UNICON

eLux RP

Administrator´s Guide

Last edited: 2022-05-27

0. Legal information

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

Abbreviations and acronyms

Abbreviation	Description
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 (`.epm`, software package)
FPM	Feature package module (`.fpm`, 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 (`.idf`)
IIS	Internet Information Services: Microsoft Web server
MB	Megabyte
OU	Organizational unit Unit or group within the organizational structure
VPN	Virtual Private Network

2. Overview and general information

2.1. About eLux RP

eLux®RP is a hardware-independent operating system designed for cloud-computing environments. It can be run by both, common PCs and Thin Clients. eLux is based on Linux and provides a write-protected file system which makes it secure against computer viruses and other malware.

This guide supports the system administrator in setup, maintenance and operation of Thin Clients and PCs running eLux RP, hereafter referred to as **eLux**. The documentation refers to the current version eLux RP 6.x. Documentation for earlier versions can be found as PDF on our download page PDF downloads.

This guide assumes knowledge of

- installation, maintenance and operation of computer networks and peripherals
- operating system skills of the server machines in use

Note
eLux RP 6 clients can be centrally managed through the Scout Enterprise Management Suite version 15.x. For further information, see Compatibility client platform and Scout Enterprise Management Suite in our **Releases** Whitepaper.

Beginning with Scout Enterprise Management Suite 15.1 and eLux RP 6.1, the management protocol for communication between Scout Server and eLux client offers end-to-end encryption via TLS 1.2. TLS-encrypted communication is done via port 22125. Older clients communicate with the server via port 22123 with AES-256 encryption.

For support periods and the compatibility matrix, see the Whitepaper **Releases, Lifecycles and Compatibility**.

2.2. Keyboard shortcuts

Shortcut	Function
CTRL+ALT+↓	Switch between open applications to the left.
CTRL+ALT+↑	Switch between open applications to the right.
CTRL+ALT+←	Switch between desktops to the left
CTRL+ALT+→	Switch between desktops to the right.
CTRL+WIN	Switch from other applications to eLux: The eLux taskbar/system bar with open applications is shown.
WIN+ALT+I	Open the device information
CTRL+ALT+HOME	Unlock the **Configuration panel**): Requests the local device password

Shortcut	Function
CTRL+ALT+END	Lock the client screen If user authentication is active, the user password is required for unlocking.
CTRL+ALT+F UNCTION KEY	Switch between the consoles, if the **Console switch** option is enabled. For further information, see "Keyboard dialog" on page 46. The following consoles are available: F1: eLux desktop F4: Message console

2.3. Touchpad gestures for mobile devices

Mobile devices often need to be operated via a touchpad and do not always have hardware mouse buttons.

By default, mouse actions are mapped to the following touchpad gestures:

Mouse action	Touchpad gesture
Click with left mouse button	Tap one finger on the touchpad (single-tap)
Right-click (right mouse button)	Tap two fingers on the touchpad (single-tap)
Middle-click (wheel button)	Tap three fingers on the touchpad (single-tap)
Move cursor	Drag your finger on the touchpad
Scroll	Slide two fingers at the same time

3. Installation

eLux can be installed directly on the flash memory of a Thin Client or on a hard disk. The installation procedure is a kind of recovery installation and can be performed in two ways:

- from USB stick: For all supported operating system versions, we provide an **eLux USB Stick** image, available for download on our portal www.myelux.com and suited to create a stick for installation.
- via PXE recovery: For large environments, PXE-capable devices can be installed through the network if the eLux software container and Scout Enterprise Management Suite are already installed.

Both procedures are described in detail in our short guide **eLux Recovery procedures**.

