

# Scout Enterprise Management Suite

## Administrator's Guide

## How to manage a client infrastructure through the Scout Console 15

Last edited: 2023-08-29

|  |    |
|--|----|
| 0. Legal information .....                                   | 5  |
| 1. Representation .....                                      | 6  |
| 2. Overview .....  | 7  |
| 2.1. Features of the Scout Enterprise Management Suite ..... | 7  |
| 2.2. Communication between devices and Scout Server .....    | 9  |
| 2.3. Installation .....                                      | 10 |
| 2.4. Keyboard shortcuts .....                                | 11 |
| 3. Interface of the Scout Console .....                      | 13 |
| 3.1. Organizational structure .....                          | 13 |
| 3.2. Icons in the tree view .....                            | 14 |
| 3.3. Windows .....   | 14 |
| 3.4. Status bar .....  | 21 |
| 3.5. Display settings .....                                  | 21 |
| 3.6. Changing the language .....                             | 22 |
| 3.7. Search for devices, OUs or applications .....           | 22 |
| 3.8. Moving and copying elements .....                       | 26 |
| 3.9. Switching OU to top-level .....                         | 27 |
| 4. Device management .....                                   | 28 |
| 4.1. Self-registration of devices .....                      | 28 |
| 4.2. DHCP configuration .....                                | 30 |
| 4.3. Searching for devices (Discovery) .....                 | 34 |
| 4.4. Reserving device profiles .....                         | 36 |

|  |            |
|--|------------|
| 4.5. Device names .....  | 36         |
| 4.6. MAC address .....   | 37         |
| 4.7. Secure device management with Scout .....                     | 38         |
| 4.8. OU filter .....   | 39         |
| 4.9. Dynamic Device Groups .....                                   | 46         |
| 4.10. Device relocation between Scout Servers .....                | 51         |
| <b>5. Device configuration .....</b>                               | <b>59</b>  |
| 5.1. Concept .....   | 59         |
| 5.2. Configuration method .....                                    | 66         |
| 5.3. Evaluating configuration data .....                           | 68         |
| 5.4. FollowMe Desktop .....  | 69         |
| 5.5. General tab .....   | 73         |
| 5.6. Network tab .....   | 75         |
| 5.7. Desktop tab .....   | 89         |
| 5.8. Display tab .....   | 97         |
| 5.9. Mouse/Keyboard tab .....                                      | 105        |
| 5.10. Firmware tab .....   | 107        |
| 5.11. Security tab .....   | 122        |
| 5.12. User authentication .....                                    | 125        |
| 5.13. Multimedia tab .....   | 136        |
| 5.14. Drives tab .....   | 138        |
| 5.15. Printer tab .....  | 141        |
| 5.16. Hardware tab .....   | 147        |
| 5.17. Diagnostics tab .....  | 154        |
| 5.18. Power management tab .....                                   | 154        |
| 5.19. Troubleshooting device configuration .....                   | 161        |
| <b>6. Advanced device configuration and Advanced options .....</b> | <b>164</b> |
| 6.1. Devices .....   | 165        |
| 6.2. Update/Delivery .....   | 166        |
| 6.3. Management .....  | 166        |
| 6.4. Predefined commands .....                                     | 167        |
| 6.5. Predefined IDFs and containers .....                          | 167        |
| 6.6. Wake On LAN .....   | 169        |
| 6.7. VPN .....   | 170        |
| 6.8. Files configured for transfer .....                           | 173        |
| 6.9. Advanced file entries .....                                   | 178        |
| 6.10. Rules .....  | 181        |
| 6.11. Environment variables .....                                  | 183        |
| 6.12. TPM 2.0 support .....  | 183        |
| <b>7. Defining applications .....</b>                              | <b>186</b> |
| 7.1. General .....   | 186        |
| 7.2. Connecting to a Citrix farm .....                             | 196        |

|  |            |
|--|------------|
| 7.3. RDP .....   | 209        |
| 7.4. Virtual Desktop .....                                   | 214        |
| 7.5. Browser .....   | 217        |
| 7.6. Local and user-defined applications .....               | 225        |
| 7.7. Emulation .....   | 229        |
| 7.8. Applications in kiosk mode .....                        | 230        |
| 7.9. Local web sites .....                                   | 244        |
| 7.10. Troubleshooting application definition .....           | 246        |
| 7.11. Third party software .....                             | 248        |
| <b>8. Client remote management by commands .....</b>         | <b>251</b> |
| 8.1. Available commands .....                                | 251        |
| 8.2. Executing commands .....                                | 253        |
| 8.3. Scheduling commands .....                               | 254        |
| 8.4. Command options .....                                   | 254        |
| 8.5. Command results and update information per device ..... | 257        |
| 8.6. Command history .....                                   | 259        |
| 8.7. Factory reset command .....                             | 260        |
| 8.8. User-defined Commands .....                             | 262        |
| 8.9. Creating predefined commands .....                      | 264        |
| 8.10. Defining templates for standard commands .....         | 265        |
| 8.11. eLux Command Scheduler .....                           | 267        |
| <b>9. Remote maintenance .....</b>                           | <b>272</b> |
| 9.1. Device identifier for support .....                     | 272        |
| 9.2. Mirroring .....   | 272        |
| 9.3. Device diagnostics .....                                | 275        |
| <b>10. Firmware update .....</b>                             | <b>282</b> |
| 10.1. Requirements .....                                     | 283        |
| 10.2. Access to applied images .....                         | 283        |
| 10.3. Planning firmware updates .....                        | 286        |
| 10.4. Performing firmware updates .....                      | 286        |
| 10.5. User information before update .....                   | 291        |
| 10.6. Delivering software in advance .....                   | 294        |
| 10.7. Dynamic proxy .....                                    | 297        |
| 10.8. Static proxy .....                                     | 300        |
| 10.9. Troubleshooting firmware update .....                  | 302        |
| <b>11. Passwords .....</b>                                   | <b>303</b> |
| 11.1. Local device password .....                            | 303        |
| 11.2. Scout Console password .....                           | 306        |
| <b>12. Managing administrators .....</b>                     | <b>307</b> |
| 12.1. Activating administrator policies .....                | 307        |
| 12.2. Adding administrators .....                            | 307        |
| 12.3. Deleting administrators .....                          | 308        |

|   |            |
|---|------------|
| 12.4. Administrator policy .....                      | 309        |
| 12.5. Viewing administrator activities .....          | 314        |
| 12.6. Pass-through authentication .....               | 315        |
| 12.7. Maintenance windows .....                       | 316        |
| <b>13. Scout Keep Alive service .....</b>             | <b>318</b> |
| 13.1. Configuring status messages for devices .....   | 318        |
| 13.2. Log files of the Scout Keep Alive service ..... | 319        |
| <b>14. Console communication .....</b>                | <b>322</b> |
| 14.1. Closing a console .....                         | 322        |
| 14.2. Sending messages .....                          | 322        |
| 14.3. Managing consoles .....                         | 323        |
| 14.4. Managing console commands .....                 | 323        |
| <b>15. Import/Export .....</b>                        | <b>325</b> |
| 15.1. Exporting .....                                 | 325        |
| 15.2. Importing .....                                 | 325        |
| <b>16. Log files and optimizing .....</b>             | <b>326</b> |
| 16.1. Log files .....                                 | 326        |
| 16.2. Optimizing .....                                | 330        |
| <b>17. Appendix .....</b>                             | <b>333</b> |
| 17.1. Program and file directories .....              | 333        |
| 17.2. eLux partitions .....                           | 333        |
| 17.3. IP ports .....                                  | 335        |
| 17.4. SNMP .....                                      | 339        |

## 0. Legal information

© 2023 Unicon GmbH

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 GmbH in the European Union, GB and the United States.

ScoutaaS® is a registered trademark of Unicon GmbH in the European Union, GB, the United States and Japan.

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

Unicon GmbH  
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   |
|-------------------------------|---|
| <b>Control element</b>        | All graphical user interface controls are displayed in <b>bold</b>  |
| <b>Menu &gt; menu command</b> | Whenever running a command involves clicking a series of menus, the single GUI controls such as menu commands or dialog tabs are linked by <b>&gt;</b> .  |
| 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 (Tool for creating eLux software packages) |
| 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<br>Unit or group within the organizational structure     |
| VPN          | Virtual Private Network  |

## 2. Overview

The Scout Enterprise Management Suite, or Scout for short, is a lean and easy-to use end-point management solution for devices running eLux. Administrators can easily manage, configure, upgrade, update, secure and monitor even large numbers of devices.

This manual serves as a reference for the Scout Console functionality and related tools. It includes features from version 15.3 onwards. Scout and eLux features that have been added since version 2101 are referred to via footnotes.

### 2.1. Features of the Scout Enterprise Management Suite

Scout Enterprise Management Suite is the management solution for cloud devices, Hybrid Clients, mobile devices and 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.  | ScoutInstaller.exe |
| Scout Console    | User interface for the management of eLux devices and Windows-based devices on which Scout Agent for Windows has been installed<br><br>Server communication only via database<br><br>Multiple consoles can be managed with one Scout database. | ScoutInstaller.exe |
| Scout Board      | Web user interface for the management of eLux devices and Windows-based devices on which Scout Agent for Windows has been installed  | ScoutInstaller.exe |
| Recovery service | Customized TFTP service to realize a PXE recovery environment for eLux endpoints   | ScoutInstaller.exe |

| Component                             | Description  | Installation                  |
|---------------------------------------|--|-------------------------------|
| ELIAS <sup>1</sup>                    | 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. | ScoutInstaller.exe            |
| 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<br>Is launched from the Scout Console  | ScoutInstaller.exe            |
| Scout Keep Alive service <sup>2</sup> | Windows service processing keep alive packets from eLux devices  | ScoutInstaller.exe            |
| Web API                               | 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   | ScoutInstaller.exe            |
| Scout Command Interface               | Command line interface for Scout commands  | ScoutInstaller.exe            |
| Scout Database Connection Editor      | Tool for modifying database connection settings of the Scout Server and Scout Console  | ScoutInstaller.exe            |
| Further products                      |  |                               |
| 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 eLux devices using the Scout Console

<sup>1</sup>The legacy ELIAS is no more included in the standard installation. To include it, choose **User-defined**.

<sup>2</sup>Replaces the Scout Statistics Service from Scout 15 2209

- Scout Board
- Scout Cloud Gateway
- ELIAS
- ELIAS 18
- Scout Report Generator
- Scout Command Interface

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 ELIAS 18 installation. If you use the legacy ELIAS instead, you need an eLux container for the software packages, see [Installing a container](#).

---

## 2.2. Communication between devices and Scout Server

---

#### Note

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

---

During system start, the eLux devices connect to their Scout Server and verify if their configuration data is up-to-date. Updated data may 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" on page 66.

The communication between a device and the server may proceed in three ways:

- The device accesses the Scout Server. The Scout Server has no updated configuration data.
  - The device continues starting up with its configuration.
- The device accesses the Scout Server. The Scout Server reports new configuration data and transfers the data to the device.
  - The device restarts using the new configuration.
- The device cannot access the Scout Server due to network or other problems which result in a management timeout (see "Advanced network settings" on page 78).
  - The device continues starting with its configuration.  
Depending on the handshake settings, the device retries connecting to be able to synchronize the configuration data. For further information, see "Optimizing with handshake" on page 330.

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

During operation of a user's device there is no data exchange between the Scout Server and device. During shutdown, the device 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 in the Installation guide](#).

## 2.4. Keyboard shortcuts

| Keys              | Selected element  | Description  |
|-------------------|---|--|
| CTRL+SHIFT+INSERT | Individual OU   | Opens the <b>Advanced device configuration</b> of the selected OU                          |
|                   | <b>Applications</b>   | Opens the <b>Application Properties</b> dialog to define a new application                 |
|                   | <b>Devices</b>  | Opens the <b>Information</b> 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 "Search for devices, OUs or applications" on page 22 field for simple search |
| CTRL+SHIFT+F      | —   | Opens the "Search for devices, OUs or applications" on page 22 window for advanced search  |
| CTRL+X            | Individual device   | Cuts the selected device   |
| CTRL+V            | <b>Devices</b> or individual device                         | Pastes the device from the Clipboard to the selected position                              |
| CTRL+A            | Individual application or device in the <b>List</b> window. | Selects all applications/devices in the <b>List</b> window                                 |
| CTRL+E            | Individual device   | Performs a <b>setup comparison</b>   |

| Keys   | Selected element | Description  |
|--------|------------------|--|
| CTRL+P | —                | Opens the <b>Print dialog</b> to print the list of available devices |

## 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** 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: **RDP**, **StoreFront** and **VMware Horizon**. For further information, see "Defining applications" on page 186.

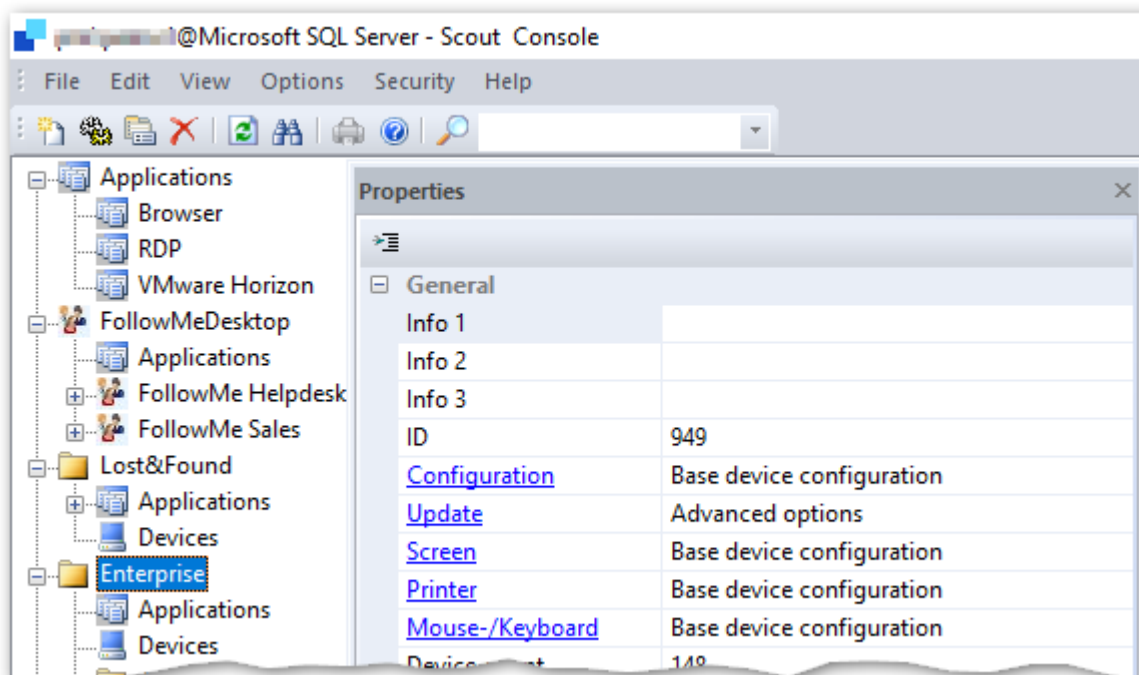
To each organizational unit - hereafter referred to as OU - you can add applications, devices and other OUs. Each OU can contain subordinate OUs, applications and devices.

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 "Concept" on page 59



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

## Adding a new OU

1. For the relevant OU, from the context menu, choose **Add > Organization unit...**  
*The **Advanced device configuration** dialog opens.*
2. Enter a unique name for the new OU.









### Note

Back slashes are not supported.

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 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<br>For further information, see "Properties" on page 16.   |
| Assets (only for devices) | Hardware information of the selected device<br>Is shown as a tab of the <b>Properties</b> window<br>For further information, see "Hardware information" on page 19. |

| Window                     | Description  |
|----------------------------|--|
| Dynamic Device Groups      | Shows the defined Dynamic Device Groups (list view)  |
| Independent configurations | Shows OUs and devices that do not use the parent device configuration (list view)<br><br>For further information, see "Blocking inheritance - independent device configuration" on page 61   |
| Compare configurations     | Shows differences in the device configuration between devices or OUs   |
| OU devices/applications    | Devices or applications of an OU view without icons (list view)<br><br>Double-clicking on a device shows the corresponding device in the tree view.<br>This feature can be disabled, see below.  |
| All devices                | Shows all devices without icons (list view)<br><br>The device data are only loaded from the Scout database when you click the  <b>Refresh</b> button. This is meant to prevent unintentional loading of huge amounts of data.<br><br>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<br><br>Double-clicking on a device shows the corresponding device in the tree view.<br>This feature can be disabled, see below.<br><br>To search window content, use the <b>Search</b> 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 "Search for devices, OUs or applications" on page 22. |

## 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.

## 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.

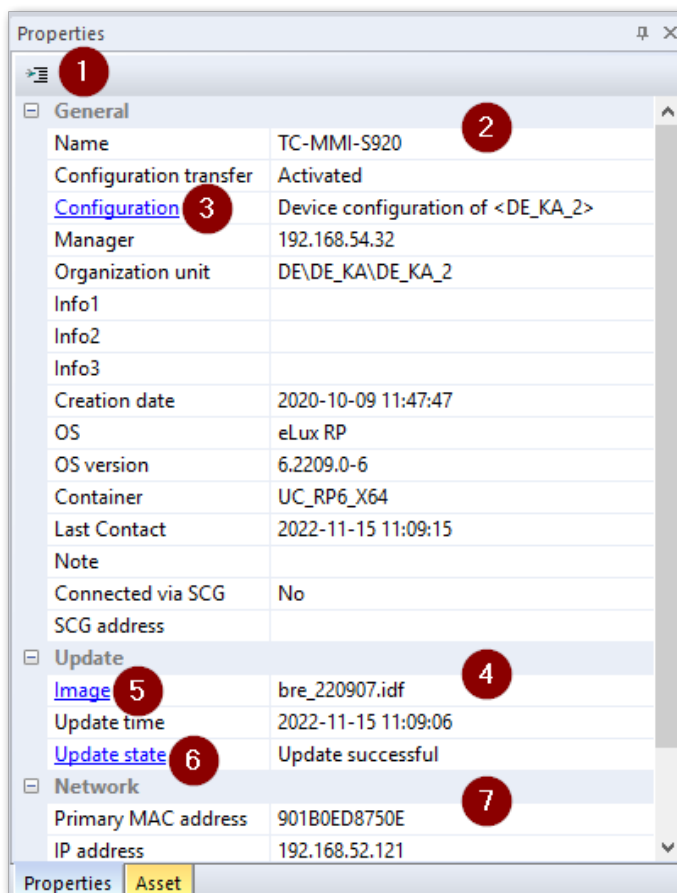
Many properties come from the device configuration (devices and OUs) and application definition (applications) and are updated with each configuration update. For further information, see "Configuration method" on page 66.

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



The figure shows the properties of a selected device.

- 1 Show, hide or move fields
- 2 General information on the device
- 3 Click to open the device configuration the device is assigned to
- 4 Information on the last firmware update
- 5 Click to open the assigned image in ELIAS (provided **Options > ELIAS settings** is configured)
- 6 Click to open the update log
- 7 Network information on the device

### 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 <b>Info</b> fields are shown on the device in the <b>Configuration panel</b> under <b>Information</b> 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<br><br>For further information, see "Command results and update information per device" on page 257   |
| Last contact                     | Time stamp of the last contact between server and device<br><br>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                           | <b>Example:</b> <code>Switched on</code><br><br>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  |
| Connected via SCG <sup>1</sup>   | Indicates whether a device is connected via Scout Cloud Gateway  |
| SCG address <sup>2</sup>         | For SCG connections: Shows the FQDN and IP address of the Scout Cloud Gateway  |
| Primary "MAC address" on page 37 | Device address of the hardware (MAC=Media Access Control)  |
| Simple device identifier         | Temporary device identifier users may request for support cases  |
| Client identifier                | Globally unique identifier for a device or eLux Portable USB stick   |
| Public address                   | If a device is connected via VPN, its public IP address is displayed next to its actual <b>IP address</b> . You can filter by the public IP address in the Scout Report Generator.   |

---

<sup>1</sup>from Scout 15 2209 and eLux RP 6 2209

<sup>2</sup>from Scout 15 2209 and eLux RP 6 2209

| Option               | Description   |
|----------------------|---|
| Partitions           | The system, setup and update partitions are displayed with their respective sizes.  |
| Screen (Screen info) | Shows the configured resolution and frequency of all connected monitors<br>For multiple monitor layouts, additionally the output port and defined properties such as primary screen, rotation and the monitor's position (row/column) are displayed. <sup>1</sup> If a monitor is not active, this is shown as a dedicated property. <sup>2</sup> The values for row and column are then shown as -1. |

## OU properties

Examples:

| Option       | Description   |
|--------------|---|
| OU           | Shows the ID of an OU<br><br>In addition to the decimal value, you can show the hexadecimal value. This requires a new registry entry:<br><br>Key: HKEY_CURRENT_USER\Software\UniCon\Scout\Settings<br>Value name: DisplayHexOUID<br>Value type: DWORD: 32<br>Value data: 1 |
| 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           | <a href="#">Configuration</a> | Opens the relevant <b>Device configuration</b>  |
| Device           | <a href="#">Image</a>         | Opens ELIAS with the image configured for this device in the relevant container<br><br>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 283 |

<sup>1</sup>from Scout 15 2204

<sup>2</sup>from Scout 15 2209

| Selected element | Option                                 | Description  |
|------------------|--|--|
| Device           | <b>Update State</b>                    | Double-click or ... opens the <b>Update-Info</b> for the device providing information on performed updates. For further information, see "Command results and update information per device" on page 257 |
| OU               | <b>Configuration</b>                   | Opens the relevant <b>Device configuration</b>   |
| OU               | <b>Update</b>                          | Opens the relevant <b>Update</b> settings in the <b>Advanced device configuration</b> or <b>Advanced options</b> .   |
| OU               | <b>Screen, Printer, Mouse/Keyboard</b> | Opens the relevant configuration ( <b>Device configuration</b> or <b>Advanced device configuration</b> ) for Screen, Printer or Mouse/Keyboard   |

## Application properties

The details of an application depend on its type (for example **Browser**). They correspond to the details of an application definition. For further information, see "Adding applications" on page 186.

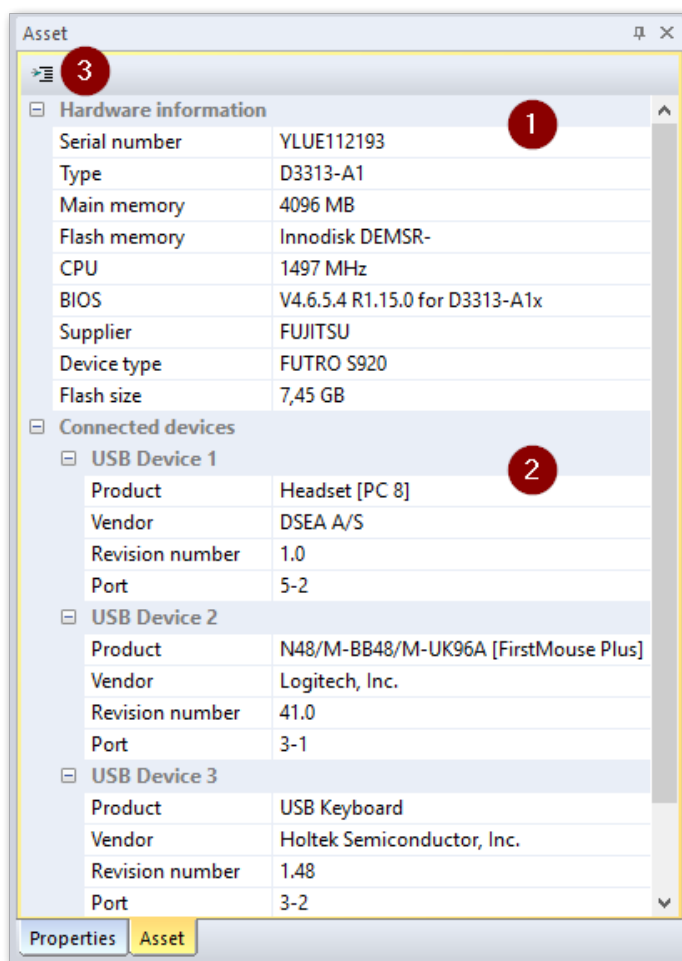
### 3.3.2. Hardware information

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.



- 1 Information on the managed client device
- 2 Information on connected devices
- 3 Show, hide or move fields

## Hardware information of a 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   |

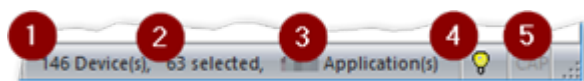
## Hardware information of connected devices

Examples for a USB device:

| Option  | Description        |
|---------|--------------------|
| Product | Type of USB device |
| Vendor  | Vendor name        |

| Option                   | Description  |
|--------------------------|--|
| Serial number            | Serial number of the USB device  |
| Revision number          | Firmware version of the USB device   |
| Port number <sup>1</sup> | Number of the port the USB device is connected to: <i>&lt;bus number&gt;-&lt;port number&gt;</i> |

### 3.4. Status bar



- 1 Number of all devices
- 2 Number of devices you have selected in a list, for example, in the **All devices** window  
Use this information as feedback before applying any function to the devices.
- 3 Number of all applications
- 4 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.  
▶ To show the alert messages, double-click the icon.
- 5 Indicates whether the CAPS LOCK key is active

When you perform large operations such as importing, moving, exporting or deleting a large number of devices, the process is displayed on the status bar.<sup>2</sup>

### 3.5. Display settings

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

| 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 |

<sup>1</sup>from Scout 15 2209 and eLux RP 6 2209

<sup>2</sup>from Scout 15 2110

| Option  | Description  |
|---|--|
| Show new devices automatically in tree view           | 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.  |
| Show confirmation messages / Before view is refreshed | After you press F5 or click <b>View &gt; Refresh</b> , the system prompts you before refreshing the view.  |
| Check independent configurations                      | <p>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.</p> <p>For further information, see "Blocking inheritance - independent device configuration" on page 61.</p> |
| Verbose level   | For level 1, a confirmation message is shown before commands are executed, indicating the number of affected devices.  |

### 3.6. Changing the language

The console is started with the display language you have chosen for the Scout Enterprise Management Suite installation. 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 a language change.

### 3.7. Search for devices, OUs or applications

Die Scout Console This offers various search options for objects within the infrastructure.

Search for devices, OUs or applications:

- Quick search in the tree view
- Search via dialog and use search options

Search for devices

- Quick search in the **All devices** window
- Advanced search

#### Note

These search functions refer to the current Scout infrastructure and are not to be confused with the **discovery** function which is meant for devices in the entire network and outside the infrastructure.

## Devices / Search for MAC addresses

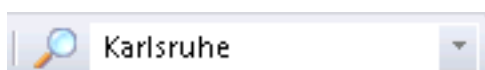
All described search functions allow you to find devices based on their MAC address. To do so, use one of the following formats:

|   |                   |
|---|-------------------|
| 12-digit MAC address without separators                                 | 001122334455      |
| 12-digit MAC address with the 6 pairs separated by colons <sup>1</sup>  | 00:11:22:33:44:55 |
| 12-digit MAC address with the 6 pairs separated by hyphens <sup>2</sup> | 00-11-22-33-44-55 |

### 3.7.1. Searching the tree view (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.

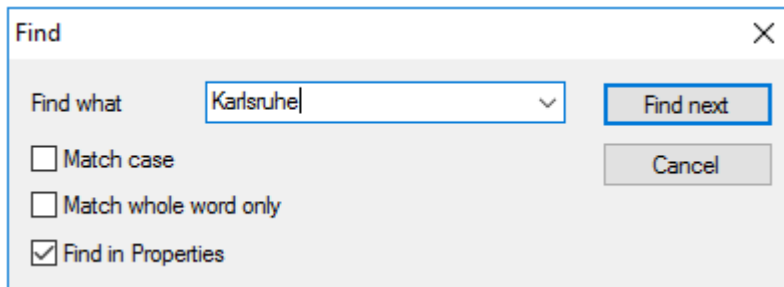
<sup>1</sup>from Scout 15 2204

<sup>2</sup>from Scout 15 2204

### 3.7.2. Searching the tree view including search options (dialog)

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 may type only 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 <b>Properties</b> and <b>Assets</b> 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.

### 3.7.3. Searching for devices 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.

---

### 3.7.4. Searching for devices using the Advanced search view

The **Advanced search** window 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.*

### 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 OU. For further information, see "Uploading applications from a device to Scout " on page 193.

---

### 3.9. Switching OU to top-level

---

**Note**

This feature can only be applied to an OU.

---

- For the relevant OU, from the context menu, choose **Edit > Convert to base-OU**.

*The relevant OU is moved to the highest level. It becomes one of the base-OUTs. 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 must know their "MAC address" on page 37. There are several approaches to register new devices such as

- "Self-registration of devices" below
- "Searching for devices (Discovery)" on page 34: 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" on page 39 according to definable criteria
- are created in terms of proxy profiles even before connecting ("Reserving device profiles" on page 36)

The way you want to deal with new devices is mainly defined under **Options > Advanced Options > "Devices"** on page 165.

---

### Note

As the devices are organized hierarchically in OUs, you can use "Dynamic Device Groups" on page 46 to apply commands to several devices irrespective of their OUs.

---

### 4.1. Self-registration of devices

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

Requirements for self-registration:

- The device must be in initial state (either upon delivery or by performing a factory reset)
- The device must be connected to the network
- The Scout 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" on page 30.

or

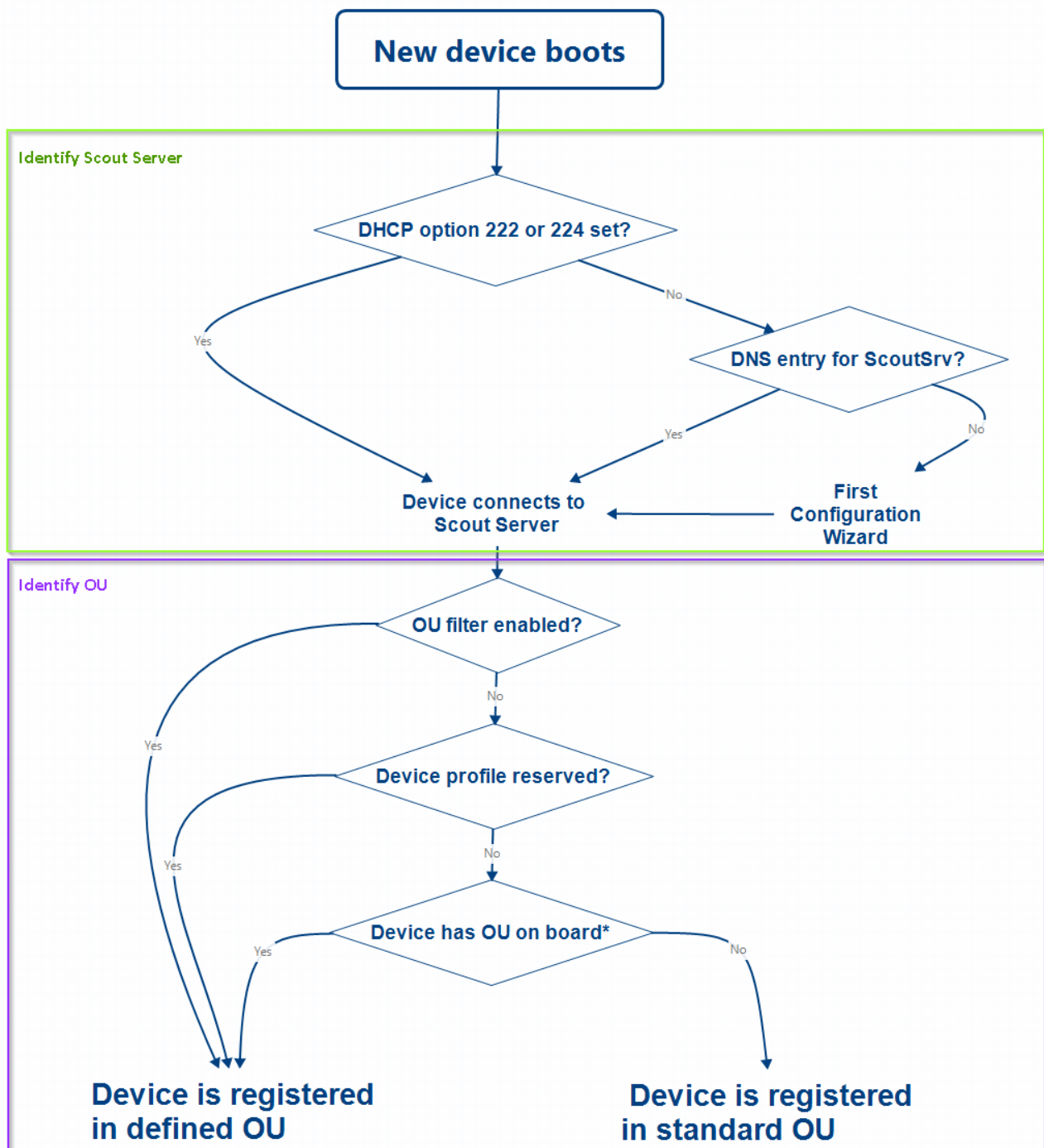
- DNS: The DNS server resolves the host name `ScoutSrv` (no case-sensitivity).

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 device to help the local user through the initial configuration.

## Registering a device automatically

- ▶ Turn the device on.

*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 devices.

A new device 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<br>(in ASCII<br>column) | ELUXNG<br><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 |

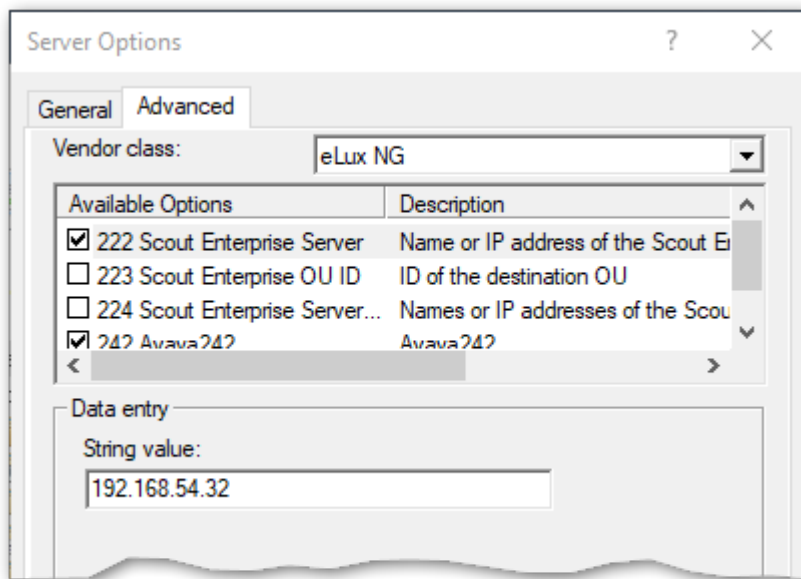
7. To define a specific OU that you can assign new devices to, click **Add...** and edit the new option as follows:

| Option      | Value                    |
|-------------|--------------------------|
| Name        | Scout 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 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 Enterprise server list, String, 224
  - Scout 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 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                | The default 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 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 "Devices" on page 165.

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 your destination OU is configured correctly.
2. Select **Options > Search devices**.

The screenshot shows the 'Discover devices' dialog box with the following fields and callouts:

- 1**: IP address start (192.168.54.116)
- 2**: Count (1)
- 3**: IP address end (192.168.54.116)
- 4**: Password (masked with dots)
- 5**: Destination OU (Tree view showing AT, DE, DE\_KA, DE\_MA, FRANCE, IT, NL. DE\_MA is selected)
- 6**: When the device is restarted - Inform user for (0) seconds
- 7**: User can cancel the command (checked)

Buttons: OK, Cancel

3. Edit the following fields:

- 
- 1 First IP address of the range
  - 2 Number of IP addresses within the range (restricted to 255)
  - 3 Last IP address of the range
  - 4 Device password (default: `elux`)  
The password must match the password currently set on the individual devices.
  - 5 OU you want to assign the devices to  
Default is the predefined `Lost&Found` 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.

- 
- 6 The user is informed by a message about the upcoming device restart.  
Specify in seconds how long the message shall be displayed. If the time period is set to 0, the system will wait until the user confirms.
  - 7 Allows the user to suppress the device restart. The configuration is not updated until the device 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 devices 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 device, 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 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 device profile by its "MAC address" on the facing page. 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. Below the OU, open the  **Devices** context menu 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 reserves a profile for the device with the respective MAC address. The actual registration is made at the time of the first device 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" on page 325.

---

## 4.5. Device names

The devices' host names can either be taken from the devices without modification or 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 165.

Device names are subject to the following format rules:

- Allowed characters are letters (a–z, A–Z) and digits (0–9).
- Additionally, hyphens (–) are allowed within the string, but not at the beginning and end of a device name.
- A device name must be at least one character long (letter or digit).

## 4.6. MAC address

The MAC address is the hardware address or physical address of a network device. Scout used to identify devices by their MAC addresses. In the meantime, the **client identifier** does this job.

MAC addresses can be used for the following tasks, for example:

- Import devices
- Reserve device profiles
- Create dynamic device groups

In Scout, MAC addresses are normally represented as 12-digit numbers without separators.

Example: 901B0E01CE84

From Scout 15 2204, you can also use colons or hyphens as separators between the 6 pairs:

|   |                   |
|---|-------------------|
| 12-digit MAC address without separators                                 | 001122334455      |
| 12-digit MAC address with the 6 pairs separated by colons <sup>1</sup>  | 00:11:22:33:44:55 |
| 12-digit MAC address with the 6 pairs separated by hyphens <sup>2</sup> | 00-11-22-33-44-55 |

### Note

The MAC address usually is determined from the network interface (Lan or WLAN card).

---

<sup>1</sup>from Scout 15 2204

<sup>2</sup>from Scout 15 2204

## 4.7. Secure device management with Scout

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

Clients that are registered with their "MAC address" on the previous page in the Scout database ("Reserving device profiles" on page 36) are accepted by the Scout Server and can be integrated into the Scout management. In contrast, devices having an unknown MAC address are not accepted and therefore cannot be managed by Scout. Unknown devices are not provided with a license from Scout's license pool.

### Accepting known devices 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 device stating that a connection to the Scout Server was denied.*

---

#### Note

Only the requests of those devices are accepted whose MAC addresses have been saved to the Scout database by a device import or device profile.

---

## 4.8. OU filter

OU filters 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 an OU filter:

- The **subnet OU filter** uses the devices' network address for filtering
- The **user-defined OU 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
- selecting the OU in the First Configuration Wizard locally on the device
- the default OU specified in **Advanced options > Devices**.

