optional starting parameters for the PowerTerm application:</p> <table> <tr> <td>-fullscreen</td><td>full screen</td></tr> <tr> <td>-maximize</td><td>maximized window</td></tr> <tr> <td>-no-menu-bar</td><td>no menu bar</td></tr> <tr> <td>-no-tool-bar</td><td>no toolbar</td></tr> <tr> <td>[myName].pts</td><td>name of an individual PowerTerm configuration file of the client</td></tr> </table> <p>Example 1: -fullscreen -no-menu-bar -no-tool-bar</p> <p>Example 2: -fullscreen ptconfig001.pts</p>	-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
-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										
Terminal setup file	Select the relevant .pts file of the reference device from the file system.										
Communication file	Select the relevant .ptc file of the reference device from the file system.										
Keyboard file	Select the relevant .ptk file of the reference device from the file system.										
Power PAD file	Select the relevant .ptp file of the reference device from the file system.										
x button	<p>Delete previously selected configuration file from the Scout Enterprise database if required.</p> <p>To delete the file physically from the device, you need to perform a factory reset.</p>										

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

PowerTerm InterConnect is available for all devices of the relevant OU on the next restart.

7.8. Applications in kiosk mode

Some applications can be configured so that users can only operate them in kiosk mode.

In kiosk mode, the application opens as a full-screen window. Users cannot open any additional windows and cannot close the application. The connection settings and the resources that users are allowed to access at the back-end, such as Citrix stores, are predefined in a configuration file. As a consequence, defining applications for the user becomes obsolete.

After system start, the client starts the application defined by the configuration files in kiosk mode, ensuring that the user is directly in the intended work environment and cannot break out.

Version information for kiosk mode support

	Configuration via .ini file	Configuration via console (GUI)
Citrix Self-Service-user interface with extensions	from eLux RP 6.2	from Scout 15 2107 and eLux RP 6 2110.1
Builtin Browser	from eLux RP 6.5 ¹	from Scout 15 2107 and eLux RP 6 2110.1
Konfigurationsdatei	kioskmode.ini	kioskconfig.ini

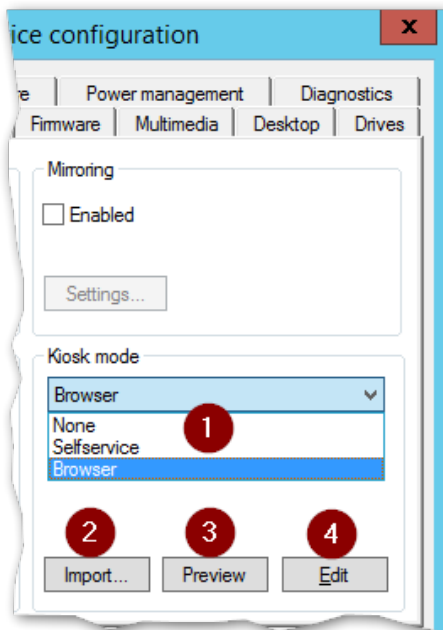
7.8.1. Setting up kiosk mode via console

- from Scout 15 2107² -

The Scout Console interface allows you to define kiosk mode for Citrix Self-Service (A) as well as for the Builtin Browser (B). The corresponding function is located in the device configuration under **Security**. The kiosk mode can be configured differently depending on the OU.

¹For earlier versions, use Firefox in kiosk mode.

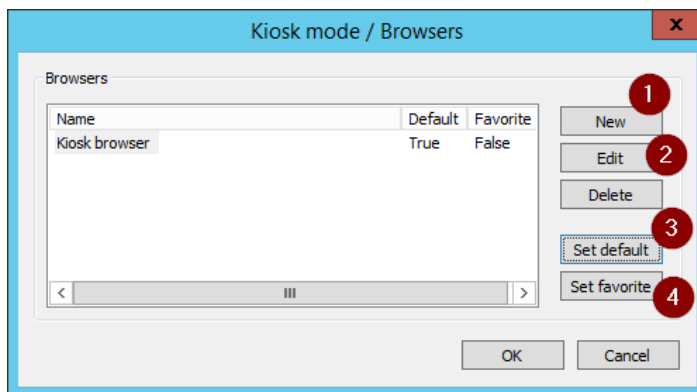
²The devices support the new settings only from eLux RP 6 2110.1.



- 1 Enable kiosk mode and select type
- 2 Import existing configuration
- 3 View configuration
- 4 Configure kiosk mode for selected type (browser or Citrix)

1. For the relevant devices, open **Device configuration > Security**.
2. Under **Kiosk mode** in the list-field, choose whether you want to activate the kiosk mode for Citrix Self-Service (A) or Browser (B).
3. If you already have a `kioskmode.ini` or `kioskconfig.ini`, click **Import...**
4. Click **Edit**.

Depending on the selected type, the configuration dialog for Citrix Self-Service stores (A) or for browsers (B) opens.



- 1 Create new browser
- 2 Edit selected browser
- 3 Set selected browser as default
- 4 Mark selected browser as favorite

5. Create and configure at least one store (A) / browser (B) for kiosk mode.
6. If you have created multiple stores (A) / browsers (B), you can then set one as default.
On logon, default stores (A) / browsers (B) are pre-selected or started automatically.
7. If you have created multiple stores (A) / browsers (B), you can mark one or more as favorites.
*Favorites are shown to the user on the store selector of the system bar with an asterisk.
Favorites for stores can only be defined without **MultiStore**.*

Your configuration is written to the `kioskconfig.ini` file. To check it, click the **Preview** button. The next time the server connects to the devices, your selected kiosk mode type (`terminal.ini` entry) will be transferred along with the `kioskconfig.ini`.

(A): On the devices, after start-up, the Citrix Self-Service interface opens in kiosk mode. The configured stores are available to the user. No other applications can be started apart from the Self-Service interface.

(B): On the devices, after start-up, the Builtin browser opens in kiosk mode. The configured functions are available to the user. No other applications can be started apart from the browser.



Note

For correct use of the kiosk mode, we recommend that you restrict the user rights for the client as required.

7.8.2. Configuring browser for kiosk mode

- from Scout 15 2107¹ -

1. In the **Kiosk-Modus / Browser** dialog, create a new browser definition. To do so, click **New**.
2. Select and edit the newly created browser definition:

- 1 Display name of the browser
- 2 Web page (URL) that opens after starting the browser
- 3 Web page (URL) that opens when you click **Home**
- 4 The first URL users load after the home page will be saved as new startup page.²
- 5 Unhide navigation bar
- 6 Elements of the navigation bar to be shown

3. Confirm with **OK**.

¹The devices support the new settings only from eLux RP 6 2110.1.

²How users access the Home page (Home button, link on the startup page, address bar or configured Home page is identical to startup page) is irrelevant. Nevertheless, we recommend that you show the navigation bar with Home button when selecting this option.

7.8.3. Configuring Citrix Self-Service for kiosk mode

- from Scout 15 2107¹ -



Note

The eLux package **Citrix Workspace app for Linux** must be installed on the clients.
The eLux package **Citrix Extensions 2.x** or later and the included feature package **Self-service wrapper** must be installed on the clients.

For modifications on the Citrix dialog design, further feature packages must be installed on the clients:

Dialog Extension and **Self-service dialog themes**

This may require modifications of the image definition file on the web server via ELIAS.

1. For Citrix Self-Service, first configure the settings, see below. These apply to all stores.
2. In the **Kiosk mode / Citrix Self-Service** dialog, create a new store. To do so, click **New**.
3. Edit the new store:

Option	Description
Name	Display name of the Citrix-Store
Store URL	Web page (URL) that opens immediately after starting the browser
Autostart resources	List of Citrix applications/desktops you want to start automatically after logon Currently only available in combination with the MultiStore option

4. Confirm with **OK**.

*If multiple stores are defined, users can switch between stores using the **Store** button on the system bar (store selector). Stores marked as favorites are displayed with an asterisk. If **MultiStore** is configured, users can switch between stores via the logon dialog. For further information on the **MultiStore** option, see below.*

Self-Service settings for kiosk mode

- ▶ To access the general settings, in the **Kiosk mode / Citrix Self-Service** dialog, click **Settings**.

¹The devices support the new settings only from eLux RP 6 2110.1.

The screenshot shows the 'Self-Service / Settings' dialog box. It is divided into several sections: 'MultiStore', 'Log off', 'Reconnect', 'General options', and 'Domains'. Red circles with numbers 1 through 12 point to specific UI elements: 1 points to the 'Provide MultiStore option on logon' checkbox; 2 points to the 'Pass-through mode' dropdown menu; 3 points to the 'Automatically' checkbox under 'Log off'; 4 points to the 'Logoff delay' input field; 5 points to the 'Logoff timeout' input field; 6 points to the 'On logon' checkbox under 'Reconnect'; 7 points to the 'On app start or store refresh' checkbox; 8 points to the 'Self-Selection' checkbox under 'General options'; 9 points to the 'Shared user mode' checkbox; 10 points to the 'Show session in window' checkbox; 11 points to the 'New' button in the 'Domains' table; 12 points to the 'Helper' button. The 'Domains' table has columns 'Name' and 'Domain' with one entry 'INT' and 'int.sampletec-01.com'.

- 1 MultiStore: During logon, users can choose between pre-defined stores.
- 2 Logon can be done without passthrough credentials, via Active Directory or with a defined username+password. The password must be ICA-encrypted.
- 3 Logoff can be done automatically. Set the timer for it.
- 4 Delay in seconds when the logoff timer is started
- 5 Display duration for message on logoff
- 6 Self-Service tries to reconnect all sessions for a store directly after logon to that store (Citrix Self-Service option).
- 7 Self-Service tries to reconnect all sessions as soon as an application is started or the store is updated (Citrix Self-Service option).
- 8 Users are allowed to subscribe to extra applications (Citrix Self-Service option)
- 9 Use one system account for multiple users (Citrix Self-Service option)

The user data are deleted when they close the app or log off.

We do not recommend combining this option with **MultiStore**.
- 10 The session is displayed in windowed mode (instead of full-screen) (Citrix Self-Service option).
- 11 Define domains
- 12 Define helpers for **MultiStore**

You no longer have to group stores into environments.

MultiStore

The **MultiStore** option allows you to predefine multiple stores - optionally in different domains. Define one of the stores as the default store. Users are then presented with a Citrix Self-Service logon dialog

from which they can choose between the preconfigured domains and stores. The default store is pre-selected as the **Home location** with its domain.

- 1 Configurable title text (**MultiStore title**)
- 2 Users must log on with their username and password.
- 3 Predefined domains
- 4 Predefined stores
- 5 Users are redirected to your password reset page, to be defined under **Helper**.

If you have defined auto resources for a store, the specified desktops or applications are started automatically after logon.



Note

The store selector on the system bar is not available to the users. To switch to another store, users log off and return to the logon dialog.

Note the following for configuration:

- Define one domain as a minimum.
- If you define multiple stores, one store must be set as the default.
- Logon with passthrough is not available.
- We do not recommend combining **MultiStore** with **Shared User Mode**.

Domains

Domain definition is required if you use **MultiStore** or - without **MultiStore** - if you configure **Passthrough** for Active Directory.

- ▶ In the **Self-Service / Settings** dialog, click **New** to create one or more domains. Then edit the new entries.

- 1 Display name for domain
- 2 Domain as FQDN
- 3 URL for a page that allows resetting passwords (MultiStore only).

Helper

- only MultiStore -

A helper URL links to an existing password reset page. To access this page, users click a button in the **MultiStore** logon dialog.



Note

You can define one helper URL per domain. This is normally done when you define a domain.

To configure the button for the users and the behavior of the browser with reset page, use the **Helper** dialog.

- ▶ In the **Self-Service / Settings** dialog, under **Domains**, click **Helper**.

Option	Description
Button text	<p>Button label in the MultiStore logon dialog</p> <p>Example: <code>Forgot password?</code></p> <p>By default, this text is additionally shown in the browser title bar above the reset page.</p>
Timeout	<p>Timeout for launching the Bultin browser and loading the password reset page</p>
Options	<p>Optionally, specify additional parameters for the browser start.</p> <p>Example: <code>--title "Reset password"</code></p>

If users do not remember their password, they click the relevant button in the **MultiStore** logon dialog. This launches the Bultin browser and loads the helper URL defined for the domain the user is logging on to.

Design of the Citrix dialogs

- ▶ To change the design of the Citrix dialogs for all Citrix connections, in the **Kiosk mode / Citrix Self-Service** dialog, click **Theme**.

Option	Description
Name	Name of the Citrix theme Default: <code>ucselfservice</code>
Window decoration	The windows are displayed with window decoration.
On hovering...	Background color for list elements on mouse hover (Citrix list selection widgets) Default: <code>#e6f1f7</code>
Unselected...	Background color for unselected list elements (Citrix list selection widgets) Default: <code>#ffffff</code>
Selected...	Background color for selected list elements (Citrix list selection widgets) Default: <code>#cce3f0</code>

7.8.4. Citrix Self-Service in kiosk mode (< eLux RP 6 2110.1)

- for eLux RP 6.2 and later versions -

The Citrix Self-Service user interface with extensions is no longer configured as a user-defined application `ucselfservice` with free parameters. For eLux RP 6.2 and later versions, you do not need to define an application; instead, you configure the kiosk mode. All relevant parameters are defined in the configuration file `kioskmode.ini`. Advanced functionality and MultiStore option are also configurable.

Defining Citrix Self-Service UI in kiosk mode



Note

The eLux package **Citrix Workspace app for Linux** or **Citrix Receiver for Linux 13.x** must be installed on the clients.

The eLux package **Citrix Extensions 2.x**¹ or later and the included feature package **Self-service wrapper** must be installed on the clients.

For modifications on the Citrix dialog design, further feature packages must be installed on the clients:

Dialog Extension and Self-service dialog themes

This may require modifications of the image definition file on the web server via ELIAS.

1. For the relevant clients, open **Advanced device configuration**² > **Advanced file entries** and define the following entry:

File	/setup/terminal.ini
Section	Layout
Entry	KioskMode
Value	1

For further information, see [Advanced file entries](#).

This parameter enables the kiosk mode for the Citrix Self-Service user interface with extensions.

2. Create a text file named `kioskmode.ini` and add the section header `[Parameters]`. Enter the relevant parameters:³

Parameter	Description
ReconnectOnLogon=true false	Determines whether the Self-Service UI tries to reconnect to all sessions for a given store, immediately after logon to that store (Citrix Self-Service option)
ReconnectOnLaunchOrRefresh=true false	Determines whether the Self-Service UI tries to reconnect to all sessions when an application is launched or the store is refreshed (Citrix Self-Service option)

¹formerly Citrix Receiver Extensions

²formerly **Advanced settings**

³Default values are displayed in **bold**

Parameter	Description
SharedUserMode=true false	<p>If the Shared User Mode is enabled, the Self-Service UI uses one technical user account for multiple users. The user data are removed from the device when users log off or close the UI. (Citrix Self-Service option)</p> <p>We recommend that you do not use this parameter together with <code>Prelogin=true</code></p>
SelfSelection=true false	<p>Is used to disable the search box and the Self-Selection panel (legacy UI)</p> <p>Disabling these UI elements prevents users from subscribing to extra applications.</p>
LogoffMode=0 1 2 3	<p>0 = No automatic logoff 1 = Logoff timer is started with logon 2 = Logoff timer is started when the last Citrix app/desktop is closed 3 = Logoff timer is started when the first Citrix app/desktop is opened</p>
LogoffDelay= <seconds>	Delay in seconds after the logoff timer is started
LogoffInfoTimeout= <seconds>	Shows a message for n seconds during logoff
ShowLastUser=true false	Shows last logged-on username in User field
PreLogin=true false	<p>Determines, whether on logon a dropdown list with pre-configured stores is shown (MultiStore).</p> <p>We recommend that you do not use this parameter together with <code>SharedUserMode=true</code></p>
PreLoginTitle	Dialog title for the stores list (MultiStore)
PassThroughMode=0 1	<p>0 No pass-through logon data 1 Active Directory</p>
Domain<1-N>= <Domain display name, domain>	Each entry contains a domain.

- To define access to the stores, in the `kioskmode.ini` file, add one or more sections named `[Store<1-N>]` or `[Environment_Store<1-N>]`.

If you define stores by using `[Environment_Store<N>]`, the user can switch between the stores by clicking the **Store** button on the taskbar. The Stores are shown in groups (Environment) as defined.