3.1. System requirements

Hardware requirements

	Minimum requirements	Recommended requirements
Processor	x86, 1 GHz (dual-core), 64-bit capable	x86, 2 GHz (quad-core) or more, 64-bit capable
RAM	1 GB available for operating system	4 GB or more
HDD	4 GB (2 GB for limited functionality)	16 GB or more (8 GB for current functionality/partitions)
GPU (Graphics processing unit)	AMD or Intel graphics chipset	AMD or Intel chipset
Network	Ethernet or WLAN	Ethernet or WLAN
I/O ports	USB 2.0	USB 3.0 or USB 2.0, USB boot support
Resolution	1024 x 768 (XGA)	1920 x 1080 (Full HD) or higher

The recommended hardware requirements are minimum hardware requirements for the upcoming eLux major release to take advantage of the new functionalities.

Hardware Compatibility List

The supported hardware models (Hardware Compatibility List) for each operating system version are published on our technical portal www.myelux.com within the relevant eLux container under **Supported Hardware**.

For support periods and the compatibility matrix, see the Whitepaper **Releases, Lifecycles and Compatibility**.

3.2. First boot procedure

The first boot procedure for a Thin Client in initial state, after a factory reset or after a Recovery installation, is processed as follows:

a. Scan BIOS

b. Make a DHCP server request

> **Note**
> To enable the client to connect to the Scout Server, either DHCP or DNS must be configured. For further information, see Self-registration of devices in the **Scout** guide.

c. Start the eLux operating system

If either DHCP or DNS has been configured for the Scout Server, the device is automatically registered in the Scout infrastructure and receives a new configuration.

If the client cannot retrieve the IP address of the Scout Server, the First Configuration Wizard opens and leads you through the first configuration.

3.3. First configuration

During the first boot procedure, a Wizard is launched which helps you through the first configuration. The First Configuration Wizard is also started when you reset the device to factory state.

The First Configuration Wizard offers the following options:

- Manage the device through the Scout Console
  The configuration data are transferred from the Scout Server.
- Connect the device through the Scout Cloud Gateway and manage it via the Scout Console
  The configuration data are transferred from the Scout Server.
- Configure eLux manually, which means locally on the device

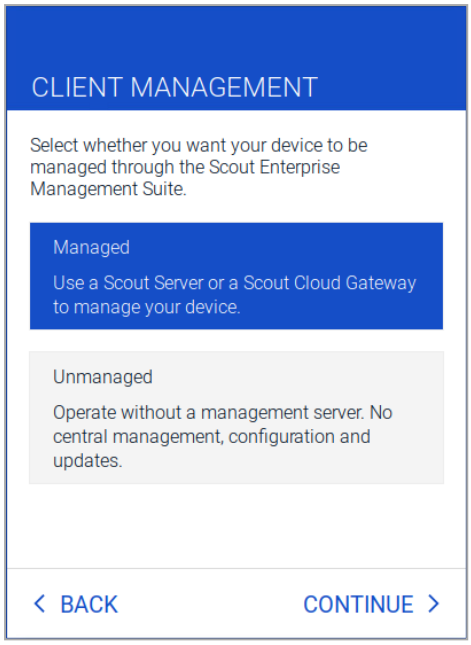
Going through the first configuration and connecting to a Scout Server

1. Select the display and keyboard language.

   The following languages are supported: English, German, French[1] and Spanish[2]

2. Read and accept the license terms.
3. To manage the device via Scout, click **Managed**.

[1] for eLux RP 6.9 and later versions
[2] for eLux RP 6.9 and later versions



4. Enter the address of the Scout Server as FQDN or IP address.

   If your device is to be connected via Scout Cloud Gateway, enter the address of the Scout Cloud Gateway.

5. Select the destination OU for the device in the Scout Console.
6. Optionally, modify the device name and enter further details.
7. Confirm with **Finish**.

The device is registered in the Scout infrastructure, added to its destination OU, and is restarted. The client contacts the Scout Server and downloads the configuration and application data of the destination OU.

If a profile for this device has already been created in the Scout Console, the device is assigned the configuration of the existing profile.

For further information on connecting via the Scout Cloud Gateway, see Integrating new devices in the Scout Cloud Gateway guide.
For further information on managing devices with Scout, see the **Scout** guide.

3.4. Device password

All Thin Clients managed by a Scout Server receive the same device password. There is only one device password for all clients of the same infrastructure which is defined in the base device configuration.