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

---

### Note

OU filters are included when you export the data category **Advanced options**. For further information, see "Import/Export" on page 325.

---

### 4.8.1. 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 OU filter** option. If required, click **...** to open the **OU assignment** dialog.
3. Under **Filter type**, select `Subnet filter (device network address)`.
4. Create a new filter rule. Edit the following fields:

| Option          | Description  |
|-----------------|--|
| Network address | Enter the scope of IP addresses.<br>Example: 192.168.16.0 covers all IPs starting with 192.168.16. |
| Netmask         | Enter the relevant network prefix to define relevant devices.                                      |
| Destination OU  | To browse the OU list, click ... and select the OU you want the specified devices to go.           |

5. Click **Add**.

*The filter rule is displayed in the field below.*

6. If required, add more filter rules and configure them. For further information, see "Options for OU filter rules" on page 42.

7. In the bottom section, from the list **Non-matching devices**, 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.

8. Review all active filter rules thoroughly to avoid unintentional assignments.

9. 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 additional user-defined filter rules will not be taken into account.*

#### 4.8.2. OU filter as a user-defined filter

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

## Filter rules wit OU filter text

eLux 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 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, UEFI/BIOS, CPU speed, model, kernel version, flash type, flash size, RAM size, graphics, IDF name, MAC address.

- A filter rule can contain 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=6.2302.0-3;
ELUX_SERIAL=72500422542;
ELUX_SUPPLIER=WYSE;
ELUX_DEVICEYPE=ZQ Class;
ELUX_BIOS=V4.6.5.4 R1.15.0;
ELUX_CPU=1500;
ELUX_PRODUCT=ZQ Class;
ELUX_FLASH=16GB SATA Flash;
ELUX_FLASHSIZE=15272;
ELUX_MEMORY=4096;
ELUX_GRAPHICS=ATI AMD Radeon HD8330E;
ELUX_IDF=recovery.idf;
ELUX_MAC=7CD30A22D0AE
```

- Use the logical operators **AND** and **OR** to link multiple filter criteria. Use capital letters for the operators.
- Wildcards are not supported, but all matches will be found that begin with the specified string.

Examples filter rules:

```
ELUX_OSNAME=eLux RP AND ELUX_OSVERSION=6.2302.1
ELUX_DEVICEYPE=D3314-A1 OR ELUX_DEVICEYPE=ZQ Class
```

## Setting up a user-defined OU filter

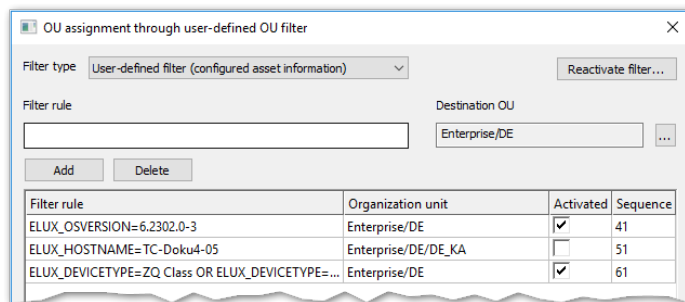
1. Click **Options > Advanced options > Devices**.
2. Under **New devices**, select the **Assign OU depending on OU filter** option. If required, click **...** to open the **OU assignment** dialog.
3. Under **Filter type**, select **User-defined filter (configured asset information)**.

4. Create a new filter rule. Edit the following fields:

| Option         | Description  |
|----------------|--|
| Filter rule    | Create a filter rule consisting of one or more filter criteria, see above.               |
| Destination OU | To browse the OU list, click ... and select the OU you want the specified devices to go. |

5. Click **Add**.

*The filter rule is displayed in the field below.*



6. If required, add more filter rules and configure them. For further information, see "Options for OU filter rules" below.
7. From the list **Non-matching devices**, 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.

8. Review all active filter rules thoroughly to avoid unintentional assignments.
9. 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 additionally defined subnet filter rules will not be taken into account.*

#### 4.8.3. Options for 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:

| Option  | Action  | Description   |
|---|---|---|
| Create new filter rule                              | Click <b>Add</b>                                | <p><b>User-defined filter:</b></p> <p>The filter criteria of the <b>Filter rule</b> field and the selected <b>Destination OU</b> are added as a new filter rule to the list.</p> <p>Syntax of a filter criterion:<br/> <code>&lt;String from OU filter text&gt;=&lt;value&gt;</code></p> <p>You can combine two or more filter criteria by using one of the logical operators <b>AND</b> or <b>OR</b>. Use capital letters for the operators.</p> <p>For examples, see "OU filter as a user-defined filter" on page 40.</p> <p><b>Subnet filter:</b></p> <p>The data from the fields <b>Network address</b>, <b>Netmask</b> and <b>OU</b> are added as a new filter rule to the list.</p> |
| Delete a filter rule                                | Select filter rule and click <b>Delete</b>      | The selected filter rule is deleted.  |
| Edit filter rule                                    | Select filter rule and press F2 or double-click | Modify the elements of a filter rule right in the list.   |
| Activate / deactivate a filter rule                 | Select/Clear <b>Activated</b> 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 <b>Sequence</b> field                      | Filter rules with low sequence number are processed prior to filter rules with high sequence number.  |

- ▶ Review all active filter rules thoroughly to avoid unintentional assignments.
- ▶ For the entire filter, under **Non-matching devices**, 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.

#### 4.8.4. 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 > Management**.
2. Under **New devices**, select **Ignore OU filter**.
3. Confirm with **OK..**

Or:

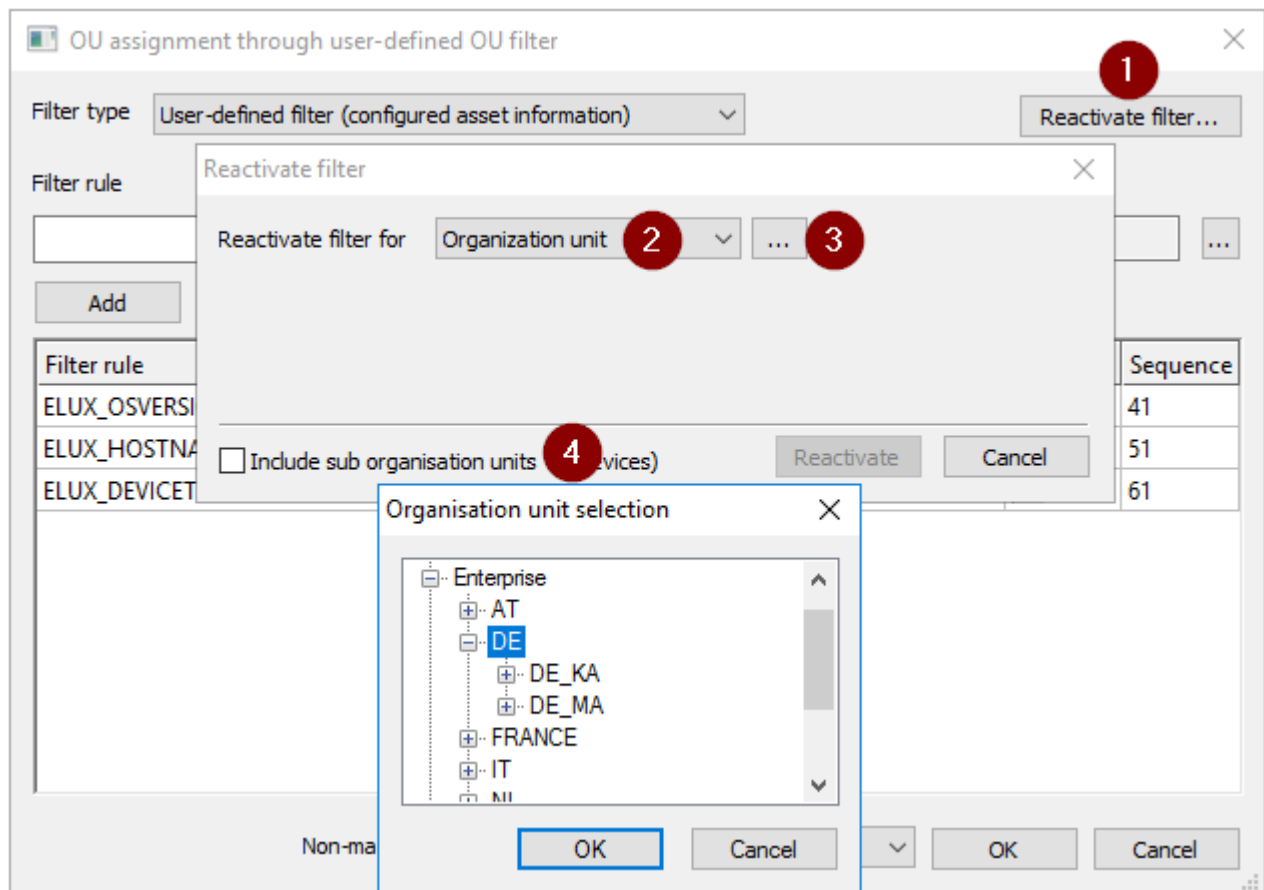
1. By using a drag-and-drop operation, move the device to another OU.
2. Confirm with **OK..**

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

#### 4.8.5. 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 **Assign OU depending on OU filter** option. If required, click **...** to open the **OU assignment** dialog.
3. In the upper right section, click **Reactivate filter...(1)**.



4. Under **Reactivate filter for** (2), select the scope of devices for which you want to re-activate the OU filter: for all devices, for an individual OU or for Dynamic Device Groups.
5. To re-activate the OU filter for OUs or Dynamic Device Groups, click **...** (3) next to the list-field and select an OU or Dynamic Device Group.  
To include devices of subordinate OUs, select **Include sub organization units** (4).
6. Confirm with **Reactivate** and **OK**.

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

## 4.9. Dynamic Device Groups

Dynamic Device 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 UEFI/BIOS update on all devices with a specific UEFI/BIOS version, across all OUs. Even device 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 Device 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 Device Groups.

---

### Note

The report layout must include the Client Identifier field. The report type must be a list of **Devices** or **Assets**.

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

---

Dynamic Device 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 Device 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. 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**.

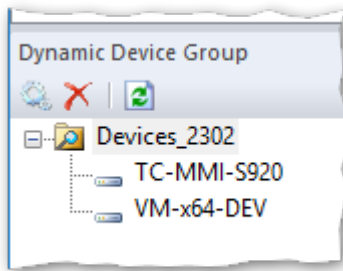
### 4.9.1. Using Dynamic Device Groups

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

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

## Displaying Dynamic Device Groups

- ▶ In the Scout Console, click **View > Window > Dynamic Device Groups....**



*The **Dynamic Device Groups** window is displayed. The Dynamic Device 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 Device Groups

1. In the **Dynamic Device Groups** window, select the relevant device group.
2. On the toolbar of the **Dynamic Device 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 Device Groups

1. In the **Dynamic Device 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.*

### 4.9.2. Special form of Dynamic Device Groups by import

To create a Dynamic Device Group, instead of using the Scout Report Generator, you can use the **Import** feature of the Scout Console and make up a device 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. Note that the **Import** feature here is not used to import devices.

#### Creating Dynamic Device Groups by import

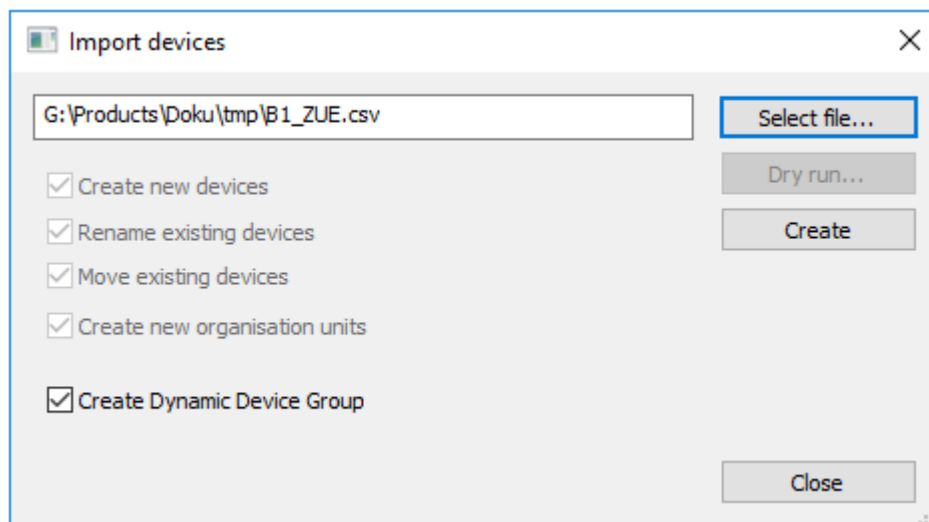


##### Requires

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 Device Group** option.

*All options related to the device import are disabled.*

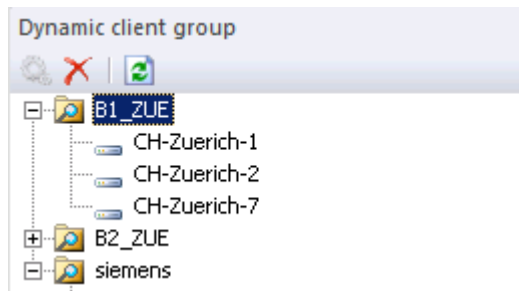


3. Click **Select file...** and select the relevant `.csv` file from the file system.
4. Click **Create**.

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


#### Displaying Dynamic Device Groups

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



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

### Note

Dynamic Device 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 Device Groups

1. In the **Dynamic Device 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.*

## 4.10. Device 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 devices 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 device relocation procedure also in MSP installations. Here, there is no need to carry license information.

---

### 4.10.1. 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 for the relevant devices is triggered by a notification named **Initiate device relocation** 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. Then, the relocation process will be started and the devices will be 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.

### 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 Server<sup>1</sup>

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 device relocation. If the devices are already registered on the target server, licenses and Subscription will not be updated.

#### 4.10.2. Relocation procedure / offline

The relocation procedure is initiated by the source server (device-releasing server) and completed by the relevant 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 device 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:

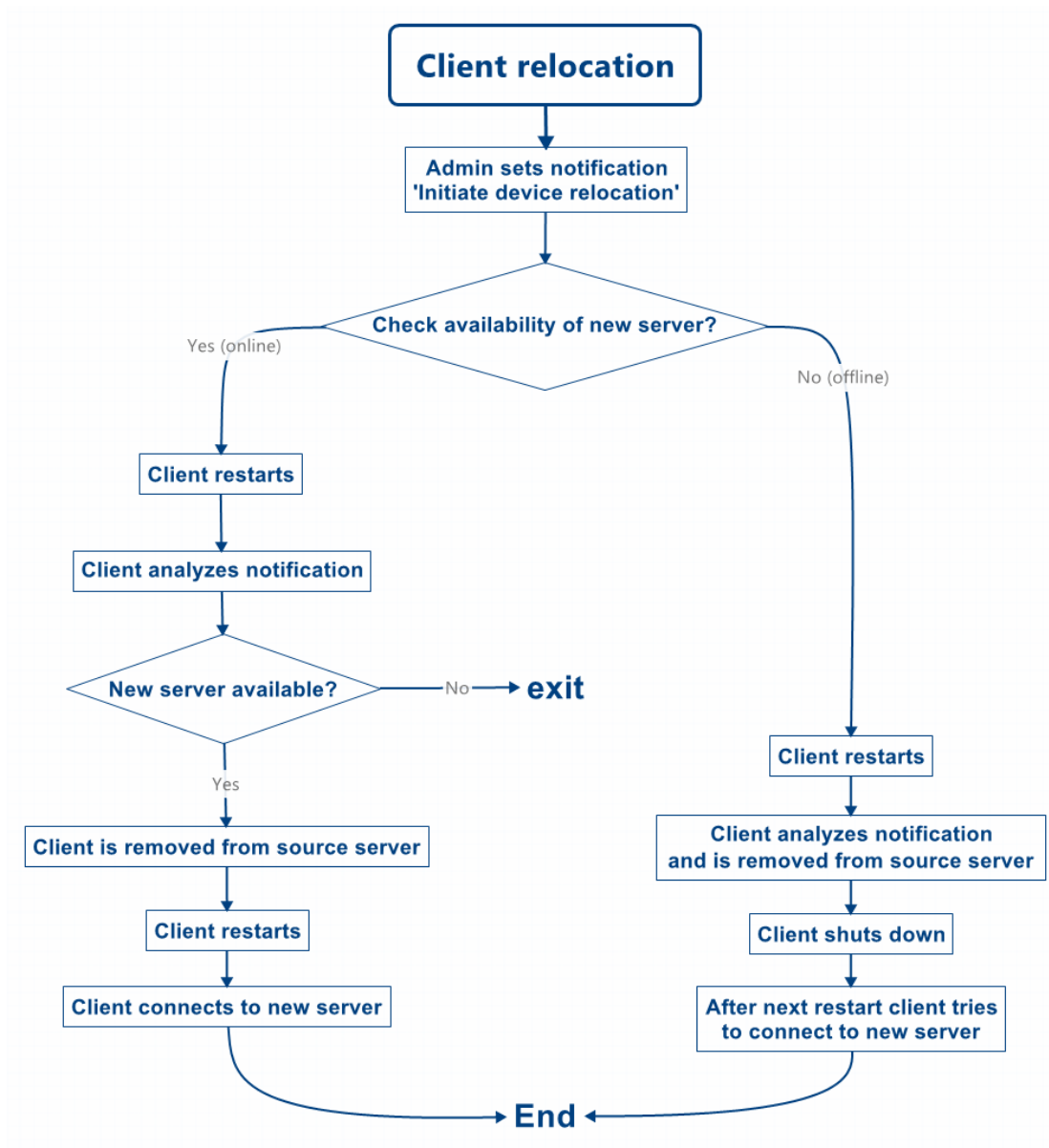
The relevant devices are removed from the source server without further verification. On the next restart, the devices will try to connect to the target server.

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

---

<sup>1</sup>from Scout 15 2110

## 4.10.3. Relocation flow chart



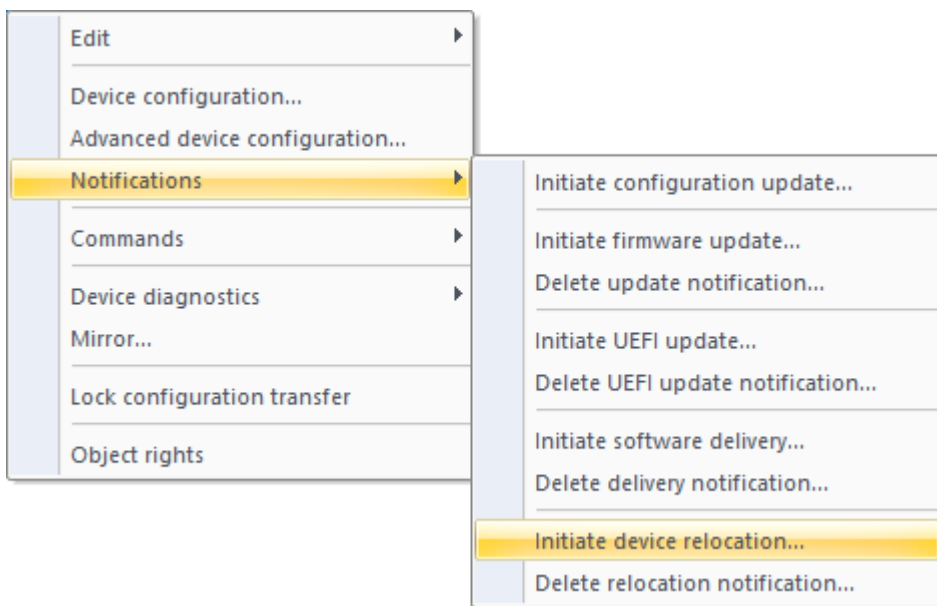
#### 4.10.4. Initiating device relocation



##### 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 device 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 Device Groups or devices within the **All devices** window.
2. On the context menu, click **Notifications > Initiate device relocation....**



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

##### 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:

Device relocation notification

New Scout server

scout2.sampletec-01.com

New OU-ID

132

☐ Relocation without transfer of licenses

☒ Check availability of new Scout server on device before relocation

☐ Retain local configuration on the new Scout server

Notice : The Scout server DHCP options (e.g. 222/223/224) are not evaluated during a device relocation process.

☐ Include subordinated OUs (5 Devices)

OK

Cancel

|   |   |
|---|---|
| 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 on the source server. |

**Important** In case you want to move devices from a standard to an **MSP** installation, licenses cannot be transferred with them. Select the option **Relocation without transfer of licenses** to leave the licenses on the source server. Otherwise, the licenses will be lost.

|   |  |
|---|--|
| 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 <sup>1</sup> | User-defined values of the local device configuration in unlocked fields will be retained. This is relevant if the corresponding option in <b>Advanced Options &gt; Devices</b> is used. |
| Include sub-ordinate OUs                                    | 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.

<sup>1</sup>from Scout 15 2110

The notifications for device 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....

## 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.

### 4.10.5. Scheduling the relocation process

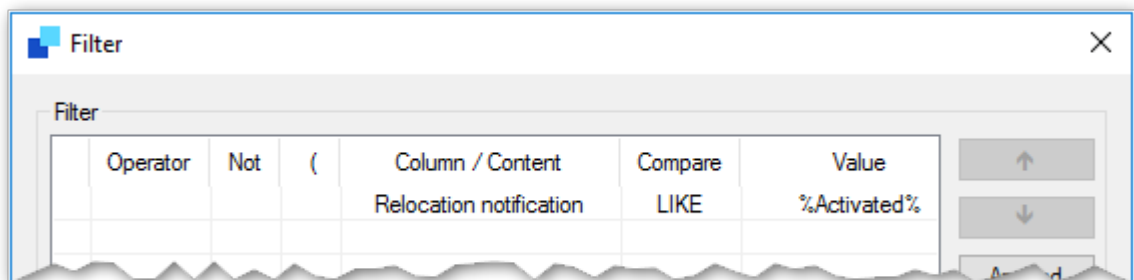
To carry out the device relocation outside working hours, for example, and to add a slight delay after each device is processed, proceed as follows.



#### 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.

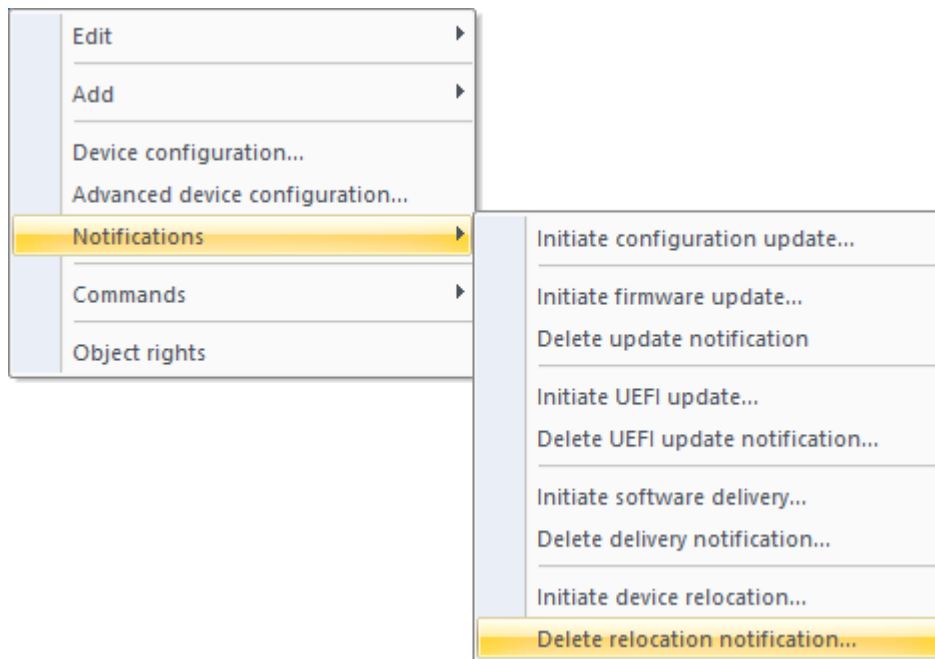


2. Export the identified devices to a Dynamic Client Group.
3. In the Scout Console, for your Dynamic Client Group, schedule a **Restart device** command:
  - In the Command dialog, choose date and time of the execution.
  - Specify a delay in milliseconds, that will be applied after the command execution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

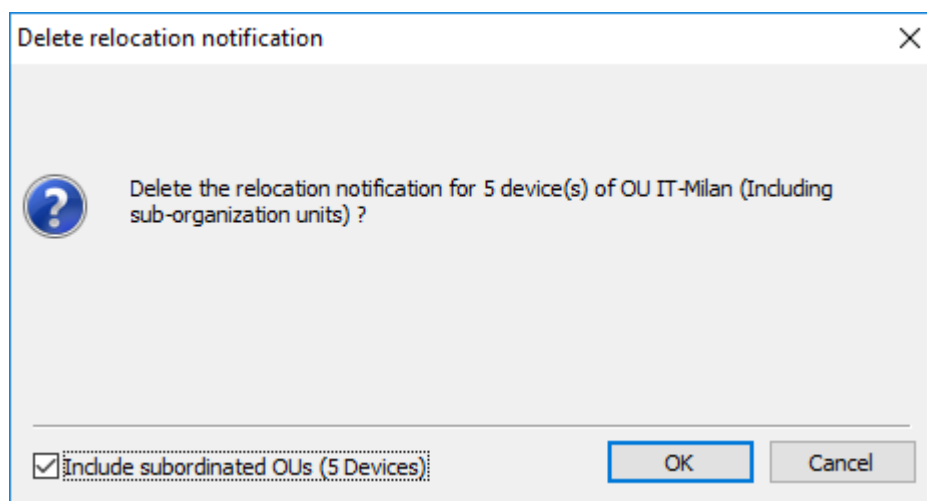
The relevant devices are restarted at defined time and then start the relocation process. They obtain their new configuration data from the target server. If you perform the relocation offline, the relevant devices will be removed from the source server, but will only connect to their new server when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

#### 4.10.6. Deleting relocation notification

1. For the relevant devices, from the context menu, choose **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, you will see that 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 devices efficiently. Configuring as many devices 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 provides flexibility to override any settings on all levels.

---

#### Note

Changes to the device configuration take effect on the next device restart.

---

**Important** The device configuration of a device 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** is active, the configuration of the superordinate 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**)

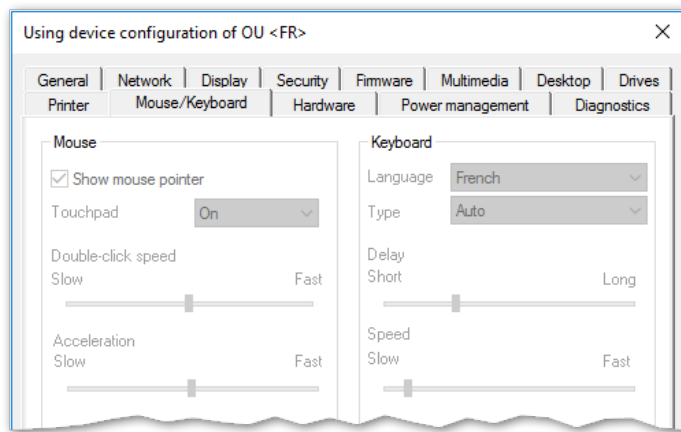
On each level, you can inherit the device configuration from the parent level or define independent settings. To be able to override settings, you must block inheritance, that is disable the use of the parent device configuration.

---

#### Note

Pay attention to the **Device configuration** dialog title. It indicates the location of the current configuration. This can be the base device configuration, or a parent OU, or the individual device.

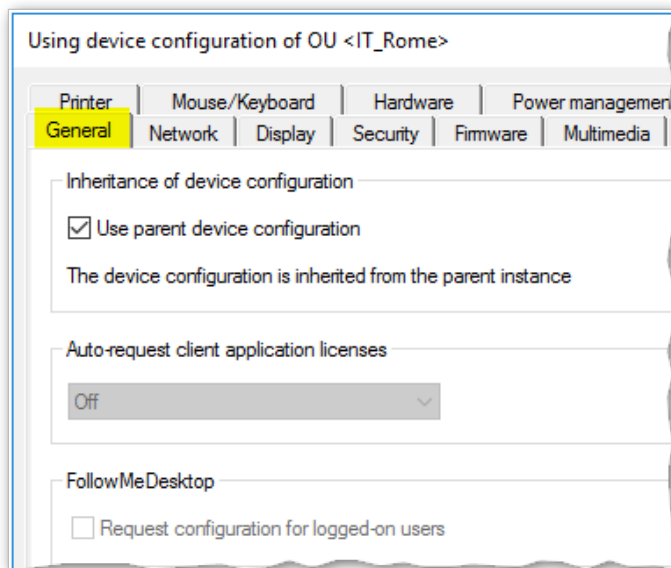
---



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...**

*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 parent OU. For further information, see "Accessing device configuration" on page 63.*

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

---

### 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 "User rights" on page 122.

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

#### Retaining local device configuration

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

*When the Scout 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

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 device 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" on page 260.

### 5.1.4. Initiating a one-time update of all device configuration data

For example, 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 device restart.

1. In the Scout Console, for the relevant device or OU, from the context menu, choose **Notifications > Initiate configuration update...**
2. For OUs, in the notification message, select whether you want to apply this on all subordinated devices (default).<sup>1</sup>

*The relevant devices will be marked to obtain a copy of the relevant Scout device configuration data including unlocked fields, on the next device restart.*

---

<sup>1</sup>from Scout 15 2209

## 5.1.5. Accessing device configuration

### Opening the base device configuration

- ▶ In the Scout Console, 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.

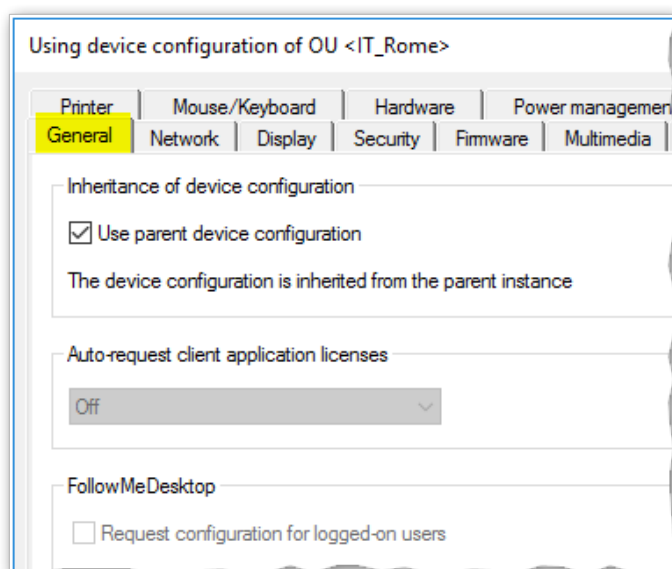
### Opening Device configuration dialog for OUs and devices

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

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** 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.

### Opening the relevant Device configuration dialog (preferred method)

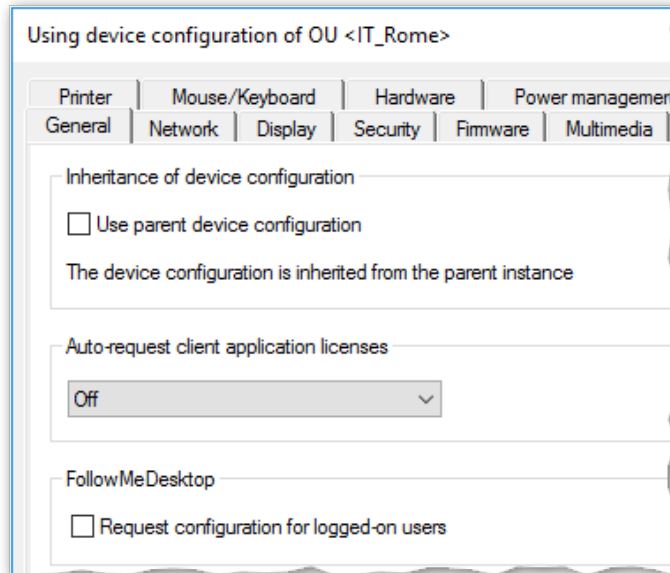
This method allows you to quickly and easily access the point where the device configuration is defined for the relevant devices.

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*.

### 5.1.6. 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  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" on page 68.

---

### 5.1.7. Locking configuration transfer

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 management.*

---

#### Note

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

---

## 5.2. Configuration method

During system start of the devices managed by the Scout Enterprise Management Suite, the devices 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
- Application definition
- Files configured for transfer
- Advanced file entries

The Scout Server identifies the relevant configuration data at run-time. 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 device, the relevant modified data are identified, compressed and saved to the database. They are then transferred to the device in one step.

When modifying the configuration of a large number of devices (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 device restart, which might be on the next working day.

### Performing a configuration run

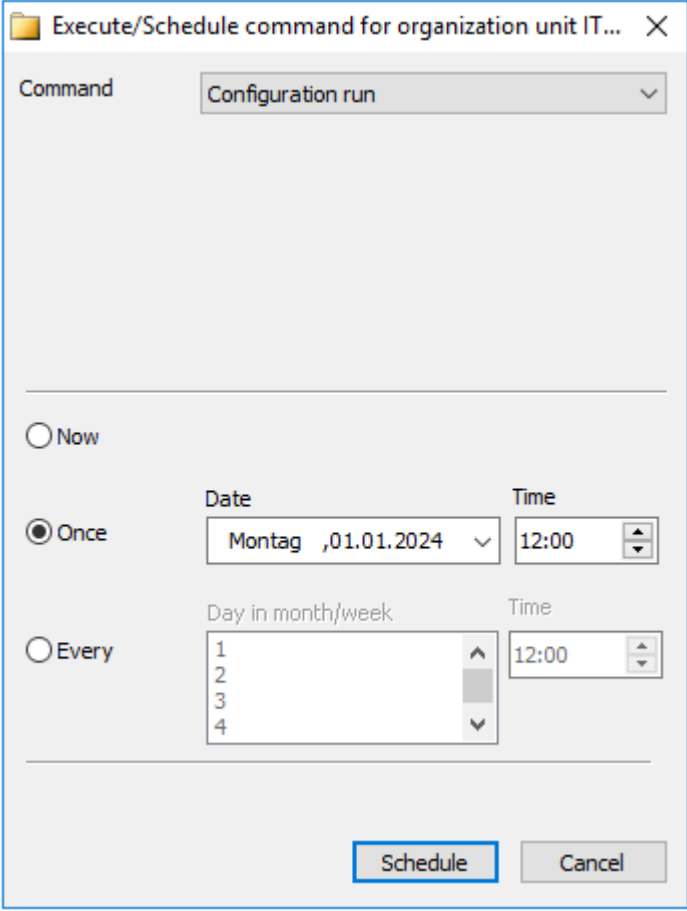
---

#### Note

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

---

1. For the relevant OU or Dynamic Device Group, from the context menu, choose **Commands**.



Execute/Schedule command for organization unit IT... X

Command: Configuration run

☐ Now

☒ Once

Date: Montag ,01.01.2024 Time: 12:00

☐ Every

Day in month/week: 1, 2, 3, 4 Time: 12:00

Schedule Cancel

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

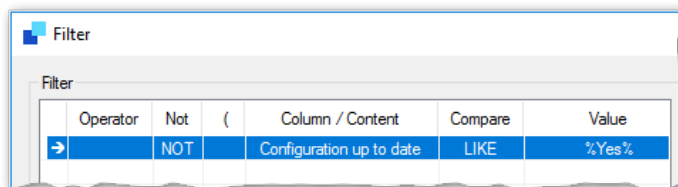
*The processing progress is shown in the **Command history**.*

### 5.3. Evaluating configuration data

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

|                          |   |
|--------------------------|---|
| Configuration ID         | <p>ID for a compressed data object holding configuration data</p> <p>Is created either as a result of a configuration run, or by synchronizing configuration data on the first device to server contact after the configuration settings have been modified</p> |
| Configuration up-to-date | <p>Yes - the device has the configuration that is currently defined for it in the Scout Console</p> <p>No - the device is running an earlier eLux version which cannot evaluate the field</p>   |
| Configuration transfer   | <p>The option <b>Lock configuration transfer</b> is active for the device</p> <p>For further information, see "Locking configuration transfer" on page 65</p>   |

Example:



## 5.4. FollowMe Desktop

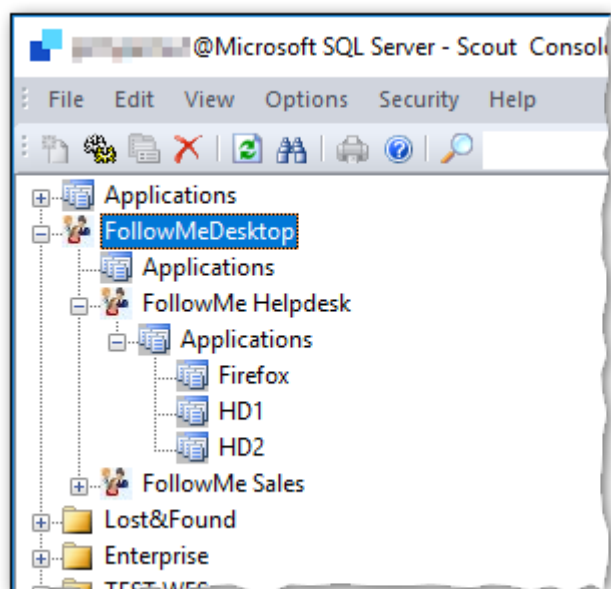
### Note

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 71.

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.*

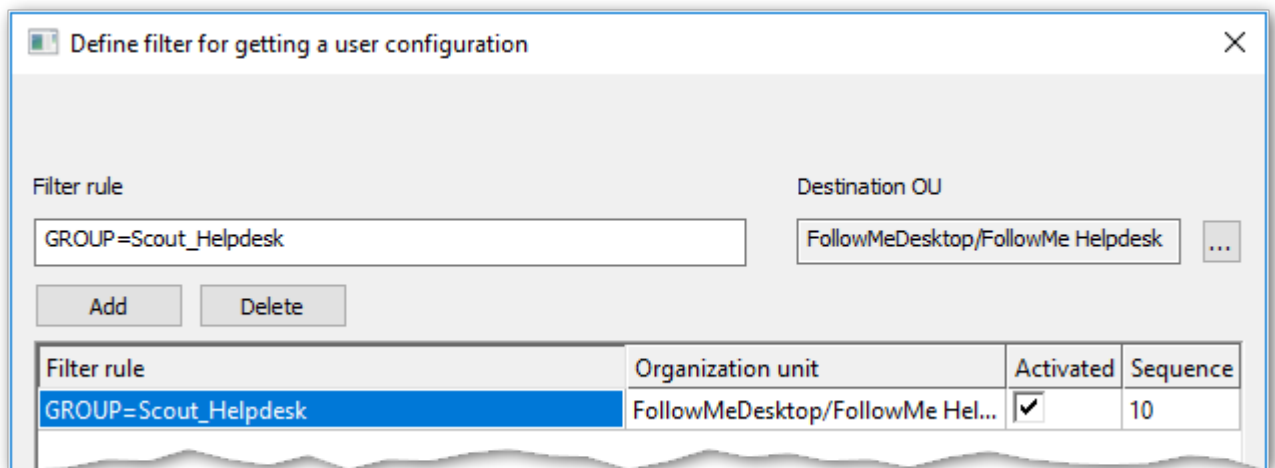
3. For each FollowMe OU, define a filter that filters for an AD membership. To do so, from the context menu, choose **Set filter**.

---

#### Note

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

---



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<br>System bar<br>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.

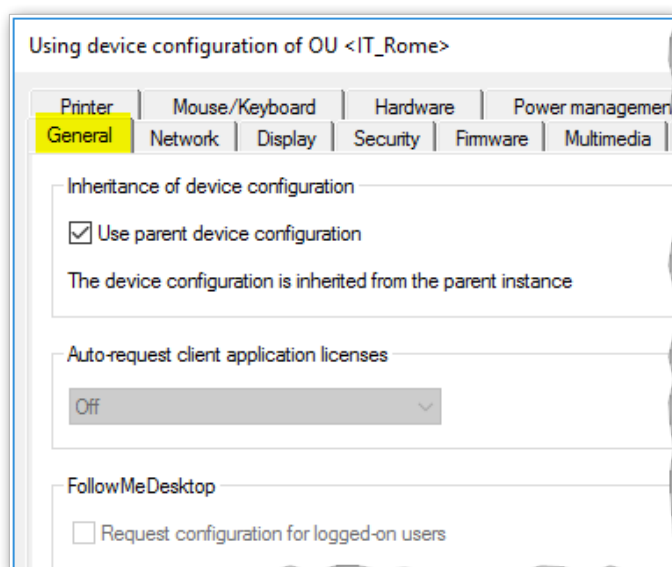
---

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 - independent device configuration" on page 61.

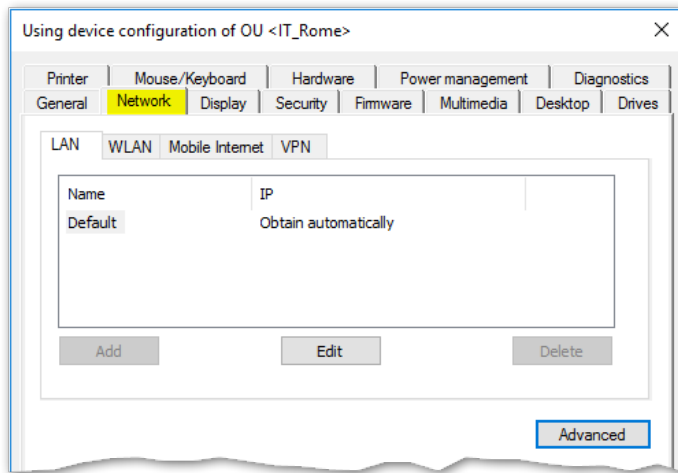
### Additional options

| 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 <b>License information</b> dialog, select <b>Auto-assign</b>. For further information, see <a href="#">Automatic assignment of application licenses</a> in the <b>License management</b> 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" on page 70.</p>  |

Hardware information for individual devices is listed in the **Properties** window of the Scout Console. For further information, see "Properties" on page 16.

## 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)
- VPN<sup>1</sup>

---

### Note

To create VPN network profiles, use the **Advanced device configuration** for individual devices. For further information, see "VPN" on page 170.

---



---

<sup>1</sup>from Scout Enterprise Management Suite 15 2101 For earlier versions, see "VPN" on page 170 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 <b>Advanced</b>, 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, 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         | <p>Define a system-wide proxy server for this network profile, see "Proxy configuration" on page 86.</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:

|   |   |
|---|---|
| Activate  | Enable IEEE 802.1X authentication in general.   |
| Allow LAN connection without 802.1X if 802.1X fails | <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> |
| Number of auto-connect retries                      | Number of connection retries before aborting  |
| Number of authentication retries                    | 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" on page 81.

---

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

Use the **Internet connection test** option to check anytime whether web addresses are accessible via the Internet. For further information, see "Options for all network profiles" on page 85.

### 5.6.2. Advanced network settings

In **Device configuration > Network > Advanced** you will find a Hosts 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 a connection is set up
  - when a connection is in idle state

*After the specified time, the connection will be terminated.*

The option **Send Keepalive packet** ensures that the device sends keepalive signals to the Scout Server in the specified time interval, provided the Scout Keep Alive service is installed. For further information, see "Configuring status messages for devices" on page 318.

#### Defining a Hosts 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.

1. Click **New**.
2. Enter an IP address and one or more host names.

---

##### Note

To specify multiple host names for your IP address, enter the IP names one after the other, separated by spaces. Example:

```
127.0.0.1 host1.domain.com host2.domain.com host3.domain.com
```

---

3. Confirm with **OK**..

*The Hosts list is automatically transferred on the next device restart.*

### 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 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 device. Configured WLAN networks can connect automatically depending on location and priority. For further information, see "WPA support" on page 81.

### Creating a WLAN profile in the Scout device configuration

1. In the Scout Console, for the relevant OU, open **Device configuration > 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   | For further information, see "Options for all network profiles" on page 85.   |
| Medium > Network name/SSID | Wifi name / Service Set Identifier  |
| Medium > Timeout           | Time period in seconds waiting to connect   |
| Medium > Channel           | Selected automatically by default   |

| Option  | Description  |
|---|--|
| Medium > Encryption   | <p>Authentication type</p> <ul style="list-style-type: none"> <li>■ None</li> <li>■ WPA with pre-shared key (PSK)</li> <li>■ WPA2 with pre-shared key (PSK)</li> </ul> <p>To authenticate via EAP (Extensible Authentication Protocol), use a WPA configuration file. For further information, see "WPA support" on the facing page.</p> |
| Medium > Hidden SSID  | <p>Select this option if a WLAN is hidden.</p> <p>Below, the access point MAC address (BSSID) may be entered. If the network has multiple access points, the MAC addresses are separated by semicolons.</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><b>Note</b></p> <p>If you do not use DHCP options for Scout, we recommend that you select <b>Ignore Scout Server DHCP options</b>.</p> |  |
| Advanced / Proxy  | <p>Define a system-wide proxy server for this network profile, see "Proxy configuration" on page 86.</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**.

**Note**

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

**Note**

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

#### 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 devices.

`wpa_supPLICANT` is a free software application. For further information, see [http://w1.fi/wpa\\_supPLICANT/](http://w1.fi/wpa_supPLICANT/).

#### 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 devices, use the Scout feature **Files configured for transfer**. Use the following destination:

|      |             |
|------|-------------|
| LAN  | setup/scep/ |
| WLAN | setup/wlan/ |

For further information, see "Files configured for transfer" on page 173.

#### 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"
    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" on the previous page.

With a corporate WLAN, you can allow users to create their own WLAN profiles in parallel. For example, a mobile device 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 further information, see [Adding a WLAN profile](#) in the **eLux** guide.

### 5.6.6. Defining a Mobile Internet profile (WWAN)

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 > 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 device automatically attempts to connect to the cellular network.  |
| APN                   | Access Point Name: Address used by the device to connect to the Internet when the cellular data connection is used                                     |
| PIN                   | PIN of the SIM card (if used)<br><br>If you leave the field empty and the SIM card requires a PIN, the PIN will be requested on each connection setup. |
| 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 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 170.

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

1. In the Scout Console, for the relevant OU, open **Device configuration > Network**.
2. On the **VPN** tab, click **Add**.

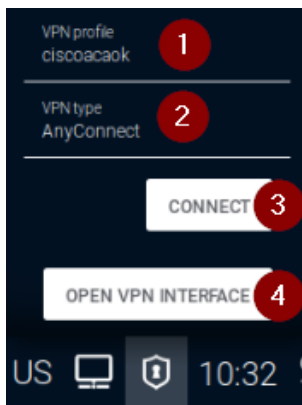
3. In the **Edit network profile** dialog, edit the following options:

| 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 the following options: <ul style="list-style-type: none"> <li><input type="checkbox"/> OpenVPN</li> <li><input type="checkbox"/> CiscoAnyconnect <p>Use this option also for the Cisco Secure Client<sup>1</sup> - both Cisco VPN clients can be used to connect to an AnyConnect VPN.</p> </li> <li><input type="checkbox"/> User-defined VPN client <p>Specify the ID number of your VPN client.</p> </li> </ul> |
| Configuration (only OpenVPN) | Name of the OpenVPN configuration file without file name extension<br>The specified configuration file must be available on the devices.  |

4. Confirm with **OK**.

Note that the eLux devices need to have the VPN software packages and the relevant certificate. A configuration file may be added. For further information on creating OpenVPN and Cisco AnyConnect profiles, see also "VPN" on page 170.

Once users have an active VPN connection, they can use the live information icon on their system bar:



|   |                         |
|---|-------------------------|
| 1 | Name of the VPN profile |
| 2 | Active VPN network      |
| 3 | Connect or disconnect   |
| 4 | Open VPN interface      |

<sup>1</sup>from eLux RP 6 2302.1000

### 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 | <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 (<b>Device configuration &gt; Network &gt; Handling of network profiles &gt; Internet connection test</b>) and by a dedicated user right.<sup>1</sup></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.  |                |   |    |   |     |   |

---

<sup>1</sup>from Scout 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** 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<br>(Proxy:Port)  | Specify fixed proxy server with port number<br>Example: <code>proxy.sampletec-01.com:3800</code><br><br>To define destinations that you do not want to access via proxy, in the <b>Proxy exception list</b> , enter the relevant network addresses separated by semicolons. |
| Auto (URL)  | Proxy auto-config (PAC): Determines the appropriate proxy for each URL<br><br>Examples:<br><code>http://proxy.sampletec-01.com/proxy.pac</code><br><code>http://wpad.sampletec-01.com/wpad.dat</code>   |
| Pass-through<br>logon for proxy<br>(with AD user<br>authentication) | If a central <b>system proxy</b> is configured with AD authentication, the AD logon data are used for authentication.<br><br>Proxy authentication may be required if you use browser content redirection under Citrix.  |
| Proxy username  | Username for authentication on the system proxy   |
| Proxy password  | 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" on page 217.

### 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).

- ▶ To disable IPv6, in the Scout Console, for the relevant devices, 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" on page 178.

### 5.6.11. Firewall for eLux devices

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 devices. This may require modifications of the image definition file on the web server via ELIAS.

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

```
table ip filter {chain input {tcp dport 22 accepttcp sport 80
accept}chain output {tcp sport 22 accepttcp 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** 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 devices. This may require modifications of the image definition file on the web server via ELIAS.

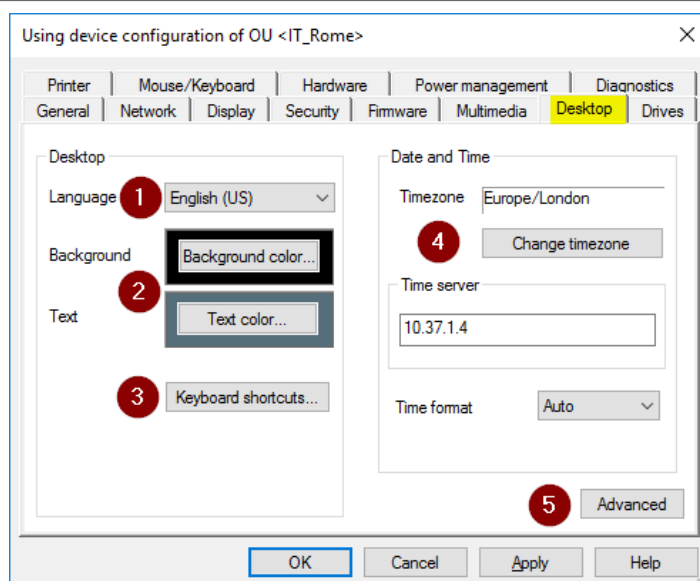
---

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** guide.

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

## 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 > Desktop**.
2. In the **Language** list, click the preferred desktop and application language.

The following languages are supported: English, German, French and Spanish

#### 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. 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 94.

### 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.

## 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<br><br>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             | Log off currently logged-on user (AD users)<br>The logon dialog is then displayed.   | Specify the desired key combination as free-text, see below.   |
| Lock screen         | Activate password-protected screen saver (AD users)<br><br>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.<sup>1</sup> For further information, see "Multiple monitors" on page 98.

## 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`

---

<sup>1</sup>from Scout 15 2101 and eLux RP 6 2101

## Examples

| Option  | Description   |
|---|---|
| <Ctrl><Alt>Escape                                     |   |
| <Shift><Ctrl>l  |   |
| <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<br>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

### Note

May be configured via user interface from Scout 15 2204, see "Advanced mouse and keyboard settings" on page 106.

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 instead of numbers while pressing CAPS LOCK, for the relevant devices, configure the following Advanced file entry:<sup>1</sup>

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

For further information, see "Advanced file entries" on page 178.

*The CAPS LOCK key then behaves like the SHIFT key.*

<sup>1</sup>from eLux RP 6 2107

## 5.7.3. Date and time

| Option                   | Description   |
|--------------------------|---|
| Time zone                | Click <b>Change time zone</b> and select the required time zone from the list..   |
| Time server              | <p>Under <b>Time server</b>, 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 <b>W32Time</b> 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 <a href="http://www.ntp.org">http://www.ntp.org</a>.</p> |
| Time format <sup>1</sup> | <p>The time can be displayed in 24 hour or 12 hour time format.</p> <ul style="list-style-type: none"> <li>• Auto (default)<br/>The displayed time format depends on the configured display language (see same dialog).</li> <li>• 12 hour</li> <li>• 24 hour</li> </ul>  |

## 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.<br>(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.<br>(selected by default)  |

---

<sup>1</sup>from Scout 15 2101 and eLux RP 6 2209

| Option                      | Description  |
|-----------------------------|--|
| Show live information icons | These icons allow users to view current status information such as plugged USB devices via right-click.<br>(selected by default) |
| Show time                   | Shows the current time<br>When users point the mouse to the time, the current date is shown.<br>(selected by default)            |
| Show Config panel icon      | Allows users to open the device configuration (Configuration panel)<br>(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: 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 login.

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

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

| 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"> <li>The following file formats are supported: .svg, .png, .jpg<sup>1</sup></li> <li>Maximum file size 500 KB</li> </ul> |
| Delete                | Remove the current background image from the database.   |
| Set URL               | 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 (active by default)  |
| Timer for shutdown confirmation <sup>2</sup> | <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 <b>Cancel</b> 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                           | <p>Sort order of the desktop icons</p> <p>The administrator can specify the sort order for users without the user right <b>Sorting desktop icons</b>. Users who have this user right can freely place desktop icons on the desktop.</p>  |

#### 5.7.5. eLux RP 6 User Interface

eLux RP 6 devices 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**

<sup>1</sup>.jpg cannot be previewed

<sup>2</sup>from Scout 15 2103 and eLux RP 6 2103

guide.

## Customizing the layout of the eLux RP 6 User Interface

1. For the relevant OU, use the "Advanced file entries" on page 178 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.<br>Example: <code>/setup/public/myPic.png</code><br><br>Option 2 removes the eLux Logo in the lower right section. |

### Note

To show an individual picture file, transfer the picture to the devices. For further information, see "Files configured for transfer" on page 173.

|                              |                           |   |
|------------------------------|---------------------------|---|
| DesktopTextColor             | <code>#&lt;rgb&gt;</code> | Text color of application icons   |
| DesktopHighlightedTextColor  | <code>#&lt;rgb&gt;</code> | Text color of application icons when the mouse pointer is moved over them |
| DesktopTitleTextColor        | <code>#&lt;rgb&gt;</code> | Color of the folder/tab title (All Applications, StoreFront store name)   |
| DesktopSearchTextColor       | <code>#&lt;rgb&gt;</code> | Text color in the search field  |
| DesktopSearchBackgroundColor | <code>#&lt;rgb&gt;</code> | Background color of the search field                                      |
| DesktopSearchIconColor       | <code>#&lt;rgb&gt;</code> | Color of search icon (magnifier)  |
| DesktopSortIconColor         | <code>#&lt;rgb&gt;</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" on page 92.

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

### 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.

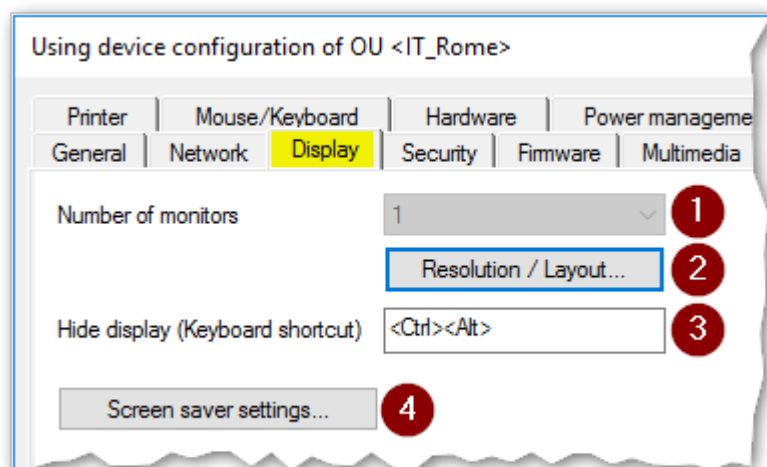
To set a gradient background color, use the RGB values R 102, G 138, B 185.

4. To configure the position of the system bar, 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<br>1: top of the screen |

## 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.



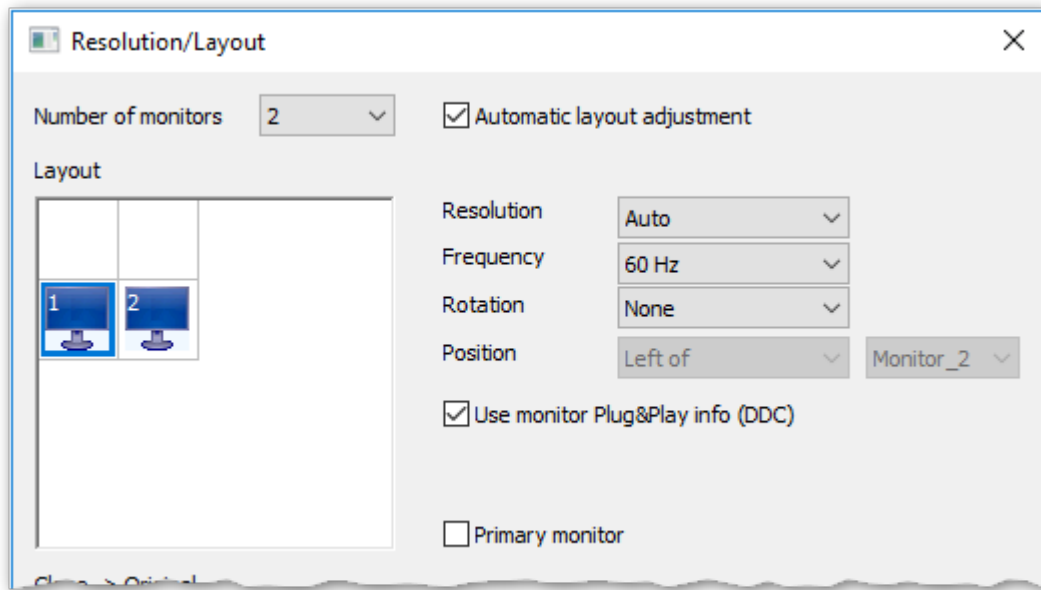
- 1 Define the number of monitors together with further display options in the **Resolution/Layout** dialog.
- 2 Configure the display:
  - Display options per monitor
  - Multiple monitors
- 3 Keyboard shortcut to hide/show the content of a monitor
- 4 Select and configure a screen saver

### Note

Power saving options can be found on a dedicated tab, see "Power management tab" on page 154.

### 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.



- 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 <code>dbo.Resolution</code> . 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  |

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

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

#### Note

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

- To define the selected monitor as the primary one, select **Primary monitor**.
- 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

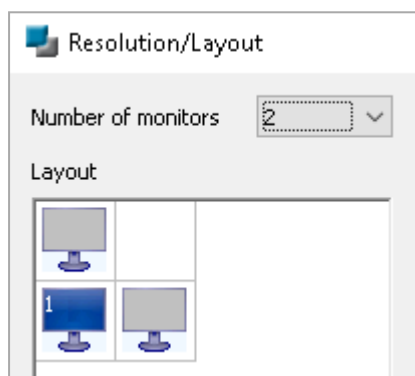
1. In **Device configuration > Display**, click **Resolution/Layout** to open the dialog of the same name.

*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 devices.

*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.

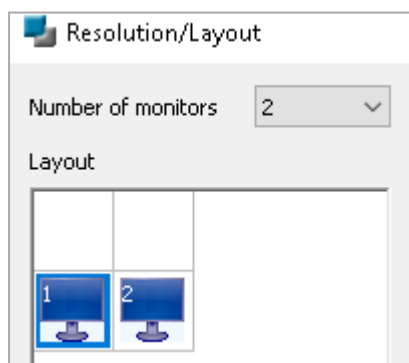
*The selected monitor icon is shown in blue with the number 2.*

---

### 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**.

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

**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

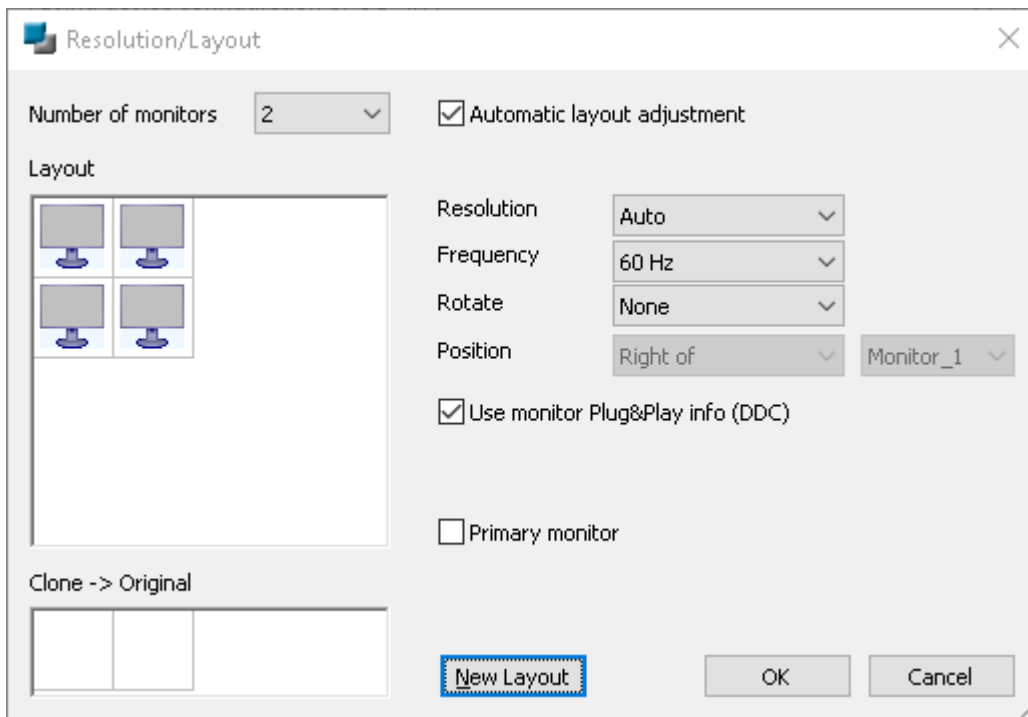
To define the position of the first monitor, use a new layout.

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

*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:*

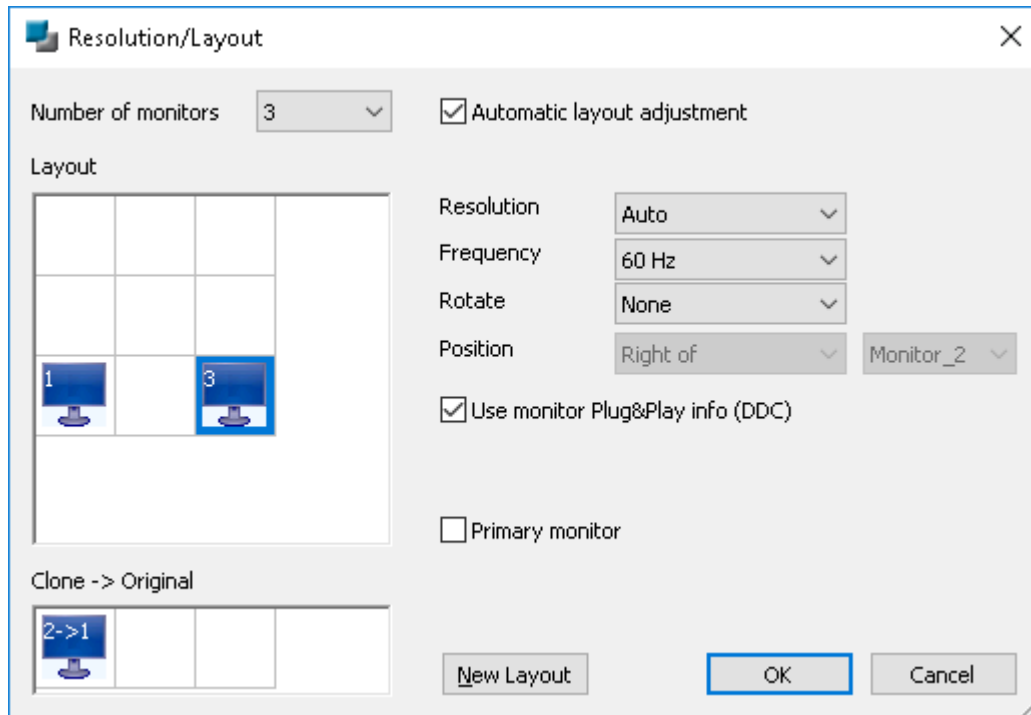


3. Double-click the desired monitor position for the first monitor. Then, double-click the desired monitor positions of the remaining monitors.

## 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 from the context menu, choose **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 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" on page 178 in the **Scout** 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.

---

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.

### 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.

---

The password is set to `$ELUXPASSWORD`. For further information, see "Where to apply user variables" on page 133.

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     |

---

| 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: File: <code>/setup/terminal.ini</code>, <b>section:</b> <code>xscreensaver_dialog</code>, <b>entry:</b> <code>MessageEnabled</code>, <b>value:</b> <code>false</code></p>  |
| Another user authenticates to log off the previous user (and to log on), restart or shut down the device. | 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 <b>Restart</b>, <b>Shut down</b> and <b>Log off</b> 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>, <b>section:</b> <code>xscreensaver_dialog</code>, <b>entry:</b> <code>ShowSysCommandButtons</code>, <b>value:</b> <code>true</code></p> |

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

## Downloading picture files for screen saver

Optionally, Scout administrators may configure direct download of picture files to the devices 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 devices. 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`

- For the relevant devices, 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 | <code>/setup/terminal.ini</code> |
|------|----------------------------------|

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

For further information, see "Files configured for transfer" on page 173.

*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 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:

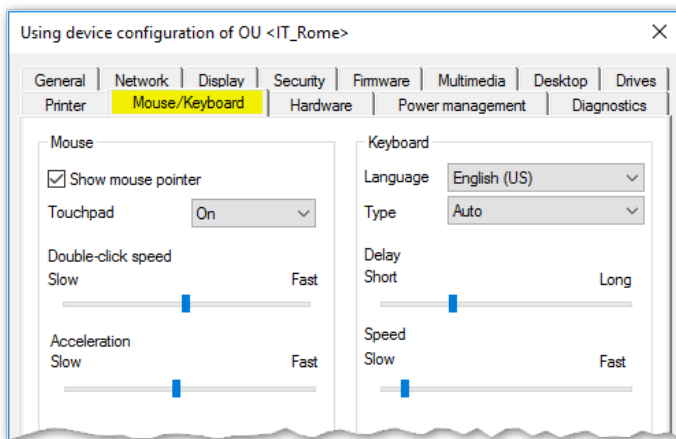
|   | Option  | Default keyboard shortcut |
|---|---|---------------------------|
| 1 | Hide display of primary monitor               | <Ctrl><Alt>1              |
| 2 | Hide display of second and all other monitors | <Ctrl><Alt>2              |

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 89.

## 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.<br>The mouse type is automatically identified.  |
| Touchpad (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.  |

### 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                                       | <p>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 =&gt; à ).</p> <p>Note: Some hardware platforms and some applications do not support this option.</p>                                  |    |  |     |   |      |   |
| Console switch                                  | <p>Users can use key combinations to switch between consoles.</p> <p>If the option is not selected, console 1 (eLux desktop) is always shown.</p> <p>For further information, see <a href="#">Shortcuts</a> in the <b>eLux</b> guide.</p>  |    |  |     |   |      |   |
| Extended keys                                   | Enables multimedia keys and other keys with special functions on the keyboard.   |    |  |     |   |      |   |
| Handle Caps Lock always like Shift <sup>1</sup> | With CAPS LOCK being activated, the number keys above the letter block output special characters instead of numbers. So these keys behave in combination with CAPS LOCK in the same way as in combination with SHIFT. For further information, see "Keyboard shortcuts" on page 89.  |    |  |     |   |      |   |
| Num Lock  | <table> <tr> <td>On</td><td>Enables the numeric keypad of the keyboard on device start (default)</td></tr> <tr> <td>Off</td><td>Disables the numeric keypad of the keyboard on device start</td></tr> <tr> <td>Auto</td><td>Enables the numeric keypad on mobile devices and disables it on other devices</td></tr> </table> | On | Enables the numeric keypad of the keyboard on device start (default) | Off | Disables the numeric keypad of the keyboard on device start | Auto | Enables the numeric keypad on mobile devices and disables it on other devices |
| On  | Enables the numeric keypad of the keyboard on device start (default)   |    |  |     |   |      |   |
| Off   | Disables the numeric keypad of the keyboard on device start  |    |  |     |   |      |   |
| Auto  | 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 device restart.*

---

<sup>1</sup>from Scout 15 2204

## 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 VPN<sup>1</sup>
- 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 installed<sup>2</sup>
- 7 From 1-4 a URL is generated, which is used by the devices to update the firmware.  
If the web or FTP server is password-protected, the user name and parametrized password are also included in the URL.
- 8 If a UEFI file is specified, the system generates a URL which is used by the devices to update the UEFI system.

<sup>1</sup>from Scout 15 2107 and eLux RP 6 2204

<sup>2</sup>from Scout 15 2107

**Note**

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


The image file, UEFI file and container path can be predefined globally by the administrator so that you may select them from the respective list-field. For further information, see "Predefined IDs and containers" on page 167.

### 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**.
2. Edit the following fields:

| Option                                    | Description   |
|---|---|
| Protocol                                  | Network protocol of the web server for software package transfer to the devices ( <code>HTTP</code> , <code>HTTPS</code> , <code>FTP</code> , <code>FTPS</code> )   |
| Server                                    | Name (FQDN) or IP address of the web server containing the eLux software packages and the image definition file   |
| 2nd web server for VPN devices (optional) | Click  to specify an alternative web server for devices connected via VPN: <sup>1</sup> Choose the protocol ( <code>HTTP</code> or <code>HTTPS</code> ) <sup>2</sup> and enter the server name as FQDN or IP address. The system displays a message if the name cannot be resolved or the IP syntax is incorrect.  |
| Proxy (optional)                          | <p>Static (Consumer): IP address and port number (3128) of the proxy server<br/> Format: <code>IP address:port</code><br/> Example: <code>192.168.10.100:3128</code></p> <p>Dynamic: Within the subnet, one of the devices is automatically used as a proxy device.</p> <p>Note that for the definition of a static proxy device, from Scout 15 2204 the entry <code>None</code> must be selected. For further information, see "Static proxy" on page 300.</p> |
| User and Password (optional)              | Username and password (if required) to access the eLux software container of the web or FTP server  |

<sup>1</sup>from Scout 15 2107 and eLux RP 6 2204

<sup>2</sup>from Scout 15 2204

| Option                                    | Description  |
|---|--|
| Path                                      | <p>Directory path of eLux software packages on the web server</p> <p>Use slashes / to separate directories.</p> <p>For ELIAS 18, specify the path name defined during installation.<br/>Example: <code>elias/UC_RP6_X64</code></p> <p>For the legacy ELIAS, use <code>eluxng/&lt;container name&gt;</code></p> <p>To account for different eLux major versions, use a specific parameter. For further information, see "Different eLux versions" on page 113.</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 image file name may be specified or an image must be selected from the list-field. For further information, see "Protecting firmware configuration" on the next page.</p> <p>To account for specific hardware models, use the release parameter. For further information, see "Different hardware models" on page 111.</p> <p>To update devices with an earlier partition layout to a current version with an extended system partition, see "Update to new partition layout" on page 115.</p> |
| Check for new version on start / shutdown | <p>The device checks during start or shutdown whether any firmware updates are available and necessary.</p> <p>To allow users to decline or defer an update on start-up, specify the <b>User confirmation</b> options. For further information, see "Updates initiated by the system" on page 289.</p>   |
| ELIAS... button                           | Starts the ELIAS tool and opens the image definition file indicated in the <b>Image file</b> field   |
| Security... button                        | The <b>Security settings</b> allow you to define a signature check before update through the device. Signature checks can be performed for the image definition files and/or eLux software packages.   |
| Reminder... button                        | <p>The <b>Reminder Settings</b> 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.</p> <p>For further information, see "Update deferment by users" on page 120.</p>  |

- Test the **Firmware** settings on a device . 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 systems<sup>1</sup> 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 alternative to selecting a predefined entry from the list-field.



#### Requires

Administrator policies are enabled.

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

|                              |  |
|------------------------------|--|
| Image file<br>(predefined)   | <p>The administrator can only select one of the IDFs provided in the <b>Image file</b> list-field on the <b>Firmware</b> tab.</p> <p>The list-field contains predefined IDFs (see below). If predefined IDFs are missing, the list-field shows the recently used IDFs.</p> |
| Image file<br>(user-defined) | <p>The administrator is allowed to enter any IDF name into the text field.</p>   |
| Path (pre-defined)           | <p>The administrator can only select one of the paths provided in the <b>Path</b> 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>                              |

<sup>1</sup>from eLux RP 6 2107

|                          |  |
|--------------------------|--|
| 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 <b>UEFI file</b> 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) | <p>The administrator is allowed to enter any UEFI file name into the text field.</p>   |

4. Confirm with **OK**.

For further information, see "Administrator policy" on page 309.

## Predefining Firmware configuration values

1. On the menu, click **Options > Advanced options > Predefined IDFs**.
2. To add additional IDF names, click the **Add** button and edit the new entry. Note that the spelling must match the actual names.
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 does not check the physical existence of files or container paths on the web server.

For further information, see "Predefined IDFs and containers" on page 167.

## 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 parameter 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 parameter, in the firmware configuration, an `__RM__` string is inserted into the image file name.

Before an update is executed, an appropriately configured device resolves the parameter 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: `revcovery__RM__.idf`

---

### Note

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

---

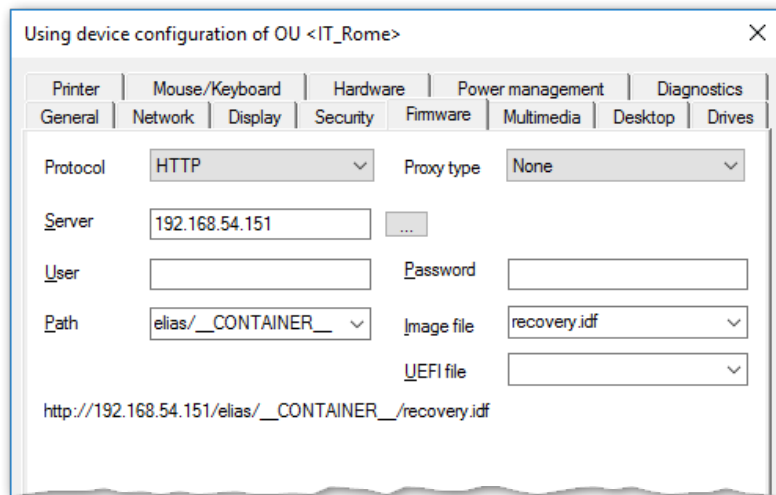
3. Confirm with **Apply** and **OK**.

*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 a container parameter, the parameter is resolved by a macro according to the installed eLux version.

Example:

If you run devices with both, eLux RP 6 and eLux 7, the eLux RP 6 devices require the `UC_RP6_X64` container, while the eLux 7 devices require the `UC_ELUX7` container. To provide all devices with their appropriate software, in **Device configuration > Firmware > Path** of all devices, use the `___CONTAINER___` parameter. The devices then resolve the container parameter according to their installed major version to `UC_RP6_X64` or `UC_ELUX7`, 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 6 and for eLux 7.

### 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:

| Major eLux version | Container name          |
|--------------------|-------------------------|
| eLux RP 6          | <code>UC_RP6_X64</code> |
| eLux 7             | <code>UC_ELUX7</code>   |

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. Update to new partition layout

Earlier eLux RP 6 versions up to eLux RP 6 2104 LTSR have created smaller system partitions during installation than current eLux versions. Beginning with eLux RP 6 2107, the system partition is created with 2.35 GB with encryption and with 2.41 GB without encryption, so that larger images can be included. For further information, see "eLux partitions" on page 333.

For updating the firmware of devices with eLux RP 6 2104 LTSR to the current eLux RP 6 version,<sup>1</sup> the system partition must be repartitioned before the actual update installation. In order to still be able to perform an update installation in one step, the solution described below uses two images to which devices are updated, one after the other. The second firmware update is automatically triggered.

#### Note

When you start from eLux RP 6 2104 LTSR CU3 or CU4, the intermediate and final image will be based on the latest eLux version and you can follow the instructions below. When you start from eLux RP 6 2104 LTSR CU1 or CU2, the intermediate image must be based on a different eLux version. In this case, please contact our support for more details.