`[Store<1-N>]`

Parameter	Description
Url= <Store URL>	URL of the Citrix store
FriendlyName= <Store display name>	Display name for the Citrix store
Default=true false	Determines whether this store is displayed as default store
AutostartResources= <App/Desktop1;App/Desktop2;...>	List of Citrix applications/desktops to be started automatically after login Currently only available with PreLogin=true

[Environment_Store<1-N>].

Parameter	Description
Url= <Store-URL>	URL of the Citrix store
FriendlyName= <Anzeigename>	Display name for the Citrix store
Default=true false	Determines whether this store is displayed as default store
Environment= <Gruppenname>	Specifies the group by which the stores are grouped (freely definable character string)
AutostartResources= <App/Desktop1;App/desktop2;...>	List of Citrix applications/desktops to start automatically after login Currently only available with PreLogin=true

- To change the design of the Citrix dialogs for all Citrix connections, in the `kioskmode.ini` file, add a section named [Theme]:

Parameter	Description
ThemeName= <Themes>	Name of the Citrix theme Default: ucselfservice
Decorated=true false	Determines whether the windows are shown with window decoration
ColorHover= <RGB-Farbcode>	Background color for list elements on mouse hover (Citrix list selection widgets) Default: #e6f1f7
ColorUnselected= <RGB-Farbcode>	Background color for unselected list items (Citrix list selection widgets) Default: #ffffff

Parameter	Description
ColorSelected= <RGB-Farbcode>	Background color for selected list elements (Citrix list selection widgets)
	Default: #cce3f0

5. Transfer the `kioskmode.ini` file to the clients to `/setup/kioskmode.ini`. To do so, use the Scout Enterprise feature **Files configured for transfer**. For further information, see [Files configured for transfer](#).

The `terminal.ini` entry along with the `kioskmode.ini` file on the client will cause the client to open the Citrix Self-Service interface in kiosk mode after start-up. The configured stores are available to the user. No other applications can be started apart from the self-service interface.



Note

If more than one store is configured, users can switch between the stores by clicking the **Store** button on the taskbar while pressing SHIFT.

Example for `kioskmode.ini`

```
[Parameters]
ReconnectOnLogon=true
ReconnectOnLaunchOrRefresh=true
SharedUserMode=true
SelfSelection=false
ShowLastUser=true
LogoffMode=3
LogoffDelay=10

[Store1]
Url=https://xd7a/int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp A

[Environment_Store1]
Url=https://xd7b./int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp B
Default=true
Environment=PROD

[Environment_Store2]
Url=https://xd7c./int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp C
Default=false
Environment=INT

[Theme]
ThemeName=ucselfservice
Decorated=false
ColorHover=#b0b0b0
```

ColorUnselected=#a0a0a0
ColorSelected=#c0c0c0

7.8.5. Browser in kiosk mode (< eLux RP 6 2110.1)

- for eLux RP 6.5 and later versions -

For kiosk mode, the Builtin Browser is used. In kiosk mode, the browser is started in full-screen mode and with limited user rights. The user cannot open other windows and cannot exit the browser. Note that the Builtin Browser if defined as a browser application is not run in kiosk mode even if address and navigation bar are hidden.



Note

Firefox can be run in kiosk mode up to version ESR 52.8 ¹. Mozilla supports kiosk mode again starting with version 71.0, but without configuration options. For further information, see [Kiosk mode for Firefox](#).

1. For the relevant devices, open **Advanced device configuration > Advanced file entries** and define the following entry:

File	/setup/terminal.ini
Section	Layout
Entry	KioskMode
Value	2

For further information, see [Advanced file entries](#).

This parameter enables the kiosk mode for the browser application.

2. Create a text file named `kioskmode.ini` and add the section header `[Browser1]`.
3. Below, enter the relevant parameters:²

Parameter	Description
Url= <URL of startup page>	Web page (URL) that opens after starting the browser
Homepage= <URL of homepage>	Web page (URL) that opens when you click Home
SaveFirstLink=true false	If true , the first URL loaded when coming from the startup page will be saved as new startup page.
Navbar=true false	Determines whether the navigation bar is shown

¹included in eLux RP 6.4 container

²Default values are displayed in **bold**

Parameter	Description
NavbarPrint= true false	Determines whether the Print button is shown on the navigation bar
NavbarForward= true false	Determines whether the Forward button is shown on the navigation bar
NavbarBackward= true false	Determines whether the Backward button is shown on the navigation bar
NavbarHome= true false	Determines whether the Home button is shown on the navigation bar
NavbarUrl= true false	Determines whether the address bar is shown
NavbarRefresh= true false	Determines whether the Refresh button is shown on the navigation bar

4. Transfer the `kioskmode.ini` file to the clients to `/setup/kioskmode.ini`. To do so, use the Scout Enterprise feature **Files configured for transfer**. For further information, see [Files configured for transfer](#).

The `terminal.ini` entry along with the `kioskmode.ini` file on the client will cause the Builtin-Browser to open in kiosk mode after system start-up. The configured functions are available to the user. No applications other than the browser can be started.



Note

For correct use of the kiosk mode, we recommend that you restrict the user rights for the client as required.

Defining different web pages for devices/OU's

- from eLux RP 6.7 -

If you want your devices to start with different browser startup pages (`Url`) or have different home pages (`Homepage`), you can parameterize the web pages using environment variables. Carry out the steps described above with the following differences:

1. In the `kioskmode.ini`, in the `[Browser1]` section, for the first and/or second value, set a variable. Example:
`Url=$URL1`
`Homepage=$URL2`
2. Define the variables used in the `kioskmode.ini` as environment variables for the relevant devices (Advanced device configuration). Example:
`URL1=https://www.unicon-software.com`
`URL2=https://www.unicon-software.com/myeluxcom/`

For further information, see [Environment variables](#).

7.9. Local web sites

- from eLux RP 6 2110 -

On the devices, browser applications can be configured to run without a network connection. To do so, the required HTML pages and scripts are transferred to the devices and the Builtin browser is configured accordingly. This allows you to provide users with a web application that starts automatically and serves as an entry point.

- Define all allowed links from here as HTML links in your scripts.
- Configure all allowed actions via the browser properties.

Combined with kiosk mode, users are restricted to a specific start application and use it as a kind of landing page.

Providing local web sites

1. Pack all files needed for displaying the local web pages into a file named `landingPage.zip`.
 - Startup page `<start>.html`, example: `index.html`
 - Additional HTML pages and Javascript files (optional)
 - Stylesheet (optional)



Note

The file name for the archive is predefined and case-sensitive (`landingPage.zip`). The archive with this name is also required for a single HTML page.

2. Transfer the file to the devices to `/setup/browser/landingPage.zip`
To do so, use the **Files configured for transfer** feature. For further information, see [Files configured for transfer](#).



Note

Note case-sensitivity (`landingPage.zip`).

The next time the Builtin browser is launched on the devices, the archive will be unpacked to `/tmp/browser/landingPage/`

3. To make the web pages available in kiosk mode, enable and configure the kiosk mode. When doing so, set the browser startup page to
`file:///tmp/browser/landingPage/<start>.html`
For further information, see "Applications in kiosk mode" on page 232.
4. To make the web pages available without kiosk mode, define a browser application with the following properties:
 - Browser type: `Builtin`
 - Startup page: `file:///tmp/browser/landingPage/<start>.html`

Optionally, select **Start Automatically** and, under **Advanced**, specify navigation elements you want to display

At the next browser start (if configured: automatically after device restart) the startup page is displayed. From here, users can connect to the link destinations you have configured via the local web pages.

Even in kiosk mode, you are free to define multiple browser applications. Each browser application has its individual startup page, and one of the browser applications is defined as the default. Users can then switch between the applications using the selector on the system bar.

7.10. Troubleshooting application definition

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 to run them non-stop, respectively.
Problems with certificates in combination with VMware server	Server problem occurred: After successful installation, the VMware server uses a self-signed certificate. If a Thin Client is configured correctly, it will not accept. The reason is that the FQDN (fully qualified domain name) is mandatory for server certificates.	Create a server certificate in the Windows-CA with FQDN . If you use mmc : Create a server certificate using the Snap-In Certificates (Local computer) . The key must be exportable. The display name of the server must be vdm . The name must be unique in the certificate store Local computer / Personal .

Error / problem	Reason	Solution
COM port redirection in RDP session does not work	Communication errors such as high latencies in the network between your serial device and the virtual desktop do not allow serial communication.	<p>Use the permissive mode for the RDP application. This parameter causes communication errors to be downgraded to warnings, and communication becomes more tolerant of timeouts.</p> <p>Define a free parameter in your RDP application definition with the permissive option.</p> <p>Example:</p> <pre>FreeRDPParams=/serial:COM1,/dev/ttyS0,Serial,permissive</pre> <p>For further information, see Defining free application parameters.</p>

7.11. Third party software

To install additional applications on the devices, carry out the following steps:

1. From our portal www.myelux.com, for the relevant eLux version, download the specified software package.
2. In ELIAS, import the software package into your container. For further information, see [Importing packages into a container](#) in the **ELIAS** guide or [Importing software packages](#) in the **ELIAS 18** guide.
3. In ELIAS, add the package to your to your image (IDF), and then save the modified image file. For further information, see [Creating an IDF](#) in the **ELIAS** guide or [Creating an image](#) in the **ELIAS 18** guide.
4. For the relevant clients, perform a firmware update to the modified image. For further information, see [Firmware Update](#).

The software package is installed on the devices.

5. Configure the software in the back-end environment.

7.11.1. Avaya Equinox

Soft phone application providing access to Unified Communications (UC) and Over the Top (OTT) services

Package name: **Avaya Equinox VDI Client**

7.11.2. Cisco JVDI

Jabber Softphone for VDI (JVDI)¹ 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 JVDI software routes all audio and video streams directly from one Thin Client to another, or to a phone, without going through the HVD.

Package names: **Cisco JVDI Client** and **Utilities for Cisco JVDI Client**

- ▶ Follow the **Cisco Deployment and Installation Workflow** on the Cisco website in order to configure the JVDI system environment.

7.11.3. deviceTRUST

Dynamic context awareness, allowing users to access their corporate workspace from any location on any device while meeting IT governance requirements

Package name: **deviceTRUST Contextualizing IT**

¹formerly VXME

7.11.4. DriveLock

DriveLock provides endpoint security for USB interfaces on the Thin Client.

Package name: **DriveLock**

7.11.5. Grundig Citrix Extensions

Digital dictation solution by Grundig Business Systems

Package name: **Grundig Citrix Extensions**

7.11.6. HDX RealTime Media Engine

The HDX RealTime Media Engine (RTME) enables better audio and video quality for VOIP and video chat.

Package name: **Citrix HDX RTME**

- ▶ Configure Microsoft Lync or Skype for Business in the back-end environment.

7.11.7. JabraXpress Device Updater

Solution installed on an end user's thin client that governs Jabra device configurations such as firmware versions and device settings

A detailed description of how to use the Jabra Xpress Device Updater can be found in the documentation of Jabra Xpress for Linux: <https://jabraxpress.jabra.com/Downloadables/Linux/UserGuide.pdf>

Package name: **JabraXpress Device Updater**

7.11.8. Microsoft Teams

Enterprise video conferencing with real-time messaging and content sharing

Package name: **Microsoft Teams Client**

Microsoft Teams Client for Linux is a local application on eLux.

Parameter for the application definition: `teams`

7.11.9. Nutanix Frame

Cloud- hosted Desktop as a Service (DaaS) that empowers any organization to deliver and manage their desktops via a single console for seamless control and administration, providing a true hybrid experience.

Package name: **Nutanix Frame Client**

Nutanix Frame Client for Linux is a local application on eLux.

Parameter for the application definition: `Frame`

Parameter with URL: `Frame -url=console.nutanix.com`

7.11.10. Olympus Dictation

Digital dictation solution by Olympus

Package name: **Olympus Dictation Drivers**

7.11.11. Philips Speech

Digital dictation solution from Philips Speech Processing Solutions

Package name: **Philips Speech Drivers**

7.11.12. SecMaker

- for eLux RP 6.5 and later versions -

SecMaker Net iD Enterprise is a middleware supporting SSL 3.0/TLS 1.0 (client identification), PKCS #7 (digital signatures), and PKCS #10 (certificate requests). To use SecMaker Net iD 6.x on the client, a separate license is required.

Package name: **SecMaker NetID**

- ▶ Use the Scout Enterprise feature **Files** to transfer the license file to the clients to `/setup/iid/netidlicense.lic`.

For further information, see [Files configured for transfer](#) in the **Scout Enterprise** guide.



Note

The license agreement (EULA) is available on the client client under `/etc/iid/SecMaker License and Support Conditions 20150202.pdf`

7.11.13. Zoom

Enterprise video conferencing with real-time messaging and content sharing

Package name: **Zoom Client for Linux**

Zoom Client for Linux is a local application on eLux that enables peer-to-peer connections between connected devices.

Package name: **Zoom Citrix Plugin**

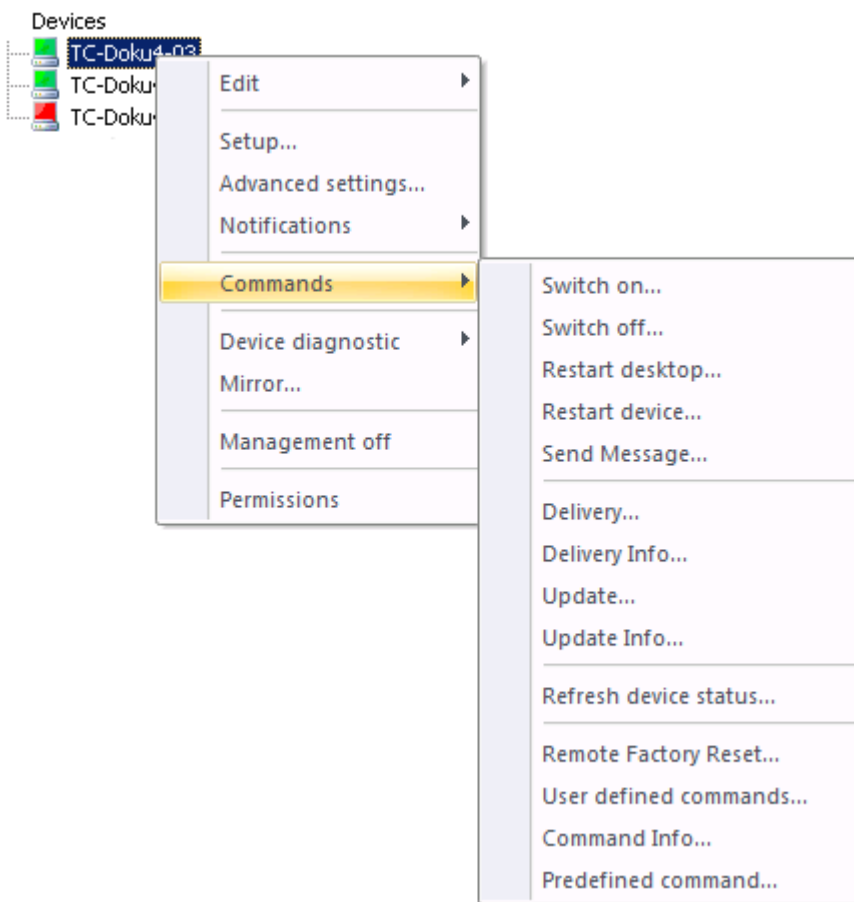
With the Zoom Citrix plugin, ZoomVDI can be used in a virtual desktop infrastructure with a Citrix solution. Peer-to-peer connections are not supported in this scenario.

8. Client remote management by commands

Administrators can use Scout commands to 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.



8.1. 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 desktop...	Restarts the eLux interface.
Restart device...	Restarts the device/devices

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
UEFI update...	Performs an update of the UEFI firmware For further information, see UEFI update in analogy to firmware update in the BIOS update guide.
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. For further information, see Factory reset command .
User-defined command...	Enter a user-defined command that will be sent to the device/devices Examples: Renew license lease, perform BIOS update



Note

After having executed a user-defined command, after a time span of 30 seconds, you can run the next user-defined command or update command.

Predefined command...	Provides user-defined commands that have been predefined globally. For further information, see Predefined commands .
Suspend eLux command scheduler	If recurring commands that are scheduled locally on the device by the eLux Command Scheduler (cron jobs) have been defined by the administrator, the execution of these commands is temporarily stopped until the next restart of the device.
Configuration run... (not available for individual devices)	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

8.2. Executing commands

1. For the relevant device, OU or Dynamic Client Group, on the context menu, click **Commands**.
2. On the sub-menu, choose a command.