The device password is used for unique assignment and authentication to the Scout Server, so that no other Scout Server can manage this device.

In the initial state, the device password is `elux`.

Note
The device password has nothing to do with a user password, which is used for example for AD user authentication.

For further information on passwords, see also Passwords in the **Scout** guide.

3.5. Self-administration on the device

With administrator rights, users can change the configuration locally on the device or completely disconnect from the Scout infrastructure. To prevent abuse, we recommend that you change the initial device password and do not release it. For further information, see Local device password in the **Scout** guide.

Logging on with full access on the device

1. Open the Configuration panel.
2. Press CTRL+ALT+HOME.
3. Enter the device password.

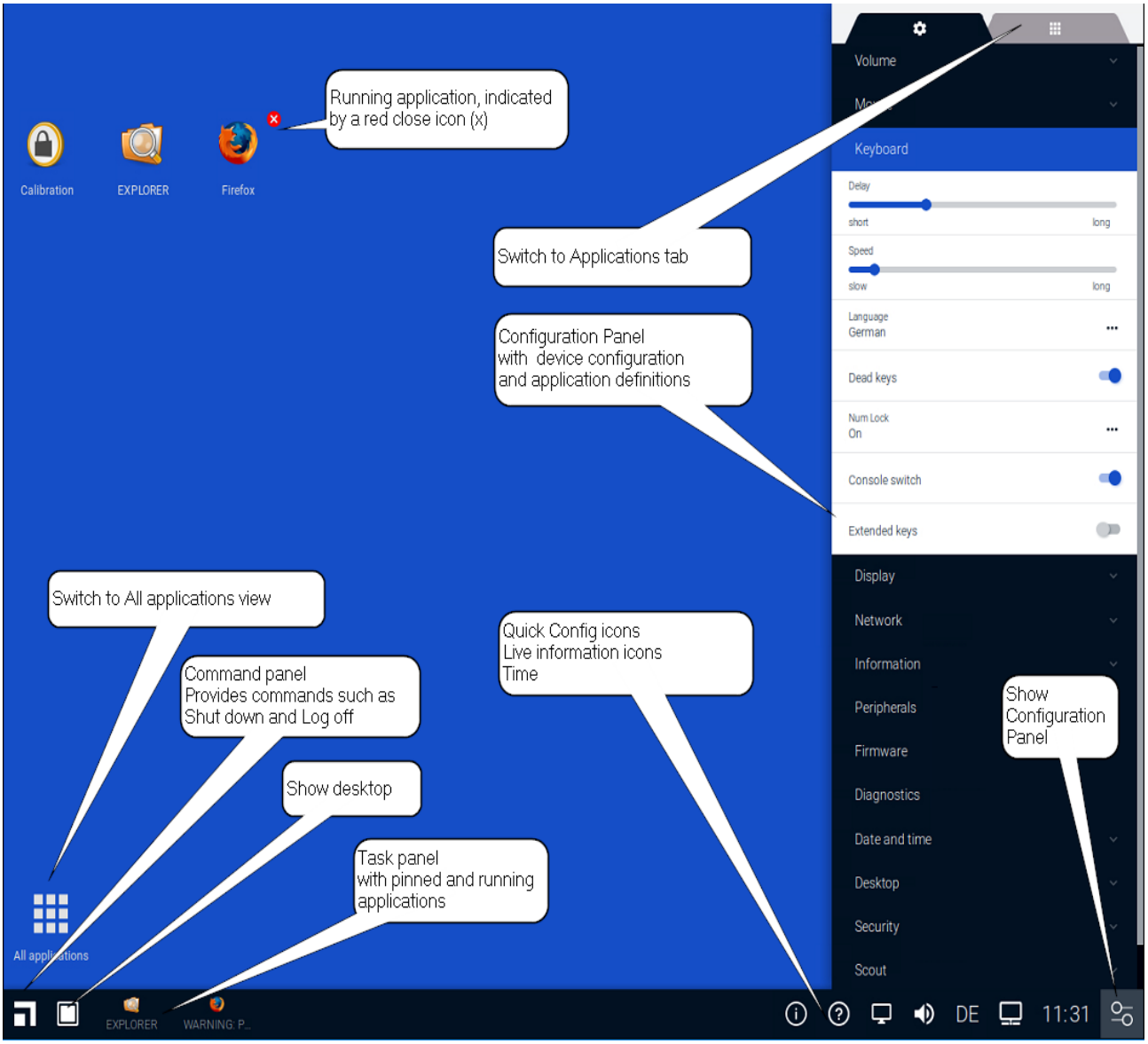
You are provided with full access rights to the device configuration and application definitions on the device.