### Two images as prerequisites

|         | Image with Partition Resize parameter   | Final image   |
|---------|---|---|
| Size    | Corresponds to the old world with a maximum of 1.77 GB  | May have a size over 2 GB   |
| Content | <ul style="list-style-type: none"> <li>Current <b>BaseOS</b> package</li> <li>Specific eLux software package named <b>Update Support Utility</b> which automatically triggers the second update on the devices</li> </ul> | <ul style="list-style-type: none"> <li>All packages from the first image</li> <li>Additional packages that did not fit into the first image (optional)</li> <li><b>No Update Support Utility</b>-package</li> </ul> |

<sup>1</sup>from eLux RP 6 2110

|      | Image with Partition Resize parameter   | Final image  |
|------|---|--|
| Name | Must contain the <code>__PR__</code> parameter as a string so that the macro can be executed later on<br><br>Example: <code>recovery__PR__.idf</code> | Same name as first image, but without the <code>__PR__</code> string<br><br>Example: <code>recovery.idf</code> |

Both images must be in the same container.

## Procedure

For the update installation of your devices you only start the update to the first image with **Partition Resize** parameter. After that it's the system's turn:

- The first update process installs the current eLux version without running the macro. The devices now have the first image on board. After installation, the **Update Support Utility** package triggers another update.
- On the second update request, the current eLux version on the devices identifies the **Partition Resize** parameter and runs the macro:
  - The `__PR__` string will be removed from the update URL.
  - An update to the final image will be performed.

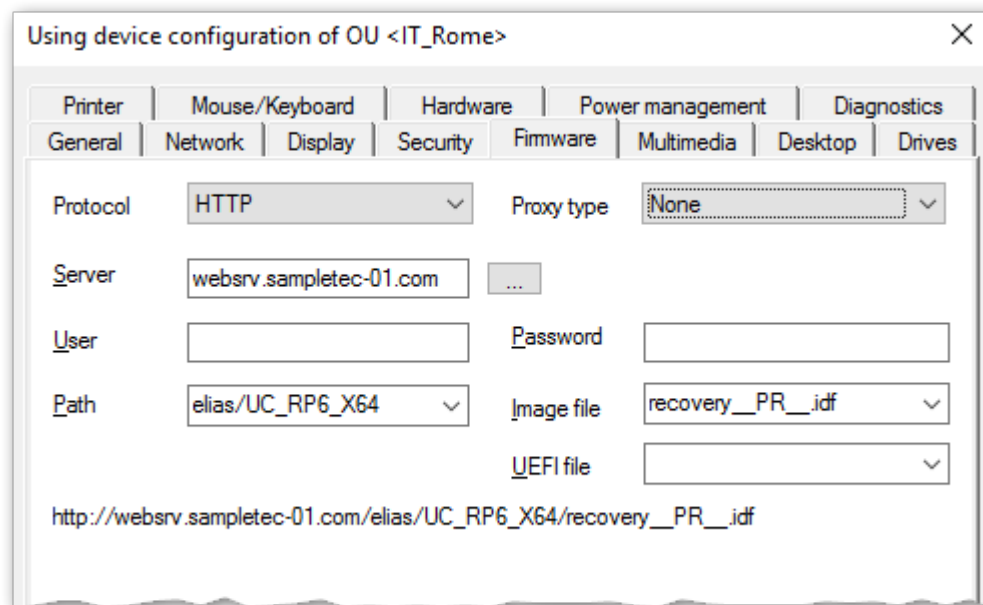
### Note

The automatic update to the final image is always performed without formatting the system partition. This is independent of whether the option was set during the first update.

- The **Update Support Utility** package will be uninstalled because it is not included in the final image.

## Configuring firmware updates with Partition Resize parameter

1. In ELIAS, create an image with **Partition Resize** parameter. Follow the specifications from the table above. The image file name must contain the string `__PR__` on any position.  
Example: `recovery__PR__.idf`
2. In ELIAS, in the same container, create a second image which will be used as the final image. Follow the specifications from the table above. The image name must match the first image name, but must not contain the string `__PR__`.  
Example: `recovery.idf`
3. In the Scout Console, for the relevant OU, open **Device configuration > Firmware**.  
In the **Image file** field, enter the name of the first image (the one with `__PR__` parameter).



The image file specified in the figure above requires the existence of a second image named `recovery.idf` which is the final image.

Edit the other fields of the **Firmware** tab. For further information, see "Configuring firmware updates" on page 108.

4. For the relevant OU, perform a firmware update.

*The devices update to the first image with current eLux version. Then, the **Update Support Utility** package triggers a second automatic update that installs the final image on the devices. This automatic update is retried on each system restart until a successful installation uninstalls the **Update Support Utility** package.*

*For devices connected via VPN, the automatic update is triggered only after the VPN tunnel is established. The installation is performed without user interaction.*

## Spelling of the Partition Resize macro string

Make sure to use the correct spelling:

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

### Note

You can use the **Partition Resize** parameter in the firmware configuration or in the recovery settings **Options > Recovery settings...**

## 5.10.6. Firmware security through signatures

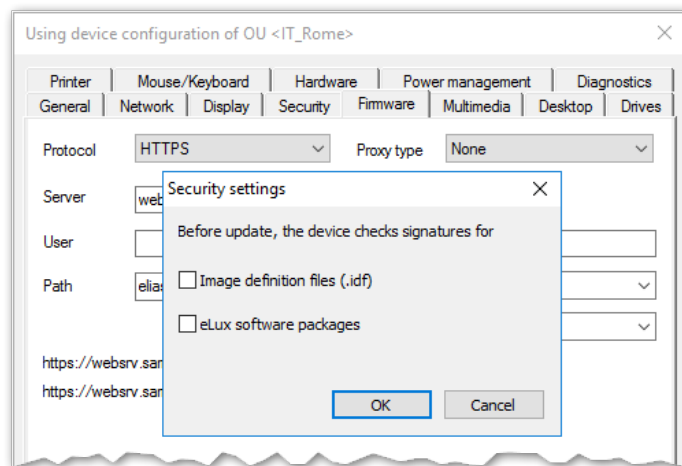
You can configure the firmware configuration in the Scout Console or on the device to have the device check signatures each time before an update is performed. An update is then only performed if the signature of the image definition file (IDF) and/or the signature of the eLux software packages

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 device. 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](#).

## Activating signature check

1. In the Scout Console, under **Device configuration > Firmware**, click **Security...**  
On the eLux RP 6 device, 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**.

### Note

In eLux, both options are provided in the Config panel, under **Firmware**.

*The signature verification results are documented in the update log file on the device. 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 device directory `/setup/cacerts`. If you use own certificates for signing IDFs or individually composed eLux packages, configure their transfer to the devices. To do so, use the Scout feature **Files configured for transfer**. For eLux packages provided by Unicon, all required certificates are included in the BaseOS.

---

**Note**

When updated code signing certificate are made available on our technical portal, download and import them into ELIAS. Instructions are included.

---

For further information on how to create image signatures, see [Signing an image](#) in the ELIAS 18 guide.

### 5.10.7. Update deferment by users

- applies to firmware updates (software) and UEFI updates<sup>1</sup> -

This feature allows users to determine the update time as soon as an update is requested. This allows users to avoid updates while using the device.

With the deferment options, users may postpone updates that are initiated by an administrator's **Update** command or by the system-side **Check for new versions on start** configured in the **Firmware** settings.<sup>2</sup>

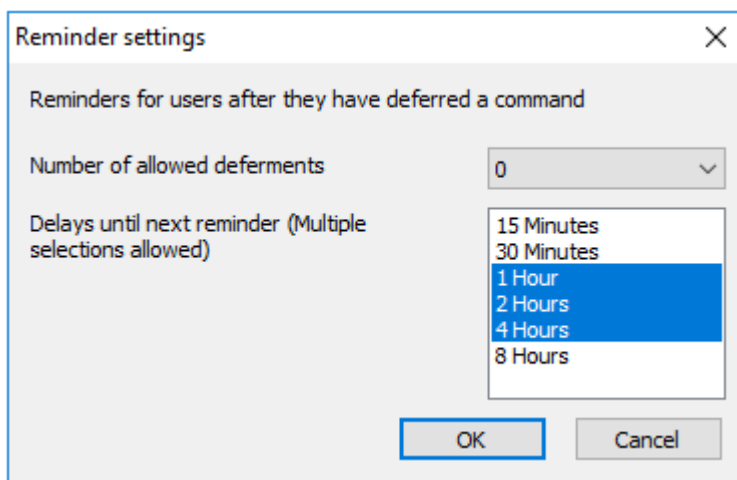
#### Note

A device 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 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.



*Users now are basically allowed to defer updates. When an admin performs an **Update** command with the **Inform user** option, the user will receive a system message including deferment options. The same applies when firmware updates are triggered by the **Check for new version on start***

<sup>1</sup>from eLux RP 6 2107

<sup>2</sup>from Scout 15 2104.3000 and Scout 15 2209 with corresponding eLux versions

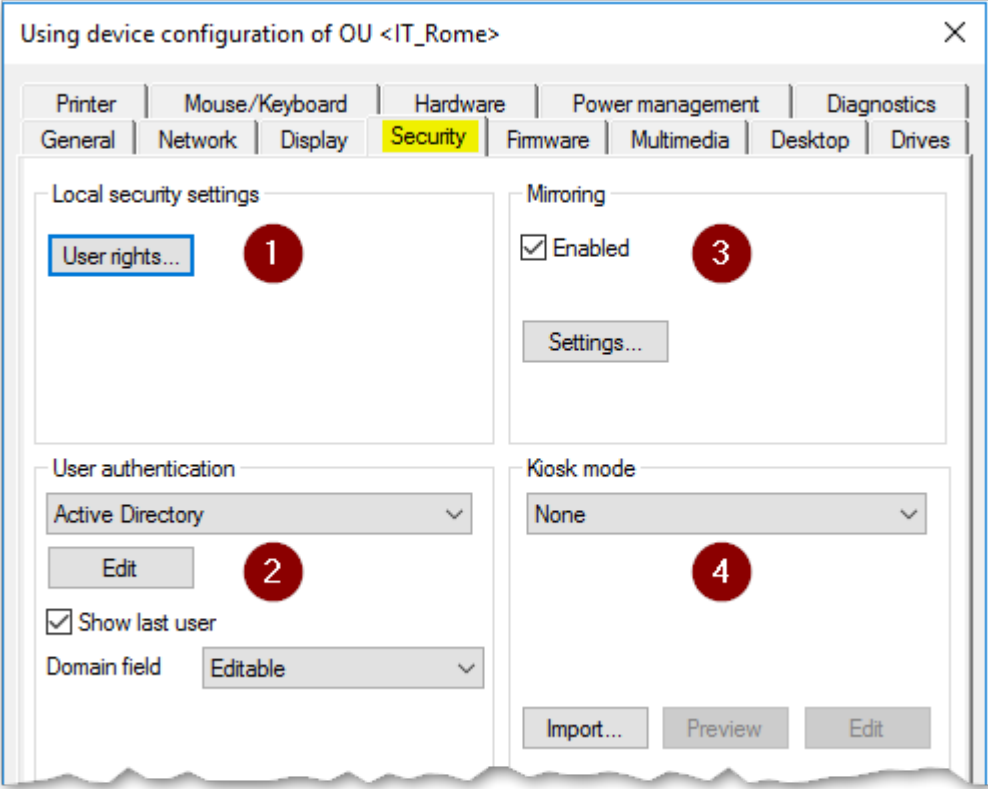
option with user confirmation.<sup>1</sup> For further information, see "User information before update" on page 291.

**Important** Update deferment must be configured on the **Firmware** tab. In addition, for each **Update** command administrators run, in the **Command** dialog, they must select the **Inform user** option. For further information, see "Performing updates via command" on page 288.

---

<sup>1</sup>from Scout 15 2104.3000 and Scout 15 2209 with corresponding eLux versions

## 5.11. Security tab



- 1 Define end-user rights to functions
- 2 Configure Identity provider and logon procedure for users
- 3 Configure mirror sessions
- 4 Configure kiosk mode

### 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

In addition to configuring user rights, you may hide various elements of the desktop via the device configuration. In addition to configuring user rights, you can hide various elements of the desktop via the device configuration. For example, you can hide the icon for opening the Config panel. For further information, see the **System bar** settings under "Advanced desktop settings" on page 92.

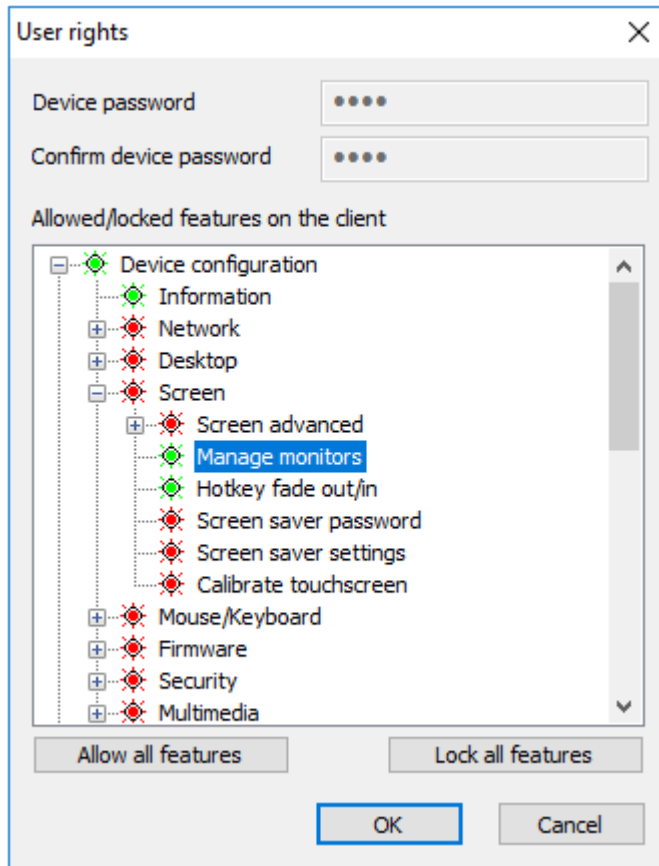
User rights are available for the following functions:

- 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 **Device configuration > Security > Scout settings**,<sup>1</sup> you will find options for the fields **Info1**, **Info2** and **Info3**.<sup>2</sup> These **Info** fields are shown in the Scout Console in the **Properties** window of a device, and on the eLux RP 6 devices, they are displayed in the **Configuration panel** under **Information**.

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 device restart.*

<sup>1</sup>on eLux RP 6 devices under Device configuration > Security > Info 1-3

<sup>2</sup>One user right for all three Info fields

## Modifying user rights for application definitions

1. In the **User rights** dialog, expand the **Application definition** 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.*

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 "Supporting local configuration" on page 62 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 device restart.*

## Local device configuration

If you allow local device configuration for some features, note that fields configured by users may be overwritten by the values set on the Scout-side when the device configuration is updated. To prevent this, protect the relevant fields or tabs using the provided option. For further information, see "Supporting local configuration" on page 62 .

### 5.11.2. 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.

---

- 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 <b>Read only</b> 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 only     | Mirroring is only allowed if the Scout Console is used.   |
| Log off on disconnection  | Automatic logoff as soon as the connection is aborted   |

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

For further information, see "Mirroring" on page 272.

### 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.

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.

### 5.12.1. Configuring user authentication

#### Note

The eLux package **User authentication modules** must be installed on the devices. 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          | 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 `LocalLogin` username and device password to correct any settings, if required.

## Active Directory (AD)

Define multiple domains that can be displayed with friendly names. In the logon dialog on the devices, 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:</p> <pre>int.sampletec-01.com dev.sampletec-01.com</pre> <p>If the server is not located in the same subnet as the device, 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 device. 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 device 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" on page 133.

## Automated logon tab

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 devices. 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 <b>Lock screen</b> , in the <b>Screen saver</b> settings, <b>Password protected</b> will be selected.   |
| Allow logon with user-name+password      | Smart card application allows user/password logon via the <b>User-name &amp; Password</b> link.   |
| Show Username+password dialog by default | Logon via username + password can be forced despite smart card configuration.<br><br>To use this option, enable <b>Allow logon with username+password</b> . |

## 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" on page 133.

For the **AD directory** and **Automated logon** tabs, see "Active Directory (AD)" on the previous page.

## 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.** 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 devices.

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

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 131.

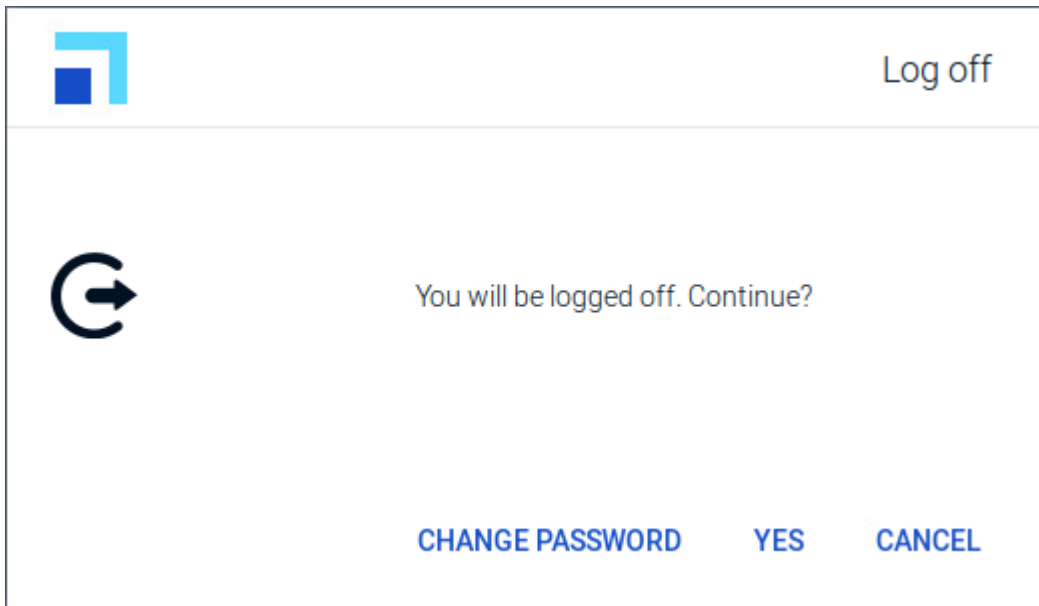
## 5.12.2. Additional options for AD users

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.

### 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.

The password is set to `$ELUXPASSWORD`. For further information, see "Where to apply user variables" on page 133.

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  |
| 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: File: <code>/setup/terminal.ini</code>, <b>section:</b> <code>xscreensaver_dialog</code>, <b>entry:</b> <code>MessageEnabled</code>, <b>value:</b> <code>false</code></p>  |
| Another user authenticates to log off the previous user (and to log on), restart or shut down the device. | 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 <b>Restart</b>, <b>Shut down</b> and <b>Log off</b> 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>, <b>section:</b> <code>xscreensaver_dialog</code>, <b>entry:</b> <code>ShowSysCommandButtons</code>, <b>value:</b> <code>true</code></p> |

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

## Service app

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" on page 194.

## Starting Configuration panel from logon dialog

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**.

*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 devices. 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 | Enable screen saver<br>(also manual activation) | \$ELUXPASSWORD      |

## Application definition

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

## 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**, select `Active Directory (AD)` or `Active Directory + Smartcard`.
2. Click **Edit**.

- 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.

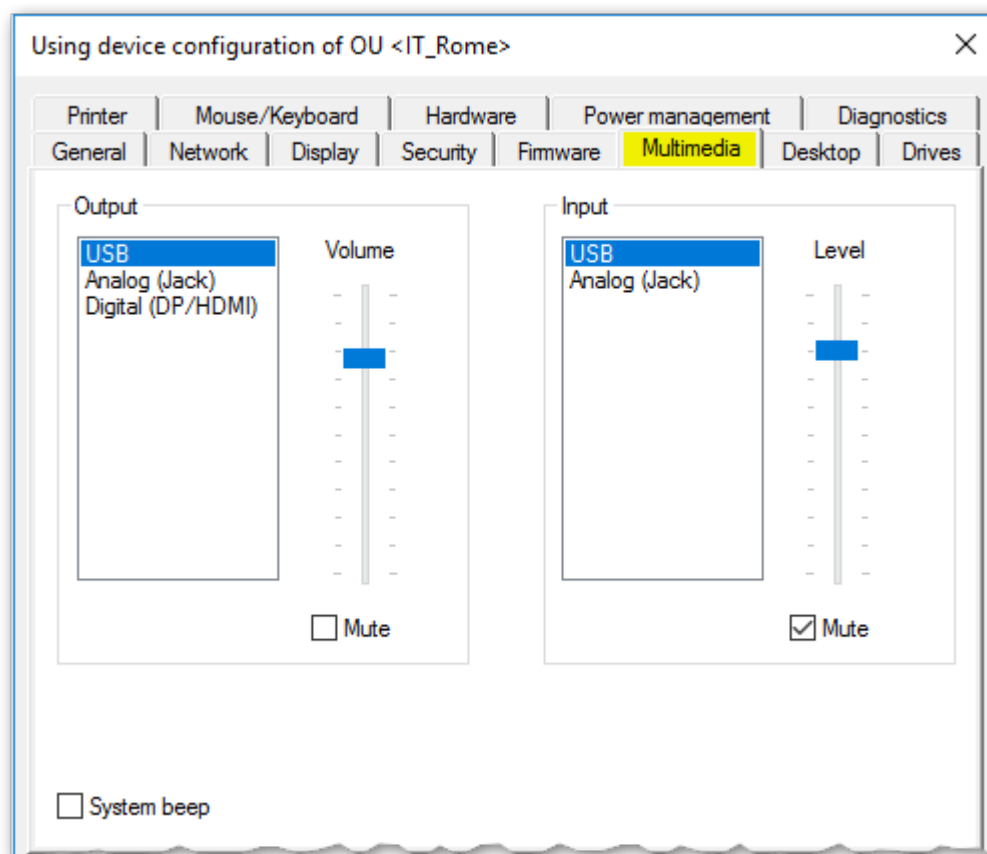
The audio **input** devices are grouped in classes depending on their connector:

|        |  |
|--------|--|
| 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 device   |
| 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 devices. 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 <b>User</b> field:<br><Domain\User> or <User@Domain>  |
| AD authentication<br>(only Scout) | The Active Directory logon data are used to access the directory.<br>The fields <b>Username</b> and <b>Password</b> are disabled. |
| Test<br>(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 devices. 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`

Define drives

Directory: share

Server: storage.int.sampletec-01.com

Share: share\users\div

User: int\mimi

Password: ••••••••

Domain: int

☐ Use Active Directory authentication

OK Cancel

### Note

Here, you may apply LDAP user variables. For further information, see "Where to apply user variables" on page 133.

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" on page 222.

## 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 tab" on page 147.

---

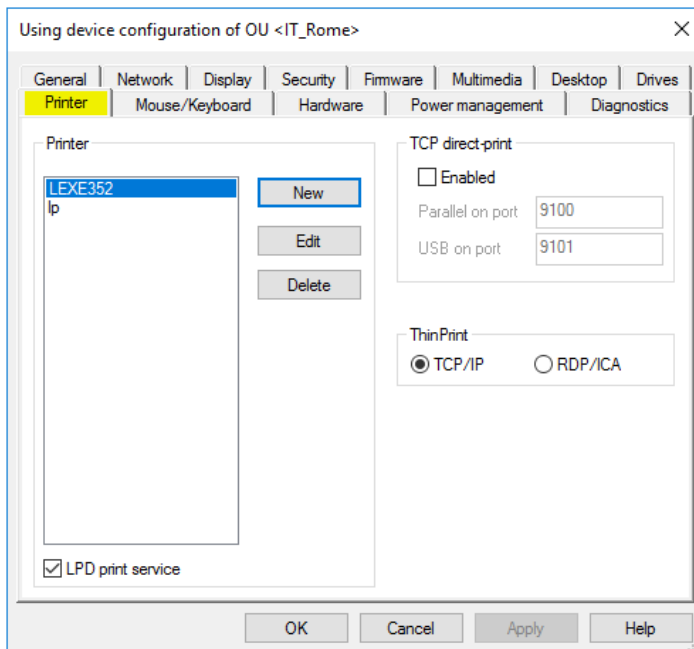
**Note**

Drive mapping for access to local resources must be defined in the relevant application definition. For Citrix ICA applications, see "Citrix software defaults" on page 204. For RDP applications, see "Advanced application settings / RDP and VMware" on page 211

---

## 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 device 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 device.
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" on the next page.
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<br>If the users do not print from a Citrix session, the connected printer must support one of the following languages: <b>PCL2</b> , <b>PS(Postscript)</b> or <b>PDF</b> . |

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" on page 145.

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 > 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 device. 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 > 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.*

### 5.15.5. CUPS

The CUPS server is installed by default on the devices (**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](http://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 device (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 devices. 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 device:

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 device 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 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 device.

---

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

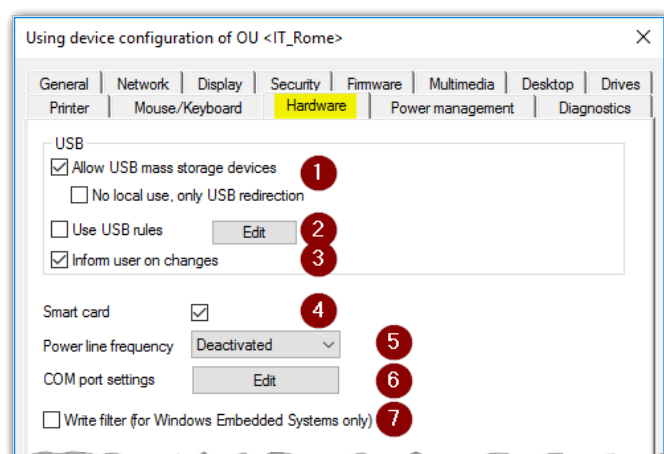
ThinPrint software from ThinPrint GmbH allows optimized network printing across various platforms. ThinPrint is a print protocol that, unlike TCP direct print, LPR or CUPS, allows bandwidth limitation. It is therefore recommended for networks with low bandwidth (WAN).

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 device 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 > 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](http://www.thinprint.com).

## 5.16. Hardware tab



### 1 Allows using connected USB mass storage devices

If the local use of USB devices via mount points is allowed, connected USB devices are shown as a live information on the system bar.

Select **No local use, only USB redirection** to restrict the use of USB mass storage devices to USB redirection within configured sessions on a backend. There are no mount points then provided locally on the eLux device.

### 2 Restricts the use of USB mass storage devices according to defined rules:

For example, you can restrict to devices with specific VID (Vendor ID) and/or PID (Product ID) such as an individual USB stick model. Moreover, USB rules can be applied to further USB device classes such as smart card readers.

To define USB rules, click **Edit**.

### 3 When a USB mass storage device is connected or disconnected, a live information message is displayed.

### 4 Enables smart card readers on a USB port

### 5 Allows to change the refresh rate of webcams to 50 Hz or 60 Hz

### 6 Set particular COM port settings such as speed, parity, stop bits

### 7 Users are not allowed to store local data on their Windows Embedded device.

## Note

To enable users to use smart card readers, ensure to install the relevant middleware on the devices. **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 devices. This may require modifications of the image definition file on the web server via ELIAS.

To display hardware information about the device itself or about connected (USB) devices, use the **Properties** window with the **Assets** tab for a selected device, see "Hardware information" on page 19.

### 5.16.1. Defining rules for using USB devices

USB rules allow you to restrict the use of USB mass storage devices to certain models, for example.

1. For the relevant OU or device, open **Device configuration > 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  | v |
| Information   | ^ |
| N48/M-BB48/M-UK96A [FirstMouse Plus]                                | v |
| USB Keyboard  | v |
| USB Optical Mouse   | v |
| SanDisk 3.2Gen1   | ^ |
| Product name<br>SanDisk 3.2Gen1                                     |   |
| Vendor name<br>SanDisk Corp.  |   |
| Serial number<br>0101394ca12729398929f56b9698f1b00c154c74f2a3edf... |   |
| Product ID<br>55a3  |   |
| Vendor ID<br>0781   |   |
| Type<br>Mass storage  |   |
| Mountpoints   Free space<br>/media/usbdisk   27.81 GB of 28.64 GB   |   |

5. Confirm with **OK**.

## Example rules

| Rule   | Code  |
|--|---|
| Allow a specific USB mass storage device model only          | <pre>ALLOW: VID=0781 PID=5151 # Allow a 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 a 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>  |
| Disable the microphone of a webcam                           | <pre>DENY: VID=045e PID=0810 CLASS=01 # Deny audio for the specified USB device</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 device will be affected. For specific hardware configurations, you might encounter issues during the boot process of the device. We strongly recommend performing tests before using this option.

### 5.16.2. Defining rules for USB redirection

For the Citrix Workspace-App 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                | ALLOW: VID=0781 PID=5151<br>DENY: CLASS=08                                       |
| VMware      | /setup/elux/.vmware/default-config | viewusb.ExcludeFamily = "storage"<br>viewusb.IncludeVidPid = "vid-0781_pid-5151" |

2. To transfer the configuration files to the devices, use the Scout feature **Files configured for transfer**. For further information, see "Files configured for transfer" on page 173.

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

### 5.16.3. 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 bar 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 devices, 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" on page 178.

### 5.16.4. Enabling Bluetooth audio devices

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 devices, configure the following Advanced file entry:

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

For further information, see "Advanced file entries" on page 178 in the **Scout** guide.

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

### 5.16.5. 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.<sup>1</sup>The app supports multiple

---

<sup>1</sup>from eLux RP 6 2107

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 "Defining custom applications" on page 225.
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.*

### Note

To disable the microphone of a webcam, define a USB rule. For further information, see "Defining rules for using USB devices" on page 149.

## 5.17. Diagnostics tab

The **Diagnostics** tab allows you to configure the **Device diagnostics** can either be requested by the Scout admin or sent from the device.

| Option   | Description   |
|--|---|
| Debug level  | <p>If the <b>Debug level</b> is set to <b>On</b> (Enhanced debugging), by using the <b>Device diagnostics</b> feature you run predefined commands on the device 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 <b>Device diagnostics</b>.</p>  |
| <p><b>Note</b></p> <p>Make sure to switch off the <b>Debug level</b> after having performed device diagnostics. Otherwise, you risk to exceed the memory capacity of the device.</p> |   |
| Send files to  | <p>FQDN of a Scout Server or URL of a FTP server to be used as the destination server to which the devices send their diagnostic files.</p> <p>By default, the diagnostic files are transferred to the Scout Server the device is connected to.</p> <p>This option allows you to specify, for example, a specific Scout Server or FTP server that will receive the diagnostic files for all devices regardless of their assigned Scout Server.</p> <p>The specified destination server is also active when diagnostic files are sent from eLux.</p> |
| Enhanced logging for smart card support  | Creates an additional log file <code>/tmp/PCSCDlog.txt</code> when PCSC Lite is used  |

Device diagnostics is performed by using a Scout command. For further information, see "Device diagnostics" on page 275.

## 5.18. Power management tab

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. 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 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.*

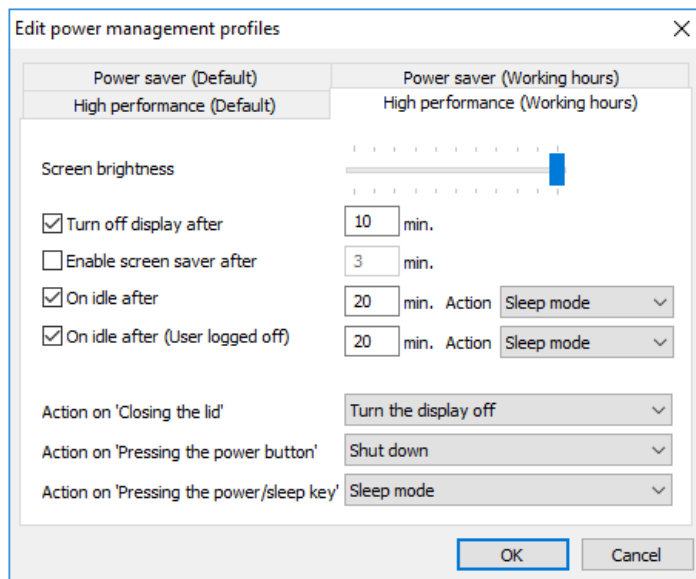
## Profile-independent options

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

### 5.18.1. Configuring power management profiles

#### Note

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



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

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

| Option                                | Description   |
|---------------------------------------|---|
| Screen brightness                     | Screen brightness in percent for the selected profile<br>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): <sup>1</sup><br><br>Shut down<br>Sleep mode<br>Restart <sup>2</sup><br>Log off <sup>3</sup> |
| On idle - Action (User logged off)    | 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). <sup>4</sup>   |
| Action on 'Closing the lid'           | Action that is performed when the user is closing the lid:<br><br>No action<br>Turn the display off<br>Shut down<br>Sleep mode  |
| Action on 'Pressing the power button' | Action that is performed when the user presses the power button:<br><br>No action<br>Turn the display off<br>Shut down<br>Sleep mode  |

<sup>1</sup>Default is sleep mode after 20 minutes (for High performance profiles)

<sup>2</sup>from Scout Enterprise Management Suite 15 2101

<sup>3</sup>from Scout Enterprise Management Suite 15 2101

<sup>4</sup>Default is sleep mode after 20 minutes (for High performance profiles)

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

3. Confirm with **OK**..

#### Note

The sleep mode corresponds to **Suspend to RAM (S3)**. For further information, see "Sleep mode (Suspend)" on page 160.

### 5.18.2. Defining working hours



#### Requires

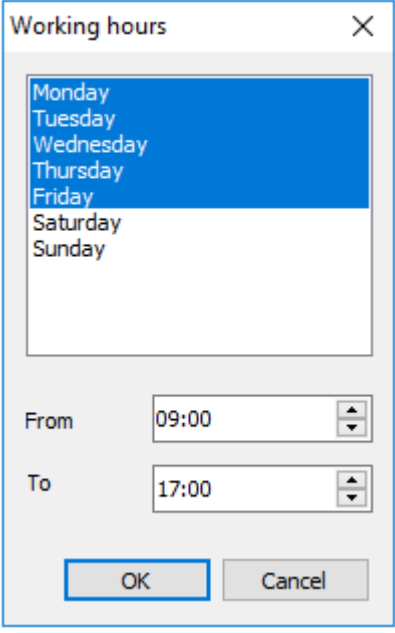
User right **Define working hours**

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.

<sup>1</sup>If this key is not available, the configuration has no effect.

<sup>2</sup>Default

5. Confirm with **OK**.

A dialog box titled "Working hours" 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 "09:00" and "To" with the value "17:00". At the bottom, there are two buttons: "OK" and "Cancel".

Working hours

Monday  
Tuesday  
Wednesday  
Thursday  
Friday  
Saturday  
Sunday

From 09:00

To 17:00

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)

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**. 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)`.

---

## 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 <b>USB multimedia devices</b> 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" on page 163</p>   |      |                                  |         |                     |       |                           |       |                    |
| Multimedia USB devices, connected via <b>DisplayPort to eLux RP 5 devices with an AMD processor</b> , 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 feature "Advanced file entries" on page 178:</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 <b>Out of range</b> 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 feature "Advanced file entries" on page 178:</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 <b>touch screen</b> , the location of a fingertip touch is not recognized precisely.                               | The monitor has not been calibrated precisely enough.   | To calibrate the monitor, configure a "Defining custom applications" on page 225 by using the parameter <code>calibrator</code> . Then start the application.  |      |                                  |         |                     |       |                           |       |                    |

| Error / problem  | Reason  | Solution   |      |                                  |         |                     |       |                                |       |                  |
|--|---|--|------|----------------------------------|---------|---------------------|-------|--------------------------------|-------|------------------|
| Only eLux RP 5.7.x:<br><br>In <b>dual monitor mode</b> , if the second monitor is configured to <b>vertical</b> , 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 feature "Advanced file entries" on page 178: <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>VerticalAlignment</code></td></tr><tr><td>Value</td><td><code>top</code></td></tr></table><br>The default value is <code>bottom</code> .   | File | <code>/setup/terminal.ini</code> | Section | <code>Screen</code> | Entry | <code>VerticalAlignment</code> | Value | <code>top</code> |
| File   | <code>/setup/terminal.ini</code>  |  |      |                                  |         |                     |       |                                |       |                  |
| Section  | <code>Screen</code>   |  |      |                                  |         |                     |       |                                |       |                  |
| Entry  | <code>VerticalAlignment</code>  |  |      |                                  |         |                     |       |                                |       |                  |
| Value  | <code>top</code>  |  |      |                                  |         |                     |       |                                |       |                  |
| Display/general <b>graphics issues</b>   | The feature package for hardware acceleration <b>HwVideoAccDrivers</b> is not installed.<br><br>Hardware acceleration (installed with the <b>HwVideoAccDrivers</b> FPM) is not supported by the device and causes problems. | Activate the <b>HwVideoAccDrivers</b> FPM within the <b>XOrg</b> package in the IDF.<br><br>To exclude individual device types from hardware acceleration, create a blacklist that is transferred and locally saved to the devices by using the Scout feature "Files configured for transfer" on page 173:<br><br><code>/setup/hwaccBlacklist</code><br><br>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 <b>Properties</b> window under <b>Asset &gt; Hardware information &gt; Type</b> .<br><br>Example:<br><code>FUTRO S920</code><br><code>D3314-B1</code><br><code>HP t620 Dual Core TC</code><br><br>For all device types listed in the blacklist, hardware acceleration is disabled. |      |                                  |         |                     |       |                                |       |                  |
| <b>AD logon</b> 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 devices, open **Advanced options > Advanced file entries**.
2. Define the following entry

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

For further information, see "Advanced file entries" on page 178.

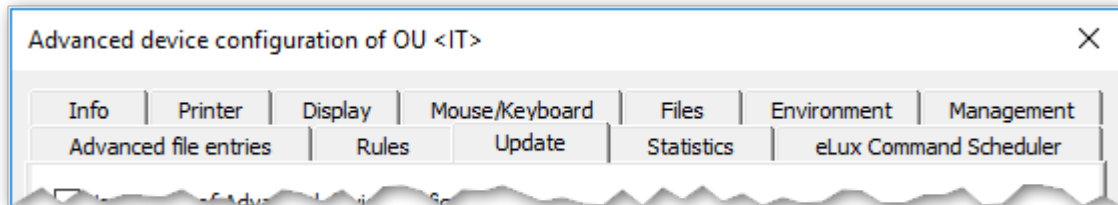
### Note

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**



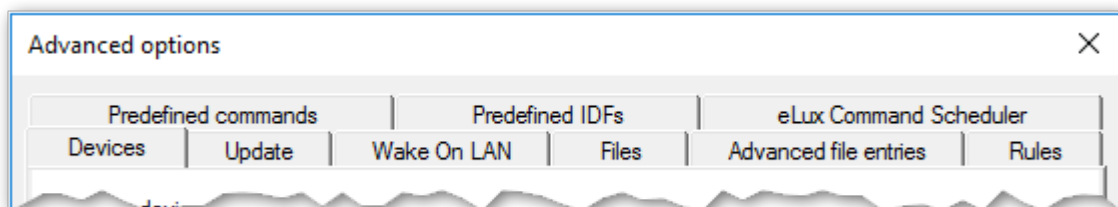
The **Advanced device configuration** is applied on OU or device level.