The screenshot shows a dialog box titled "TC-MMI-S920" with a close button (X) in the top right corner. Inside the dialog, there is a "Command" dropdown menu set to "Restart device". Below this, there are two checkboxes: "Inform user for" (checked) and "User can cancel command" (unchecked). The "Inform user for" checkbox is followed by a text input field containing "60" and the unit "sec.". Below these options, there are three radio buttons for scheduling: "Now" (selected), "Once", and "Every". The "Once" option has a "Date" dropdown set to "Freitag ,06.09.2019" and a "Time" spinner set to "19:00". The "Every" option has a "Day of Month" spinner set to "1" and a "Time" spinner set to "12:51". At the bottom of the dialog are two buttons: "Execute" and "Cancel".

*The **Command** dialog opens. The options shown depend on the selected command.*

3. To show the complete title, move the mouse pointer over the title bar.

The title bar shows the affected device or OU.

- Edit the following fields:

Option	Description
Command	Allows to switch to other commands
Inform user	<p>The user is informed by a notification before the command is executed.</p> <p>Specify a time period in seconds for displaying the notification. The command will be executed after the time period has expired.</p> <p>If the time period is set to 0, the notification will be displayed until the user confirms the execution of the command via button.</p>
User can cancel	Users are allowed to prevent the execution of the command via button.
Run with system rights	Some commands require system rights which are checked before execution.
Now/Once/Every	Specify the time of execution or define a periodic scheduling.
On more devices wait	Delay after execution if more than one device is concerned
Include sub-OUs	Include subordinate OUs, if available

- Confirm with **Execute** or **Schedule**.

The command is executed at the specified time. Depending on the command, you are asked to confirm.

8.3. Scheduling commands

The execution of most commands can be scheduled for a specified time instead of being executed immediately. Many commands such as firmware updates can also be scheduled on a recurring monthly or weekly basis.

- For the relevant device, OU or Dynamic Client Group, from the context menu, choose **Commands**.
- From the sub-menu, choose a command.
- To schedule a command to be executed once, select **Once**. Then select the date and time.
- To schedule repeated execution, select **Every**. Then select the day of the month or week and the time.
- Edit the other options of the **Command** dialog.
- Confirm with **Execute**.

*The command is executed at the defined time. All scheduled commands (once and repeating) can be displayed, modified and deleted under **View > Schedule...***

8.4. Command results and update information

Feedback on performed update, delivery and user-defined commands is available both for

- individual devices in their **Properties** window
- all devices 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. For further information on the command history, see [Command history](#).


Viewing command results on a particular device



Note

The following instructions are related to **Update** commands. Viewing results of a UEFI update, delivery or user-defined command is done accordingly.

1. To show the **Properties** window, click **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	Origin of software packages (web server or proxy)
Update size	Size of the transferred packages in compressed format



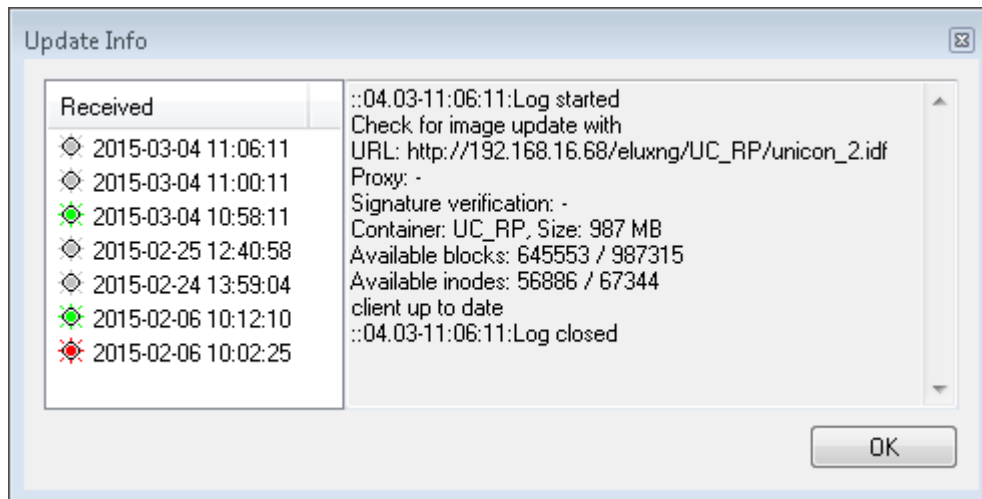
Note

The properties **Update provider** and **Update size** are evaluated for updates, but not for the migration to a major version or a downgrade.

3. Double-click the term **Update status** or click ... at the end of the line.

*The **Update Info** window is displayed. On the left, you can see all updates that have been processed, aborted or not processed because the image had been up-to-date. For a selected update command, you can view all logged data on the right side, among them the installed software pack-*

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](#).

8.5. 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 object rights 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
Start	Date and time of sending command to the devices / starting time

Option	Description
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 <code>Successful</code> or <code>Failed</code> 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. <i>A first click sorts the jobs ascending and the second one sorts descending. To reproduce the default sorting order click F5.</i>

Apply the following options to a selected job:

Option	Action
View details	Click Details.... <i>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.</i>
Search object in Scout Enterprise tree view	Right-click an object name, and then click Find in tree view . <i>The first result is selected in the tree view.</i>
Terminate running job	Select the running job, and then click Terminate . <i>A command terminating request is sent to the Scout Server and the transmission of the command to the devices is stopped.</i>

8.6. Factory reset command

Use the **Remote factory reset** command to reset the relevant devices to their initial state. By default, the local device configuration and local application definitions are deleted.

The following data are retained by default:

- Connection data to the Scout Server including server address and OU ID
- License information
- The installed image with all software packages (firmware)

After the device has received the **Remote factory reset** command, the current configuration of the client is reset and the device is restarted. The device connects to the Scout Server and obtains the configuration of the OU to which it is assigned.

The command can be run with the following additional options:

Option	Description
Retain local configuration (unlocked fields) ¹	<p>User-defined values of the local device configuration in unlocked fields are retained. This only applies to fields that the user is allowed to edit.</p> <p>- only available if allowed in Advanced options > Devices -</p> <p>For further information, see Supporting local configuration.</p>
Delete Scout Server address on the client	<p>In addition to the configuration, the following data are deleted:</p> <ul style="list-style-type: none"> ■ Address of the Scout Server machine ■ Certificates in <code>/setup/cacerts</code> ■ WLAN configuration ■ 802.1X configuration ■ Private key of SCEP client certificate stored in TPM 2.0 module² ■ An encrypted setup partition (TPM 2.0) is decrypted.³
Delete license information stored on device ⁴	<p>The license lease is deleted in addition to the configuration and the data listed above. This option can be used for the resale of devices, for example.</p> <p>Subsequently, the device is shut down and remains switched off.</p> <p>If this option is used to run the Remote factory reset command, the function corresponds to resetting the client locally by using the Factory reset button of the extended eLux Command panel. For further information, see Resetting thin client to factory status in the eLux RP guide.</p>

¹from Scout Enterprise 15.7 and eLux RP 6.7

²from eLux RP 6.7

³from eLux RP 6.7

⁴for Scout Enterprise Management Suite 14.9 / eLux RP 5 and earlier versions

**Note**

The **Remote factory reset** affects the setup partition of the thin client. The system partition with the installed firmware is not affected by the factory reset and is only changed using the **Update** command with the option **Format system partition before update**.

8.7. Creating predefined commands

User-defined commands can be pre-defined and provided globally to administrators via **Commands > Predefined Command...** For example, you can pre-define scripts for the BIOS update of particular hardware or a script to renew the license lease of eLux RP 6 clients.

These commands are then available via the **Command** dialog and can be used by authorized administrators. To create a predefined command:

1. On the Scout Enterprise menu, click **Options > Advanced options > Predefined commands**.
2. Click **Add**.

3. For your new entry, edit the following options:

Option	Description
Name	The command name is shown to administrators in the Commands dialog. The command is not shown.
Command	<p>Syntax for the command to be executed</p> <p>To enable administrators to set individual values when executing a pre-defined command, you can use variables.¹ The values for each variable are prompted when the administrator selects the predefined command in the Command dialog.</p> <p>Example: <code>ls -%PARAM% %FILES%</code></p> <p>Correct spelling of variables: Free variable name surrounded by percent signs <code>%variable%</code>²</p> <p>The variable name may contain upper and lower case letters, numbers and special characters.</p> <p>To use a percent sign in the command definition outside the variable name, type <code>% %</code></p>
System	System rights are required to execute the command.
Activated	The command is displayed in the list-field for predefined commands.
Admins ³	<p>A predefined command is shared with all administrators by default.</p> <p>▶ To restrict to specific administrators or groups,⁴ click the cell under Admins and then select the desired administrators/groups from the list.</p> <p>Note that in the default case (no restrictions) the list of administrators displayed does not contain a selection. The command is nevertheless enabled for all administrators.</p>

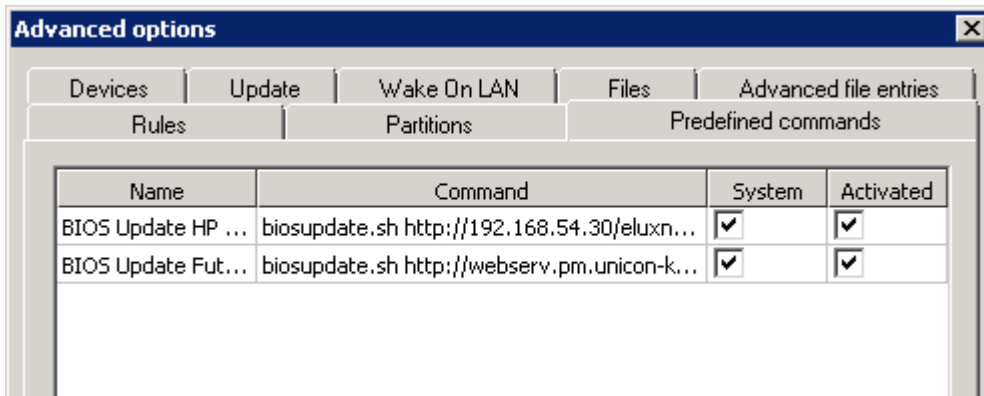
4. Confirm with **Apply** and **OK**.

¹from Scout Enterprise Management Suite 15.9

²for Scout Enterprise Management Suite 15.9: `__variable__` (two underscores each)

³from Scout Enterprise Management Suite 15 2101

⁴with active administrator policies



You can find all activated predefined commands under **Commands > Predefined command...** in the relevant list-field. They can be applied on individual devices, on OUs and on Dynamic Client Groups.

For authorized administrators, the name of the command is displayed instead of the command itself.

- in the **Command** dialog
- in the device properties window under **Command line**¹
- in the **Command Info** window (command history for relevant device)²

8.8. Defining templates for standard commands

For standard commands such as **Restart** or **Update**, you can define preferences via templates.³

1. On the Scout Enterprise menu, click **Options > Advanced options > Predefined commands**.
2. Under **Command templates**, select **Use template for command** and then, in the list-field, select the relevant command.
3. To define the preferences as mandatory, select **Template is mandatory**.
If a template is not mandatory, the operative administrators can overwrite the specified default values.
4. Specify the values for the selected command.

A template may contain command-specific preferences as well as general preferences such as

Inform user for x seconds

User can cancel command

¹from Scout Enterprise Management Suite 15.7

²from Scout Enterprise Management Suite 15.7

³from Scout Enterprise Management Suite 15.2



Note

Templates for standard commands are only available in the Scout Console but not in the Scout Dashboard.

8.9. eLux Command Scheduler

- from eLux RP 6.8 and Scout Enterprise 15 2103 -

Recurring commands can be defined so that they are scheduled and executed locally on the device by the eLux Command Scheduler. Like cron jobs, these commands are initiated by the device at defined points in time, whereas Scout Enterprise commands are initiated on the server side. The time of execution depends on the time zone in which the device is located.

The eLux Command Scheduler can process the following commands:

- Update firmware
- Synchronize device configuration
- Restart device
- Shut down device
- User-defined command

The commands for the eLux Command Scheduler may be defined either on the top level in the **Advanced options** or in the **Advanced device configuration** of an OU. For each OU, you can define whether you want the jobs of the eLux Command Scheduler defined and scheduled above to be applied or not.

8.9.1. Defining eLux Commands

- from Scout Enterprise 15 2103 -

The eLux Command Scheduler is configured in the Scout Console.

Define eLux command

Command

Update

1

Schedule

Weekly

20:00:00

Sunday

2

User interaction

☒ Inform user for

30

seconds

3

Reminder...

☐ User can cancel command

Command execution

Spread factor

0

seconds

4

☒ Persistent

5

☒ Wake device from sleep

6

OK

Cancel

1 Select command

2 Configure periodic scheduling

3 Configure user interaction and deferment options

4 Generate random delays between devices

5 Missed jobs are caught up

6 Devices are woken up from suspend to execute jobs

1. Open **Options > Advanced options** or the **Advanced device configuration** of an OU. Then choose the **eLux Command Scheduler** tab.
2. To define a new command, click **Add**.
3. In the **Define eLux Command** dialog, edit the following fields:

Option	Description
Command	Type of command To execute user-defined commands , system rights are required. Therefore, include the password.
Schedule	Periodic scheduling of the command If the provided options are still too few, in the <code>schedule.ini</code> , you can define a string using the systemd syntax. For further information, see "Command definition parameters" on page 269.

Option	Description
User inter-action	Determine whether and how long you want to inform the users before the command is executed, and whether they are allowed to defer it. For further information, see "Deferment options for users" below.
Spread factor	<p>Time span in which random delays are generated to prevent simultaneous execution on many devices</p> <p>Example 600 seconds: If the execution time is 6:00 pm, a randomly generated time value for the execution of the command per device, which may be a maximum of 600 seconds, is added to the time 6:00 pm. The command is therefore executed between 6:00 and 6:10 for all devices.</p> <p>Default: 0</p>
Persistent	Missed command executions (jobs) are immediately caught up after the next device start. If multiple repetitions of the same command were scheduled, the command is repeated once.
Wake device from sleep	Devices will be woken up from sleep mode (suspend) to execute scheduled commands.

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

*The scheduled command is displayed in the **eLux Command Scheduler** tab of the **Advanced Options** and in the **eLux Command Scheduler** tab of the **Advanced Device Configuration** for all OUs. Creating and editing is only allowed in the **Advanced Options**.*

5. Define which OUs you want (not) to inherit the jobs of the eLux Command Scheduler. By default, the settings (jobs) in **Advanced Device Configuration > eLux Command Scheduler** are inherited from the next higher instance.

The scheduled command is executed by all devices whose OU inherits the jobs of the eLux Command Scheduler at the next due point in time.



Note

To view information on the status and the next execution of a command, on the device, use `systemctl status <jobId>.service` and `systemctl status <jobId>.timer`.

8.9.2. Deferment options for users

Similar to Scout Enterprise commands you can also define for the command definitions of the eLux Command Scheduler whether the users are informed before the command is executed and whether they are allowed to cancel or defer it.

Option	Description
Inform user	<p>The user is informed by a notification before the command is executed.</p> <p>Specify the time period in seconds for displaying the notification. The command is subsequently executed.</p> <p>If the value is 0, the notification will be displayed until the user confirms the execution of the command via button.</p>
User can cancel	The user is allowed to prevent the execution of the command via button.
Reminder > Number of allowed deferrals	Define how often the user is allowed to postpone.
Reminder > Delays until next reminder	Select one or more time periods users can choose to defer.

For further information, see also "User information before update" on page 289

8.9.3. Suspending eLux Command Scheduler

The recurring execution of defined commands by the eLux Command Scheduler can be temporarily suspended from the Scout Console. To do so, the administrator sends a command to the relevant devices, which stops the eLux Command Scheduler until the next restart of the devices. After the next device restart, the eLux Command Scheduler continues to process the scheduled commands as planned.

1. For the relevant device, OU or Dynamic Client Group, on the context menu, click **Commands > Suspend eLux Command Scheduler**.
2. Confirm with **Execute**.

The execution of all commands scheduled by the eLux Command Scheduler is suspended with immediate effect until the next restart of the devices.



Note

If commands are defined with `Persistent=true` and the device is switched off at the time of scheduled command execution, these commands (persistent jobs) are started subsequently after the next restart.

8.9.4. Command definition parameters

For each command definition, in the `scheduler.ini` file, a new `[Job<N>]` section is created. Find all command definition parameters with their possible values below.