4. eLux RP 6 user interface

Note
eLux RP 6 clients can be centrally managed through the Scout Enterprise Management Suite version 15.x. For further information, see Compatibility client platform and Scout Enterprise Management Suite in our **Releases** Whitepaper.

Users can choose between a personalized desktop view and the **All Applications** view.

The eLux RP 6 user interface provides the following elements:

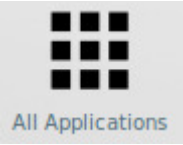
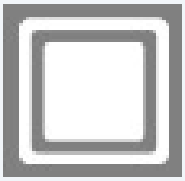


Legend to numbers	
1	Running application, indicated by a red close icon (x)
2	Switch to **All applications** view

Legend to numbers	
3	**Command panel** Provides commands such as **Shut down** and **Log off**
4	Show desktop
5	**System bar** Includes the **Command panel**, **Task panel**, **Live-Information**, time and a button for opening the **Configuration panel**
6	**Live-Information**: In the figure, the current LAN connection is shown.
7	Time and date
8	Show **Configuration panel**
9	Opened **Configuration panel** Contains the device configuration and application definitions
10	Opened **Configuration dialog** in the **Configuration panel**
11	Switch to **Applications** tab

4.1. Desktop views

The desktop offers two views. To switch between views, click the desktop icon in the lower left section of the screen:

View	Click	Description
All Applications		Shows all defined applications as application icons on the desktop
Desktop		Shows only few predefined applications and user-selected application icons on the desktop (Personal Desktop)

As soon as the user has set up a personal desktop and defined applications for it, the **Desktop** view is displayed by default after start-up. Otherwise, the **All Applications** view is displayed.[1]

Specifics for Citrix StoreFront

When you use Citrix StoreFront, each store is also displayed as a separate view:

After the user has successfully connected to a store, a separate view is created with the applications provided by the Citrix backend in that store. The StoreFront applications are additionally shown in

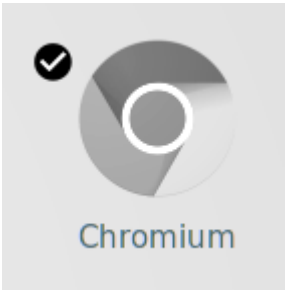
[1] for eLux RP 6.4 and later versions

the **All Applications** view. The separate Store view is closed when the user disconnects from the store. The Citrix icon changes the appearance depending on the connection status.

4.2. Setting up a personal desktop

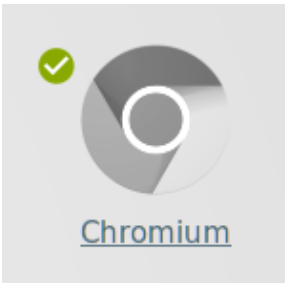
Selecting applications for a personal desktop

1. In the **All Applications** view, right-click an application icon.



   At the top left of the application icon, a black symbol with a check mark is displayed.

2. Click the black check mark symbol.



   *The check mark symbol is shown in green and the application name is underlined. From now on, the relevant application is displayed additionally in the **Desktop** view.*

Deleting applications from a personal desktop

1. In the **Desktop** view, right-click the relevant application icon.

   At the top left of the application icon, a green symbol with a check mark is displayed.