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

### Note

Inheritance is also used for Advanced device configuration. By default, the option **Use parent of Advanced device configuration** 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.

## 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 devices 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) | <p>Editable fields of the local device configuration are free for individual user configuration and will not be overridden by Scout. 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 <b>Device configuration &gt; Security &gt; User rights</b>.</p> <p>The local user configuration values of unlocked fields can additionally be retained during a factory reset of the device.</p> <p>For further information, see "Supporting local configuration" on page 62.</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" on page 62

### 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" on page 39.</p> |
| 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 registered MAC addresses. For further information, see "Reserving device profiles" on page 36. |

## 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<br><br>Can be overridden for particular OUs ( <b>Advanced device configuration &gt; Management</b> )          |
| 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 36.

## 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 individual system.

## 6.3. Management

- only available for individual devices and OUs -

| Option  | Description  |
|---|--|
| Note  | Free text field for internal comments<br>Can be shown in the <b>Properties</b> window  |
| Visibility<br>- only for OUs -                      | The visibility refers to the list of OUs that new devices request when they initially connect to the Scout Server to select an OU.<br>Hidden OUs are not shown in the list.<br>Visible OUs can be selected in the list but can be protected by password.   |
| New devices<br>- only for OUs -                     | When new devices register automatically, they can be subject to a predefined name template.<br>Device names are configured globally in the <b>Advanced options</b> on the <b>Devices</b> tab. For further information, see "Devices" on page 165.  |
| Ignore OU filter<br>- only for individual devices - | If the OU filter is active ( <b>Advanced options &gt; Devices</b> ), new devices are assigned to OUs due to the defined criteria.<br>Individual devices can be excluded from the OU filter.<br>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 devices 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" on page 264.

## 6.5. Predefined IDFs and containers

- only globally available for all devices (**Options > Advanced options**) -

By predefineding 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" on page 110.

- ▶ 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.
  - Specify file names 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 firmware configuration under <b>Image file</b></p> <p>Example: <code>recovery_x.idf</code></p> <p><b>Used</b> shows the number of devices using the image<br/> <b>Assigned</b> 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 <b>Path</b> if marked as valid</p> <p>Example: <code>elias/UC_RC6_X64</code></p>  |
| Predefined UEFI files <sup>1</sup> | UEFI file  | <p>Name of a <code>.udf</code> file that if marked as valid can be selected in the firmware configuration under <b>UEFI file</b></p> <p>An UEFI file is needed to update a device's UEFI firmware with the appropriate binary data.<sup>2</sup></p> <p>Example: <code>uefi.udf</code></p>   |

The **Valid** option allows you to specify for each defined entry whether it is displayed in the **Firmware** dialog.

---

<sup>1</sup>from Scout 15 2107

<sup>2</sup>from 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 that helps you start turned-off devices.



### Requires

Wake On LAN is supported by the device and configured in the device's UEFI/BIOS.

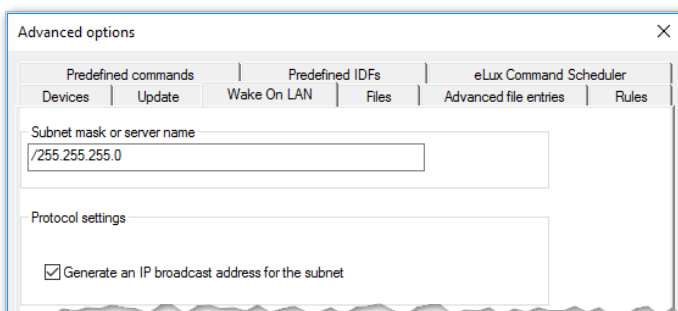
The Scout Server sends a so-called magic packet that is identified by the network adapter of the turned-off devices. The devices are woken via port 67.

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 device in remote subnets, subnet directed broadcasts are required.

### Subnet directed broadcasts

Subnet directed broadcasts can directly address the device's subnet to be woken up via IP. The IP broadcast address of the relevant subnet is determined from the IP address of the device 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<br>(for earlier versions: IP address of Wake On LAN server - option also available in the <b>Advanced device configuration</b> )  |
| Generate an IP broadcast address for the subnet<br>(only globally available in Advanced options) | The packet is sent to the relevant subnet (dedicated subnet). Requires a subnet address in the <b>Server name</b> field using the format /255.255.255.0 (Note the leading slash).<br><br>Example: To wake up a device with IP address 192.168.10.44, enter /255.255.255.0 in the <b>Server name</b> field. This causes Scout to generate the IP broadcast address 192.168.10.255 for the subnet.<br><br>By default, this option is disabled. |

## 6.7. VPN

- only available for individual devices -

---

### Note

One or more VPN profiles can be defined for entire OUs in **Device configuration > Network**.<sup>1</sup>

---

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

- Cisco AnyConnect / Cisco Secure Client<sup>2</sup>
- OpenVPN

Depending on the VPN client used, the devices must have a configuration file. You can modify the configuration file by using the Scout feature "Advanced file entries" on page 178.

### 6.7.1. Configuring Cisco AnyConnect / Cisco Secure Client

Cisco renamed its VPN **AnyConnect** Client from version 5 to **Cisco Secure Client**. The VPN technology remains the same, and the protocol is still called AnyConnect. Unicon ships the Cisco Secure Client for the first time with eLux RP 6 2302.1000, in parallel with the well-known AnyConnect Client. Their configuration for eLux is the same for both packages.

The following instructions refer to individual devices. To define VPN profiles for entire OUs, use **Device configuration > Network > VPN**. For further information, see "Defining a VPN profile" on page 83.

---

### Note

The eLux package **Cisco AnyConnect** or **Cisco Secure Client** must be installed on the devices. This may require modifications of the image definition file on the web server via ELIAS.

---

1. Transfer the root certificate to the devices to `/setup/cacerts`. If you use the Scout feature "Files configured for transfer" on page 173, specify the destination file with destination path `/setup/cacerts`.<sup>3</sup>

---

### Note

Use the `.pem` format for the certificate.

---

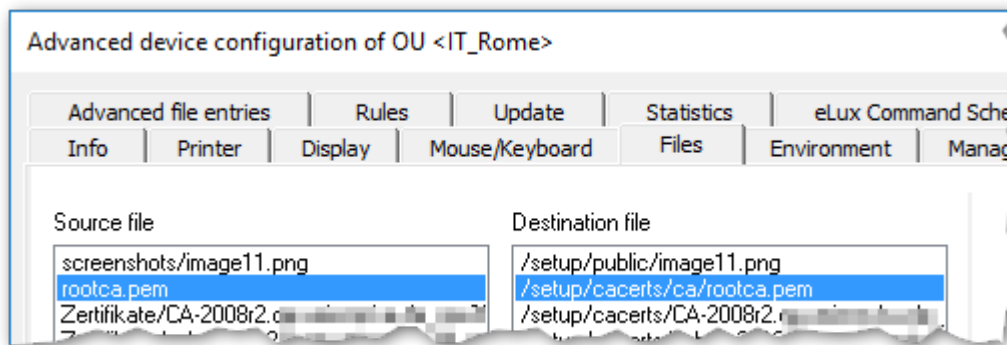


---

<sup>1</sup>from Scout Enterprise Management Suite 15 2101

<sup>2</sup>from eLux RP 6 2302.1000

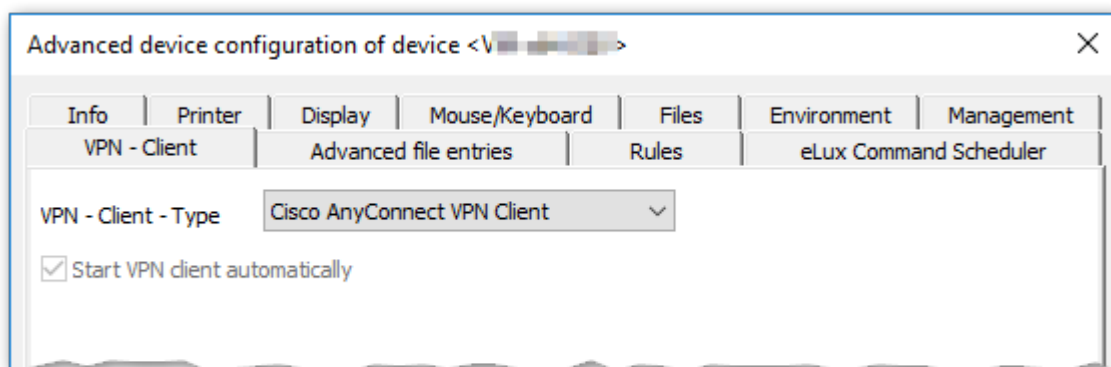
<sup>3</sup>from eLux RP 6 2302. Earlier versions require the certificate in `/setup/cacerts/ca`



### 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**. Use this option also for the Cisco Secure Client.



3. Restart the device. The device might require one more restart to activate the VPN configuration data locally.

*The device connects via AnyConnect on the next restart. Users have the active VPN connection as a live information on their system bar.*

## Configuration file

As an option, you can create an AnyConnect or Cisco Secure Client configuration file or copy one from a reference device, and then transfer the file to `/setup/elux/.cisco/profile/` via the Scout feature "Files configured for transfer" on page 173. In the configuration file, you can specify your back-end server address.

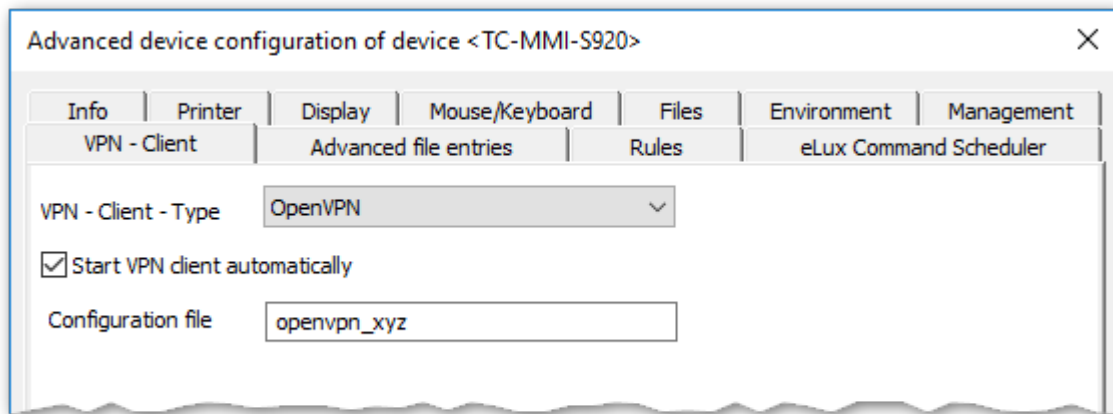
### 6.7.2. Configuring OpenVPN

The following instructions refer to individual devices. To define VPN profiles for entire OUs, use **Device configuration > Network > VPN**. For further information, see "Defining a VPN profile" on page 83.

#### Note

**OpenVPN** is an integral part of the eLux operating system. There is no need to have a separate package installed on the devices.

1. Transfer the `.ovpn` configuration file and certificates to the devices to `/setup/openvpn`. If you use the Scout 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.*

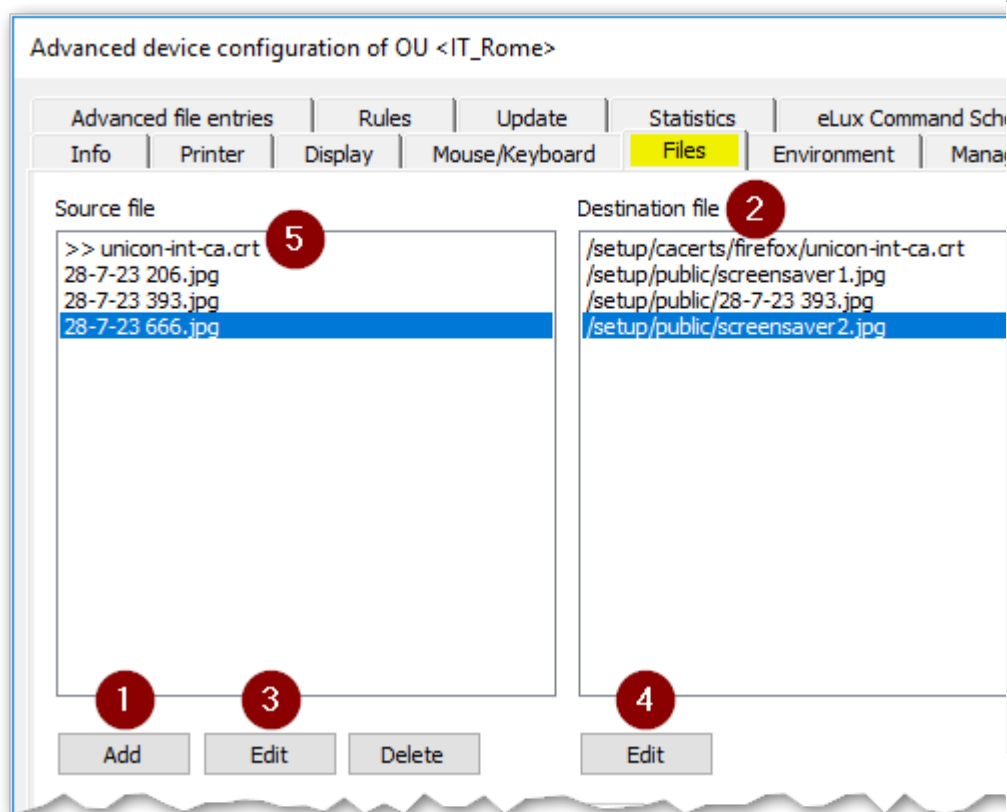
#### Note

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 database and therefore are included in an SQL database backup.



Example:  
Picture files are copied to the devices as screen savers.

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 >>.

You cannot edit these source files. With the corresponding object right, however, you can view them,<sup>1</sup> see below.

---

## 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 device restart. The files will not be reloaded unless you modify the file configuration.*

---

<sup>1</sup>from Scout 15 2101

## 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, from the context menu, choose **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

- ▶ To remove a transferred file from a device, on the **Files** tab, on the relevant level, select the file and click **Delete**.<sup>1</sup>

---

### Note

To remove all transferred files on all levels, alternatively perform a factory reset. Also use a factory reset for earlier eLux versions.

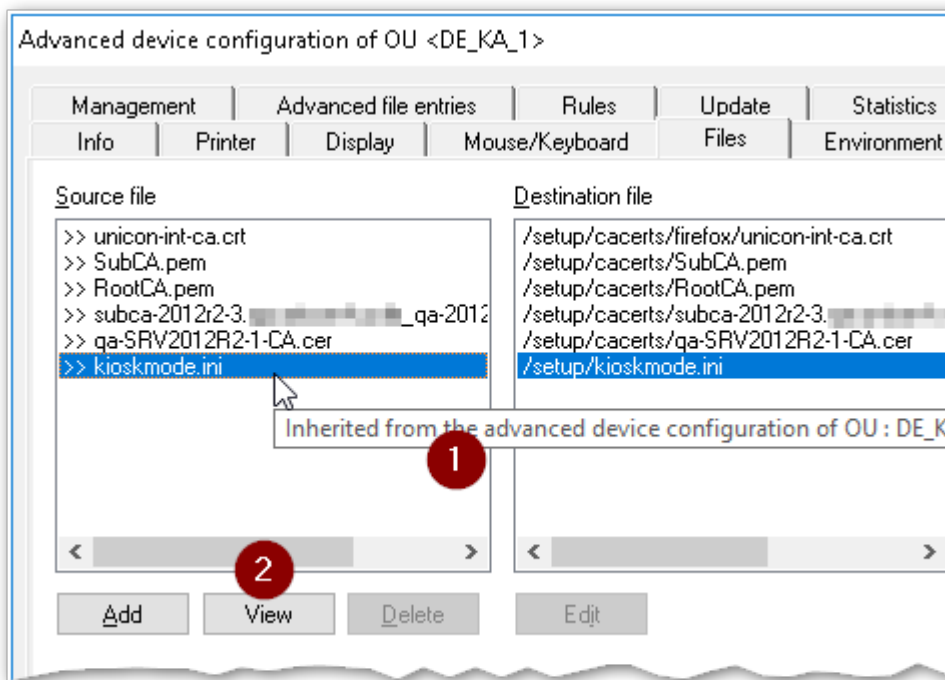
---

## 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 >> character and are protected from access by default.

---

<sup>1</sup>from eLux RP 6 2209



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.<sup>1</sup>

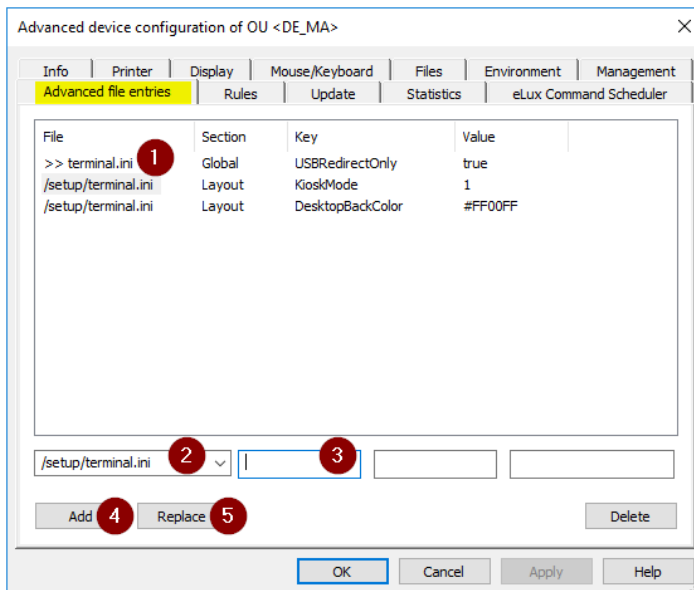
- ▶ To disable the object right, for the required OU and for the required administrator, open the object rights, and then navigate to **Edit properties > Files > Inherited file privacy**.

For further information, see "Changing object rights" on page 313.

<sup>1</sup>from Scout 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.



- 1 Entries from a parent OU or the global **Advanced options** are shown with a **>>**.  
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.
- 4 Click **Add** to add the new entry.
- 5 Click **Replace** to replace the selected entry in the list by the new entry.

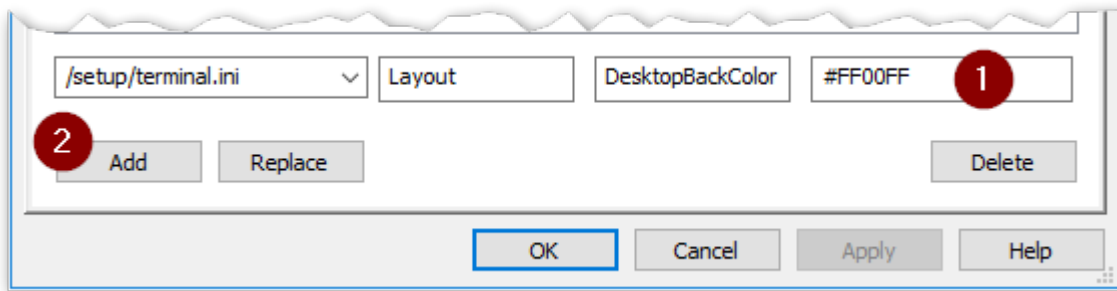
The following applies to the `.ini` files:

- `.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 keyword is used more than once in the same section, the last occurrence has precedence.

### 6.9.1. Adding individual file entries

1. In the Scout Console, click **Options > Advanced Options**.  
Or:  
For the relevant OU, open the context menu and click **Advanced device configuration...**

- Click the **Advanced file entries** tab.



- Below the list, edit the following fields (1):

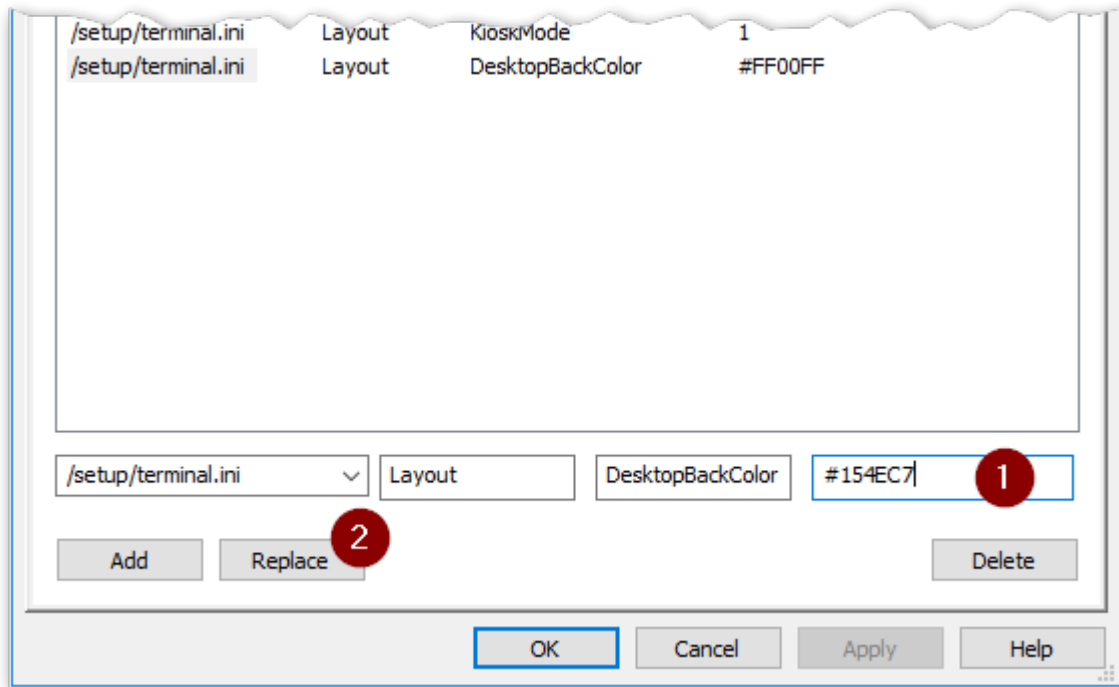
| Option  | Description   |
|---------|---|
| File    | Enter the full path including file name or select from the list:<br>Terminal: /setup/terminal.ini<br>Citrix ICA: /setup/ica/wfclient.ini and /setup/ica/appsrv.ini<br>Cisco VPN: /setup/ciscovpn/sample.pcf |
| Section | Section heading without brackets  |
| Key     | Keyword   |
| Value   | Value you want to assign to the keyword<br>Blanks, hyphens and multiple values are allowed.<br>Example: valueA,valueB,valueC;comment  |

- Click **Add** (2).
- Confirm with **Apply** and **OK**.

*The new entry is written to the .ini file on the next device restart.*

### 6.9.2. Changing values of individual file entries

- In the Advanced device configuration > Advanced file entries, select the entry whose value you want to change.

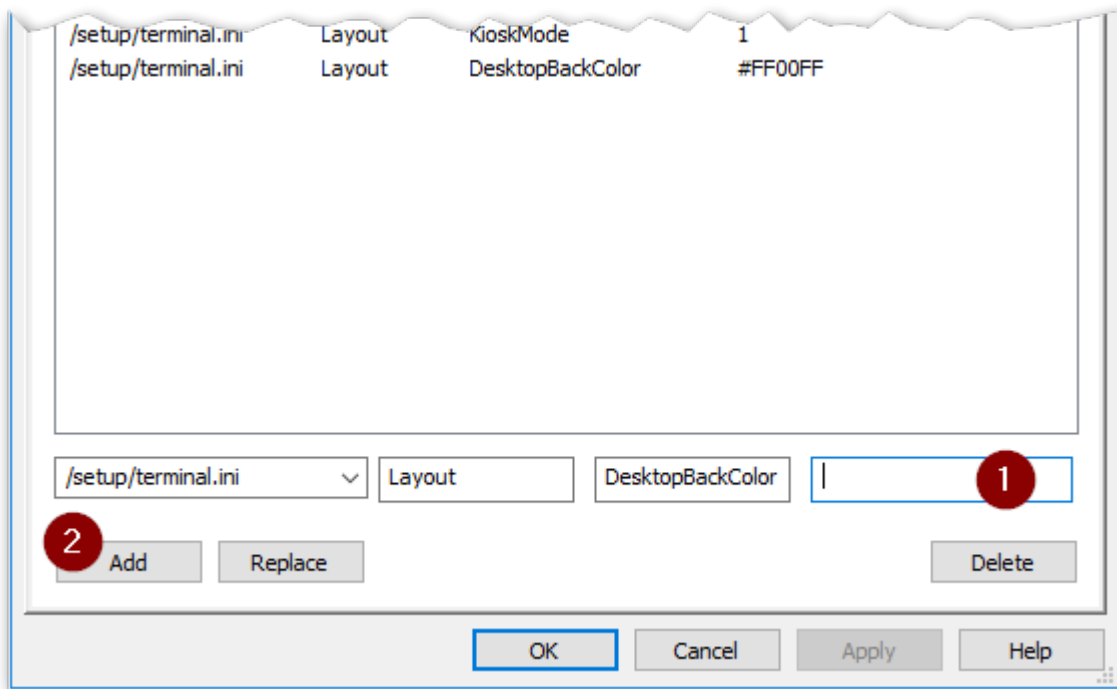


2. Below, in the **Value** box, replace the current value.
3. Click **Replace**.

*The new values are written to the .ini file on the next device restart.*

### 6.9.3. Deleting individual file entries

1. In **Advanced device configuration > Advanced file entries**, define a new entry:
2. Enter **File**, **Section** and **Key** of the relevant file entry, but leave the **Value** box empty (1).



3. Click **Add**. (2)

*The 'empty' file entry overrides previous instructions. The file entry is deleted from the relevant section on the next device restart.*

#### Note

If you use the **Delete** button to delete a selected row from the list, then Scout will no longer update the respective entry. However, the entry with its value remains.

### 6.9.4. Deleting complete sections

1. In the **Advanced device configuration > Advanced file entries**, define a new entry:  
Specify the **File** and **Section** of the relevant file entry, but leave the **Key** and **Value** fields empty.
2. Click **Add**.

*The 'empty' section overrides previous instructions. The section is deleted from the file on the next device 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 for the first time.

| Option  | Description   |
|---|---|
| After terminating the last application execute the following action | Choose between the options of the list-field<br>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.

- Define the following entry by using the Scout feature "Adding individual file entries" on page 178:

|         |                      |                   |
|---------|----------------------|-------------------|
| 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 device. They contain strings.

### Defining environment variables

1. In the **Advanced device configuration**, click the **Environment** tab.  
*Previously defined variables are shown in the list. Entries from a parent OU are shown with a >>.*
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 from the context menu, choose **Encrypt value**.

---

#### Note

When you apply the defined variables later on, make sure you prefix the variable with a dollar sign: `$<Variable name>`. For further information, see also "Where to apply user variables" on page 133.

---

## 6.12. TPM 2.0 support

A TPM 2.0 chip built into a device can be used for basic security functions:

- Encryption of the setup partition and system partition

The setup partition on a device'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.

- Store the private key of a SCEP client certificate inside the TPM 2.0 module

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.

---

#### Note

If you want to use TPM 2.0 via WLAN, note the special parameters in the configuration file `wpa.conf`. For further information, see [Configuring WPA supplicant](#) in the **IEEE 802.1X** short 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

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 you install the BaseOS package on the devices with the feature package **Partition encryption** enabled, the system will automatically be 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

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

|         |                     |                             |  |
|---------|---------------------|-----------------------------|--|
| File    | /setup/terminal.ini |                             |  |
| Section | Security            |                             |  |
| Entry   | DiskEncryption      |                             |  |
| Value   | true                | The default value is false. |  |

For further information, see "Advanced file entries" on page 178.

*For the relevant devices, a firmware update is forced with previous disk formatting.*

The configuration parameter has no effect on devices without TPM 2.0.

---

### Note

You can find information on whether the disk of the device is encrypted in the **Properties** window.

---

When new devices with TPM 2.0 chip are on-boarded to the Scout infrastructure 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 device after the setup partition has been encrypted.

## Update from earlier versions with disk encryption

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 a current eLux RP 6 version, one more update may be required on the next device restart. This is due to the partition formatting that is required for encryption.

## 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 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` 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.*

## 7. Defining applications

The devices 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 device 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" on page 181.

---

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 device (control panel, start menu)   |
| Sorting ID                | Specifies the sorting order for applications pinned to the system bar<br>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 logon        | 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).<br><br>For further information, see "User variables" on page 133. |
| 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)<br><br>(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. Object rights for the advanced settings and free parameters can be assigned separately.

### 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.

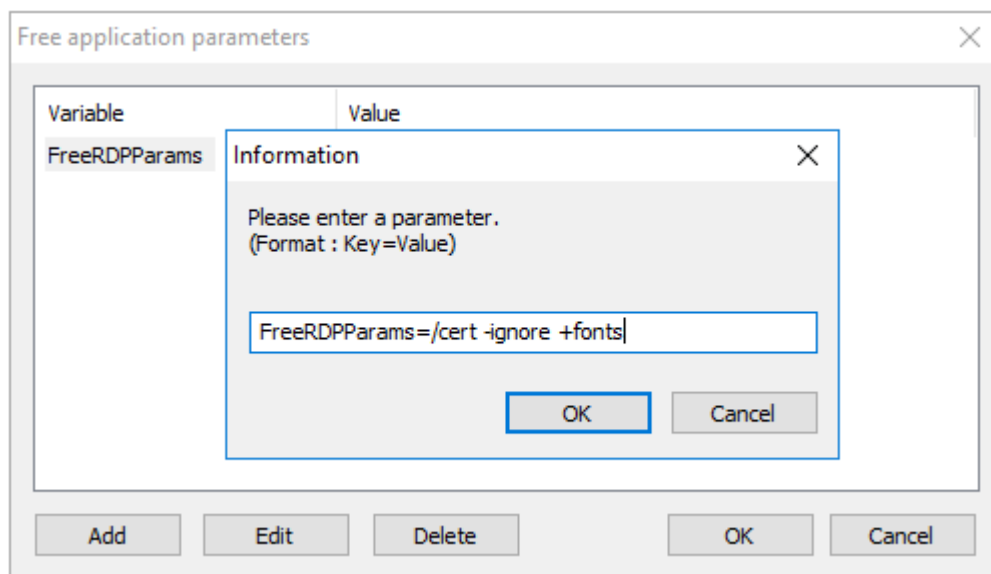
1. Open the **Application properties** of the relevant application.
2. Click **Free Parameters**.
3. Click **Add** and enter one or more parameters in the following format. Example:

`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.

For information on which parameters are available, refer to the description of the respective application definition.

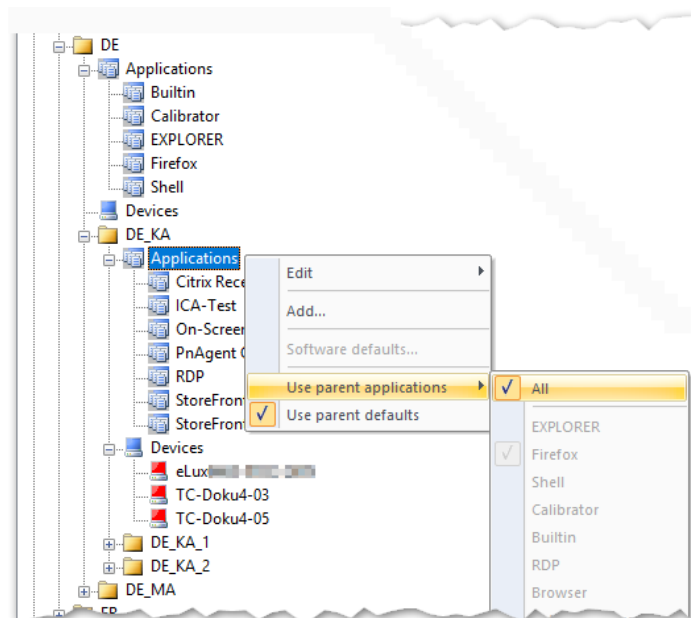
The following parameters can be used across applications:

| Parameter | Values | Description                                  |
|-----------|--------|--|
| pinned    | true   | The application is pinned on the system bar. |

### 7.1.4. 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 device restart for that OU.*

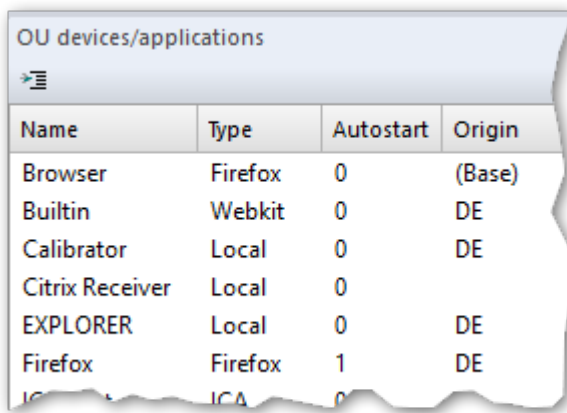
### Note

Inherited properties of the selected applications will be lost if you move the respective OU to another parent OU. For moved OUs, the system automatically enables **Use parent applications > All**.<sup>1</sup>

## 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 *Base*.



| Name            | Type    | Autostart | Origin |
|-----------------|---------|-----------|--------|
| Browser         | Firefox | 0         | (Base) |
| Builtin         | Webkit  | 0         | DE     |
| Calibrator      | Local   | 0         | DE     |
| Citrix Receiver | Local   | 0         |        |
| EXPLORER        | Local   | 0         | DE     |
| Firefox         | Firefox | 1         | DE     |
| ICA             | ICA     | 0         |        |

The selected OU of the figure above has one own application (no entry in the **Origin** column), four applications from the higher-level OU **DE**, and one top-level application.

### Note

To also apply the default settings of the parent applications, on the **Applications** context menu, select the **Use parent defaults** option. For further information, see "Software defaults" on the facing page.

<sup>1</sup>from Scout 15 2101

### 7.1.5. 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)  
For further information, see "Citrix software defaults" on page 204.
- Browsers  
For further information, see "Browser home directory" on page 222

We recommend to apply the default settings at top level (root applications) to use inheritance across all OUs. If you still need different software default settings, you need to disable inheritance for the relevant OUs.

### Defining software defaults

1. In the tree view, for the relevant OU, 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. By default, this is the top-level instance.

---

2. In the list-field, select the relevant software and click **Edit**.
3. Edit the relevant options on the tabs and confirm with **OK**.

*The software defaults are applied to all applications of subordinate OUs, provided, on the OU's **Applications** context menu, the **Use parent defaults** option is selected. This is the default.*

### Disabling inheritance of software defaults

1. In the tree view, for the relevant OU, open the  **Applications** context menu.
2. Disable the **Use parent defaults** option.

*The parent software defaults are saved for the OU.<sup>1</sup> On this basis, from now on, you may configure the settings individually.*

### 7.1.6. Defining application templates

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**

---

<sup>1</sup>ab Scout 15 2204

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.

## 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**.

### 7.1.7. Uploading applications from a device to Scout

Application definitions of a reference device 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 device (outside of Scout Enterprise Management Suite)

1. In the Scout Console, click **File > Application upload....**

*The **Application upload** dialog opens.*

2. Enter the IP address or name of the device you want to upload application definitions from.
3. Select the **Destination** OU.
4. Click **Start**.

*The application definitions of the specified device (or its OU) are uploaded to the specified OU. Already existing applications are deleted.*

#### Uploading from a device 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 device (or 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 devices' desktop. For the icon files, the high-resolution formats **.svg** und **.png** are supported.

1. In the tree view, for the top-level  **Applications**, from the context menu, choose **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" on the previous page.

1. For the relevant application, from the context menu, choose **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 device restart.*

## 7.1.10. Defining a service app

### 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 device, the AD logon dialog contains a **Service** button.*



## 7.1.11. Limiting applications to one logon domain

### 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 device, 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 a device to a Citrix back-end is performed by one of the following applications:

- by a "StoreFront application" on the facing page to a StoreFront server
- by the Citrix "Self-Service user interface" on page 201 to a StoreFront server
- via a browser to a StoreFront server or Web Interface server, see "Browser session to access published resources" on page 203

### Requirements

- The eLux package **Citrix Workspace-App for Linux** must be installed on the devices.
- To connect via HTTPS, for the application types **Storefront**, **Self Service** and **PNAgent**, the relevant root and intermediate certificates must be available on the devices.
  - 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 devices.
  - 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 devices 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" on page 92.

### 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" on page 94.

### Defining a StoreFront application

#### Note

HTTPS connections require the relevant StoreFront application on the device.

1. Add a new application (see "Adding applications" on page 186) 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) | <p>Enter the Citrix store provisioning file name without the file name extension. The Provisioning file must be located on the device in the directory /setup/ica/. For further information, see "StoreFront / Store provisioning file" on page 199.</p> <p>This option excludes the specification of Store URLs (next option).</p>   |
| Stores                      | <p>Specify the URL of one or more stores</p> <ul style="list-style-type: none"> <li>▶ Click <b>Add</b> and replace the automatically created default value by your individual value (double-click or F2)</li> </ul> <p>Example: (https://CtrXd76.sampletec-01.com/Citrix/Store33/discovery)</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          | The user is logged on to the store via single sign-on. The AD user credentials are used.  |

**Note**

If you want to use predefined credentials or pass-through authentication, the eLux package **Citrix Extensions** and the included feature package **Dialog Extension** must be installed on the devices.

For further information, see "StoreFront / Authentication" on the facing page.

|  |  |
|--|--|
| Show last user   | The user credentials (except for password) of the last logon are displayed in the XenApp logon dialog.<br>This option has no effect if you specify fix user credentials for automatic logon under <b>Logon</b> .   |
| 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.<br>Example: MyApp1 ; MyApp2<br><br>If only one resource is defined for a store, alternatively use the free parameter <code>AutostartUniqueResource=true</code> |
| Application restart<br>Start automatically<br>Desktop icon | See "Adding applications" on page 186  |
| Free parameters (optional)                                 | Individual parameters for application start<br><br>For further information, see "Defining free application parameters" on page 188.  |

- 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 <b>Logoff after</b> option and specify a delay in seconds. Automatic logoff does not affect the launched desktop.<br><br>Alternatively, automatic logoff can be configured to be performed after the last StoreFront application has been closed. |

| Option                   | Description  |
|--------------------------|--|
| Application reconnection | <p>Determine the actions to be done on a reconnect to the StoreFront server</p> <p><b>Do not reconnect:</b> The connection to the desktop or the published applications is not restored (default).</p> <p><b>Disconnected sessions only:</b> The connection to a disconnected session is restored.</p> <p><b>Active and disconnected sessions:</b> 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><b>Logoff only server:</b> Logoff is performed only from the StoreFront server</p> <p><b>Logoff server and applications:</b> Logoff is performed from the StoreFront server and from the virtual desktop or published applications.</p> <p><b>Logoff server and disconnect session:</b> 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.