Parameter	Description																		
Id	Character string for unique identification of the command																		
Type	<p>Command type</p> <table> <tr><td>1</td><td>Update</td></tr> <tr><td>2</td><td>Synchronize configuration</td></tr> <tr><td>3</td><td>Restart device</td></tr> <tr><td>4¹</td><td>User-defined</td></tr> <tr><td>5²</td><td>Shut down</td></tr> </table>	1	Update	2	Synchronize configuration	3	Restart device	4 ¹	User-defined	5 ²	Shut down								
1	Update																		
2	Synchronize configuration																		
3	Restart device																		
4 ¹	User-defined																		
5 ²	Shut down																		
Schedule	<p>The format follows the systemd calendar events. Syntax for a timestamp: Tue 2020-01-21 11:12:13</p> <table> <tr><td>Minutely</td><td>*-*-* *:*:00</td></tr> <tr><td>Hourly</td><td>*-*-* *:00:00</td></tr> <tr><td>Daily</td><td>*-*-* 00:00:00</td></tr> <tr><td>Monthly</td><td>*-*-01 00:00:00</td></tr> <tr><td>Weekly</td><td>Mon *-*-* 00:00:00</td></tr> </table> <p>Examples:</p> <table> <tr><td>*-*-* 4:00:00</td><td>Every day at 4:00 am</td></tr> <tr><td>Mon..Fri *-*-* 22:30</td><td>Every workday at 10:30 pm</td></tr> <tr><td>*-1,5 11:12</td><td>Every first and fifth day of any month at 11:12. am</td></tr> <tr><td>Sun 2020-*-* 17:15</td><td>Every Sunday of the year 2020 at 5:15 pm</td></tr> </table> <p>For further information, see https://www.freedesktop.org/software/systemd/man/systemd.time.html</p>	Minutely	*-*-* *:*:00	Hourly	*-*-* *:00:00	Daily	*-*-* 00:00:00	Monthly	*-*-01 00:00:00	Weekly	Mon *-*-* 00:00:00	*-*-* 4:00:00	Every day at 4:00 am	Mon..Fri *-*-* 22:30	Every workday at 10:30 pm	*-1,5 11:12	Every first and fifth day of any month at 11:12. am	Sun 2020-*-* 17:15	Every Sunday of the year 2020 at 5:15 pm
Minutely	*-*-* *:*:00																		
Hourly	*-*-* *:00:00																		
Daily	*-*-* 00:00:00																		
Monthly	*-*-01 00:00:00																		
Weekly	Mon *-*-* 00:00:00																		
--* 4:00:00	Every day at 4:00 am																		
Mon..Fri *-*-* 22:30	Every workday at 10:30 pm																		
*-1,5 11:12	Every first and fifth day of any month at 11:12. am																		
Sun 2020-*-* 17:15	Every Sunday of the year 2020 at 5:15 pm																		
SpreadFactor	<p>Time span in which random delays are generated to prevent simultaneous execution on many devices</p> <p>Default: 0</p>																		
Persistent	<p>true false</p> <p>If true, missed command executions (jobs) are immediately recovered after the next device start.</p>																		
Command	Only for Type=4: Command for user-defined command																		
WakeSystem	<p>true false</p> <p>If true, the system will be woken up from sleep mode (suspend) to execute scheduled commands.</p>																		

¹from Scout Enterprise 15 2103

²from eLux RP 6.9.1000

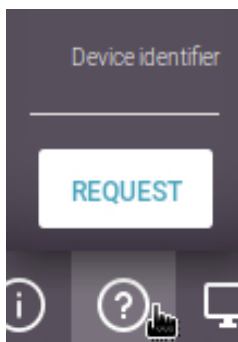
9. Remote maintenance

For maintenance, user help-desk and troubleshooting purposes, the administrator can use different tools to access the client devices.

9.1. Device identifier for support

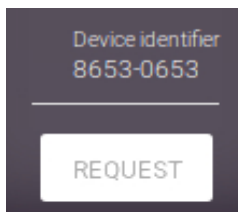
- from Scout Enterprise 15 2101 and eLux RP 6 2101-

To provide support for users, the first step is to identify the relevant device. As an alternative to the IP address or MAC address in the **Information** dialog, eLux provides a temporary device identifier that users can easily request.



The users have a question mark icon on the system bar if the user right **Request simple device identifier** is enabled, which is by default.

- ▶ To request the so-called **Simple device identifier**, users click ¹ the question mark icon and then **Request**.



The system generates and transmits a temporary device identifier for the requesting device.

The user gives this device identifier to the support staff or administrator. By default, the device identifier has a validity of five minutes.

The validity time and optional additional text to be displayed can be specified by the administrator in the Scout Console under **Options > Advanced options > Rules**.

9.2. 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. On the mirrored device, control of the mouse and keyboard can be given to the mirroring administrator. This can be very helpful in a variety of scenarios such as when administrators assist users or when administrators need to check correct functioning of firmware updates or newly installed software.

¹or right-click

9.2.1. Requirements

- VNC viewer
On the administrator's system, a VNC viewer must be installed. This is provided by the Scout Console
- VNC server
On the target device, a VNC server must be installed. For eLux clients, the **VNC Server extension** feature package which is part of the **XOrg** eLux package needs to be installed. This may require modifications of the image definition file on the web server via ELIAS.
- Configuration
For the target device, in **Device configuration**¹ > **Security** > **Mirror settings**, mirroring must be enabled and configured. For further information, see [Configuring Mirroring](#).

9.2.2. Mirroring from Scout Console

Throughout a mirror session, the user receives a system message which is displayed on both the client screen and the administrator's screen. The system message remains in the foreground 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 device, both monitors are mirrored. To obtain the best result, on the Scout Console machine, connect two monitors with the same or a higher resolution.



Note

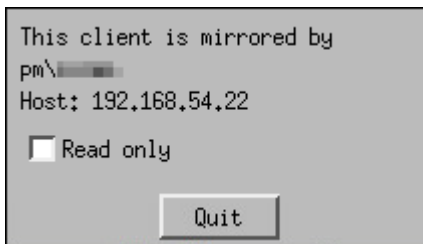
During the mirror session, the keyboard layout of the Scout Console machine is used and not the one of the client.

1. For the relevant device, on the context menu, click **Mirror...**
2. On the **Mirroring** dialog, confirm with **OK**.
3. Depending on your configuration in **Device configuration** > **Security**, the session can only be started after
 - the administrator enters the defined password
 - the user confirms the mirror session

For further information, see [Configuring Mirroring](#).

The mirror session is started. On the client screen, a system message is displayed that can be moved but not closed unless the mirror session is closed.

¹formerly Setup



The user has the following options:

Option	Description
Read only	The administrator has only read-access on the mirrored device. Mouse and keyboard input are not transmitted into the mirror session.
Quit	The connection is disconnected and mirroring is stopped.
Quit and logoff (only if configured)	The connection is disconnected and the user is logged off. This option is only available if, in Device configuration > Security , the option Logoff after disconnect is selected.

The mirror session is closed when

- the administrator closes the session window or clicks the **Quit** button of the system message, or
- the user clicks the **Quit** button of the system message.

If configured in **Device configuration > Security**, the mirror session is logged in a `*mirror.txt` file and saved to a sub-directory of the Scout Server files directory.¹

9.2.3. Troubleshooting mirroring

Error / problem	Reason	Solution
From a Scout Server with multiple network adapters, establishing a mirror session fails	The mirror session is not set up via the correct network adapter.	In the Registry, set the key <code>BindIPAddress</code> to the IP address of the network adapter the client is connected to: <code>HKEY_CURRENT_USER\Software\Unicon\Scout\Settings\BindIPAddress</code>

¹for Scout Enterprise 15.4 and later versions with the device's MAC address

9.3. Device diagnostics



Note

This feature can only be applied to an individual device.

Device diagnostics help you run predefined commands on the client and retrieve protocol and configuration files from the client. These are then sent to Scout Enterprise or other destinations for diagnostic purposes. The requested client files support the administrator in error analysis and are required when opening a support ticket.

Depending on the user rights, the reverse way can be used: Users send diagnostic files or screenshots from the client.

Administrators are free to use the **Request diagnostic files** feature to request freely definable files from a device.



Note

To compare actual and target device configuration settings of individual devices, use a report. For further information, see [Evaluating configuration data](#).

9.3.1. Logging on the devices

Two log levels are provided in the device configuration of the eLux devices: **Standard** and **Enhanced**. These levels correspond to the debug levels **On** and **Off** in the Scout Console.

In normal operation, the standard level is adequate. Before performing device diagnostics, however, temporarily enable the enhanced log level on the device to make sure you retrieve all data needed. After the device diagnostics, we recommend that you reset the log level in order not to unnecessarily strain the flash memory capacity of the device.

Enabling enhanced logging

1. Open the device's context menu and click **Device configuration....**
2. On the **General** tab, clear the option **Use parent device configuration**.
3. On the **Diagnostics** tab, set the **Debug level** option to **On**.
4. Confirm and restart the device.

Enhanced logging for the device is active and you can pull off the diagnostic files.

Disabling enhanced logging

1. Open the device's context menu and click **Device configuration....**
2. On the **Diagnostics** tab, set the **Debug level** option to **Off**.
3. On the **General** tab, select the option **Use parent device configuration**.
4. Confirm with **Apply** and **OK**.

Enhanced logging for the device is reset to standard and device configuration inheritance is restored.

9.3.2. Requesting diagnostic files



Note

Before you perform device diagnostics, we recommend that you temporarily enable enhanced logging on the device. For further information, see "Logging on the devices" on the previous page.

1. From the device context menu, choose **Device diagnostics > Request files...**

*In the **Edit diagnostic files** dialog all templates defined so far are shown. Only active templates (check mark) are processed.*

2. If you have the required object right, you can select or clear further templates of the list.

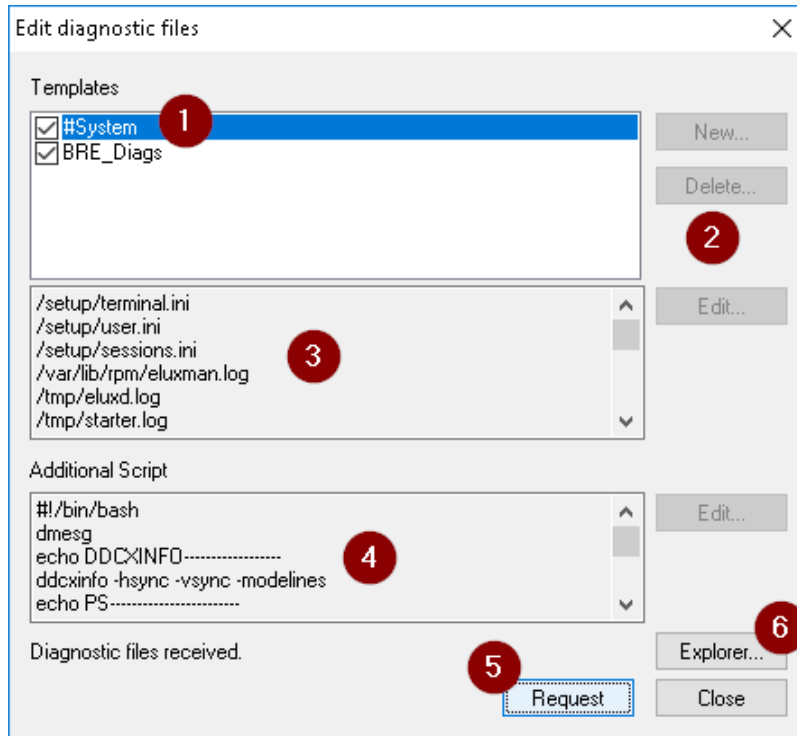
3. Click **Request**.

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 a .zip file in the **local user directory** <userprofile>\Documents\UniCon\Scout\Console\Diag.*

4. Click **Explorer**.

The Windows Explorer opens showing the diagnostics target directory.



Legend to numbers

- 1 Predefined template
#System

This template is always active and can neither be deleted nor edited.
- 2 Provided an administrator is given the object **Edit diagnostic templates**, he can create, edit and delete additional templates.
- 3 Log and configuration files defined by the selected template and requested by the device
- 4 Additional commands defined by the selected template to be executed on the device
- 5 The defined files are requested from the device and the defined commands are executed.
- 6 Once the requested files are available, open the Explorer with the diagnostics target directory.

9.3.3. 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 plus a script code to be run on the client. Neither of them can be edited. The `#System` template is used each time a device diagnosis is performed via **Request**.

In addition, authorized administrators can define further templates containing file lists and script. The templates are available globally, no matter where you define them.

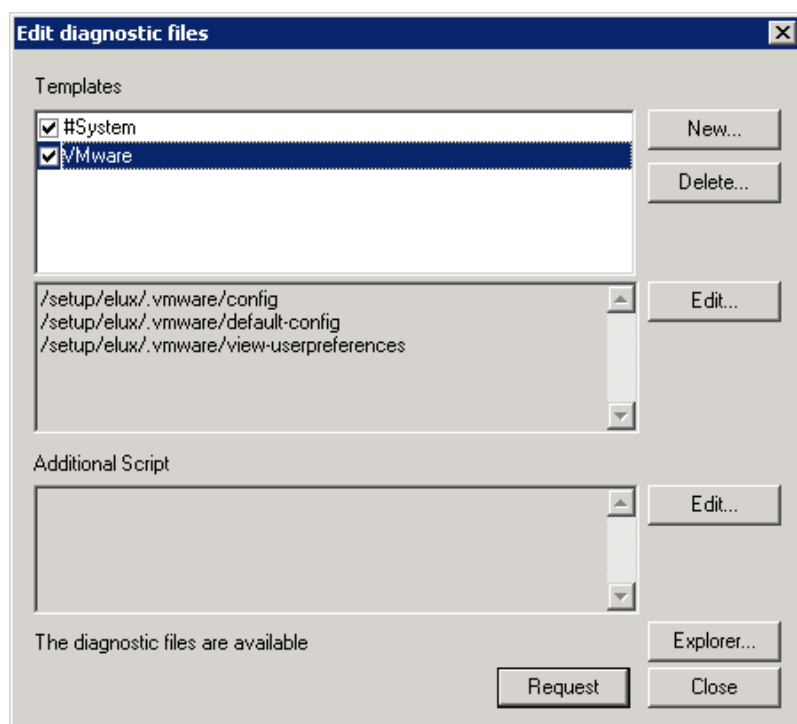
Defining a template for device diagnostics



Requires

Object right **Edit diagnostic templates** (disabled by default)¹

1. Open the context menu of a device and click **Device diagnostics > Request files**.
*In the **Edit diagnostic files** dialog, the predefined `#System` template and, if defined, further templates are shown.*
2. Click **New...** Enter a name for your new template and confirm with **OK**.
3. To define diagnostic files for your template, select the new template and, next to the file list, click **Edit**.
4. In the text box, enter the relevant file names with path line by line. Confirm with **Save**.



¹from Scout Enterprise 15.8

5. To enter script code you want to run on the device, next to **Additional script**, click **Edit...** Authenticate with the device password.¹
6. In the text box, enter your code and confirm with **Save**.



Note

When you perform the device diagnostics feature with **Request**, all active templates are included. However, whether all of the listed files of the #System template are written and transferred, depends on the selected debug level. For further information, see [Device configuration² > Diagnostics](#).

9.3.4. Further diagnostic adjustments

- from Scout Enterprise 15.11 and eLux RP 6.11 -

Diagnostic files over multiple device restarts



Requires

Enhanced logging must be enabled.

When you request diagnostic files, a set of log and configuration files is retrieved and packed on the target device. Included is the file `last_boot.zip`, which contains diagnostic files over a device restart. This `.zip` file contains all files defined for the system template plus some additional ones. The number of cycles for which the file is created and saved on shutdown of the client device is configurable. The default is five.

The most recent file is named `last_boot.zip.0`. The further back a file was created, the later its sequential number in the file name.



To define the number of cycles yourself, use the **Advanced file entries** feature with the following parameter:

File	/setup/terminal.ini	
Section	Global	
Entry	LogCycles	
Value	2-n	The default value is 5.

Note that the `last_boot.zip` file is only created, if enhanced logging is active. For further information, see "Requesting diagnostic files" on page 275.

Store diagnostic files persistently

By default, the diagnostic files are stored on the device under `/setup/logs`.

¹from Scout 15 2107

²formerly Setup

- ▶ To define a different storage location, use the **Advanced file entries** feature with the following parameter:

File	/setup/terminal.ini	
Section	Global	
Entry	LogPath	
Value	<Directory on the device>	The default is /setup/logs
	Example: /update/logs	A location on the update partition may also be defined.

If you use disk encryption via TPM 2.0, the setup partition will be encrypted. To have the diagnostic files accessible, define the update partition as their storage location. The update partition is then mounted automatically.