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

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 devices, note the following:

- The file must be located on the devices in the directory `/setup/ica/`  
Transfer the `.cr` file by using the Scout feature **Files configured for transfer**. For further information, see "Files configured for transfer" on page 173.

### 7.2.3. StoreFront / Authentication

If on a device, smart card packages are installed and the Citrix Workspace-App for Linux identifies smart card middleware on the device, smart card logon has precedence by default. In order to still

authenticate via username and password for certain devices, 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 feature "Adding individual file entries" on page 178:

|         |                             |
|---------|-----------------------------|
| 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.

### Note

Using a smart card requires the smart card middleware to be installed on the device. In addition, smart card authentication must be enabled on the Citrix farm.

- ▶ Define the following entry by using the Scout feature "Adding individual file entries" on page 178:

|         |  |
|---------|--|
| File    | /setup/sessions.ini                        |
| Section | ICADefaults                                |
| Entry   | SmartcardRemovalAction                     |
| Value   | noaction   forcelogoff (Default: noaction) |

## Further parameters for authentication

To define further parameters for authentication, use the configuration file `/setup/ica/AuthManConfig.xml.template`. This file is transferred to the devices 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 devices. For further information, see "Files configured for transfer" on page 173.

For the function to become active on the device, one restart is necessary to transfer the file, and another restart to activate the new parameters.

### 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** and the included feature package **Self-service** 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 select the application type **Local**.
2. Edit the following fields:

| Option                   | Description  |
|--------------------------|--|
| Name                     | Name for the application   |
| Local application        | Select <code>Custom</code> .   |
| Parameter<br>(mandatory) | Enter the following program name to start the application:<br><code>selfservice</code> |

---

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

##### Note

The `selfservice` application cannot be configured individually. To use configuration options, alternatively use the "Citrix Self-Service in kiosk mode (current eLux versions)" on page 237.

---

## 7.2.5. Custom design for Citrix Workspace-App

### Note

The eLux package **Citrix Workspace-App**<sup>1</sup> must be installed on the devices.

To customize the layout of your Citrix session, transfer the relevant layout files to the devices into the Citrix directory structure. The files then are merged with the Citrix layout files.

To transfer the files, use the Scout feature **Files configured for transfer**. For further information, see "Files configured for transfer" on page 173.

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.

<sup>1</sup>>= version 18.08

### 7.2.6. 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 device, the relevant software package for Firefox or Chromium must be installed on the devices. 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 device.

1. Add a new application (see "Adding applications" on page 186) 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.<br><br>Examples:<br><code>https://&lt;Servername&gt;/Citrix/StoreWeb</code><br><code>https://&lt;Servername&gt;/Citrix/XenApp</code> |

3. For the remaining parameters, see "Defining a browser application" on page 217.

*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.*

### 7.2.7. Citrix software defaults

For all Citrix applications, in the Scout Console, you can define Citrix Workspace-App 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 "Software defaults" on page 191.

---

#### Note

To define parameters in individual configuration files, use the "Advanced file entries" on page 178 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 \$ICANAME and \$ICADOMAIN to set a unique client session name. This is required for Citrix Roaming and some XenApp programs. For further information, see Citrix software defaults.</p>                       |

## 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"> <li><input type="checkbox"/> E = enable</li> <li><input type="checkbox"/> R = read</li> <li><input type="checkbox"/> W = write</li> </ul>  |
| 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" on page 139.

## COM ports tab

To connect via COM port, the device name of the client device's 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 devices' 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`

### 7.2.8. 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.

### Defining the Citrix Connection Center

#### Note

The **Citrix Workspace-App** and the included feature package **Utilities and tools** 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 (see "Adding applications" on page 186) and select the application type **Local**.
2. Edit the following fields:

| Option               | Description                               |
|----------------------|---|
| Name                 | Name for the application                  |
| Local application    | Select Citrix Connection Center.          |
| Parameter (optional) | Command-line parameters for program start |

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

### 7.2.9. 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**.

## 2. Define the following entry

|         |                       |   |  |
|---------|-----------------------|---|--|
| File    | /setup/ica/module.ini |   |  |
| Section | WFClient              |   |  |
| Entry   | SyslogThreshold       |   |  |
| Value   | 0 3 7                 | 0 Logging disabled (default)<br>3 Only errors are logged<br>7 Logs for all levels are generated |  |

For further information, see "Advanced file entries" on page 178.

*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** 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" on page 173.

*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 "Device diagnostics" on page 275.

*After retrieving the diagnostic files, you can find the log files in the `hdxrtcengine` and `webrpc` directories.*

## 7.2.10. 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.

---

### Behavior of default values

- from Scout 15 2204 -

When you update to a later version of the Citrix Workspace-App, the vendor's default values are applied. This overwrites individually set values in favor of a consistent situation between updated devices and freshly installed devices.

The vendor's default values are set for the following scenarios:

- Firmware update to newer CWA package (with and without formatting the system partition)
- Firmware update to newer eLux version including new CWA version (with and without formatting the system partition)
- Factory reset
- PXE or USB installation

## 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 (see "Adding applications" on page 186) 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 logon | 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 <b>eluxRDP</b> in the format:</p> <pre>FreeRDPParams=&lt;Parameter&gt; &lt;Parameter&gt; &lt;Parameter&gt;...</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 <code>eluxrdp</code> command in a shell.</p> <p>For further information, see "Defining free application parameters" on page 188.</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 (see "Adding applications" on page 186) 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<br>System variables are allowed.<br><br>Examples:<br><code>c:\Program Files\Microsoft Office\Office\EXCEL.EXE</code><br><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.  |
| Free parameters              | Allows to define any parameters supported by <b>eluxRDP</b> in the format:<br><br><code>FreeRDPPParams=&lt;Parameter&gt; &lt;Parameter&gt; &lt;Parameter&gt;...</code>   |

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

*For the users, the application runs full-screen in the session window.*

### 7.3.3. Defining a load-balanced RDP session

If you are running a remote desktop server farm with load balancing, have your eLux RDP sessions load-balanced via the following configuration.

1. Define an RDP session/application or open the **Properties** dialog of an existing one. Edit the following options:

| Option          | Description   |
|-----------------|---|
| Server          | Name of your RD connection broker<br><br>Example:<br><code>RDPLoadMaster.int.sampletec-01.com</code>  |
| Free parameters | Parameter for the load balancer server collection<br><code>FreeRDPParams=/load-balance-info:tsv:'//MS Terminal Services Plugin.1.&lt;Load balancer collection&gt;'</code><br><br>Example:<br><code>FreeRDPParams=/load-balance-info:tsv:'//MS Terminal Services Plugin.1.RDS-01&gt;'</code> |

2. Confirm with **Apply** and **OK**.

#### 7.3.4. 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

##### Note

Access to the advanced settings can be restricted via the object rights.

- ▶ Scout: 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. |
| Colors                 | Color depth for the session (8-32 Bit)   |

## Note

If you use multiple monitors but wish to display content on only one of them, under **Device configuration > Desktop > Advanced > Windowmanager**, the **Maximize/fullscreen to single monitor** option must be selected.

## Local Resources tab

- 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.

| 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, define the assignment with <code>/media</code></p> <p>Internally, the mount point for USB devices is set to <code>/media/usbdisk</code>. If multiple USB devices are plugged in, they use the same mapping. Each USB device is displayed in its dedicated folder. A digit is appended to the folder name and incremented (<code>usbdisk0</code>, <code>usbdisk1</code>).</p> <p>For further information, see "Mount points" on page 139.</p> |
| Connect printer  | <p>Up to four printer definitions can be created automatically for a session. The printers must be configured on the "Defining a locally connected printer" on page 141 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 <b>Set as default</b> in the eLux printer configuration.</p>  |
| Sound            | <p><b>Play local</b> reproduces the sound locally on the device. <b>Play remote</b> 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 logon.   |

## 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 <b>Auto</b> 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                 | The server does not accept encrypted sessions. You can use this option to increase performance.<br>By default, the option is disabled.   |
| Deactivate mouse move events          | 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.<br>By default, the option is disabled. |
| Show connection bar on full screen    | Shows connection list in full-screen mode  |
| Bandwidth                             | Choose between <code>standard</code> , <code>modem</code> , <code>broadband</code> or <code>LAN</code> .   |

### 7.3.5. 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 device 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.

As **Virtual Desktop** VMware Horizon is supported.

### 7.4.1. Defining a virtual desktop

1. Add a new application (see "Adding applications" on page 186) 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<br>Pass-through<br>logon         | See "Adding applications" on page 186                                |
| Protocol<br>(VMware Hori-<br>zon only) | Choose between the following values:<br>RDP<br>PCoIP<br>VMware Blast |

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" on page 211 (for VMware Horizon) or
  - Advanced XenDesktop settings in PNAgent application
4. Confirm with **Apply** and **OK**.

### 7.4.2. VMware Horizon

### Note

This application type is only available on eLux RP 6 devices. In the Scout Console, select the **Virtual Desktop** application type and as VD-Broker **VMware View**.

Application type  
VMware Horizon

Name  
VMwareX1

Start automatically

Desktop icon

Properties

VD broker  
VMware Horizon

Server

Pass-through logon

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<br><br>Note that HTTPS connections require the relevant SSL certificates on the device. |
| 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:<br>RDP<br>PCoIP<br>VMware Blast   |

For information on **Display**, **Local resources** and **Advanced** settings, see [Advanced application settings](#).

You may configure the VMware Horizon client by using the application definition in the Scout Console or locally on the . To set additional parameters that are not included in the interface, use a configuration file:

- ▶ With the help of VMware documentation,<sup>1</sup> create the file `view-userpreferences`. Transfer the file via the Scout feature [Files configured for transfer](#) to the s 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.

---

<sup>1</sup>Installation 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. The Builtin Browser is based on the WebKit2 engine which is part of the **Desktop environment** 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 devices with 2 GB of RAM.

For eLux RP 6, the Java browser plugin is no longer supported.

### 7.5.1. Defining a browser application

1. Add a new application (see "Adding applications" on page 186) 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> .  |
| Start page   | Web page (URL) that opens when you click <b>Home</b>   |
| Called page  | Web page (URL) that opens after starting the browser   |
| Proxy type   | <ul style="list-style-type: none"> <li>■ <code>No proxy</code>: No proxy server is used</li> <li>■ <code>Manual (Proxy:Port)</code>: Specify a proxy server and port number</li> <li>■ <code>Auto (URL)</code>: Use a proxy configuration file</li> <li>■ <code>Use system proxy (default)</code>: 'System-wide' proxy setting defined in the device configuration under <b>Network &gt; Advanced</b> per network profile</li> </ul> <p>Note that the setting behind <code>System proxy</code> can also be <code>No proxy</code>).</p> |

For further information, see "Proxy configuration" on page 86.

### Note

For the Builtin Browser, the setting must be left on `Use system proxy`.

|                            |   |
|----------------------------|---|
| Application restart        | See "Adding applications" on page 186   |
| Start automatically        |   |
| Desktop icon               |   |
| Free parameters (optional) | Individual parameters for application start<br>see "Defining free application parameters" on page 188 |

3. To enable the **Kiosk** mode for Firefox, see "Kiosk mode for Firefox" on page 223.
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" on page 222.

Further browser-specific preferences can be set through policies (Chromium) or configuration file entries (Firefox.). For further information, see the Scout guide:

"Preferences Chromium" below

"Preferences Firefox" on the facing page

"Preferences Builtin Browser" on page 220

### Deploying SSL certificates for the browser

- Use the Scout feature **Files configured for transfer** to transfer certificate files to the required target directory on the device:

|                 |  |
|-----------------|--|
| Mozilla Firefox | /setup/cacerts/firefox or /setup/cacerts/browser (current versions) <sup>1</sup> |
| Google Chromium | /setup/cacerts/browser   |

For further information, see "Files configured for transfer" on page 173.

Note that a second restart of the device is required to assign the certificates that have been transferred during the first boot to the certificate store of the browser.

#### 7.5.2. Preferences Chromium

By using policies, you can set mandatory (managed) and recommended preferences for the Chromium browser. Mandatory preferences define fixed values that cannot be changed by the user. Recommended preferences define default values that can be changed by the user. For further information, see <https://www.chromium.org/administrators/>.

<sup>1</sup>The certificates can be located in either directory.

- ▶ Use the Scout feature **Files configured for transfer** to transfer policy files (.json) to the required target directory on the device:

---

Fixed values     /setup/chromium/managed

Default values   /setup/chromium/recommended

---

For further information, see "Files configured for transfer" on page 173.

### 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.<sup>1</sup> 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)

- from Firefox 60 ESR and later versions -

You can use all options that are listed in the [README on the Mozilla GitHub repository](#).<sup>2</sup>

One or more options are transferred in a .json file to the device by using the Scout 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. Use the syntax shown in the example.<sup>3</sup>

Example:

```
{
  "BlockAboutConfig": false,
  "DisableBuiltinPDFViewer": true
}
```

2. In the Scout Console, for the relevant devices, open **Advanced device configuration > 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 page 173.

*On the next device restart, the files are transferred and evaluated.*

---

<sup>1</sup>This method will not work if Firefox is already being managed by using Windows group policies.

<sup>2</sup>Note that the current Firefox version may differ from that of the eLux version you are using.

<sup>3</sup>No "policies" brackets!

## Note

You can deploy multiple `.json` files to the device 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).

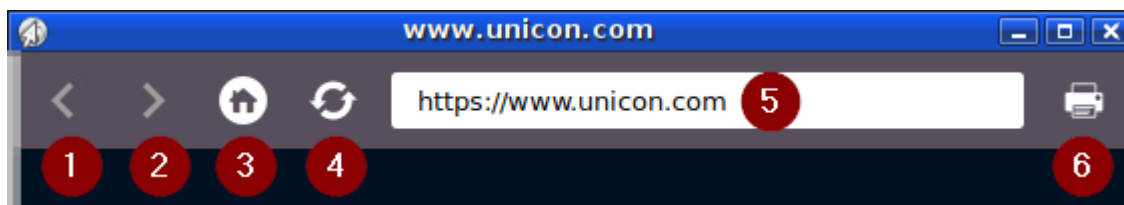
## 7.5.4. Preferences Builtin Browser

### 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**.<sup>1</sup>

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:

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

<sup>1</sup>from 15 2101 und eLux RP 6 2103

|         |  |
|---------|--|
| File    | /setup/sessions.ini  |
| Section | [BuiltinBrowserDefaults]   |
| Entry   | UserAgentString  |
| Value   | <name/version> <individual string><br>Example: Mozilla/5.0 (X11; Linux x86_64) |

For further information, see "Advanced file entries" on page 178.

#### 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 183.

## Clearing the browser cache

- ▶ To delete all browser data including cookies, press CTRL+SHIFT+DELETE

### 7.5.5. Browser home directory

By default, the browser settings are temporarily saved to the flash memory. However, they are deleted with each device restart.

Defining a browser home directory on the network, however, allows you to let users save and make available their browser settings such as bookmarks persistently. To do so, use a network share that you have configured for access:

#### Defining browser home directory

---




##### Requires

Configured Windows network share (**Defined drive**).

Example: `/smb/share`

For further information, see "Defining a network drive" on page 138.

---

1. In the tree view, for the relevant level, open the  **Applications** context menu and click **Software defaults...**  
For further information, see "Software defaults" on page 191.
2. On 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 > 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.*

## 7.5.6. Kiosk mode for Firefox

- for Firefox from ESR version 71.0 -

### Note

For current eLux RP 6 versions, you can use the Builtin Browser in kiosk mode. For further information, see "Browser in kiosk mode (current eLux versions)" on page 242.

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 device. For correct use of the kiosk mode, we recommend that you disable related functions such as restarting the device and opening the Config 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 <sup>1</sup> | Allows using browser tabs despite kiosk mode<br>Users can view multiple web pages of the defined web site concurrently |
| Add print button <sup>2</sup>       | Allows using browser tabs and provides a <b>Print</b> feature despite kiosk mode                                       |
| Add address bar <sup>3</sup>        | Allows using browser tabs and provides the address bar including navigation buttons despite kiosk mode                 |

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

<sup>1</sup>up to Scout 15 2107

<sup>2</sup>up to Scout 15 2107

<sup>3</sup>up 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 (see "Adding applications" on page 186) 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<br>Start automatically<br>Desktop icon | See "Adding applications" on page 186  |
| Free parameters (optional)                                 | Individual parameters for application start<br>see "Defining free application parameters" on page 188. |

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

### 7.6.2. Defining custom applications

1. Add a new application (see "Adding applications" on page 186) 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 <i>Custom</i> .   |
| Parameter<br>(mandatory)                                   | <p>Enter the program name required to start the application.<br/>If required, add start parameters.</p> <p>Example:<br/> <code>calibrator</code> calls the <b>Calibrator</b> tool<br/> <code>squid</code> calls the <b>Squid</b> application<br/> <code>squid /tmp/mycache</code> calls <b>Squid</b> using the specified cache directory</p> |
| Hidden   | <p>The application is not shown on the desktop.</p> <p>This is meant for automatically started applications. Select <b>Start automatically</b> or <b>Application restart</b> instead.</p>  |
| Application restart<br>Start automatically<br>Desktop icon | See "Adding applications" on page 186.   |
| Free parameters<br>(optional)                              | Individual parameters for application start<br>see "Defining free application parameters" on page 188  |

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

The screenshot shows the 'Application properties' dialog box with the 'Local' tab active. The fields are filled as follows: 'Name of application' is 'Calibrator', 'Display name' is 'Calibration', 'Sorting ID' is '1', 'Local application' is set to 'Custom' in a dropdown menu, and 'Parameter' is 'calibrator'. At the bottom, the 'Desktop icon' checkbox is checked, while 'Hidden', 'Restart application', and 'Start automatically after' (set to 0 s) are unchecked. Action buttons at the bottom include 'OK', 'Cancel', 'Apply', and 'Help'. A 'Free parameters' button is also present next to the 'Start automatically after' field.

The figure shows the application definition for the **Calibrator** tool . After the next device restart, the **Calibration** application is provided on the device's desktop and can be started (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 (see "Adding applications" on page 186) and 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 (see "Adding applications" on page 186) and 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 "Defining free application parameters" on page 188.

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

Applications of the `Emulation` type can only be defined in the Scout Console but not locally on eLux RP 6 devices.

Currently, the **5250 terminal emulation** is still supported.

## 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 device 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 xxxx (not yet specified) |
| Builtin Browser                                    | from eLux RP 6.5 <sup>1</sup> | from Scout 15 2107 and eLux RP 6 xxxx (not yet specified) |
| Configuration file                                 | kioskmode.ini                 | kioskconfig.ini   |

#### 7.8.1. Setting up kiosk mode via console

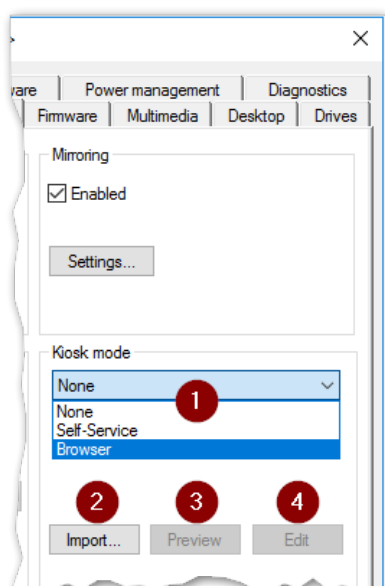
- from Scout 15 2107<sup>2</sup> -

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.

---

<sup>1</sup>For earlier versions, use Firefox in kiosk mode.

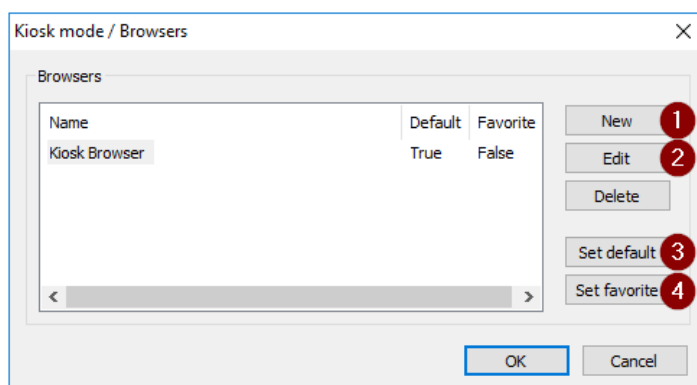
<sup>2</sup>Note: Current eLux versions do not yet support the new settings on the devices.



- 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 device as required.

## 7.8.2. Configuring browser for kiosk mode

- from Scout 15 2107<sup>1</sup> -

1. In **Device configuration > Security**, 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 **Home**
- 4 The first URL users load after the home page will be saved as new startup page.<sup>2</sup>
- 5 Unhide navigation bar
- 6 Elements of the navigation bar to be shown

3. Confirm with **OK**.

<sup>1</sup>The devices support the new settings only from eLux RP 6 23xx.

<sup>2</sup>How 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 2107<sup>1</sup> -

#### Note

The eLux package **Citrix Workspace-App for Linux** must be installed on the devices.

The eLux package **Citrix Extensions 2.x** or later and the included feature package **Self-service wrapper** must be installed on the devices.

For modifications on the Citrix dialog design, further feature packages must be installed on the devices:

**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 <b>MultiStore</b> 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**.

<sup>1</sup>Note: Current eLux versions do not yet support the new settings on the devices.

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 11 point to specific settings: 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; 4 points to the 'Logoff delay' input field; 5 points to the 'Logoff timeout' input field; 6 points to the 'On logon' checkbox; 7 points to the 'On app start or store refresh' checkbox; 8 points to the 'Self-Selection' checkbox; 9 points to the 'Shared user mode' checkbox; 10 points to the 'Show session in window' checkbox; and 11 points to the 'Domains' table.

| Name | Domain               |
|------|----------------------|
| INT  | 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 <b>MultiStore</b> 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     | Timeout for launching the Bultin browser and loading the password reset page  |

| Option  | Description  |
|---------|--|
| Options | Optionally, specify additional parameters for the browser start.<br><br>Example: <code>--title "Reset password"</code> |

If users do not remember their password, they click the relevant button in the **MultiStore** logon dialog. This launches the Builtin 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<br><br>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)<br><br>Default: <code>#e6f1f7</code> |
| Unselected...     | Background color for unselected list elements (Citrix list selection widgets)<br><br>Default: <code>#ffffff</code>     |
| Selected...       | Background color for selected list elements (Citrix list selection widgets)<br><br>Default: <code>#cce3f0</code>       |

### 7.8.4. Citrix Self-Service in kiosk mode (current eLux versions)

The Citrix Self-Service user interface with extensions is configured as kiosk mode. All relevant parameters are defined in the `kioskmode.ini` configuration file. 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** must be installed on the devices.  
The eLux package **Citrix Extensions 2.x** or later and the included feature package **Self-service wrapper** must be installed on the devices.

For modifications on the Citrix dialog design, further feature packages must be installed on the devices:

### 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 devices, open **Advanced device configuration > 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" on page 178.

*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:<sup>1</sup>

| Parameter                                     | Description  |
|---|--|
| ReconnectOnLogon=true  <b>false</b>           | 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  <b>false</b> | 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) |

<sup>1</sup>Default 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 combine SharedUserMode=false and Prelogin=true</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</p> <p>1 = Logoff timer is started with logon</p> <p>2 = Logoff timer is started when the last Citrix app/desktop is closed</p> <p>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 <b>User</b> 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 combine SharedUserMode=false and Prelogin=true</p>   |
| PreLoginTitle                              | Dialog title for the stores list (MultiStore)  |
| PassThroughMode=0 1                        | <p>0 No pass-through logon data</p> <p>1 Active Directory UserPassword</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>]`, users 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  <b>false</b>                         | Determines whether this store is displayed as default store   |
| AutostartResources=<App/Desktop1;App/Desktop2;...> | List of Citrix applications/desktops to be started automatically after logon<br>Currently only available with PreLogin=true |

[Environment\_Store<1-N>].

| Parameter  | Description  |
|--|--|
| Url=<Store-URL>                                    | URL of the Citrix store  |
| FriendlyName=<Display name>                        | Display name for the Citrix store  |
| Default=true  <b>false</b>                         | Determines whether this store is displayed as default store  |
| Environment=<Group name>                           | 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 logon<br>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<br>Default: <code>ucselfservice</code>  |
| Decorated=true  <b>false</b>     | Determines whether the windows are shown with window decoration  |
| ColorHover=<RGB color code>      | Background color for list elements on mouse hover (Citrix list selection widgets)<br>Default: <code>#e6f1f7</code> |
| ColorUnselected=<RGB color code> | Background color for unselected list items (Citrix list selection widgets)<br>Default: <code>#ffffff</code>        |

| Parameter                      | Description   |
|--------------------------------|---|
| ColorSelected=<RGB color code> | Background color for selected list elements (Citrix list selection widgets) |
|                                | Default: #cce3f0  |

5. Transfer the `kioskmode.ini` file to the devices to `/setup/kioskmode.ini`. To do so, use the Scout feature **Files configured for transfer**. For further information, see "Files configured for transfer" on page 173.

*The `terminal.ini` entry along with the `kioskmode.ini` file on a device will cause the device to open the Citrix Self-Service interface in kiosk mode after start-up. All 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 (current eLux 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 could be run in kiosk mode up to version ESR 52.8. Mozilla supports kiosk mode again starting with version 71.0, but without configuration options. For further information, see "Kiosk mode for Firefox" on page 223.

#### Defining Builtin Browser in kiosk mode<sup>1</sup>

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" on page 178.

*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:<sup>2</sup>

| Parameter                        | Description  |
|----------------------------------|--|
| Url=<URL of startup page>        | Web page (URL) that opens after the browser is started   |
| Homepage=<URL of homepage>       | Web page (URL) that opens when users click <b>Home</b>   |
| SaveFirstLink=true  <b>false</b> | If <b>true</b> , the first URL loaded when coming from the startup page will be saved as the new startup page. |
| Navbar= <b>true</b>  false       | The navigation bar will be shown.  |

<sup>1</sup>Kiosk mode via console (GUI) will be supported by future eLux versions

<sup>2</sup>Default values are displayed in **bold**

| Parameter                      | Description  |
|--------------------------------|--|
| NavbarPrint=<br>true false     | The <b>Print</b> button will be shown on the navigation bar    |
| NavbarForward=<br>true false   | The <b>Forward</b> button will be shown on the navigation bar  |
| NavbarBackward=<br>true false  | The <b>Backward</b> button will be shown on the navigation bar |
| NavbarHome=<br>true false      | The <b>Home</b> button will be shown on the navigation bar     |
| NavbarUrl=true false           | The address bar will be shown                                  |
| NavbarRefresh=<br>true false   | The <b>Refresh</b> button will be shown on the navigation bar  |
| Favorite=true false            | If <b>true</b> , the object is marked as a favorite.           |
| FriendlyName=<br><Anzeigename> | Display name for the user                                      |

- Transfer the `kioskmode.ini` file to the devices to `/setup/kioskmode.ini`. To do so, use the Scout feature **Files configured for transfer**. For further information, see "Files configured for transfer" on page 173.

*The `terminal.ini` entry along with the `kioskmode.ini` file on the device 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 device as required.

---

## Defining different web pages for devices/OU's

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:

- In the `kioskmode.ini`, in the `[Browser1]` section, for the first and/or second value, set a variable. Example:  
`Url=$URL1`  
`Homepage=$URL2`
- Define the variables used in the `kioskmode.ini` as environment variables for the relevant devices (Advanced device configuration). Example:  
`URL1=https://www.unicon.com`  
`URL2=https://myelux.com`

For further information, see "Environment variables" on page 183.

## 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" on page 173.

---

#### 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 230.
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 device   | Install the software on the device. For further information, see <a href="#">Creating an IDF</a> in the ELIAS guide and "Firmware update" on page 282.  |
| 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 <b>custom</b> type.   | Enable the option <b>Start automatically</b> or <b>Application restart</b> to start hidden applications on start or to run them non-stop, respectively.   |
| Problems with certificates in combination with VMware server | Server problem occurred:<br>After successful installation, the VMware server uses a self-signed certificate. If a device is configured correctly, it will not accept. The reason is that the <b>FQDN</b> (fully qualified domain name) is mandatory for server certificates. | Create a server certificate in the <b>Windows-CA</b> with <b>FQDN</b> .<br>If you use <b>mmc</b> : Create a server certificate using the Snap-In <b>Certificates (Local computer)</b> .<br>The key must be exportable.<br>The display name of the server must be <b>vdm</b> . The name must be unique in the certificate store <b>Local computer / Personal</b> . |

| 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 <b>permissive</b> 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 <b>permissive</b> option.</p> <p>Example:</p> <pre>FreeRDPParams=/serial:COM1,/dev/ttyS0,Serial,permissive</pre> <p>For further information, see "Defining free application parameters" on page 188.</p> |

## 7.11. Third party software

To install additional applications on the devices, carry out the following steps:

1. From our [myelux.com](https://myelux.com) portal, 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 devices, perform a firmware update to the modified image. For further information, see "Firmware update" on page 282.

*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)<sup>1</sup> 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 device 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**

---

<sup>1</sup>formerly VXME

#### 7.11.4. DriveLock

DriveLock provides endpoint security for USB interfaces on the devices.

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 device 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

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 device, a separate license is required.

Package name: **SecMaker NetID**

- ▶ Use the Scout feature **Files** to transfer the license file to the devices to  
`/setup/iid/netidlicense.lic`.

For further information, see "Files configured for transfer" on page 173 in the **Scout** guide.

---

#### Note

The license agreement (EULA) is available on the device 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**

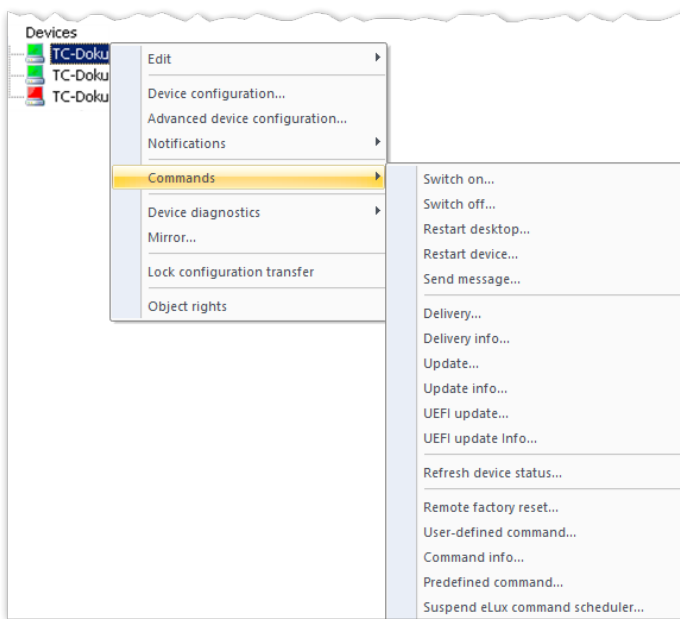
With the Zoom Citrix plugin, ZoomVDI can be used in a virtual desktop infrastructure with a Citrix solution. Peer-to-peer connections are not supported in this scenario.

## 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 Scout commands on individual devices, on OUs and on Dynamic Device Groups.

In addition, the context menu of an individual device provides the commands for device diagnostics and for mirroring.



By default, before Scout commands are sent to the selected devices, their current device status is determined. Devices that are switched off are then switched on, if possible, and after command execution are switched off again.

In contrast to commands processed by the eLux Command Scheduler, commands cannot be "stored" and executed at a later time when a device is up again.

### 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 devices      |
| Switch off...      | Switches off the devices     |
| Restart desktop... | Restarts the eLux interface. |
| Restart device...  | Restarts the devices         |

| Command  | Description  |
|--|--|
| Send message...  | Sends a message to the devices   |
| Delivery...  | Delivers software for a firmware update  |
| Update...  | Performs a firmware update   |
| UEFI update...   | Performs an update of the UEFI firmware<br>For further information, see <a href="#">UEFI update in analogy to firmware update</a> in the UEFI/BIOS update guide.   |
| Refresh device status...                                       | Requests the current device status and refreshes the status of the devices in the tree view  |
| Remote factory reset...  | Sets the devices back to initial state<br>The configuration is deleted, the IDF remains.<br>For further information, see "Factory reset command" on page 260.  |
| User-defined command...  | Enter a user-defined command that will be sent to the devices.<br>For further information, see "User-defined Commands" on page 262.  |
| Predefined command...  | Provides user-defined commands that have been predefined globally. For further information, see "Creating predefined commands" on page 264.  |
| Suspend eLux command scheduler                                 | If recurring eLux 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...<br>(not available for individual devices) | Prepares the configuration data for an OU or Dynamic Client Group. For further information, see "Configuration run" on page 66.<br>This command is not available for an individual device.   |

For further information on options you can add to the respective commands see "Command options" on page 254.

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 Allows to switch to other commands
- 2 Users are informed before command execution, see "Command options" on the next page.
- 3 Users are allowed to prevent the command execution.
- 4 Command-specific option
- 5 Only switched-on devices<sup>1</sup>
- 6 Time of command execution, see "Scheduling commands" on the next page
- 7 Delay of execution between devices
- 8 Apply command additionally on devices in subordinate OUs

1. For the relevant device, OU or Dynamic Client Group, from the context menu, choose **Commands**.
2. From the sub-menu, choose a command.  
*The **Command** dialog opens. The options shown depend on the selected command.*
3. Check the target devices to which the command is sent: To show the complete title with relevant device or OU, move the mouse pointer over the title bar.
4. Edit the relevant options. For further information, see "Command options" on the next page and "Scheduling commands" on the next page.
5. Confirm with **Execute** or **Schedule**.

*The command is executed at the specified time. Depending on the command, you are asked to confirm.*

<sup>1</sup>from Scout 15 2204

### 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.

1. For the relevant device, OU or Dynamic Client Group, from the context menu, choose **Commands**.
2. From the sub-menu, choose a command.
3. To schedule a command to be executed once, select **Once**. Then select the date and time.
4. To schedule repeated execution, select **Every**. Then select the day of the month or week and the time.
5. Edit the other options of the **Command** dialog.
6. Click **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 options

The options you can use to execute a command vary to some extent depending on the selected command.

#### General and common options

| Option          | Description   |
|-----------------|---|
| Command         | <p>The selected command is displayed.</p> <p>The list-field allows to switch to other commands.</p>   |
| Inform user     | <p>Users are 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 and the system waits until the user confirms the command execution.</p> <p>For firmware updates or UEFI updates, additional deferment options can be configured in the device configuration. For further information, see "Update deferment by users" on page 120.</p> |
| User can cancel | Users are allowed to prevent the command execution.   |

| Option   | Description   |
|--|---|
| Send only to devices with <b>Switched-on</b> status <sup>1</sup> | <p>Only for <b>Update</b>, <b>Delivery</b>, <b>User-defined</b> and <b>Pre-defined</b> commands</p> <p>The command is sent only to devices shown with <b>Switched-on</b> status. Switched-off devices are skipped. The actual device status is not determined before command execution.</p> <p>If the <b>Check reachability</b> option is also selected, a <b>ping</b> command is used to determine the current status of the relevant devices before the command is issued. The command is only sent to the responding devices. This avoids timeouts that can be caused by devices that are not ready for operation despite showing a <b>Switched-on</b> status.</p> <p>Default (both options disabled): The device status of the relevant devices is determined before the command is executed. If possible, switched-off devices are switched on for command execution and then switched off again. If a large number of devices is affected, we recommend that you select the above options instead. This allows for a faster and smoother operation.</p> |
| Run with system rights   | Some commands require system rights which are checked before execution.   |
| Now/Once/Every   | Time of execution, see "Scheduling commands" on the previous page   |
| On more devices wait   | Delay command execution between individual devices  |
| Include sub-OUs  | The command is additionally applied to all devices in subordinate OUs.  |

## Command-specific options

|  |   |
|--|---|
| <b>Send message</b> / Message                            | Select the message to send from the list or enter your message text. To format your message text, use HTML tags.  |
| Title  | Optionally edit the title of the message.   |
| Visible  | Optionally specify the display duration in seconds. With 0 seconds, the system message will be shown until the user clicks <b>OK</b> .  |
|  | Selected or all previously sent message texts can be deleted from the list via button.  |
| <b>Delivery</b> / Clean update partition before delivery | <p>Before writing to the flash memory, the update partition is cleaned up.</p> <p>All files of the current software image must be re-transferred from the web server. For further information, see "Performing deliveries via command" on page 294.</p> |

<sup>1</sup>from Scout 15 2204

|  |  |
|--|--|
| <b>Update</b> / Format system partition before update                                      | <p>Before the software is installed, the system partition of the flash memory is formatted.</p> <p>For the installation if the firmware update, All files of the current software image must be re-transferred from the web server. For further information, see "Performing updates via command" on page 288.</p> |
| <b>UEFI update</b> / Overwrite identical or higher version                                 | The UEFI system is always overwritten. This is necessary for a downgrade, for example. For further information see Performing UEFI updates via Scout command.  |
| <b>Remote factory reset</b> / Retain local configuration<br>Delete Scout<br>Server address | See "Factory reset command" on page 260  |
| <b>User-defined command</b>  | Below the command name, select a command from the list or enter a command. For further information see "User-defined Commands" on page 262.  |
| <b>Predefined command</b> / Selection  | Select a predefined command from the list. The function requires that commands have been predefined centrally, see "Creating predefined commands" on page 264.   |

## 8.5. Command results and update information per device

Feedback on performed Update, Delivery and User-defined commands is available for individual devices

- in the **Properties** window
- in the **Update info/Command info/UEFI update info** dialog (via device context menu)

### Note

In addition, all executed commands for all devices are displayed in the **Command history** window. For further information, see "Command history" on page 259.


All processes are recorded, even if the commands turn out to be obsolete and haven't been run or have been aborted. Successfully completed commands are shown with a green symbol.