Diagnostic adjustments via software package

Provide diagnostic settings for new devices you wish to connect before their initial contact with the Scout Server, during installation. To do so, integrate the eLux software package **Diagnostic adjustments** into the image to be installed.

The **Diagnostic adjustments** package contains two feature packages that you can activate separately:

- **Enhanced logging:** Corresponds to the device configuration **Diagnosis > Debug level** and enables enhanced logging
- **Logs on update partition:** Sets the location for diagnostic files to /update/logs

Note that the diagnostic settings set via software package are only effective until the first contact of the device to its Scout Server. Then the device configuration is synchronized and the device receives the configuration data defined for its OU.

10. Firmware Update

On delivery, the Thin Clients are normally 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 flash drive. Whenever new software versions are available or demands change and software components need to be added or removed, the firmware can be updated.

Basic steps

- Download the relevant software packages from myelux.com
- Modify the image file (IDF) on the web server via ELIAS.
- Check firmware configuration of the relevant Thin Clients
- Perform the update
 - Software delivery
 - Installing new software packages

To perform the update in one step, use an **Update** command. In this case, the required software packages are delivered and then automatically installed. Alternatively, the two actions can be uncoupled: The software is delivered in a first step when you use a **Delivery** command. It is subsequently installed when you run the **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) via the **Update** command feature.
- The devices can be configured to automatically check for new image versions on start or shut-down. If an updated version is available, the update process is started.

The **Check for new version** option is part of **Device configuration > Firmware** and can be applied to individual devices, OUs and all devices.
- The definition of an **Update notification** results in updating the firmware on the next device restart

If configured, users can defer the execution of a firmware update to a later point in time.

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** window (multiple selection via CTRL and SHIFT allowed)
- OU
- Dynamic Client Groups

Recovery-Installation

To reset your devices to initial state, perform a recovery installation. A recovery might 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. With a recovery installation, all data on the storage medium are wiped (except license data) and the eLux software is installed. For further information, see [Recovery procedures](#) in the **Recovery** short guide.

10.1. Requirements

The following components are required to perform a firmware update:

- Web server (for example IIS) to provide the eLux software packages and image definition files (`.idf`) via HTTP/HTTPS or FTP/FTPS, with the relevant web server role enabled.
- Software container with eLux software packages on the web server
- ELIAS (eLux Image Administration Service) to create and modify image definition files in the software container
- Scout Console to configure firmware updates for the devices

Scout Server, Scout Console and ELIAS¹ are part of the Scout Enterprise Management Suite. The current software bundle `eLuxversion_AllPackages.zip` and further optional software packages are installed with the eLux container.

Alternatively, install ELIAS 18 and import the software bundle into your container. Then there is no need for the container installation.

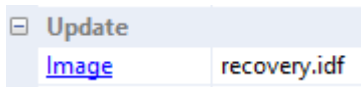
For further information on the installation of the Scout Enterprise Management Suite and the eLux container, see the [Installation](#) guide.

10.2. Access to applied images

Firmware images are created and modified in ELIAS. They are applied to the devices in the Scout Console, in the firmware configuration. To open an image used for specific devices directly in the relevant ELIAS container, you have two options in the Scout Console:

¹Choose user-defined installation and select it as a feature.

- In the **Properties** window of a device, double-click the **image** link.

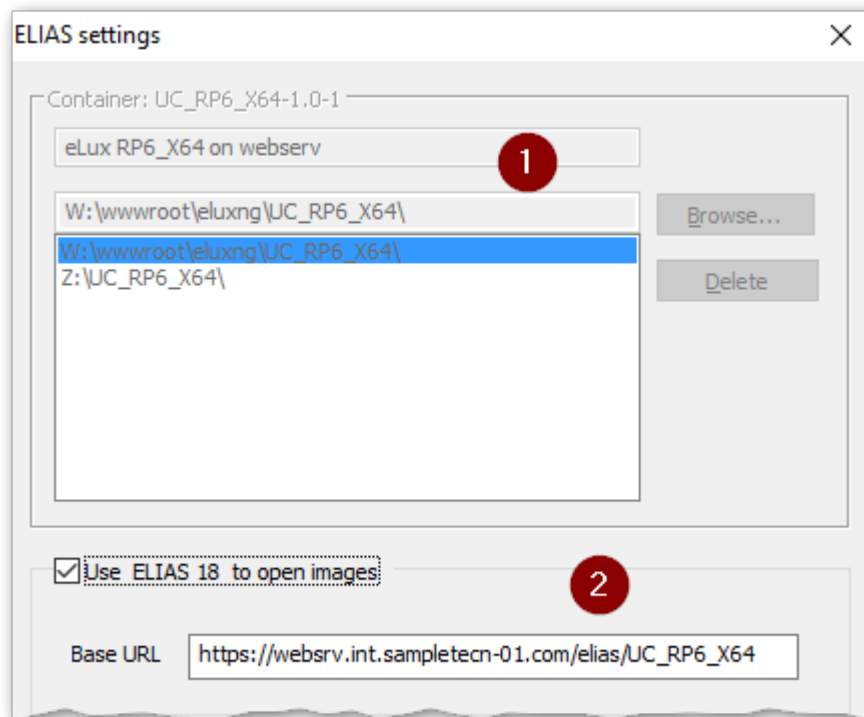


- In the device configuration of an OU or device, in the **Firmware** dialog, click the **ELIAS** button.

The connection to ELIAS is made with the data from the ELIAS settings. Here, you set either the legacy ELIAS or ELIAS 18¹ as the default application for editing images:

Specifying ELIAS settings

1. Select **Options > ELIAS settings**.



- | | |
|---|--------------|
| 1 | Legacy ELIAS |
| 2 | ELIAS 18 |

2. If you use the legacy ELIAS, in the top section, click **Browse**. From your web server, for the required container, select the `container.ini` file.

Optionally specify multiple containers.

3. If you use ELIAS 18, select the option in the bottom section.²

Enter your ELIAS 18 URL including the container path.

(ELIAS 18 is designed to manage multiple versions in one container.)

4. Confirm with **OK**.

¹from Scout 15 2110

²from Scout 15 2110

**Note**

The menu entry **View > ELIAS** offers another way to call ELIAS from the console.

10.3. Planning and performing firmware updates



Note

With the appropriate firmware configuration of the devices, you only need to provide an updated image to trigger a firmware update.

Providing new image

1. Download new software packages that are not included in your container from our portal and import them into your container in ELIAS. For further information, see [Importing packages into a container](#) in the **ELIAS** guide or [Importing software packages](#) in the **ELIAS 18** guide.
2. In ELIAS, add the relevant software packages to your image. Then save the modified image file. For further information, see [Creating an IDF](#) in the **ELIAS** guide or [Creating an image](#) in the **ELIAS 18** guide.

Checking firmware configuration of the devices

1. For the relevant devices, open the **Device configuration > Firmware**¹.
To apply the update to all devices, choose **Options > Base device configuration**.
2. Check whether the following fields are configured correctly for a firmware update: **Protocol**, **Server**, **Path** and **Image file**.

The URL shown below the **Path** box is generated based on this data. The URL is relevant for the transfer of the image file (.idf and eLux software packages).

The specified image file name must be identical to the name of the image file updated in ELIAS.
3. For firmware updates via command: To allow users to postpone the update, configure the reminder settings. User can then control the time of execution themselves. For further information, see [Update deferment by user](#).
4. To update the devices automatically on start or shutdown, select the relevant **Check for new version** option in the bottom area.



Note

Since in this case the update is initiated by the device, the firmware parameters stored locally on the device are used.

5. Confirm with **OK**.

For further information on the firmware update configuration, see [Device configuration > Firmware](#).

*As soon as an updated image file is available on the web server and if one of the **Check for new version** options is selected, the update is performed on the next device restart or shutdown.*

¹formerly Setup

**Note**

If the device is connected via VPN, the **Check for new version** options cannot be used. Use an **Update notification** instead.

Alternatively, you can initiate a firmware update via one of the following procedures:

- Perform an update command
- Schedule an update command for a specified time, once or periodically
- Define an update notification

10.3.1. Performing updates via command



Note

To deliver the software packages in a separate step before performing the update, use the **Delivery** command.

1. Select a device, an OU, a Dynamic Client Group or devices within the **All devices** window.
2. On the context menu, click **Commands > Update...**
3. To inform users before the update, select the **Inform user** option. Optionally, specify the display duration of the system message in seconds. With 0 seconds, the system message will be shown until the user clicks one of the buttons.

*This option triggers a system message displayed to users immediately before the update process. Depending on the configuration (**Firmware > Reminder settings**), users can defer a requested firmware update.*

Optionally select the **User can cancel command** option.

For further information on the impact, see [User information before update](#).

4. To format the system partition of the device's flash memory before writing, select the option **Format system partition before update**.

IT_Rome

Command: Update

☒ Inform user for 20 sec.

☐ User can cancel command

☐ Format system partition before update

☒ Now

☐ Once
Date: Dienstag, 30.04.2019 Time: 11:32

☐ Every
Day of Month: 1, 2, 3, 4 Time: 11:32

On more devices wait for 0 ms after each command

☒ Include sub organisation units

Execute Cancel

5. Define the point in time for the update process. For further information, see [Executing commands](#).
6. Click **Execute**.

*The update process is triggered at the defined time. The update status is displayed for each device in its **Properties** window. During the update process, the status *Update in progress* is shown. Detailed information about the currently processed action with time stamp is shown additionally.¹ Example:*

Update in progress (Transfer started - 2018-08-20 11:34:23)

Update in progress (Transfer completed - 2018-08-20 11:35:45)

Update in progress (Installation started - 2018-08-20 11:35:48)

Update in progress (Installation completed - 2018-08-20 11:37:56)

For further information, see [Command results and update information](#).

Note that updates are only performed, if the relevant IDF has been modified. If an update fails, no efforts will be made to retry.



Note

When you execute an **Update** command, the relevant information is transferred to the clients as a URL. To create the URL, the system uses the values set in **Device configuration > Firmware** at the time when the command is run. Note that if the client initiates the update, the local **Firmware** configuration is relevant.

10.3.2. Performing updates via notification

By using update notifications, you can send an explicit one-time update request to selected devices to be evaluated with the next connection. The devices then are updated to the image 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 firmware update...**

*The **Firmware update notification** dialog is shown.*

3. Specify whether you want to inform users, and if they are allowed to cancel the command. For further information, see [Performing updates via command](#).
4. To format the system partition before performing the update, select the relevant option.
5. Confirm the notification and confirmation.


The notifications for firmware updates are defined for the relevant devices.

*For each device, in the **Properties** window, the **Update notification** field shows the value *Activated*.*

¹for Scout Enterprise 15.3 and later versions



Note

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

For the relevant devices, a firmware update notification is set. As soon as a device restarts and reconnects to Scout Enterprise, it receives an update request¹ 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 [User information before update](#).*

The update status is displayed for each device in its **Properties** window. For further information, see [Update log](#). If an update fails, no system-side efforts will be made to retry.

For devices without update partition², 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 Report Generator, you can filter devices by the field **Image update notification**.

Deleting the update notification for one or more devices

An update notification can be deleted before the firmware has been updated:

- ▶ On the context menu, click **Notifications > Delete update notification**.



Note

Notifications are always set or deleted for all selected devices regardless of whether they are only available for individual devices.

10.3.3. Updates initiated by system

The client can be configured to automatically check on start-up or shutdown whether a firmware update is available and install it.

Procedure for system-side initiated firmware update

- Depending on the configuration, the client checks on each system start or shutdown whether a firmware update is necessary.

An update is necessary, if the image definition file on the web server specified by the firmware configuration has changed compared to the local version. The client determines the delta

¹Note that updates are only performed if the relevant IDF has been modified.

²flash memory less than 4 GB

between the software packages defined by the image definition file on the web server and the installed software packages. If a delta exists, a firmware update is necessary.

- If a firmware update is necessary, the client downloads all software packages defined in the image that are not yet on its update partition from the web server or proxy server.
- Subsequently, the installation starts.



Note

Since the update is initiated by the client, in this case, the firmware parameters locally stored on the device are used.

Exception for VPN connections

If **Check for new version / On Start** is configured and the VPN connection can only be set up after the eLux desktop is loaded, the firmware will not be updated regardless of whether an update is necessary.¹ The user can continue working without interruption.

Configuring firmware updates initiated by the system

- ▶ For the relevant clients, in the device configuration, under **Firmware**, select **Check for new version**. Then select whether the check is to be done on the system start or shutdown.

For further information, see [Device configuration/Firmware](#).

After the clients have received the new device configuration, the option to check for new firmware versions becomes active.

10.4. User information before update



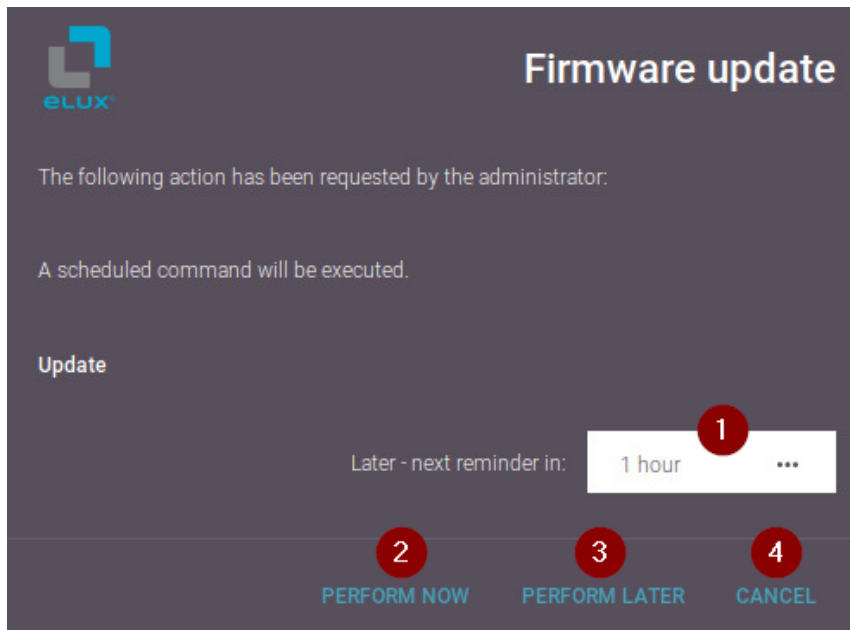
Note

This feature refers to firmware updates and UEFI updates.²

Any **Update** command run with the **Inform user** option selected, provokes a system message on the device which includes the defined user options. If configured in **Firmware > Reminder settings**, users are provided with buttons they can use to defer or abort the request.

¹for eLux RP 6.7 and later versions

²from eLux RP 6 2107



While the message is displayed, users may close applications, disconnect sessions, or - if configured - defer the update. If the display duration for the message has been set to 0, the message will be displayed until the user clicks a button.

Users have the following options:

1 Select a time interval until the next reminder for the firmware update

The list-field contains the values specified in **Firmware > Reminder > Delays until next reminder**.

Displayed only, if the **Number of allowed deferments** is set to 1 or higher, and if at least one more deferment is possible.

2 Perform firmware update immediately

3 Postpone firmware update by the time period selected (1)

If the device is shut down before the time interval expires, the update is performed during shut-down.

Displayed only, if the **Number of allowed deferments** is set to 1 or higher, and if at least one more deferment is possible.

4 Abort update process definitively

Displayed only, if the command option **User can cancel the command** is selected.

There will be no automatic restart of the update process.

10.5. 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 as successful on all relevant devices, start the installation by using an **Update** command or notification.



Requires

- Clients are provided with an update partition, see [eLux partitions](#)
- Firmware device configuration of the relevant clients must be configured correctly, see [Planning an update](#)

The software delivery can be triggered by a Scout Enterprise command or a notification¹.

During delivery, a live information icon  is shown on the system bar.

The subsequent installation of the software packages and the update to the new IDF is initiated with an update command or an update notification.



Note

If you initiate the subsequent firmware update via an **Update** command with **Format system partition**, the system might have to download additional packages. This is because a **Delivery** command only triggers the download of packages that are not installed on the system partition and are not available on the update partition.

10.5.1. Performing deliveries via command

1. Select a device, an OU, a Dynamic Client Group or devices in the **All devices** window.
2. From the context menu, choose **Commands > Delivery...**
3. In the **Command** dialog, specify whether and how long you want to inform the user.
4. To allow users to deny the delivery, select **User can cancel command**.
On the device, a pop-up dialog is displayed that allows users to cancel or start the delivery.
5. To first clean the update partition of the devices, select the **Clean update partition before delivery** option.



Note

After cleanup, all files of the current software image must be re-transferred and the dynamic proxy cache rebuilt.

6. Specify a time for the delivery.

¹from Scout Enterprise 15.10

For further information, see [Scheduling and executing commands](#).

7. Click **Execute**.

The delivery is triggered at the defined time. If there is an updated IDF, and if the required software packages do not exist on the update partition of the relevant devices, the delivery of the software packages is started. The system will only download the packages that are missing. If there is less than 30 MB storage space available on the update partition, old packages are deleted before new packages are transferred.

- ▶ To check which files have actually been transferred, view the diagnostic file
`/var/lib/rpm/eluxman.log`

In the Scout Console, for each device, the delivery status is shown in the **Properties** window. During the delivery process, the status `Delivery in progress` is shown, including detailed information about the currently processed action with time stamp.¹ Example:

Delivery in progress (Transfer started - 2018-08-20 11:34:23)

Delivery in progress (Transfer in progress - 2018-08-20 11:35:45)

Delivery in progress (Transfer completed - 2018-08-20 11:35:48)

For further information, see [Command results per device](#).

10.5.2. Performing deliveries via notification

- for Scout Enterprise 15.10 and later versions-

By using delivery notifications, you send an explicit one-time delivery request to selected devices. The request is evaluated with the next connection of the device to its Scout Server. Then, the delivery of all required software packages for the image configured in the Scout Enterprise firmware configuration is started for this device.

1. Select a device, an OU, a Dynamic Client Group or devices in the **All devices** window.
2. From the context menu, choose **Notifications > Initiate software delivery...**
*The **Software delivery 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 deliveries via command" on the previous page.
4. To clean the update partition before performing the delivery, select the relevant option.
5. Confirm the notification and confirmation.

The notifications for software deliveries are defined for the relevant devices.

¹for Scout Enterprise 15.3 and later versions

For each device, in the **Properties** window, the **Delivery notification** field shows the value *Activated*.

**Note**

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

For the relevant devices, a delivery notification is set. As soon as a device restarts and reconnects to its Scout Server, it receives a delivery request and the delivery notification is automatically deleted.

The delivery status of a device is shown in its **Properties** window. For further information, see [Command results and update information](#). If an update fails, no efforts will be made to retry.

**Note**

In the Scout Report Generator, you can filter devices by the field **Image delivery notification**.

Deleting the delivery notification for one or more devices

Delivery notifications can be deleted before the software is delivered:

- ▶ From the context menu, choose **Notifications > Delete delivery notification**.
-

**Note**

Notifications are always set or deleted for all selected devices, regardless of whether they are only available for individual devices.

10.6. 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 devices 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**.

The following instructions refer to Scout Enterprise Version 15.3 and later versions.

Up to eLux RP 6.8, the concept of a dedicated proxy client was also supported.

10.6.1. 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:

- Dynamic Proxy update
- Avahi
- Squid Update Proxy

The proxy client must have an update partition. For further information on update partitions, see [eLux partitions](#).

10.6.2. Frame conditions and roles

The dynamic proxy client concept is based on the following roles:

Provider



Requires

In the device configuration, under **Firmware > Proxy type**, the device must be configured to `Dynamic`.

The provider is the device that acts as the 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, under **Firmware > Proxy type**, select `None`.

Consumer



Requires

In the device configuration, under **Firmware > Proxy type**, the device must be configured to `Dynamic`.

All devices of a subnet that are not selected for the provider role are consumers. The consumers perform their update through the provider of the subnet. The consumers do not need to download software packages from the web server.

- ▶ To exclude devices from the consumer role, under **Firmware > Proxy type**, select `None`.



Note

In the **Firmware** configuration, if `HTTP` is used, the **User** and **Password** fields must remain empty.

10.6.3. Update procedure

Update check

In the case of an update request coming either from the Scout Server or from the local **Firmware** configuration (**Update on start / 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

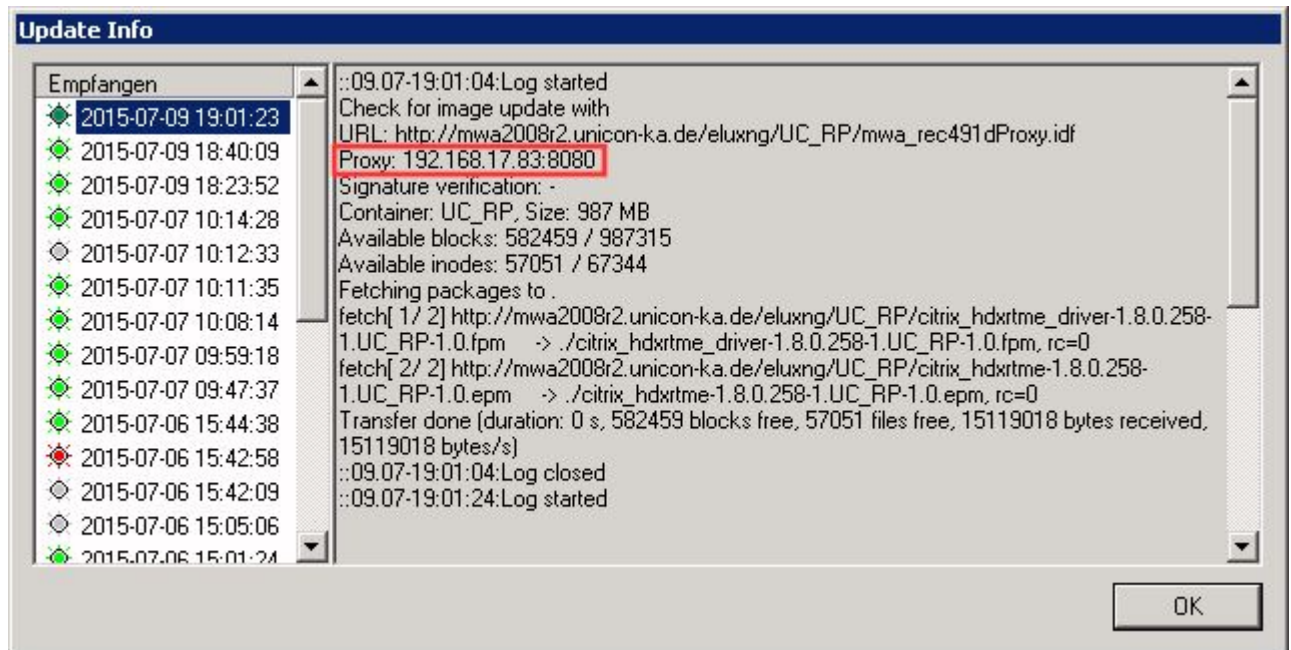
The provider checks the availability of the requested software packages on its update partition and downloads missing packages from the web server specified by the consumers.

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 can be viewed by double-clicking **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.

10.7. Troubleshooting firmware update

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	Incorrect device password	Correct the entry in Device configuration¹ > 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 Recovery procedures in the eLux Recovery procedures short guide.

Update options


If the update is still faulty, try to modify the update settings. For further information, see [Advanced setup > Update options](#).

¹formerly Setup

11. Passwords

eLux users and administrators may be required to enter passwords in various situations, for example

- AD logon for user authentication after eLux system start
- Application logon
- Device password to unlock the device configuration
On the Scout Enterprise side, the device password applies to all devices of an infrastructure and is used for additional functions.
- Accessing a password-protected OU
- Defining a mirror password
- Setting up network profiles
- Further features of the device configuration
Example: Defining a network drive

▶ To view and verify a password after typing, next to the **Password** entry field, click ¹.

▶ To reset a password entry, click .

11.1. Local device password

The device password affects the local devices. All thin clients managed by a particular Scout Server receive the same device password so that it is used to verify the access rights for the devices. The device password is requested by Scout Enterprise for management tasks such as discovery.

The device password can only be changed centrally for all devices in the Scout Console. The initial password is set to `elux`.



Note

We recommend changing the password immediately to avoid unauthorized configuration caused by local users.

Usually, the access rights do not allow users to modify their local device configuration in the **Security** dialog. However, if the user or administrator changes the device password locally for a device, this device can no longer be managed by Scout Enterprise.

For further information, see [Device password](#) in the eLux guide.

¹for eLux RP 6.7 and later versions

11.1.1. Changing local device password via Scout Console

Important Using this function you change the device password of **all** devices managed by this Scout Server

1. In the Scout Console, click **Options > Base device configuration... > Security**. Under **Local security**, click **User rights**.
2. In the **User rights** dialog, in the **Device password** field, type the new password and repeat it in the **Conform device password** field.
3. Confirm with **OK**.

The new device password is assigned to the devices on the next restart.




Note

To immediately activate the new password, perform a Scout Enterprise **Restart** command for the relevant devices (now or scheduled). For further information, see [Scheduling and executing commands](#).

11.1.2. Changing local device password on the device

1. In the eLux Configuration panel, click **Security > Device password**.
2. Under **Current password**, type the old password. and in the next two fields type the new password.

To view your entry after typing, click ¹.

3. Confirm with **Apply**.

Important The device can no longer be managed by Scout Enterprise.

¹for eLux RP 6.7 and later versions

11.2. Scout 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 lower-case).



Note

We strongly recommend that you change the password immediately in order 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 enabling the [Administrator policies](#) and using your AD accounts for Scout Enterprise.

12. Managing administrators

12.1. 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 Console, click **Security > Activate administrator policies**.
2. Confirm with **OK**.

*You are logged off and, from now on, you can only log on by using your Windows AD account. The **Security** menu options then 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.*

12.2. Adding administrators

You can define any AD users and groups as Scout Enterprise administrators.

1. In the Scout Console, click **Security > Manage administrators...**
2. In the **Administrator rights** 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 Administrator rights** dialog opens.*

4. Below of the **Group or usernames** field, click **Add...**

*The **Windows Select Users or Groups** dialog opens.*

5. Enter the relevant AD username 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 rights 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 AD groups only, and if a user is a member of more than one group, the access rights of the groups are not consolidated, but the rights of the first group 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.

12.3. Deleting administrators

1. In the Scout Console, click **Security > Managing administrators**.
2. In the **Administrator rights** 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.

12.4. Administrator policy

For all Scout Enterprise administrators there are three different kinds of access rights:

Base rights	Main access rights organized in functional blocks
Menu rights	Access rights for specific menu commands
Object rights	Access rights on OU or device level for properties, device configuration, applications and some other functions
Default object rights	Default access rights for all OUs or devices for which no different object rights have been defined

Note that in the dialog you must always first select the relevant administrator for whom you want to edit the access rights. To edit object rights, first select the relevant OU or device.

In the **Administrator rights** dialogs, the provided rights are displayed with a green or red symbol:

Access granted

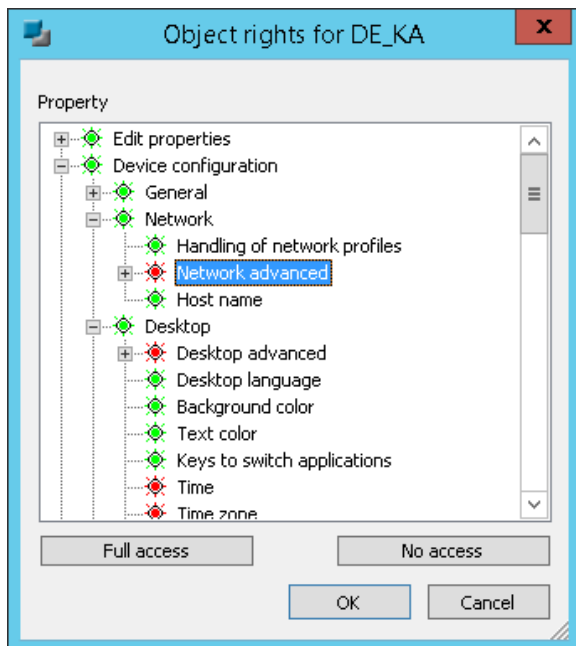


Access denied



To toggle between **Access granted** and **Access denied**, double-click the relevant right or press the space key.

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 access rights, the following applies: If a right is disabled, the relevant administrator has no longer access to the related function. For the last or the only administrator existing, you cannot disable the access rights. This is to prevent being locked out of the Scout Console

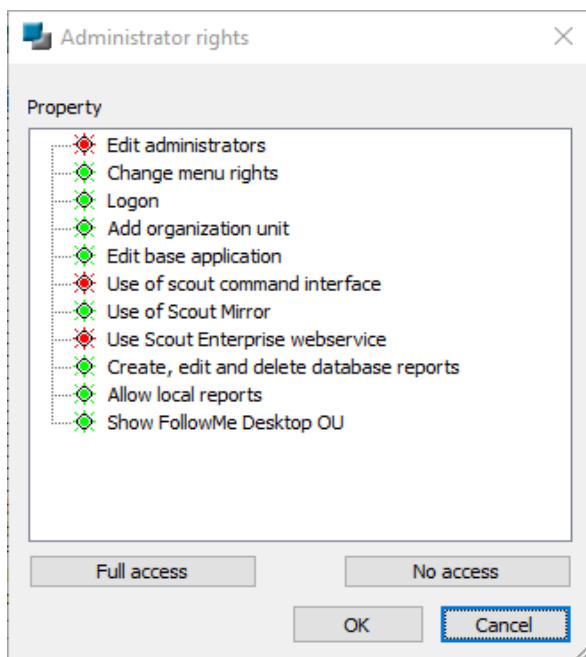
12.4.1. Changing base rights

Administrator base rights refer to entire functional blocks such as using the Scout Report Generator or configuring FollowMe Desktop.

1. In the Scout Console, click **Security > Managing administrators**.
2. In the **Administrator rights** dialog, select the relevant administrator.
3. Click **Base rights....**

*The **Administrator rights > Base rights** dialog opens.*

4. Change the relevant rights by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.



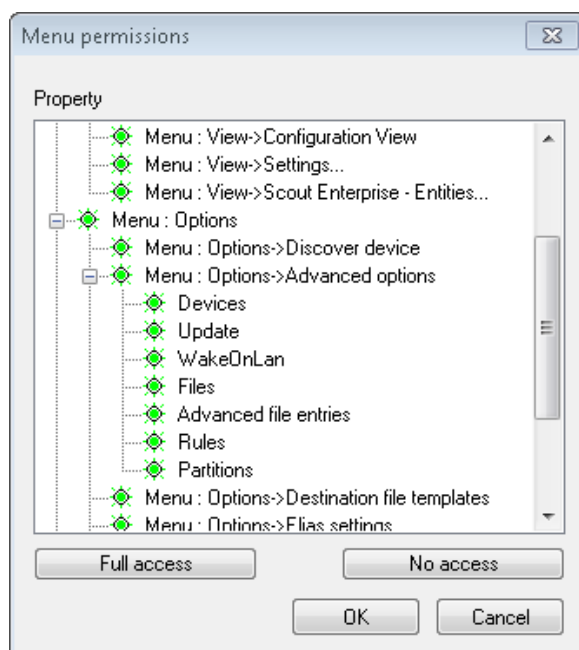
12.4.2. Changing menu rights

Menu rights refer to the executability of menu functions. If you deny an administrator access to a menu option, the menu item is dimmed and the administrator cannot perform the function.

1. In the Scout Console, click **Security > Menu rights....**
2. In the **Menu rights** dialog, select the relevant administrator.
3. Click **Menu rights....**

*The **Menu rights** dialog opens.*

4. Change the relevant rights by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.



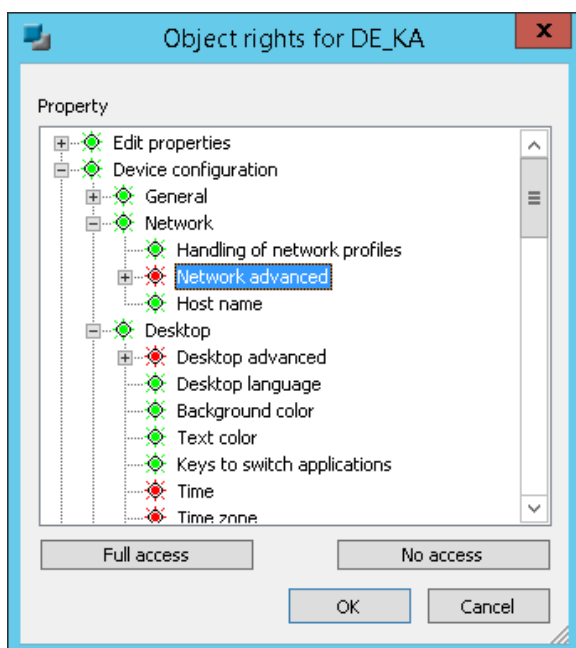
12.4.3. Changing object rights

Object rights refer to an OU or a device. You can define object rights for selected OUs or devices that differ from the general default object rights.