## Viewing command results for an individual 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:*

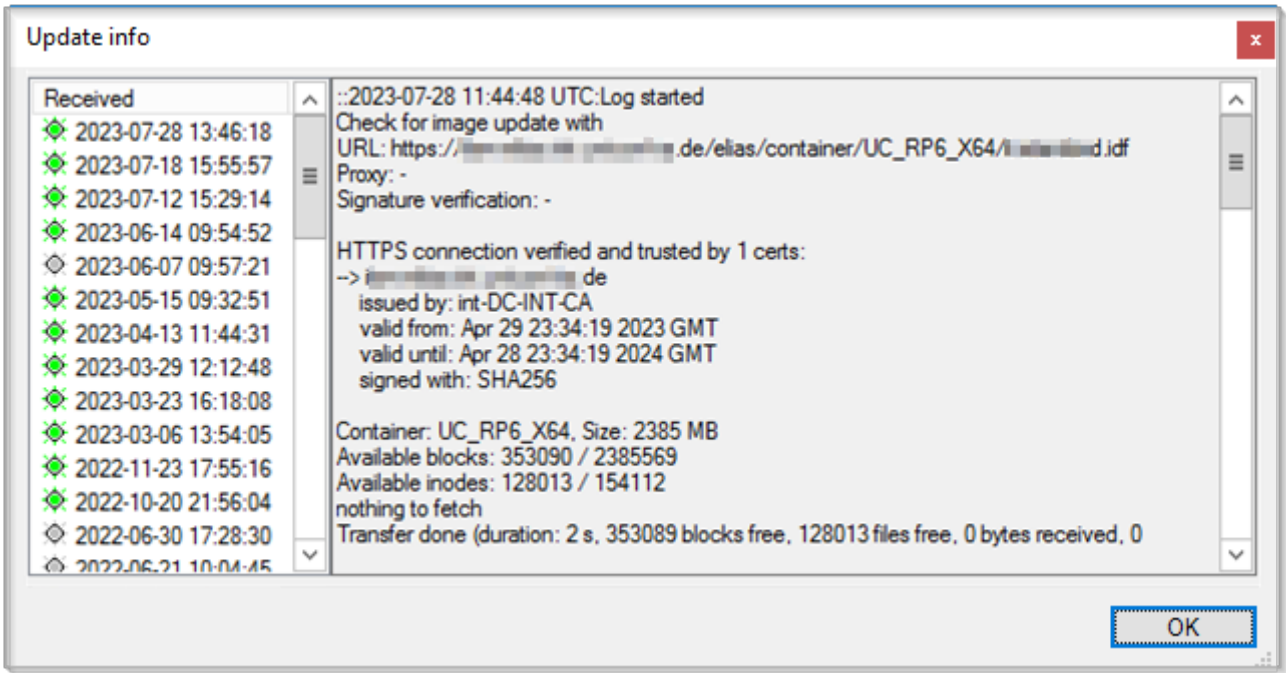
|                 |  |
|-----------------|--|
| Image           | Current image  |
| Update time     | Exact point in time of the latest update   |
| Update status   | Current status such as Update in progress, Update successful or Update not necessary |
| Update provider | Origin of software packages (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 packages.



Command Info

Information on the last command or update of a device can also be viewed by using the device context menu in the tree view.

- ▶ From the context menu, choose **Commands > Commando Info** or **Delivery Info**, **Update Info**, **UEFI update Info**.

Scout Report Generator

Use the following fields for your evaluations:

|   |  |
|---|--|
| Command name  | Executed command for user-defined commands |
| Command time<br>(UEFI) update time<br>Delivery time | Time stamp of command execution            |

Command result: Successful | Failed | Not available  
 Update state: Further values are available for Update and Delivery commands.  
 Delivery state

Command output<sup>1</sup>: Only for user-defined commands with specific results  
 Note that the **Command result** may be successful for many commands while there is no **Command output**.

For Update, UEFI update and Delivery commands, further fields are provided corresponding to the fields in the **Properties** window.

## 8.6. 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   |
| End        | Date and time of sending command to the devices / ending time<br><br>The ending time of a job is reached when either the devices report back <b>Successful</b> or <b>Failed</b> 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  |

<sup>1</sup>from Scout 15 2204

| Option        | Description   |
|---------------|---|
| 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.<br><br><i>A first click sorts the jobs ascending and the second one sorts descending.<br/>To reproduce the default sorting order click F5.</i> |

Apply the following options to a selected job:

| Option                           | Action  |
|----------------------------------|---|
| View details                     | Click <b>Details...</b><br><br><i>The <b>Command details</b> 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 tree view | Right-click an object name, and then click <b>Find in tree view</b> .<br><br><i>The first result is selected in the tree view.</i>  |
| Terminate running job            | Select the running job, and then click <b>Terminate</b> .<br><br><i>A command terminating request is sent to the Scout Server and the transmission of the command to the devices is stopped.</i>  |

## 8.7. Factory reset command

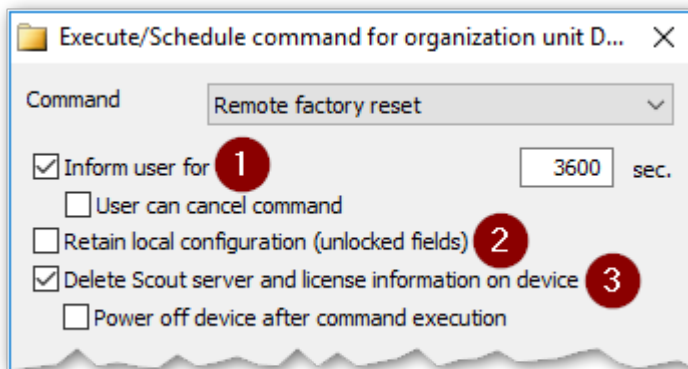
Use the **Remote factory reset** command to reset the configuration of the relevant devices to their initial state. The local device configuration and local application definitions will be deleted.

The following data are retained:

- The installed image with all software packages (firmware)
- Connection data to the Scout Server including the server address and OU ID (default)
- License information (default)

After the device has received the **Remote factory reset** command, the current device configuration and local application definitions are deleted. By default, after a restart, the device reconnects to its Scout Server and obtains the configuration of the OU to which it is assigned.

## Additional options of the Factory reset command



1 Users are informed before command execution, see "Command options" on page 254.

2 Prevent local device configuration from being overridden

3 All configuration data on the device will be deleted.

The device then loses connection to its Scout Server.

Optionally define to switch off the device afterwards.

| Option  | Description   |
|---|---|
| Retain local configuration (unlocked fields)          | <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 <b>Advanced options &gt; Devices</b> -</p> <p>For further information, see "Supporting local configuration" on page 62.</p>   |
| Delete Scout Server and license information on device | <p>In addition to the configuration data, the following data are deleted:</p> <ul style="list-style-type: none"> <li>■ Address of the Scout Server machine</li> <li>■ License information stored on device (license lease)<sup>1</sup><br/>This option can be used for the resale of devices, for example.</li> <li>■ Certificates in <code>/setup/cacerts</code></li> <li>■ WLAN configuration</li> <li>■ 802.1X configuration</li> <li>■ Private key of SCEP client certificate stored in a TPM 2.0 module</li> </ul> <p>An encrypted setup partition (TPM 2.0) will be decrypted.</p> <p>If you perform the <b>Remote factory reset</b> command with this option selected, it corresponds to a local <b>Factory reset</b> triggered by the relevant eLux command in the eLux <b>Command panel</b> on the device. For further information, see <a href="#">Resetting devices to factory status</a> in the <b>eLux RP</b> guide.</p> |
| Power off device after command execution <sup>2</sup> | <p>- only available with <b>Delete Scout Server and license information on device</b> -</p> <p>The device is shut down and remains switched off.</p>  |

<sup>1</sup>from Scout 15 2302 (previously available as a separate option)

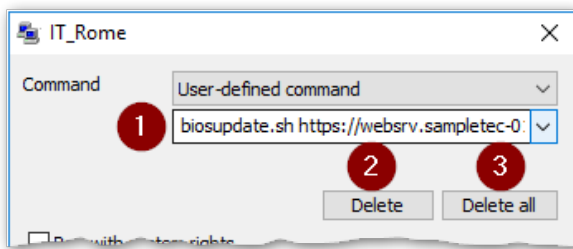
<sup>2</sup>from Scout 15 2302 (previously done automatically after deleting the license information)

### Note

The **Remote factory reset** affects the device's setup partition. The system partition with the installed firmware, in contrast, is not affected by the factory reset and is only changed using the **Update** command with the option **Format system partition before update**.

## 8.8. User-defined Commands

Authorized administrators may issue individual commands to the devices. A user-defined command can be executed with system rights so that far-reaching operations can be performed. The correct syntax is particularly important here.



- 1 Select a command from the list (recently used commands) or enter it.
- 2 Delete selected command
- 3 Delete all user-defined commands

**Important** Always test a user-defined command in a test environment before using it productively.

User-defined commands can be helpful for tasks such as the following:

- Perform a special UEFI/BIOS update
- Update a license lease
- Wipe data disks

### 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.

### 8.8.1. Wiping the data disk

- from eLux RP 6 2204 -

To permanently erase all data of devices from their flash memory, a script is available that you can apply as a user-defined command. The script overwrites all partitions of the primary disk with zeros.

1. Make sure that the devices have the required operating system version.
2. For the relevant device, OU or Dynamic Client Group, from the context menu, choose **Commands > User-defined command**.
3. To run the script, below **User-defined command**, enter the following command:  
`wipe-device really-wipe`  
*The script must be run with the `really-wipe` parameter to prevent accidental execution and wiping of the disk.*
4. Select **Run with system rights**.
5. Click **Execute**.

*The relevant devices confirm the command execution (last contact to the Scout Server) and shut down. The devices then restart one more time with the core installer, which zeros all partitions of the disk. After that, the devices shut down finally.*

## 8.9. 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 UEFI/BIOS update of particular hardware or a script to renew the license lease of eLux RP 6 devices.

These commands are then available via the **Command** dialog and can be used by authorized administrators. To create a predefined command:

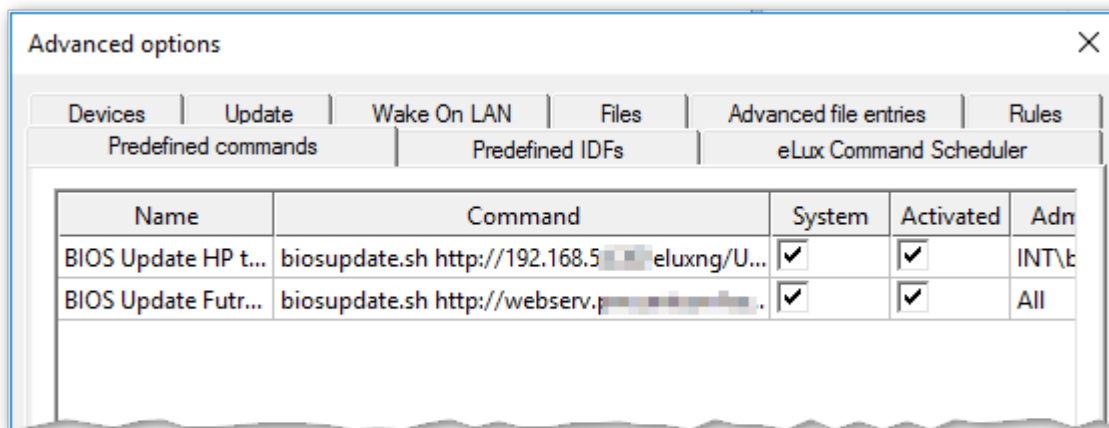
1. On the Scout menu, click **Options > Advanced options > Predefined commands**.
2. Click **Add**.
3. For your new entry, edit the following options:

| Option              | Description   |
|---------------------|---|
| Name                | The command name is shown to administrators in the <b>Commands</b> 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 predefined command, you can use variables. The values for each variable are prompted when the administrator selects the predefined command in the <b>Command</b> 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></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 <sup>1</sup> | <p>A predefined command is shared with all administrators by default.</p> <ul style="list-style-type: none"> <li>▶ To restrict to specific administrators or groups,<sup>2</sup> click the cell under <b>Admins</b> and then select the desired administrators/groups from the list.</li> </ul> <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**.

<sup>1</sup>from Scout Enterprise Management Suite 15 2101

<sup>2</sup>with active administrator policies



You will 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 Device 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**
- in the **Command Info** window (command history for relevant device)

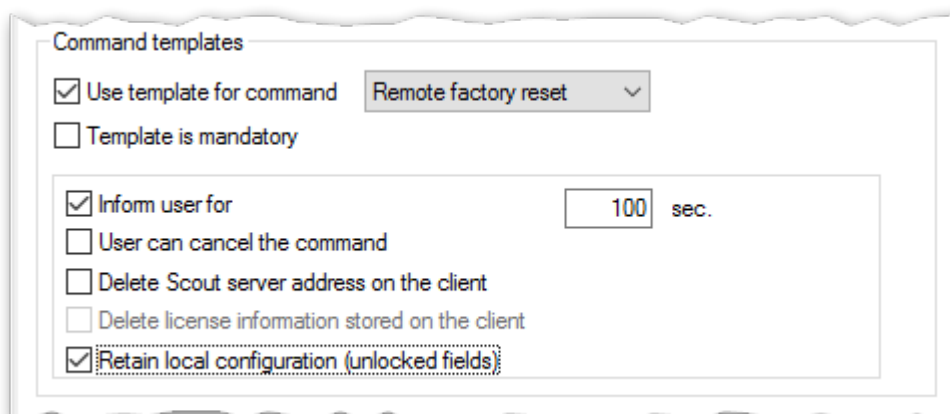
## 8.10. Defining templates for standard commands

For standard commands such as **Restart** or **Update**, you can define preferences via templates.

1. On the Scout 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   |

---

**Note**  
Templates for standard commands are only available in the Scout Console but not in the Scout Dashboard.

---

## 8.11. eLux Command Scheduler

- from Scout 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 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.

### 8.11.1. Defining eLux Commands

- from Scout 15 2103 -

The eLux Command Scheduler is configured in the Scout Console.

The screenshot shows the 'Define eLux command' dialog box with the following fields and annotations:

- Command:** A dropdown menu showing 'Update' with a red circle '1' next to it.
- Schedule:** A section containing a 'Weekly' dropdown, a '20:00:00' time input, and a 'Sunday' day dropdown, with a red circle '2' next to the day dropdown.
- User interaction:** A section with a red circle '3' next to the header. It contains a checked checkbox 'Inform user for' followed by a '30' seconds input and a 'Reminder...' button. Below it is an unchecked checkbox 'User can cancel command'.
- Command execution:** A section with a red circle '4' next to the header. It contains a 'Spread factor' input set to '0' seconds, followed by a red circle '5' next to the input. Below it are two checked checkboxes: 'Persistent' (with a red circle '5' next to it) and 'Wake device from sleep' (with a red circle '6' next to it).

At the bottom right are 'OK' and 'Cancel' buttons.

- 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<br><br>To execute <b>user-defined commands</b> , system rights are required. Therefore, include the password.  |
| Schedule               | Periodic scheduling of the command<br><br>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 270.  |
| User interaction       | 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" on the facing page.   |
| Spread factor          | Time span in which random delays are generated to prevent simultaneous execution on many devices<br><br>Example 600 seconds:<br>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.<br><br>Default: 0 |
| 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`.

### 8.11.2. Deferment options for users

Similar to Scout 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 deferments | 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 291

### 8.11.3. 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, from the context menu, choose **Commands > Suspend eLux Command Scheduler**.
2. Click **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.

## 8.11.4. 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>4<sup>1</sup></td><td>User-defined</td></tr> <tr> <td>5</td><td>Shut down</td></tr> </table>   | 1        | Update        | 2      | Synchronize configuration | 3     | Restart device | 4 <sup>1</sup> | User-defined    | 5      | Shut down          |               |                      |                      |                           |             |   |                    |  |
| 1                    | Update   |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |
| 2                    | Synchronize configuration  |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |
| 3                    | Restart device   |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |
| 4 <sup>1</sup>       | User-defined   |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |
| 5                    | Shut down  |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |
| Schedule             | <p>The format follows the <b>systemd calendar events</b>. Syntax for a timestamp:<br/>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 <a href="https://www.freedesktop.org/software/systemd/man/systemd.time.html">https://www.freedesktop.org/software/systemd/man/systemd.time.html</a></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>  |          |               |        |                           |       |                |                |                 |        |                    |               |                      |                      |                           |             |   |                    |  |

<sup>1</sup>from Scout 15 2103

| Parameter  | Description   |
|------------|---|
| Persistent | <b>true false</b><br><br>If <code>true</code> , missed command executions (jobs) are immediately recovered after the next device start. |
| Command    | Only for <code>Type=4</code> : Command for user-defined command   |
| WakeSystem | <b>true false</b><br><br>If <code>true</code> , the system will be woken up from sleep mode (suspend) to execute scheduled commands.    |

---

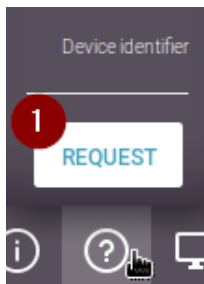
## 9. Remote maintenance

For maintenance, user help-desk and troubleshooting purposes, the administrator can use different tools to access the devices.

### 9.1. Device identifier for support

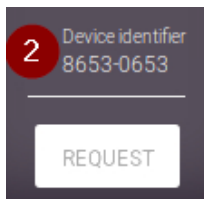
- from Scout 15 2101 and eLux RP 6 2101-

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.



Users have a question mark icon on the system bar, provided the user right **Request simple device identifier** is enabled (default).

- ▶ To request the so-called **Simple device identifier**, users click <sup>1</sup> the question mark icon and then **Request** (1).



The system generates and transmits a temporary device identifier for the requesting device (2).

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.

---

<sup>1</sup>or 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 devices, 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 > Security > Mirror settings**, mirroring must be enabled and configured. For further information, see "Configuring mirroring " on page 124.

### 9.2.2. Mirroring from Scout Console

Throughout a mirror session, the user receives a system message which is displayed on both the user's 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 user.

---

1. For the relevant device, from the context menu, choose **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 " on page 124.

*The mirror session is started. On the user's screen, a system message is displayed that can be moved but not closed unless the mirror session is closed.*



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<br>(only if configured) | The connection is disconnected and the user is logged off.<br><br>This option is only available if, in <b>Device configuration &gt; Security</b> , the option <b>Logoff after disconnect</b> 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. The MAC address of the respective devices is also recorded.

### 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 device is connected to:<br><br><code>HKEY_CURRENT_USER\Software\Unicon\Scout\Settings\BindIPAddress</code> |

### 9.3. Device diagnostics

---

#### Note

This feature can only be applied to an individual device.

---

Device diagnostics help you run predefined commands on the device and retrieve protocol and configuration files from the device. These are then sent to Scout or other destinations for diagnostic purposes. The requested client files support the administrator in error analysis and are required when you open a support ticket.

Depending on the user rights, the reverse way can be used: Users send diagnostic files or screenshots from the device.

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" on page 68.

---

### 9.3.1. Diagnostics scope and content

The amount of diagnostic files requested from a device is defined by two factors:

- Selected templates in the **Diagnostic files** dialog  
In addition to the `#System` template, further individual templates might be active.
- Configured log level ("Diagnostics tab" on page 154)  
Only the enhanced log level allows to execute all script on the device and retrieve all files defined in the `#System` template.

#### System template

To perform device diagnostics, a predefined template called `#System` is provided. This template includes a file list with relevant configuration and log files plus a script code to be run on the device. Neither of them can be edited. You cannot deactivate the system template.

The system template contains the following files:

- Log files for eLux and components
- eLux configuration files, including `terminal.ini`, `user.ini`, `sessions.ini`
- Configuration files of standard components and standard applications

The defined script contains different system commands that request software and hardware information from the device. Included are for example runtime information, installed packages, active codecs, the update partition, PCI and USB devices. Via **fwupdmgr**, firmware information about installed components such as the UEFI system or the flash memory is also retrieved.<sup>1</sup>

The output of the system commands is stored in the `mytrace.log` file, which is transmitted along with the other files in a `.zip` archive.

---

#### Note

Authorized administrators may define additional custom templates.

---

### 9.3.2. Log level

Two log levels are provided in the device configuration of eLux devices: **Standard** and **Enhanced**. These levels correspond to switching the enhanced log level **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.

---

#### Note

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.

---



---

<sup>1</sup>from Scout 15 2204

## 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.*

### 9.3.3. Requesting diagnostic files

---

#### Note

Before you perform device diagnostics, we recommend that you temporarily enable enhanced logging on the device. For further information, see "Log level" 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) will be processed.*

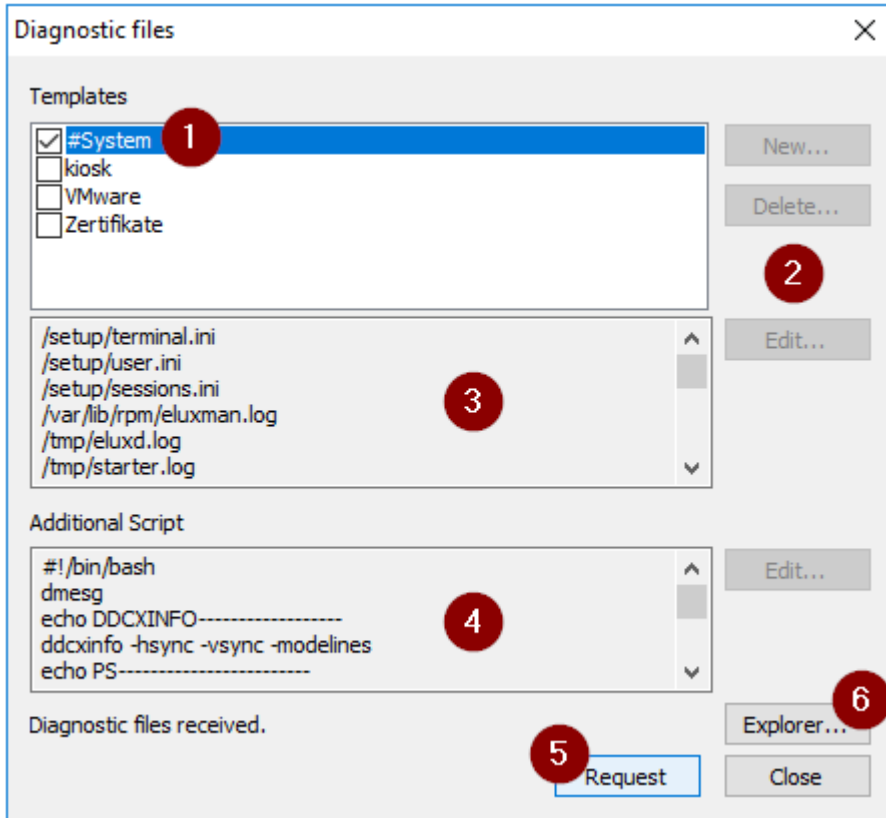
2. The required object right provided, you can select or clear further templates of the list.
3. Click **Request**.

*All scripts defined in the active templates are executed on the device.*

*All files defined in the active templates are retrieved from the device and saved as a .zip file in the local user directory <userprofile>\Documents\UniCon\Scout\Console\Diag of the Scout machine.*

4. Click **Explorer**.

*The Windows Explorer opens showing the diagnostics target directory.*



#### 1 Predefined template #System

This template is always active and can neither be deleted nor edited.

#### 2 Provided an administrator owns the **Edit diagnostic templates** object right, she/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 commands are executed and the defined files requested from the device.

#### 6 Once the requested files are available, open the Explorer with the diagnostics target directory.

### 9.3.4. Defining an individual template

In addition, authorized administrators may define further templates containing files and script. The templates are available globally, no matter where you define them.



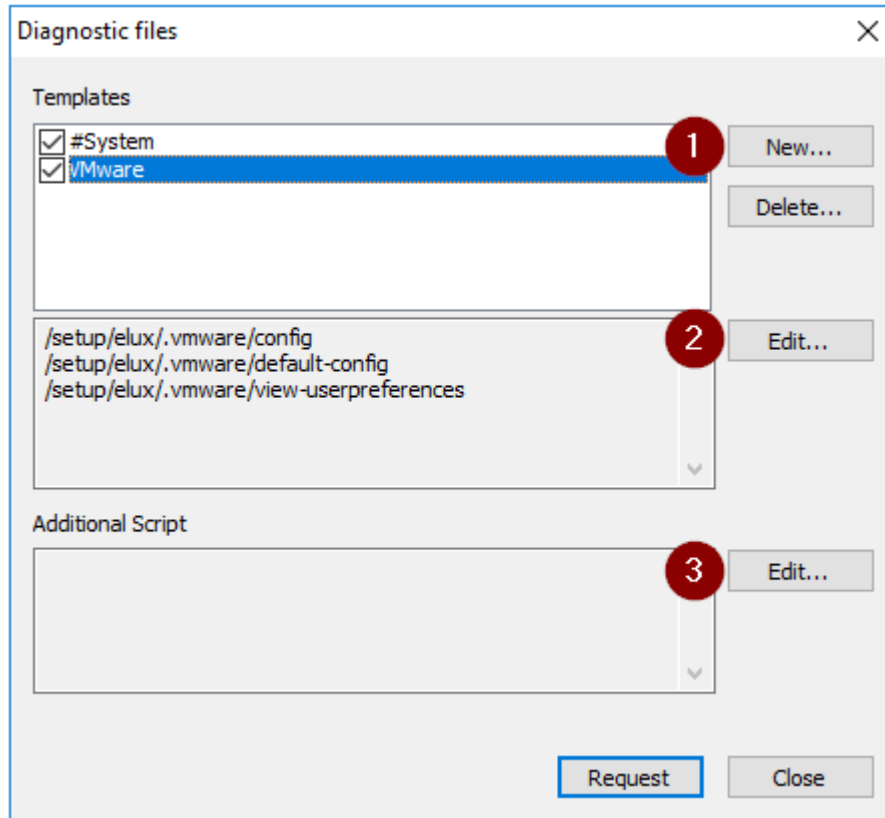
#### Requires

Object right **Edit diagnostic templates** (disabled by default)

1. On the context menu of a device, choose **Device diagnostics > Request files**.

*In the **Edit diagnostic files** dialog, the predefined #System template and, if defined, further templates are shown.*

2. Click **New...** (1). 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** (2).

In the text box, enter the relevant file names with path, line by line. Confirm with **Save**.

4. To enter script code you want to run on the device, next to **Additional script**, click **Edit** (3).  
Authenticate with the device password.<sup>1</sup>

In the text box, enter your code and confirm with **Save**.

### Note

When you perform the device diagnostics feature with **Request**, all selected templates are included. Whether all of the listed files of the #System template are written and transferred, depends on the configured log level.

<sup>1</sup>from Scout 15 2107

### 9.3.5. Further diagnostic adjustments

#### 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. You can specify the number of cycles for which the file is created and saved on shutdown of the device. The default is set to 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 277.

#### Store diagnostic files persistently

By default, the diagnostic files are stored on the device under `/setup/logs`.

- ▶ 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 <code>/setup/logs</code>                 |
|         | Example: <code>/update/logs</code> | 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 devices 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 our [myelux.com](https://myelux.com) portal.
- Modify the image file (IDF) on the web server via ELIAS.
- Check the firmware configuration of the relevant devices
- Perform the update
  - Deliver new software packages
  - Install 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 "Static proxy" on page 300.

---

### Ways to initiate a firmware update

Updates can be performed immediately or initiated automatically at a defined point in time:

- Use the **Update** command feature to execute or schedule (once or periodically) firmware updates.
- Define an **Update notification**. This will result in a firmware update on the next device restart.
- Configure the devices to automatically check for new image versions on start-up or shutdown. If an updated version is available, the update process will be started.

The **Check for new version** option is part of the **Device configuration > Firmware** and can be applied to individual devices, OUs and all devices.

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)
- OUs
- Dynamic Device 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 up-to-date eLux software packages on the web server
- ELIAS (eLux Image Administration Service) to create and modify image definition files in a software container
- Scout Console to configure firmware updates for the devices

Scout Server, Scout Console and the legacy ELIAS<sup>1</sup> 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 eLux 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.

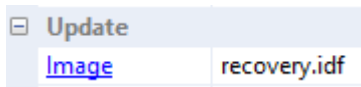
### 10.2. Access to applied images

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:

---

<sup>1</sup>Choose user-defined installation and select it as a feature.

- In the **Properties** window of a device, double-click the **image** link.

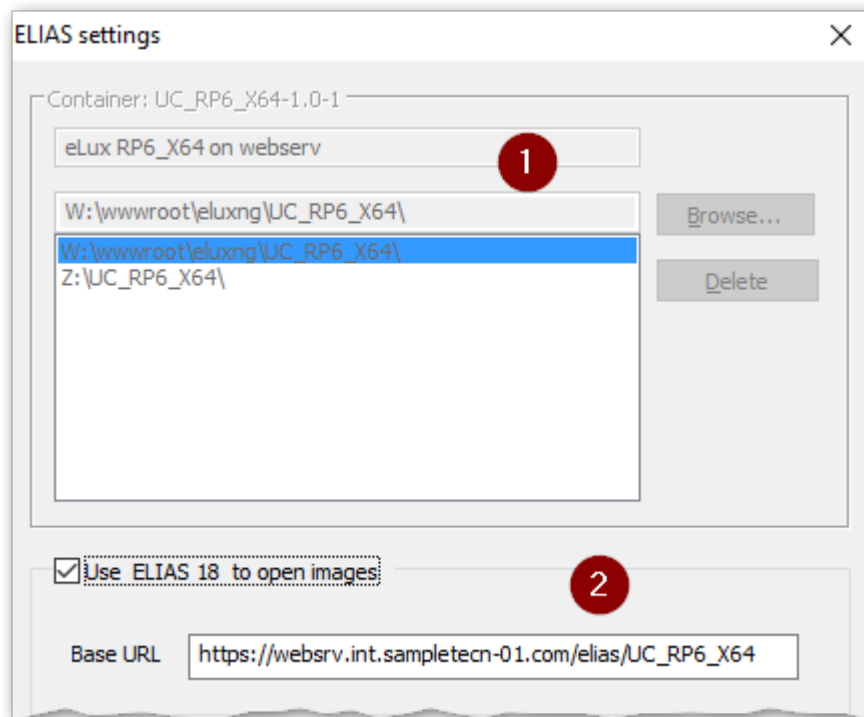


- In the device configuration of an OU or device, in the **Firmware** dialog, click the **ELIAS** button.

The connection to ELIAS is made with the data from the ELIAS settings. Here, you set either the legacy ELIAS or ELIAS 18<sup>1</sup> 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.<sup>2</sup>

Enter your ELIAS 18 URL including the container path.

(ELIAS 18 is designed to manage multiple versions in one container.)

4. Confirm with **OK**.

<sup>1</sup>from Scout 15 2110

<sup>2</sup>from Scout 15 2110

---

**Note**

The menu entry **View > ELIAS** offers another way to call ELIAS from the console.

---

## 10.3. Planning firmware updates

### Providing a new image

1. Download the latest software packages that are not yet included in your container from our portal. In ELIAS, import them 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.
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**.  
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 users" on page 120.
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 "Configuring firmware updates" on page 108.

## 10.4. Performing firmware updates

With the appropriate firmware configuration of the devices, you only need to provide an updated image to trigger a firmware update:

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.

### 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



### 10.4.1. Performing updates via command

#### Note

To deliver the software packages in a separate step before performing the update, use the **Delivery** command.

Execute/Schedule command for organization unit D... X

Command: Update

☒ Inform user for 3600 sec.

☒ User can cancel command

☐ Format system partition before update

☐ Send command only to devices with "Switched on" status

☐ Check reachability of the devices before

☐ Now

☒ Once

Date: Montag ,01.01.2024 Time: 12:00

☐ Every

Day in month/week: 1 Time: 13:10

On more devices wait for 0 ms after each command

☒ Include sub-OUs

Schedule Cancel

1. Select a device, an OU, a Dynamic Device Group or devices in the **All devices** window.
2. On the context menu, click **Commands > Update...**
3. To inform users before the update will be processed, we recommend that you select the **Inform user** option. For further information, see "Command options" on page 254 and "Update deferment by users" on page 120.

For further information on the impact, see "User information before update" on page 291.

4. To format the system partition of the device's flash memory before writing, select the option **Format system partition before update**.
5. Define the point in time for the update process. For further information, see "Scheduling commands" on page 254 and "Executing commands" on page 253.
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. Example:

---

Update in progress (Transfer started - 2022-08-20 11:34:23)

Update in progress (Transfer completed - 2022-08-20 11:35:45)

Update in progress (Installation started - 2022-08-20 11:35:48)

Update in progress (Installation completed - 2022-08-20 11:37:56)

---

For further information, see "Command results and update information per device" on page 257.

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 devices 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.

---

### 10.4.2. Updates initiated by the system

The devices 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 devices check 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 devices determine the delta between the software packages defined by the image definition file on the web server (image) and the locally installed software packages. If a delta exists, a firmware update is necessary.

- If a firmware update is necessary, a device 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 device, in this case, the firmware parameters locally stored on the device are used.

---

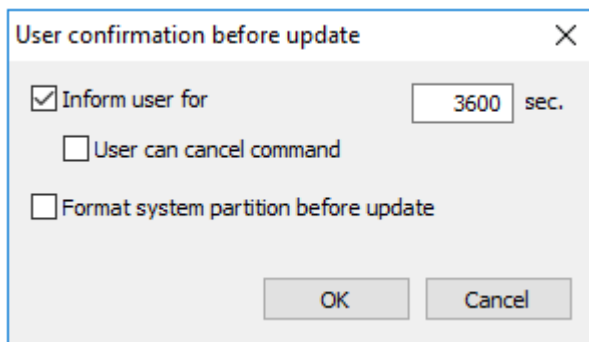
## Exception for VPN connections

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. Users can continue working without interruption.

For devices connected via the Scout Cloud Gateway, the option can be used without limitation.

## Configuring firmware updates initiated by the system

1. For the relevant devices, in the device configuration, under **Firmware**, select **Check for new version on start** or **Check for new version on shutdown**.
2. If you choose **Check for new version on start**, additionally set **User confirmation** options and whether you want the system partition to be formatted before the update is performed.<sup>1</sup>



For further information, see "Configuring firmware updates" on page 108.

*After the devices have received the new device configuration, the option to check for new firmware versions becomes active.*

### 10.4.3. 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 firmware configuration.

1. Select a device, an OU, a Dynamic Device Group or devices in 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" on page 288.
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.*

---

<sup>1</sup>from Scout 15 2104.3000 and Scout 15 2209

For each device, in the **Properties** window, the **Update notification** field shows the value *Activated*.

---

#### 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, it receives an update request<sup>1</sup> 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" below.

The update status is displayed for each device in its **Properties** window. For further information, see "Command results and update information per device" on page 257. If an update fails, no system-side efforts will be made to retry.

For devices without update partition<sup>2</sup>, 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.

---

## 10.5. User information before update

---

#### Note

This feature refers to firmware updates and UEFI updates.<sup>3</sup>

---

Before an update is executed, the relevant users can be informed by a system message. Depending on the configuration in **Firmware > Reminder settings**, users are provided with various options for deferring or aborting the request.

---

<sup>1</sup>Note that updates are only performed if the relevant IDF has been modified.

<sup>2</sup>flash memory less than 4 GB

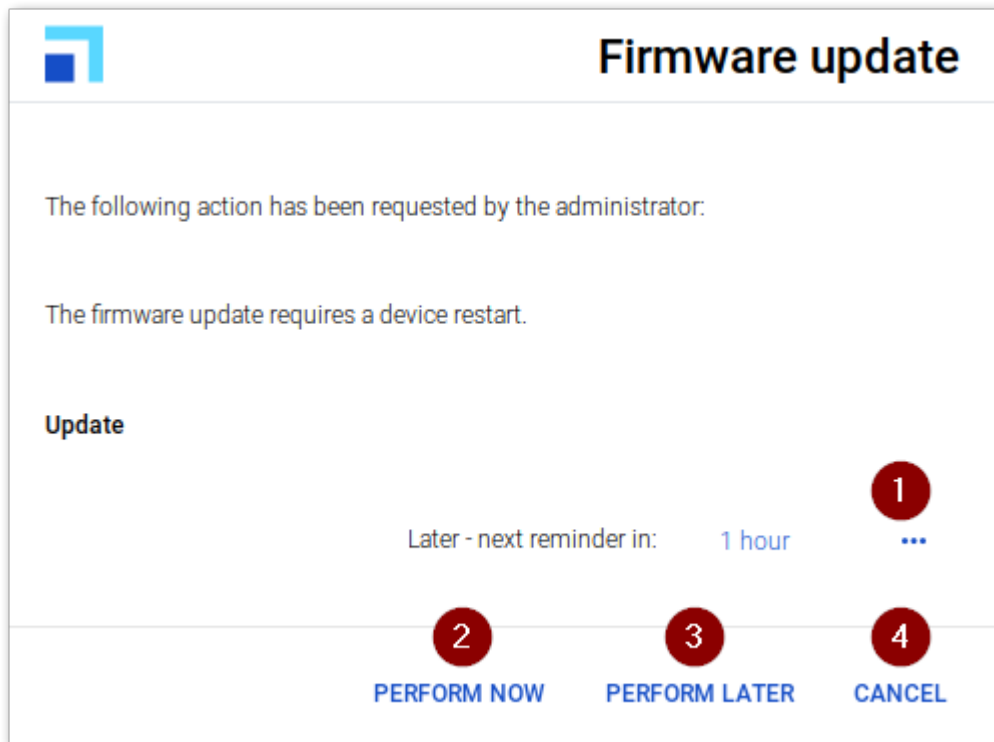
<sup>3</sup>from eLux RP 6 2107

The system message is displayed in the following situations:

- The administrator executes an **Update** command with the **Inform user** option.
- In the **Firmware** dialog, the option **Check for new version on start** with user confirmation<sup>1</sup> is configured.

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 the firmware update immediately

---

<sup>1</sup>ab Scout 15 2104.3000 und Scout 15 2209 mit zugehörigen eLux-Versionen

---

### 3 Postpone the 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 the 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.

---

## 10.6. 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 devices must be configured correctly, see "Planning firmware updates " on page 286

The software delivery can be triggered by a Scout command or a notification.

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.

### 10.6.1. Performing deliveries via command

1. Select a device, an OU, a Dynamic Device 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.  
For further information, see "Scheduling commands" on page 254 and "Executing commands" on page 253.
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. 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 and update information per device" on page 257.

### 10.6.2. Performing deliveries via notification

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 firmware configuration is started for this device.


1. Select a device, an OU, a Dynamic Device 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.*

*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 per device" on page 257. 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.

---

## 10.7. Dynamic proxy

You may use dynamic proxy devices for the software package distribution to all devices of the same subnet. A dynamic proxy 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 by using the zero-configuration networking implementation **Avahi**.