1. In the tree view, select an OU or device.
1. Click **Security > Object rights...** or, on the context-menu, click **Object rights...**
2. In the **Object rights** dialog, select the relevant administrator.
3. Click **Edit object rights....**

*The **Object rights for <OU>** dialog opens.*

4. Change the relevant rights by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.



Resetting object rights to default

You can reset object rights that you have defined differently for an OU or a device:

1. In the **Object rights** dialog of the OU or device, select the relevant administrator.
2. Click **Delete object rights**.

12.4.4. Changing default object rights

Default object rights apply to all levels to all OUs or devices for which no specific object rights are defined.

1. In the Scout Console, click **Security > Managing administrators**.
2. In the **Administrator rights** dialog, select the relevant administrator.

3. Click **Default object rights....**

*The **Default object rights** dialog opens.*

4. Change the relevant rights by double-clicking or by pressing the SPACE bar.
5. Confirm with **OK**.

12.4.5. Defining a Start OU

This feature lets you determine that an administrator is allowed to see only a particular start OU including its subordinate OUs.

1. In the Scout Console, click **Security > Manage administrators**.
2. In the **Administrator rights** dialog, select the relevant administrator.
3. Click **Set root OU ...**

*The **Root organization unit** dialog opens.*

4. Check the **Use the following root organization unit** option.
5. Select the relevant root OU.
6. Confirm with **OK**.

12.5. Viewing administrator activities

The activities of all administrators are logged according to the defined monitoring level in **Security > Manage administrators**.

You can view the logs in the Scout Console and you can export them.

1. In the Scout Console, select **Security > Manage administrators**.
2. Under **Monitoring**, click **View protocol**.

*The **Activities** dialog opens and shows the activities of all administrators.*

3. To export log entries into a text file, select the relevant entries and click **Export selected items**.

Monitoring levels

The monitoring levels 0-3 build on each other. Level 0 only logs changes to the monitoring level itself.¹ Logging with monitoring level 3 is the most detailed.



Note

Use monitoring level 3 only temporarily for diagnostic purposes, since all database transactions are additionally logged.

¹from Scout Enterprise Management Suite 15 2101

Activities / level 1	Activities / level 2 ¹	Activities / level 3 ²
Log on	Save / Delete / Rename application	All SQL statements executed due to administrator activities in the console
Log off	Upload application	
Deny logon	Save ³ / Delete / Rename device	
Add / Activate / Delete license	Save ⁴ / Delete / Rename OU	
Add administrator	Save device configuration	
Edit / Delete administrator rights	Save advanced device configuration	
Change administrator policies	Save advanced options	
Request mirroring of a device	Discover devices	
	Schedule/perform Scout Enterprise-command ⁵	
	Set / Delete relocation notification	
	Set / Delete update notification	
	Set / Delete delivery notification	
	Set / Delete UEFI update notification	
	Service Provider Mode: Assign tenant - device / Remove assignment	

12.6. 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.

³also applies to Move device

⁴also applies to Move OU

⁵specifying command type and target device/OU

12.7. Maintenance windows

- for Scout Enterprise 15.7 and later versions -

A maintenance window is a time period that is scheduled for maintenance work. In the Scout Console, authorized administrators can define maintenance windows to keep this period free for necessary IT maintenance tasks such as installing server updates. While a maintenance window is active, non-authorized administrators cannot use the Scout Console and cannot start jobs.

Defining a maintenance window



Requires

Menu right: **Menu: View > System diagnostics > Maintenance windows**

1. In the Scout Console, click the menu entry **View > System diagnostics > Maintenance windows...**
2. Click **Add**.
3. In the **Edit Maintenance window** dialog, specify the following options for your new maintenance window:

Option	Description
Name	With descriptive names, you can distinguish multiple maintenance windows.
From	Date and time when the maintenance period will be started for the first time
for	Time period of the maintenance window Specify number and unit (hours or minutes) Example: 2 hours
Repeat	Repeats the maintenance window periodically, see example below

4. Confirm with **OK**.

The maintenance window is defined and shown in the list of maintenance windows.

*For the duration of a defined maintenance window, the console will be blocked for administrators who do not have the **Maintenance window** menu right. The affected administrators can then only close the console, other actions are disabled. After the maintenance window has expired, they can restart the console as usual.*



Note

By default, the **Maintenance window** menu right is active and maintenance windows have no effect. If you disable the menu right for certain administrators, they will not be able to work with the console during the defined maintenance windows. Administrators with active **Maintenance windows** menu right are not subject to any restrictions.

Example of a periodic maintenance window

For a maintenance window, for example defined from Friday, 06.09.2019, 20:00 for 2 hours, you can set the following repeat options:

Every day	Daily, starting on Friday, 06.09.2019
Every week	Every Friday of a week
Every month	Every 6th of a month
Every first weekday in month	Every Friday of the first week of the month
Every second weekday in month	Every Friday of the second week of the month
Every third weekday in month	Every Friday of the third week of the month
Every fourth weekday in month	Every Friday of the fourth week of the month
Every last weekday in month	Every Friday of the last week of the month

13. Scout Statistics Service

The Scout Statistics Service provides the following features:

- Evaluation of configurable status messages (keep alive messages) from the clients

Within a defined time interval the configured clients send status messages to the Scout Statistics Service. These status messages allow to refresh the status of the relevant clients in the Scout Console.

- Processing of dynamic asset details for statistical analysis

In the Scout 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 Dashboard. The statistical data are stored in a separate SQL database.

The 'keep alive' messages and the dynamic asset data are transferred from the devices to the Scout Statistics Service by using the HTTPS protocol. This requires a valid SSL certificate. For further information, see [Certificate for Scout Enterprise Statistics Service](#).



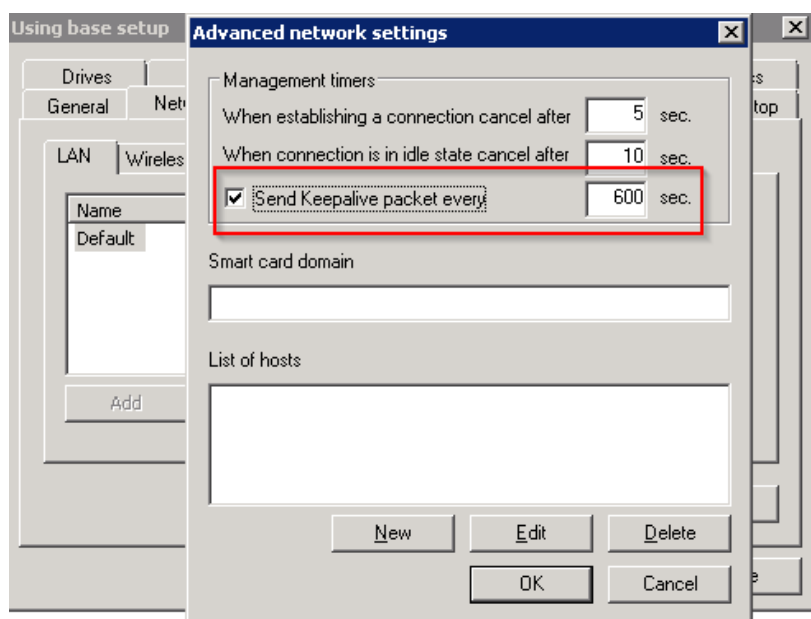
Note

The Scout Statistics Service is part of the Scout Enterprise Management Suite installation. For further information, see [Installing Scout Enterprise Management Suite](#) in the **Installation** guide.

13.1. Defining status messages (keep alive messages)

The Scout Statistics Service helps you configure automatic updating of the status messages (keep alive messages).

1. In the Scout Console, select **Options > Base device configuration > Network > Advanced** or open, for the relevant device or OU, the **Device 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:



License	eLux (Scout builtin) (W63AYRZE6K54F)
Last Contact	Fri Mar 28 11:59:27 2014
Status	Switched on

*If, however, a status message within the defined interval is missing, the device status in the Scout Console is set to *Switched off*:*



License	eLux (Scout builtin) (W63AYRZE6K54F)
Last Contact	Fri Mar 28 11:59:27 2014
Status	Switched off

13.2. 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 Statistics Service.



The client is without network connection or is switched off. Status messages cannot be forwarded to the Scout Statistics Service.



The client is reconnected to the network. Status messages are forwarded to the Scout Statistics Service.

For further information on client icons, see [Scout Enterprise interface/Icons](#).

13.3. Dynamic asset details for statistical analysis

Use the **Advanced file entries** feature of the Scout Console to configure how to transfer asset data for statistical analysis.

File	/setup/terminal.ini
Section	Statistics
Entry	Supervise
Value	usb pci

For further information, see [Advanced file entries](#).

If you specify `usb` and/or `pci` as value, the asset data of the relevant OU are sent to the Scout Statistics Service via HTTPS and they are saved to the Statistics database. This feature requires the Scout Statistics Service being installed within the Scout Enterprise installation routine stating a certificate for server authentication.

Analysis and display of the statistical data is done in the Scout Dashboard. The Scout Dashboard is installed with the Scout Enterprise Management Suite specifying the relevant databases (Scout Enterprise, Statistics and Dashboard).

For further information, see [Installing Scout Enterprise Mangement Suite](#).

14. Console communication

14.1. Closing the console

1. In the Scout 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.

14.2. 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.

14.3. 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-insensitive. By clicking the button **X** the search field is closed.

14.4. 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**.

14.5. Managing reports for Scout Dashboard

Reports that have been saved to the database are globally available and can be used by all authorized Scout Enterprise administrators (base right: **Report Generator**) in the Scout Report Generator. Additionally, all reports stored in the database can be used in Scout Dashboard.

The availability of reports in Scout Dashboard can be restricted by means of the report management in the Scout Console: Here, you can assign reports to AD users or AD groups, or vice versa.



Requires

- Activated administrator policies (**Security > Activate administrator policies**).
- Menu right 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 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 Dashboard.

Important If the option **Use report assignment for Dashboard** is not selected, all reports saved to the database are available for all administrators.

15. Import/Export

All import and export functions can be performed via the Scout Console or the SCMD interface.

Exported files are saved in an XML format. The file name extension depends on the data category.

Data category for export/import	Filename extension
Device configuration of OUs	.oustp
Device configuration of devices	.devstp
Properties of OUs	.oupro
Properties of devices	.devpro
Properties of applications	.apppro
Device list	.csv
OU tree	.outree

15.1. 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**.

15.2. 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**.

16. Log files and optimizing

16.1. Log files

Scout Enterprise provides three logging options which are saved as `.log` files on the Scout Server.

Option	Log file	Description
Scout Con- sole	<code>scout.log</code>	<p>Required for debugging</p> <p>Path:</p> <pre>%USERPROFILE%\Documents\UniCon\Scout\Console</pre> <p>In the Scout Console, click View > System diagnostics > Console log.</p>
Scout Enterprise- Server	<code>eluxd.log</code>	<p>Log file of the Scout Enterprise service, required for support calls</p> <p>Default path:</p> <pre>%PUBLIC%\Documents\UniCon\Scout\Server</pre> <p>Previous versions are renamed in <code>elux.log.1...elux.log.3</code> etc.</p> <p>In the Scout Console, click View > System diagnostic > Server log (only if the Scout Con- sole is installed on the same machine as the Scout Server).</p>
Server keep alive log	<code>keepAlive.log</code>	<p>Log file for keep alive-entries of the Scout Server created every 10 minutes</p> <p>Default path:</p> <pre>%PUBLIC%\Documents\UniCon\Scout\Server</pre>

For the Scout Statistics Service, the following log file is provided:

Scout Stat- istics Ser- vice	UniconStatisticService	Rotating log file with configurable path ¹
	e.log	Default path:
		<code>%USERPROFILE%</code>
		<code>\Documents\UniCon\Scout\StatisticService²</code>
		The location and the maximum size from which a new file is written can be configured in
		<code>%PROGRAMFILES%</code>
		<code>\Unicon\Scout\Statistic\statisticsservice.exe.config</code>

For further information about file paths, see [Program and file directories](#).

U Note Click **View > System diagnostic > Server files** to open the Unicon server files directory in the Windows File 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.

The following additional logs are available via the Scout Console and can be exported:

Option	Description
License log	All actions related to licenses such as entering, deleting and exporting licenses View > System diagnostics > License log
Administrator activity log	All administrator activities depending on the defined monitoring level Security > Manage administrators > View protocol For further information, see Viewing administrator activities .

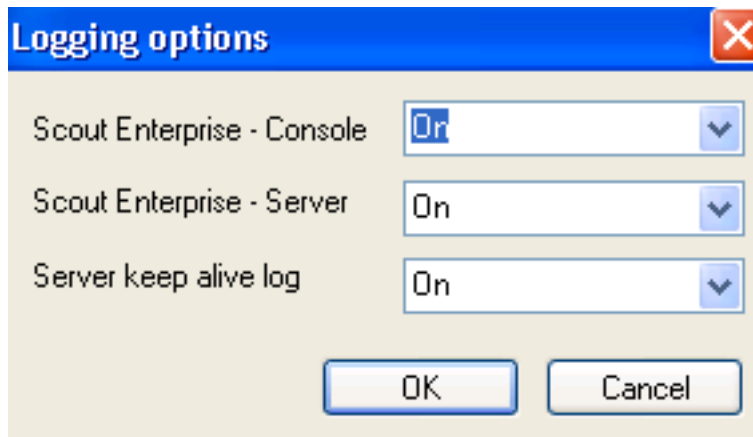
¹from 15.2101

²up to Scout Enterprise 15.10:

`%USERPROFILE%\AppData\Local\Temp\UniconStatisticService.log`

16.1.1. Enabling logging

1. In the Scout 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.

16.1.2. Configuring Scout Server log

For the Scout Server log file `eluxd.log` the Scout Server creates more than one backup (Log rotation). 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.

The log files continue recording when the server is restarted. The creation of a new log file is triggered by the following parameters:

- log file size
- maximum number of log files

You are free to configure both thresholds by yourself.

In addition, you may modify the location of the server log file and the keep alive log file (by default in `%PUBLIC%\Documents\UniCon\Scout\Server`). Specify any local directory for them, but no network directory.

Modifying log rotation and location

1. In the file system, in `%PUBLIC%\Documents\UniCon\Scout\Server`, open the `eluxd.ini` file for editing.
2. To modify the rotation parameters, add the following entries:

Section	Entry	Default	Description
[ELUXD]	MaxLogFileSizeMB	100	Maximum size of a log file in MB
[ELUXD]	MaxLogFiles	10	Maximum number of log files (eluxd.log plus backups)

3. To modify the log file location, add the following entry:

Section	Entry	Example	Description
[ELUXD]	LogFileLocation	c:\log	Local directory to be used for the log files <code>eluxd.log</code> and <code>keepAlive.log</code>

Important Specify a local directory to which the Scout Server can write. Do not use the UNC (Uniform Naming Convention) format.

After the Scout service has restarted, the log files are written to the specified directory.

If the Scout Enterprise service cannot access the directory, it cannot start and creates an entry in the Windows Event Viewer. If the Scout service is running but cannot write the log file, it creates an alert message in the Scout Console.

16.1.3. Cleaning up mirror log files

- from Scout Enterprise 15 2101 -

If configured for mirroring, Scout Enterprise creates a log file for each mirroring session and stores it in the `mirror` directory under the Scout Server files. For further information, see "Configuring mirroring" on page 118.

You can have these log files deleted automatically via a command.

1. In the Scout Console, click **View > System diagnostics > Mirror log cleanup**.
*The **Command** dialog opens with the command **Mirror log cleanup**.*
2. To select the period relative to the current date, under **Delete log files older than**, enter the number of days before which you want to delete log files.
3. Specify the point in time of the execution. To define periodic scheduling of the cleanup process, select **Every**. Then, specify a day of the month or a weekday and then the time.
4. Confirm with **Schedule**.

*Periodic scheduling of the command ensures that mirror log files have only a limited lifetime. Example: If you define **90 days** and **Friday**, the log files will remain available for a maximum of one week longer than 90 days.*



Note

Other log data such as administrator activities, executed commands, or alarms in the Scout Console can be deleted via database cleanup. For further information, see "Database

cleanup" on page 326.

16.2. 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
For further information, see the **Installation** short guide.
- Configuring the [number of ODBC connections](#) if you use a SQL database
For further information, see the **Installation** short guide.

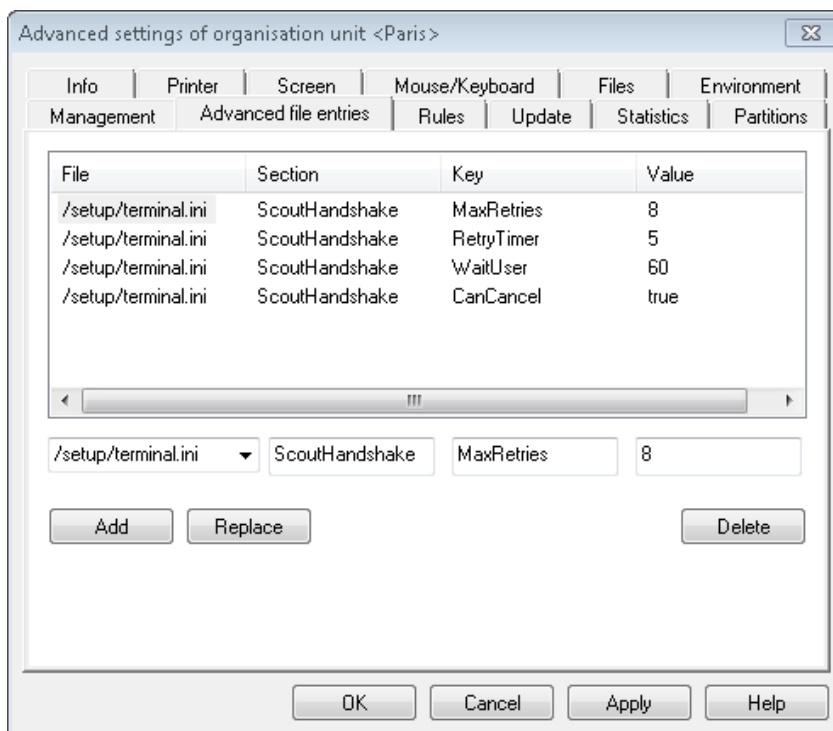
16.2.1. Optimizing with handshake

During each start-up the Thin Clients contact their Scout Server and check for new configuration data and application definition data. If they can't access the Scout 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.

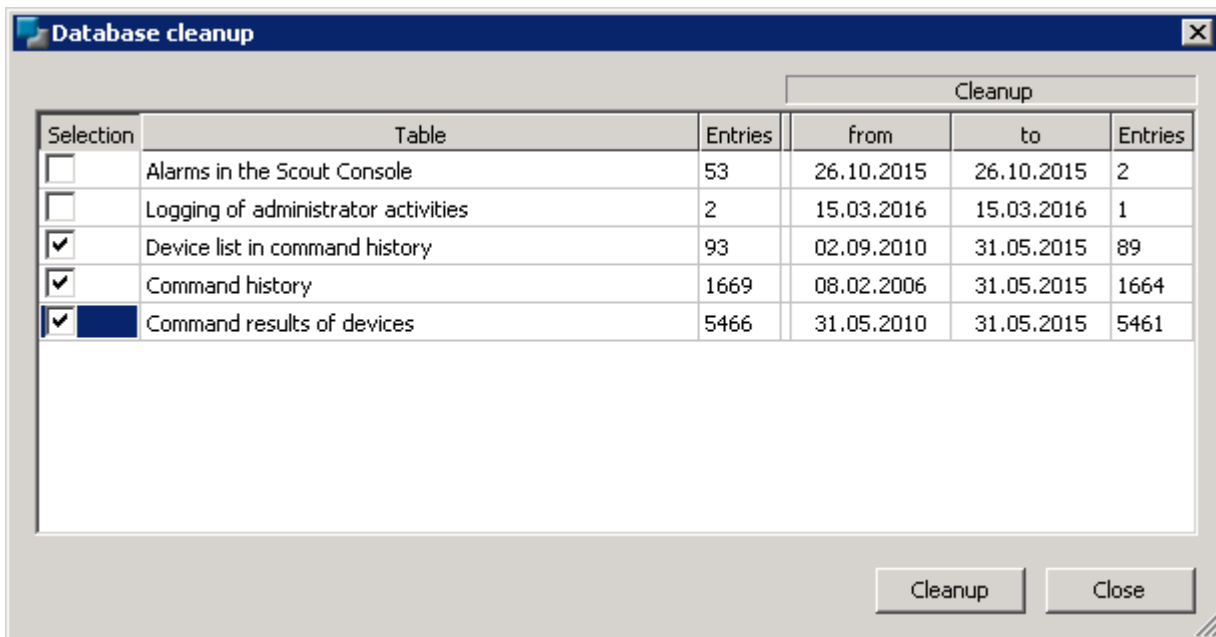
The section `ScoutHandshake` provides the following configurable parameters:

Parameter	Description
<code>MaxRetries</code>	Number of connection attempts The value 0 deactivates handshake.
<code>RetryTimer</code>	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.
<code>PermanentRetriesAfterDays</code>	Number of days (maximum) from the last successful connection until next connection attempt Ensures that after n days latest the configuration data of device and Scout Server is compared Can be combined with MaxRetries and RetryTimer
<code>WaitUser</code>	Waiting time before client restarts to give the user the chance to close applications or log off.
<code>CanCancel</code>	Defines, if the user is allowed to suppress a client restart (<code>true</code> <code>false</code>).

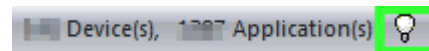
16.2.2. Database cleanup

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.

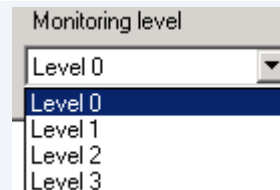
The relevant tables are listed in the **Database cleanup** dialog, each table providing the total number of entries and the creation date of the first entry. The administrator can modify only the fields **Selection** and **to**.



Alerts in the Scout Console
Alert messages (Error, Warning, Info), can be viewed by double-clicking the lamp icon on the Scout Enterprise status bar



Logging of administrator activities
Log file entries about the activities performed by an administrator according to the defined monitor level in **Security > Manage administrators...**
For further information, see [Viewing administrator activities](#).



Device list in command history
History data of commands shown in **View > Command history...** of the Scout Console (entries for particular devices)

Command history
History data of commands shown in **View > Command history...** of the Scout Console (entries for OUs)

Command results of devices
Results of commands performed on the devices (Update, Delivery, user-defined command). The log data can be viewed in the Scout 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 of a time span for the deletion of the entries (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 on the left to activate this table for cleanup.

A check mark indicates that entries from this table are selected 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.

17. Appendix

17.1. Program and file directories

Program directory

Scout Enterprise Management Suite by default is installed to

```
%PROGRAMFILES%\Unicon\Scout
```

Scout Dashboard is installed on the web server (IIS) by default to

```
<root directory>\Scout\Dashboard
```

The directory name `Dashboard` is the application name shown in the URL and can be modified during installation.

The eLux container is installed on the web server to

```
<root directory>\eluxng
```

File path for Scout 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 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 are saved to a subdirectory of the local user directory in

```
%USERPROFILE%\Documents\Unicon
```

Diagnostic files that are requested via the console are saved to

```
%USERPROFILE%\Documents\Unicon\Scout\Console\Diag
```

Diagnostic files that are requested via Scout Dashboard are saved on the web server to

```
<root directory>\Scout\Dashboard\Content\Diagnostic
```



Note

If you use anti-virus software on your Scout Server, we recommend that you exclude the specified directories from the virus scan to avoid side effects.

17.2. eLux partitions

A thin client's flash memory is generally divided into three or four partitions when eLux is installed. Each partition is reserved for a dedicated purpose and is only touched when you perform special tasks that

are related to this partition.

All partitions are created during a recovery installation.

Partition	Requires	Purpose	Recreated with	Other
System		Reserved for the firmware (software packages)	Scout Enterprise Update command with option Format system partition before update	Size for eLux RP 6 2104 LTSR CU1 and earlier versions: 1,77 GB / 1,84 GB with/without encryption Size for eLux RP 6 2107 and later versions: 2,35 GB / 2.41 GB with/without encryption
Boot	only UEFI and USB	Boot section	-	
Setup		Device configuration Local application definitions	Factory reset command	Does not affect the system partition with installed firmware
Update	4 GB flash memory	Software delivery in advance (before firmware update) via Scout Enterprise command or notification Signature check for eLux software packages Devices with update partition can be used as Dynamic Proxy (Provider) for firmware updates.	Scout Enterprise Delivery command with option Format update partition before delivery	The size of the update partition complies with the storage space provided. The update partition is no larger than the storage space provided. Devices with less than 4 GB flash memory are not provided with an Update partition.



Note

In the Scout Console, in the Properties window of a device, the system, setup and update partitions are listed including their sizes.

Extended system partition starting with eLux RP 6 2107

When you perform an update installation or a new installation (recovery) to eLux RP 6 2107 or later, the system partition is created with 2,35 GB / 2.41 GB (with/without encryption) instead of the previous

almost 2.0 GB. This creates more space for the firmware and allows larger images to be used.

■ Update installation

An update installation (firmware update) is still based on the previous partition sizes. The image size is thus still limited to the earlier values. Afterwards, the extended system partition is available and you can install images that may be up to 2.35 GB / 2.41 GB in size. This means, to install larger images on the freshly resized partition of the devices, a second firmware update is required.

■ Recovery installation

Provided an up-to-date recovery system is available, with a PXE or USB recovery installation the system partition can be partitioned to the new size directly during the installation process and a larger image with up to 2.35 GB / 2.41 GB can be written in the same process. A new installation or recovery installation thus allows the partition to be resized and used in one step.

Downgrade

Important To downgrade devices with the extended system partition (eLux RP 6 2107 or later) to an earlier version that only supports the previous system partition with less than 2 GB, you will have to go back to eLux RP 6 2104 LTSR CU1.

We therefore recommend that you update test devices to eLux RP 6 2107 or later as the first step to thoroughly test functionality.

17.3. IP ports

eLux / required ports

Port	Type	Description	How to deactivate	In/Out
	ICMP	ping must be supported to verify the status of the eLux devices		In/Out
80	TCP	Firmware update by using HTTP (and proxy port, if used)		Outgoing
443	TCP	Firmware update via HTTPS/TLS		Outgoing
5900	TCP	Mirroring eLux desktop	In Config¹ > Security , disable mirroring or uninstall VNC server in X.Org package	Incoming
22123	TCP	Scout Server (Scout Enterprise Manager / secure)		In/Out

¹Device configuration, formerly Setup

Port	Type	Description	How to deactivate	In/Out
22125	TCP	Scout Server (Scout Enterprise Manager / TLS 1.2) ¹		In/Out
22129	TCP	VPN		Outgoing

eLux / optional ports

Port	Type	Description	How to deactivate	In/Out
	ESP	VPN (data transfer)	Uninstall package <code>VPN System</code>	In/Out
21	TCP	Update via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	5250 emulations and telnet sessions		Outgoing
53	TCP, UDP	DNS server		Outgoing
67	UDP	DHCP server	Configure a local IP address (Config > Network)	Outgoing
68	UDP	DHCP client (or: BootP client)	Configure a local IP address (Config > Network)	Incoming
69	UDP	TFTP server (only used during PXE recovery)		Outgoing
88	TCP, UDP	AD authentication (Kerberos)		Outgoing
111	TCP, UDP	TCP port mapper - RPC internal use only Works with lockd (random) UDP port mapper - drive access on NFS servers Works with NFSD drive access (port 2049) and mountd (random)	Uninstall <code>Network Drive Share</code> package	In/Out
123	UDP	Windows Time server (NTP)	Do not configure a time server (Config > Desktop)	In/Out

¹for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

Port	Type	Description	How to deactivate	In/Out
139	TCP, UDP	SMB drive mapping, (NetBIOS) and SMB user authentication (CIFS)	Uninstall Network Drive Share package and User authentication modules package	Outgoing
161	UDP	SNMP	Uninstall SNMP Environment package	In/Out
162	UDP	SNMPTRAP	Uninstall SNMP Environment package	Outgoing
177	UDP	XCMCP protocol		Outgoing
389	TCP	AD authentication with user variables		Outgoing
443	TCP	VPN (connecting) via HTTPS/TLS	Uninstall package VPN System	In/Out
464	TCP, UDP	AD authentication (Kerberos) / Set password		Outgoing
514	TCP	Shell, X11 applications		Outgoing
515	TCP	Printing via LPD	Uninstall package Print environment (CUPS)	In/Out
631	TCP, UDP	CUPS (IPP) print client	Uninstall package Print environment (CUPS)	Outgoing
636	TCP	LDAPS authentication with user variables		Outgoing
2049	UDP	NFSD drive access NFS	Uninstall FPM NFS Support in Network Drive Share package	Outgoing
6000	TCP	Remote X11 application	In Config > Security, clear Allow remote X11 clients option	Incoming
7100	TCP	Font server can be assigned in (Config > Screen > Advanced)		Outgoing
8080	TCP	Firmware update via Dynamic proxy (Provider and Consumer)	Set Config > Firmware > Proxy-Type to None	In/Out
9100	TCP	Printing directly to parallel port can be assigned in (Config > Printer)	In Config > Printer, clear TCP direct print option	Incoming
9101	TCP	Printing directly to USB port can be assigned in (Config > Printer)	In Config > Printer, clear TCP direct print option	Outgoing

Port	Type	Description	How to deactivate	In/Out
20000	UDP	Wake On LAN		In/Out
22124	TCP	Scout Enterprise Statistics		Outgoing

Scout Server

Port	Type	Description	In/Out
	ICMP	ping must be supported to verify the status of the eLux devices	In/Out
1433	TCP	MS SQL Server	Outgoing
1434	UDP	MS SQL Server (Browser service)	In/Out
22123	TCP	Clients (Scout Enterprise Manager / secure)	In/Out
22124	TCP	Scout Enterprise Statistics	Incoming
22125	TCP	Clients (Scout Enterprise Manager / TLS 1.2) ¹	In/Out

Scout 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 Config > Security , disable mirroring or uninstall VNC server in X.Org package	Outgoing

Scout Dashboard

Scout Dashboard can be installed with HTTP or HTTPS.

Port	Type	Description	How to deactivate	In/Out
80	TCP	Dashboard service / web server via HTTP		Incoming
443	TCP	Dashboard service / web server via HTTPS/TLS		Incoming

¹for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

Port	Typ	Description	How to deactivate	In/Out
5901	TCP	Mirroring the eLux desktop	In Config > Security , disable mirroring or uninstall VNC server in X.Org package	Outgoing

Scout Cloud Gateway

Port	Typ	Description	In/Out
22125	TCP	Scout Server (Scout Enterprise Manager / TLS 1.2)	In/Out
22129	TCP	VPN	Incoming

17.4. SNMP

SNMP (Simple Network Management Protocol) is a network protocol for monitoring and controlling network devices.

For eLux RP 5 and eLux RP 6, version SNMPv3 is used.



Note

The command line program **snmpget** is not included in the software package. To query SNMP status information, please use third party software.

17.4.1. Configuring SNMP

1. From our portal www.mylux.com, under **eLux Software Packages**, for your eLux version, under **Add-On**, download the package **SNMP Environment** and deploy it to the clients.
2. If there is no `/setup/snmp/snmpd.conf` on the clients, transfer the configuration file `snmpd.conf` to the clients to `/setup/snmp/snmpd.conf` by using the Scout Enterprise feature **Files**.

Or:

Modify the `terminal.ini` file by using the **Advanced file entries** feature of Scout Enterprise.
Example:

File	/setup/terminal.ini
Section	SNMPD
Entry	rocommunity
Value	secret

3. Optionally, to define further **SNMPD Configuration Directives**, use the **Advanced file entries** feature and modify the `terminal.ini` file under **SNMPD**. Examples:

```
syscontact=contact@sampletec.com
syslocation=testcenter
doDebugging=1
```

For further information on SNMPD Configuration Directives, see <http://www.net-snmp.org>.

*The section **SNMPD** of the `terminal.ini` file is evaluated by the client and the file `/setup/snmp/snmpd.local.conf` is created. An existing `/setup/snmp/snmpd.conf` will be overwritten.*

If the configuration file does not exist, the file `/setup/snmp/snmpd.local.conf` is created with default values.

Notes on configuring SNMP v3

- When you define users (**createUser**), set a password with at least 8 characters.
- For the authentication method, define `authPriv` or `authNoPriv`.



Note

For SNMP v2, you can use `noAuthNoPriv` as the authentication method.

17.4.2. 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
syservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1 v2c usm security
access	name context model level prefix 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