### 10.7.1. 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](#).

### 10.7.2. 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.

---

### 10.7.3. 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

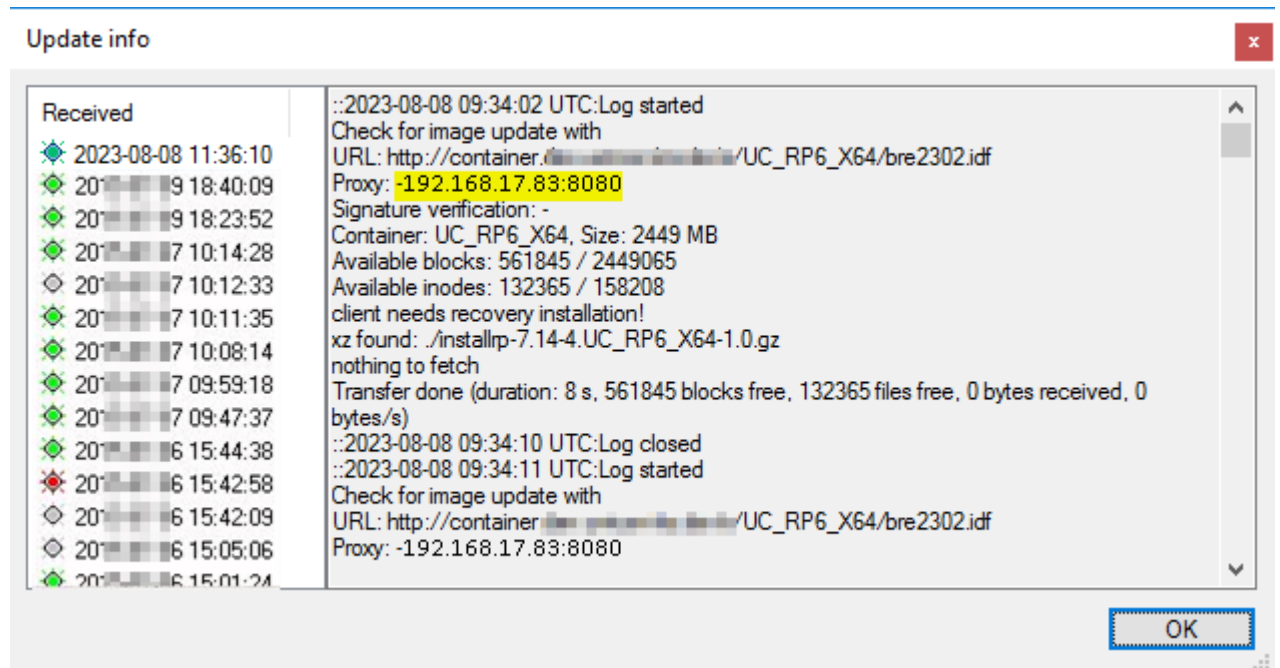
The provider checks the availability of the requested software packages on its update partition and downloads missing packages from the web server specified by the consumers.

#### 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 "Command results and update information per device" on page 257.



- The provider has a local file `/tmp/dynamic-proxy.log` containing the consumers that have been provided with software packages.

## 10.8. Static proxy

- from eLux RP 6 2204 -

If you want to update narrow-band connected devices, you might wish to use a proxy device to forward the firmware update. Proxy devices download the required software packages and distribute them to other devices.

The packages are kept locally in the RAM of the proxy device. Depending on the overall size of the packages defined in the image, 2 GB RAM or more are required.

For the proxy device, **Squid** is used as the proxy server software.

---

### Note

Squid supports the **HTTPS** protocol. To make the update process more secure, you may additionally use signatures for the image and software packages. For further information, see "Firmware security through signatures" on page 117.

---

The configuration in Scout includes three basic steps:

- Creating an application definition for Squid
- Setting up the proxy device
- Configuring the relevant devices for the proxy update

### Creating an application definition for Squid

1. Create a dedicated OU which will be configured for the proxy device.
2. For the new OU, add a local application. On the **Local** tab, edit the following fields:

| Option                              | Value  |
|-------------------------------------|--------|
| Name of application                 | Squid  |
| Local application                   | Custom |
| Parameter                           | squid  |
| Hidden                              | On     |
| Start automatically after 0 seconds | On     |

3. Move the proxy device into the OU and restart it.

*The device receives the Squid application definition.*

### Setting up the proxy device

1. Provide the proxy device with a firmware image including the **Squid Update Proxy** package. To do so, modify the relevant image by using ELIAS, and then update the device.

**Important** The **Dynamic Proxy update** package must not be included.

- For the OU of the proxy device, open **Device configuration > General** and clear the **Use parent** option.

*Inheritance is disabled and the proxy OU can be configured individually.*

- In **Device configuration > Firmware**, on the **Proxy type** list, select **None**.
- For the proxy device, open **Device configuration > Network > LAN**, and edit the LAN connection.  
In the **Edit network profile** dialog, select **Use following IP address**.  
Leave the **Domain** box empty and confirm with **OK**.

*The last obtained IP address is used as the static IP address by the proxy device.*

## Configuring devices for the proxy update

- For the OU or devices you want to receive their firmware updates through the proxy device, open the **Device configuration** dialog.
- On the **Firmware** tab, edit the following fields:

|                   |                                   |
|-------------------|-----------------------------------|
| Protocol          | HTTP                              |
| Proxy type        | Static (Consumer)                 |
| Provider          | <IP address of proxy device>:3128 |
| User and Password | <no entry>                        |

- Edit the further fields as usual, see "Configuring firmware updates" on page 108.

*Once the modifications have become active, the relevant devices receive their firmware updates from the proxy device.*

## 10.9. Troubleshooting firmware update

### Error messages



| Error message                     | Reason   | Solution  |
|-----------------------------------|--|---|
| Bad container                     | Containers are hardware-specific.  | Check whether the container matches your device specifications.   |
| Bad flash size                    | IDF size exceeds flash size  | Verify whether the image size defined by the IDF matches with the actual flash size of the device.                  |
| Bad authorization                 | Incorrect device password  | Correct the entry in <b>Device configuration &gt; Security</b> .  |
| Client needs recovery information | If critical feature packages (.fpm) are updated in the baseOS, the device requires a recovery installation before it can be updated. | For further information see <a href="#">Recovery procedures</a> in the <b>eLux Recovery procedures</b> short guide. |

### Update options

If the update is still faulty, try to modify the update settings. For further information, see "Update/Delivery" on page 166

## 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 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 .
  - ▶ To reset a password entry, click .

### 11.1. Local device password

The device password affects the local devices. All devices managed by a specific 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 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.

For further information, see [Device password](#) in the eLux guide.

#### 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 **Restart** command for the relevant devices (now or scheduled). For further information, see "Executing commands" on page 253.

---

### 11.1.2. Changing local device password on a 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 .

3. Confirm with **Apply**.

**Important** The device can no longer be managed by Scout.

## 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 lowercase).

---

### Note

We strongly recommend that you change the password immediately in order to prevent unauthorized access.

---

- ▶ To change the console password, log on to Scout as administrator and click **Options > Change console password...**

or

- ▶ Enable the "Activating administrator policies" on page 307.

*As soon as the administrator policies are enabled, the default account and console password are disabled.*

We recommend enabling the "Activating administrator policies" on page 307 and using your AD accounts for Scout.

## 12. Managing administrators

### 12.1. Activating administrator policies

Managing more than one Scout administrators requires enabling the **Administrator policies** feature. Scout administrator accounts are based on AD accounts which must be defined before. Scout 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" on page 315 now.*

*The `Administrator` default account is not available any longer and the **Change console password...** option is disabled.*

### 12.2. Adding administrators

You may define any AD users or groups as Scout administrators.

---

#### Note

Check whether the relevant SQL Server permissions are set. For further information, see SQL Server users and application roles in the **Installation** guide.

---

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 may assign the appropriate object rights to them now. For further information, see "Administrator policy" on the facing page.*

*The administrators can log on to the Scout Console now 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 administrators list without an 'Are you sure?' verification.*



## 12.4. Administrator policy

For all Scout 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             |

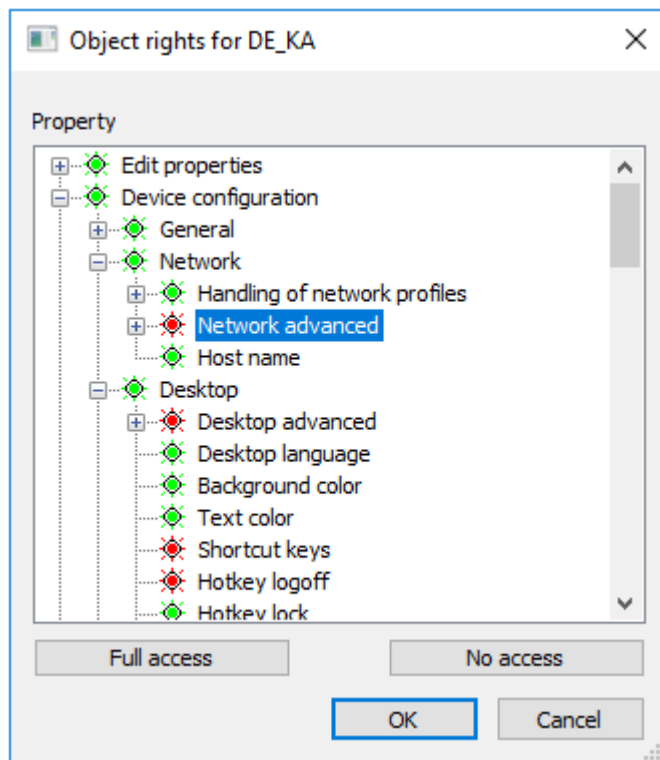
Note that in the dialog you must always first select the relevant administrator for whom you want to edit the access rights. To edit object rights, first select the relevant OU or device.

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 will no longer have access to the related function. For the last or only administrator existing, you cannot disable access rights. This is to prevent being locked out of the Scout Console

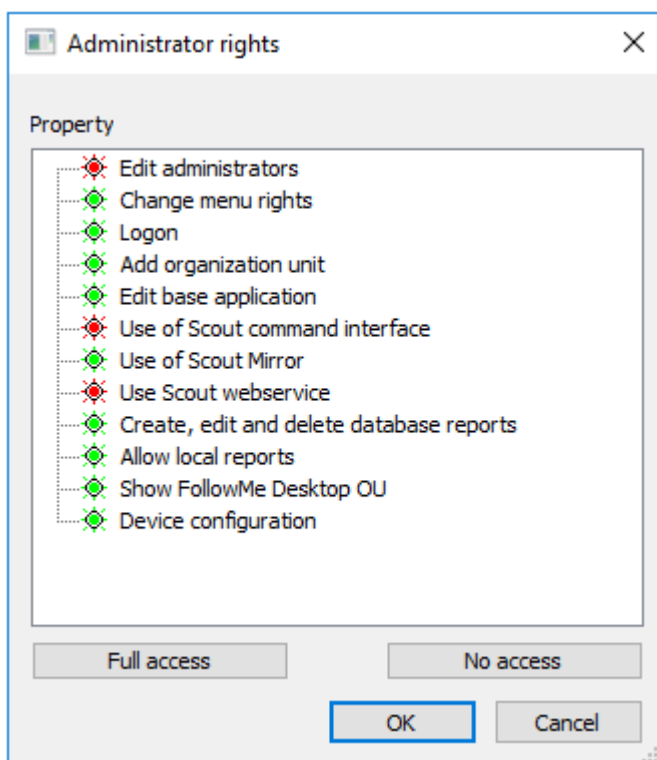
### 12.4.1. Changing base rights

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**.



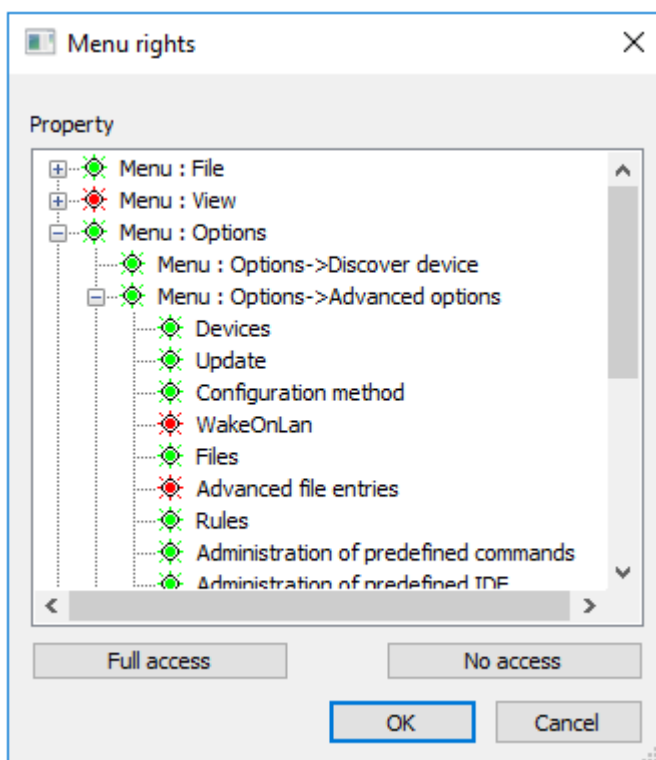
### 12.4.2. Changing menu rights

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**.



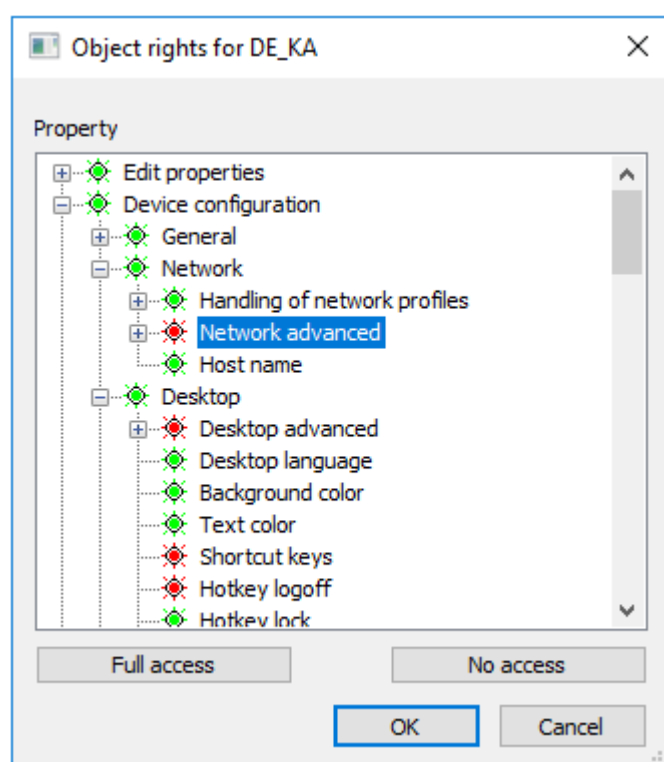
### 12.4.3. Changing object rights

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, from the context menu, choose **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.<sup>1</sup> At each level further activities are added. Logging with monitoring level 3 is the most detailed.

---

<sup>1</sup>from Scout Enterprise Management Suite 15 2101

## Note

Use monitoring level 3 only temporarily for diagnostic purposes, since all database transactions are additionally logged.

| Activities / level 1               | Activities / level 2                               | Activities / level 3   |
|------------------------------------|--|--|
| Log on                             | Save / Delete / Rename application                 | All SQL statements executed due to administrator activities in the console |
| Log off                            | Upload application                                 |  |
| Deny logon                         | Save <sup>1</sup> / Delete / Rename device         |  |
| Add / Activate / Delete license    | Save <sup>2</sup> / 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 command <sup>3</sup>        |  |
|                                    | Set / Delete relocation notification               |  |
|                                    | Set / Delete update notification                   |  |
|                                    | Set / Delete delivery notification                 |  |
|                                    | Set / Delete UEFI update notification              |  |
|                                    | MSP 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. The **Scout logon** window is not shown any longer.

<sup>1</sup>also applies to Move device

<sup>2</sup>also applies to Move OU

<sup>3</sup>specifying command type and target device/OU

## 12.7. Maintenance windows

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<br>Specify number and unit (hours or minutes)<br>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

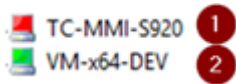
For a maintenance window, for example defined from Friday, 06.09.2019, 20:00 for 2 hours, you can set the following repeat options:

|                               |  |
|-------------------------------|--|
| 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 Keep Alive service

The Scout Keep Alive service offers an evaluation of configurable status messages of the managed devices. These status messages are called **keep alive messages**.

Within a defined time interval, the configured devices send status messages to the Scout Keep Alive service. These messages allow to refresh the status of the relevant devices in the Scout Console.



- 1 The device has no network connection or is switched off.
- 2 The device is ready for operation. The network connection is operational.

For further information, see "Icons in the tree view" on page 14.

The configuration is part of the device configuration and can be applied to the entire infrastructure or to selected OUs and devices.

The **keep alive messages** are transferred from the devices to the Scout Keep Alive service by using the HTTPS protocol. This requires a valid SSL certificate. For further information, see [Certificate for Scout Keep Alive service](#).

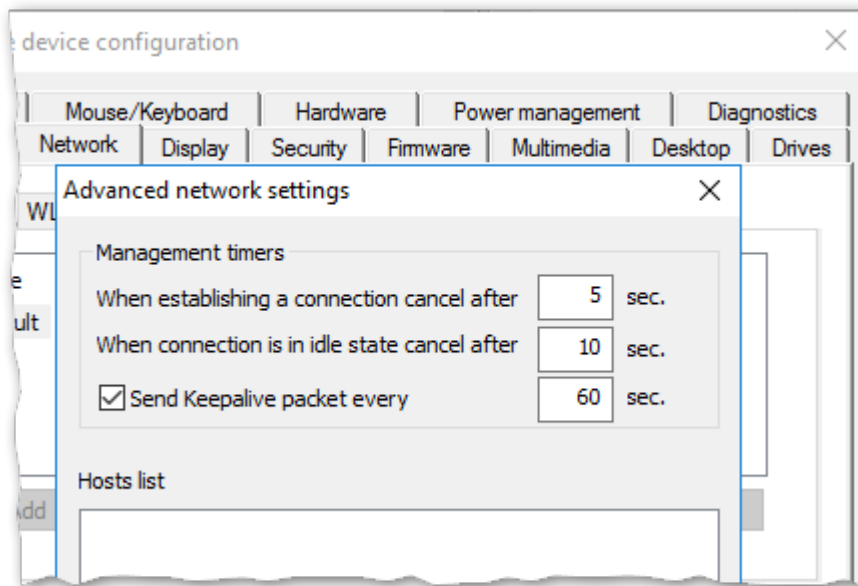
### Note

For Scout versions up to Scout 15 2204, the Scout Statistics Service as an optional component of the Scout Enterprise Management Suite performed this task. This required an additional statistics database. With Scout 15 2209, the Scout Statistics Service has been replaced by the Scout Keep Alive service: The keep alive data are now stored in the Scout database. The processing of dynamic asset details for statistical analysis is no longer supported.

### 13.1. Configuring status messages for devices

The Scout Keep Alive service helps you configure automatic updating of status of your devices (keep alive messages).

1. In the Scout Console, open the relevant network settings.  
For all devices, choose **Options > Base device configuration > Network > Advanced**. Alternatively, for a specific OU or device, open the **Device configuration > Network > Advanced** dialog.



2. Select the **Send keepalive packet** option.
3. On the right of it, enter a time interval in seconds.
4. Confirm with **OK**.

*Within the defined time interval, the configured devices send their status messages to the Scout Keep Alive service. The status messages result in a refresh of the device icons in the tree view and of the relevant device property in the Scout Console:*

|              |              |                     |
|--------------|--------------|---------------------|
| DE           | OS           | eLux RP             |
| Applications | OS version   | 6.2302.0-3          |
| Devices      | Last Contact | 2023-08-17 12:27:19 |
| TC-MMI-S920  | 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*:*

|              |              |                     |
|--------------|--------------|---------------------|
| DE           | OS           | eLux RP             |
| Applications | OS version   | 6.2302.0-3          |
| Devices      | Last Contact | 2023-08-24 06:49:13 |
| TC-MMI-S920  | Status       | Switched off        |

## 13.2. Log files of the Scout Keep Alive service

- from Scout 15 2302 -

For the Scout Keep Alive service, log file rotation is active, which writes information about the service start and errors by default. The log level and other log options may be customized via an `.ini` file.

After installation, the log files and the `scoutkeepalive.ini` are located under  
`%PUBLIC%\Documents\UniCon\Scout\ScoutKeepAlive\`

The following settings are available in `scoutkeepalive.ini` in the `Logger` section:

| Option           | Default | Value range | Description   |
|------------------|---------|-------------|---|
| MaxLogFiles      | 10      | 1..n        | Number of log files for log rotation  |
| MaxLogFileSizeMB | 100     | 100..n      | File size in MB   |
| Level            | 1       | 1..15       | <p>Log level</p> <p>1 Service start and errors</p> <p>2 Information beyond errors</p> <p>4 Program flow</p> <p>8 Program flow including further details</p> <p>To receive error messages, information beyond errors and information on the program flow, we recommend protocol level 7 (bit mask of 1+2+4).</p> |

| Option   | Default   | Value range | Description                   |
|----------|---|-------------|-------------------------------|
| Location | C:\Users\Public\Documents\Unicon\Scout\ScoutKeepAlive |             | Destination for the log files |

## 14. Console communication

### 14.1. Closing a console

1. In the Scout Console, click **File > Console Management > Close console**.
2. Click **Refresh** to receive an up-to-date list showing all active consoles.
3. Click **Find** to filter the list.
4. Select the relevant consoles in the list.
5. To send a message to the relevant users, check the **Inform user for option** and enter the seconds as desired.
6. To give user s a chance to cancel the command, select the **Command can be canceled by the user** option .
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 help of this function you may send messages to other console instances.

1. In the Scout Console, click **File > Console Management > Send message**.
2. Under **Receiver**, choose which consoles you want to receive the message.
3. Under **Valid until**, define how long you want to show the message.
4. Under **Message**, enter your text.
5. To close the message automatically after a certain period of time, select **Inform user...** and specify a time period in seconds.
6. To allow the users of the receiver consoles to close the message without confirming its receipt, choose **Command can be canceled by the user**.

*When a receiver console is restarted, the message is displayed again within the validity period. If the message display time expires without the user selecting an option, the message is considered accepted.*

7. Click **Send**.

*The message will be sent to the selected consoles.*

- Every console instance shows a message only once.
- If a console instance is not started within the validity period, the message will not be shown.

- If users, within the validity period, start a console instance which was not yet recorded in the database, the message will only be shown in case the option **To all consoles** has been set.

### 14.3. Managing consoles

As soon as administrators open a console, it will be registered in the Scout database. Registered consoles may be displayed via menu command:

- ▶ Click **File > Console management > Manage consoles**.

For each console, the logged-on user, computer name and logon domain are shown. The active console is hidden. If an administrator has multiple console instances open on the same computer, the consoles are numbered serially. For example, `mmi #2` is the second console instance of user `mmi`.

#### Deactivating console instance

- ▶ Remove the check mark in front of the relevant entry.

*This console instance will no longer be displayed in any of the console communication dialogs.*

#### Deleting console instance

This allows old consoles that are no longer in use to be removed from memory. This function has no effect on currently opened consoles.

- ▶ Select the relevant entry and click **Delete**.

*The console instance and all commands related to this instance will be deleted.*

**Important** This means that you lose part of the command history, and possibly also commands that have not yet been processed.

#### Check users for AD membership

- ▶ Click **Check** and then **Select** or **Deactivate**.

*Unknown users are selected or disabled depending on the selected option.*

#### Searching for user, computer or domain

- ▶ Click **Search**, and then in the relevant column in the search field, enter a string as search term.

To replace characters, you may use the wildcard characters `*` and `?`. Case sensitivity is not relevant.

### 14.4. Managing console 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. To filter the commands, use one of the options: **All**, **Active**, **Inactive**, **Older than** and **Younger than**.
2. To display a search field for one of the columns, click **Find**.

## Changing the validity period of commands

- ▶ Select a command, and then under **Valid until**, modify the date and time.

## Deleting commands

1. To delete all commands, click **Delete all**.
2. To delete a specific command, select it and click **Delete**.

*All changes become valid only when you confirm with **OK**.*

## List of receivers

The **Recipients** list shows to which consoles a command was sent and when the consoles processed the command.

If \* (all) is displayed for user, computer and domain, the command was sent to all consoles. Therefore, it also applies to console instances that are newly logging on to the database. An entry of this form therefore never shows a time in the **Processed** column.

## 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 provides three logging options which are saved as `.log` files on the Scout Server.

| Option                   | Log file                                | Description  |
|--------------------------|---|--|
| Scout Console            | <code>scout.log</code>                  | <p>Required for debugging</p> <p>Path:</p> <p><code>%USERPROFILE%\Documents\UniCon\Scout\Console</code></p> <p>In the Scout Console, click <b>View &gt; System diagnostics &gt; Console log</b>.</p>   |
| Scout Server             | <code>eluxd.log</code>                  | <p>Log file of the Scout service, required for support calls</p> <p>Default path:</p> <p><code>%PUBLIC%\Documents\UniCon\Scout\Server</code></p> <p>Previous versions are renamed in <code>elux.log.1...elux.log.3</code> etc.</p> <p>In the Scout Console, click <b>View &gt; System diagnostic &gt; Server log</b> (only if the Scout Console 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<sup>1</sup></p> <p>created every 10 minutes</p> <p>Default path:</p> <p><code>%PUBLIC%\Documents\UniCon\Scout\Server</code></p>   |
| Scout Statistics Service | <code>UniconStatisticService.log</code> | <p>Rotating log file with configurable path</p> <p>Default path:</p> <p><code>%USERPROFILE%\Documents\UniCon\Scout\StatisticService</code></p> <p>The location and the maximum size from which a new file is written can be configured in <code>%PROGRAMFILES%\Unicon\Scout\Statistic\statisticsservice.exe.config</code></p>  |

For further information about file paths, see [Program and file directories](#).

<sup>1</sup>For devices, also a keepalive log file exists in the `ScoutKeepAlive` directory, provided the Scout Keep Alive service is installed.

### Note

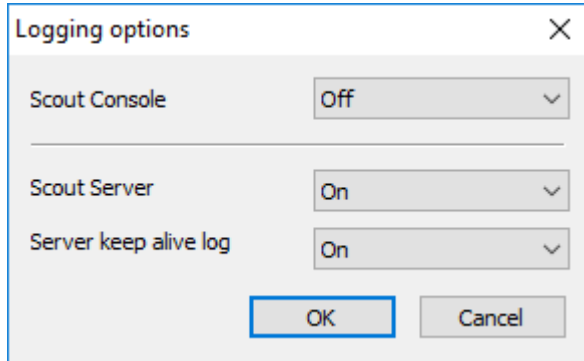
Click **View > System diagnostic > Server files** to open the `Unicon` server files directory in the Windows File Explorer (if console and server are installed on the same machine). The `Unicon` directory contains all configuration and log files organized in their application directories.

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<br><b>View &gt; System diagnostics &gt; License log</b>   |
| Administrator activity log | All administrator activities depending on the defined monitoring level<br><b>Security &gt; Manage administrators &gt; View protocol</b><br>For further information, see "Viewing administrator activities" on page 314. |

## 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 |

| Section | Entry       | Default | Description  |
|---------|-------------|---------|--|
| [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 eluxd.log and keepAlive.log |

**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 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 15 2101 -

If configured for mirroring, Scout 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 124.

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 331.

## 16.2. Optimizing

To optimize the performance and deal with high network loads you can use the following options:

- Configuring "Optimizing with handshake" below 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.

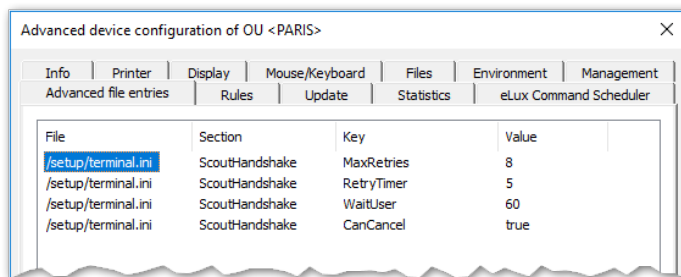
### 16.2.1. Optimizing with handshake

During each start-up the devices 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" on page 178.

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 `ScoutHandshake` section provides the following configurable parameters:

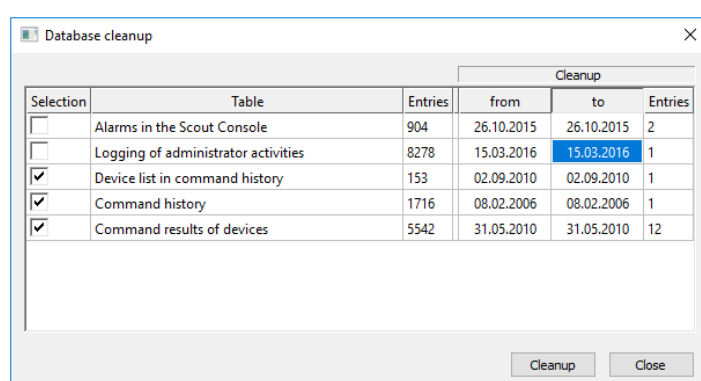
| Parameter  | Description   |
|------------|---|
| MaxRetries | Number of connection attempts<br>The value 0 deactivates handshake. |

| Parameter                 | Description   |
|---------------------------|---|
| RetryTimer                | <p>Period of time in seconds until next connection attempt (start value)</p> <p>After each attempt the interval is doubled (+/- random value).</p> <p>Example: Having defined 8 connection retries and a <b>RetryTimer</b> start value of 5 seconds, the 8. connection attempt is carried out after about 21 minutes.</p> |
| PermanentRetriesAfterDays | <p>Number of days (maximum) from the last successful connection until next connection attempt</p> <p>Ensures that after n days latest the configuration data of device and Scout Server is compared</p> <p>Can be combined with <b>MaxRetries</b> and <b>RetryTimer</b></p>   |
| WaitUser                  | Waiting time before client restarts to give the user the chance to close applications or log off.   |
| CanCancel                 | Defines, if the user is allowed to suppress a client restart ( <code>true</code>   <code>false</code> ).  |

### 16.2.2. Database cleanup

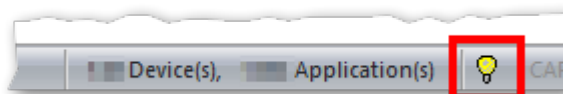
Scout stores huge amounts of data concerning various processes such as any performed update commands. To purge the Scout database tables, authorized administrators can delete database entries from particular tables for a specified period of time.

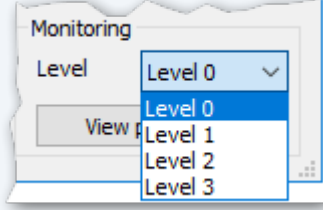
The relevant tables are listed in the **Database cleanup** dialog, each table providing the total number of entries and the creation date of the first entry. The administrator can modify only the fields **Selection** and **to**.



Alerts in the Scout Console

Alert messages (Error, Warning, Info), can be viewed by double-clicking the lamp icon on the Scout Console status bar



|                                     |   |  |
|-------------------------------------|---|--|
| Logging of administrator activities | <p>Log file entries about the activities performed by an administrator according to the defined monitor level in <b>Security &gt; Manage administrators...</b></p> <p>For further information, see "Viewing administrator activities" on page 314.</p>  |  |
| Device list in command history      | History data of commands shown in <b>View &gt; Command history...</b> of the Scout Console (entries for particular devices)   |  |
| Command history                     | History data of commands shown in <b>View &gt; Command history...</b> of the Scout Console (entries for OUs)  |  |
| Command results of devices          | <p>Results of commands performed on the devices (Update, Delivery, user-defined command). The log data can be viewed in the Scout Console in the <b>Properties</b> window or by using the context menu of a device <b>Commands &gt; Update/Delivery/Command</b>.</p> <p>For further information, see "Command results and update information per device" on page 257.</p> |  |

## 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

The Scout Enterprise Management Suite by default is installed to

```
%PROGRAMFILES%\Unicon\Scout
```

ELIAS 18 is installed according to your specifications during installation, for example on the web server IIS.

The eLux container (only required for the legacy ELIAS) is installed on the web server to

```
<root directory>\eluxng
```

#### File path for Scout Server files

Scout 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 Board are downloaded by the browser used and saved and saved in the download directory, if configured.

---

#### 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

An eLux device'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 <b>Update</b> command with option <b>Format system partition before update</b>     | Size for eLux RP 6 2104 LTSR and earlier versions:<br>1,77 GB / 1,84 GB with/without encryption<br><br>Size for eLux RP 6 2107 and later versions:<br>2,35 GB / 2.41 GB with/without encryption   |
| Boot      | only UEFI and USB | Boot section   | -  |   |
| Setup     |                   | Device configuration<br>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 command or notification<br><br>Signature check for eLux software packages<br><br>Devices with update partition can be used as Dynamic Proxy (Provider) for firmware updates. | Scout <b>Delivery</b> command with option <b>Format update partition before delivery</b> | The size of the update partition complies with the storage space provided.<br><br>The update partition is no larger than the storage space provided.<br><br>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.

We therefore recommend that you update test devices to eLux RP 6 2107 or later as the first step to thoroughly test functionality.

For further information, see "Update to new partition layout" on page 115 in the **Scout** guide.

## 17.3. IP ports

### eLux / required ports

| Port  | Type | Description  | How to deactivate   | In/Out   |
|-------|------|--|---|----------|
|       | ICMP | <b>ping</b> 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 <b>Config<sup>1</sup> &gt; Security</b> , disable mirroring or uninstall VNC server in X.Org package | Incoming |
| 22123 | TCP  | Scout Server (Scout Manager / secure)                                  |   | In/Out   |
| 22125 | TCP  | Scout Server (Scout Manager / TLS 1.2)                                 |   | In/Out   |
| 22129 | TCP  | VPN  |   | Outgoing |

<sup>1</sup>Device configuration

## eLux / optional ports

| Port | Type     | Description   | How to deactivate  | In/Out   |
|------|----------|---|--|----------|
|      | ESP      | VPN (data transfer)   | Uninstall package <b>VPN System</b>  | 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<br><b>(Config &gt; Network)</b>                         | Outgoing |
| 68   | UDP      | DHCP client (or: BootP client)  | Configure a local IP address<br><b>(Config &gt; Network)</b>                         | 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<br>Works with lockd (random)<br><br>UDP port mapper - drive access on NFS servers<br>Works with NFSD drive access (port 2049) and mountd (random) | Uninstall <b>Network Drive Share package</b>   | In/Out   |
| 123  | UDP      | Windows Time server (NTP)   | Do not configure a time server<br><b>(Config &gt; Desktop)</b>                       | In/Out   |
| 139  | TCP, UDP | SMB drive mapping, (NetBIOS) and SMB user authentication (CIFS)   | Uninstall <b>Network Drive Share package and User authentication modules package</b> | Outgoing |
| 161  | UDP      | SNMP  | Uninstall <b>SNMP Environment package</b>  | In/Out   |

| Port  | Type     | Description   | How to deactivate   | In/Out   |
|-------|----------|---|---|----------|
| 162   | UDP      | SNMPTRAP  | Uninstall <code>SNMP Environment package</code>                               | Outgoing |
| 177   | UDP      | XCMCP protocol  |   | Outgoing |
| 389   | TCP      | AD authentication with user variables   |   | Outgoing |
| 443   | TCP      | VPN (connecting) via HTTPS/TLS  | Uninstall package <code>VPN System</code>                                     | In/Out   |
| 464   | TCP, UDP | AD authentication (Kerberos) / Set password   |   | Outgoing |
| 514   | TCP      | Shell, X11 applications   |   | Outgoing |
| 515   | TCP      | Printing via LPD  | Uninstall package <code>Print environment (CUPS)</code>                       | In/Out   |
| 631   | TCP, UDP | CUPS (IPP) print client   | Uninstall package <code>Print environment (CUPS)</code>                       | Outgoing |
| 636   | TCP      | LDAPS authentication with user variables  |   | Outgoing |
| 2049  | UDP      | NFSD drive access NFS   | Uninstall FPM <code>NFS Support in Network Drive Share package</code>         | Outgoing |
| 6000  | TCP      | Remote X11 application  | In <b>Config &gt; Security</b> , clear <b>Allow remote X11 clients</b> option | Incoming |
| 7100  | TCP      | Font server<br>can be assigned in ( <b>Config &gt; Screen &gt; Advanced</b> )           |   | Outgoing |
| 8080  | TCP      | Firmware update via Dynamic proxy (Provider and Consumer)                               | Set <b>Config &gt; Firmware &gt; Proxy-Type</b> to <code>None</code>          | In/Out   |
| 9100  | TCP      | Printing directly to parallel port<br>can be assigned in ( <b>Config &gt; Printer</b> ) | In <b>Config &gt; Printer</b> , clear <b>TCP direct print</b> option          | Incoming |
| 9101  | TCP      | Printing directly to USB port<br>can be assigned in ( <b>Config &gt; Printer</b> )      | In <b>Config &gt; Printer</b> , clear <b>TCP direct print</b> option          | Outgoing |
| 20000 | UDP      | Wake On LAN   |   | In/Out   |
| 22124 | TCP      | Scout Statistics  |   | Outgoing |

## Scout Server

| Port  | Type | Description  | In/Out   |
|-------|------|--|----------|
|       | ICMP | <b>ping</b> 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 Manager / secure)                                       | In/Out   |
| 22124 | TCP  | Scout Statistics   | Incoming |
| 22125 | TCP  | Clients (Scout Manager / TLS 1.2)                                      | 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 <b>Config &gt; Security</b> , disable mirroring or uninstall VNC server in X.Org package | Outgoing |

## Scout Cloud Gateway

| Port  | Type | Description                            | In/Out   |
|-------|------|--|----------|
| 22125 | TCP  | Scout Server (Scout 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 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 [myelux.com](http://myelux.com) portal, under **eLux Software Packages**, for your eLux version, under **Add-On**, download the package **SNMP Environment** and deploy it to the devices.
2. If there is no `/setup/snmp/snmpd.conf` on the devices, transfer the configuration file `snmpd.conf` to the devices to `/setup/snmp/snmpd.conf` by using the Scout feature "Files configured for transfer" on page 173.

Or:

Modify the `terminal.ini` file by using the "Adding individual file entries" on page 178 feature of Scout. Example:

|         |                     |
|---------|---------------------|
| File    | /setup/terminal.ini |
| Section | SNMPD               |
| Entry   | rocommunity         |
| Value   | secret              |

3. Optionally, to define further "SNMPD and SNMP Configuration Directives" on page 341, use the "Adding individual file entries" on page 178 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 eLux software package **snmp**.

For further information on using SNMP with eLux, see "SNMP" on page 339.

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)   |

| Application       | Command                                 |
|-------------------|---|
| escapeQuotes      | (1 yes true 0 no false)                 |
| 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        |