2. Click the green check mark symbol.

   *The application icon is hidden and only shown in the **All Applications** view.*

Note
Application icons that have been configured via the Scout Console cannot be deleted from the desktop.

4.3. System bar

The **System bar** provides various functions and can be configured.

Legend to numbers	
1	Show **Command panel** (see below)
2	Show the desktop Minimizes all open windows and hides the **Configuration panel** if open
3	**Task panel** with open application
4	**Quick Config** [1] ▸ For quick access to a Configuration panel dialog, click the relevant live information icon such as Information, Display, Volume...
5	Request device identifier for support[2] For further information, see Device identifier for support in the **Scout** guide.
6	**Live information** ▸ To show current status information, right-click[3] a live information icon: • Connected USB devices • Current network connection • Battery level for mobile clients • Locally connected printers[4] ▸ To show information on active third-party software such as Citrix, Zoom, Cisco Anyconnect, click the **more** ••• icon
7	Time and date ▸ To show the date, move the mouse pointer over the time.
8	Show the **Configuration panel**[5]

[1] from eLux RP 6.8
[2] from Scout 15 2101 and eLux RP 6 2101
[3] for eLux RP 6.8 and later versions
[4] from eLux RP 6.5
[5] from eLux RP 6.4

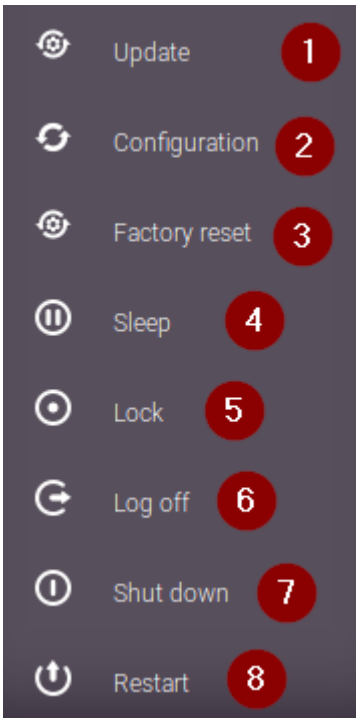
4.3.1. Command panel

eLux commands such as **Shut down** and **Restart** are located on the system bar, in the Command panel.

Which commands are displayed depends on whether the devices are managed by Scout, whether user authentication is configured, and the user rights the administrator has defined.

- To show the Command panel, on the left of the system bar, click the eLux icon [1].

Available eLux commands



1	Managed devices: Starting a firmware update The system checks if a firmware update is required. If the image definition file on the server is newer than the one on the device, the user can start the update process.
2	Managed devices: Synchronizing the device configuration The current device configuration and the current application definitions for this device or OU are reloaded from the Scout Server and the device is restarted. Local configuration changes are overridden unless they are protected.
3	Managed devices: Resetting the client to initial state (factory reset) The device configuration is set back to the factory status. Local application definitions and locally stored configuration data are deleted. The firmware image with all software packages is retained.
4	The device is set to sleep mode (Suspend to RAM).[2]
5	With AD authentication: The screen is turned off by the system. To unlock it, users have to enter their password.
6	With AD authentication: The logged-on user is logged off and the logon dialog is displayed. Before logoff, the confirmation dialog provides an option for users to change their AD password.
7	The device is shut down and turned off.
8	The device is shut down and restarted immediately.

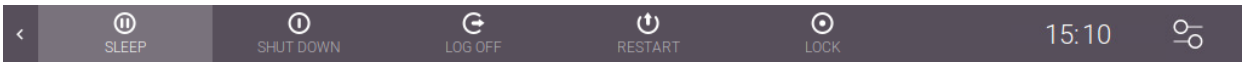
[1] from eLux RP 6.8
[2] from eLux RP 6.4

For further information, see eLux commands.

Note
Before a command is executed, the user receives a confirmation message (except for the **Lock** command).

For eLux RP 6.7 and earlier versions

- To show the **Command panel**, click the eLux button:



- To show the extended **Command panel**, click the eLux button while holding down the SHIFT key:

(only for devices managed through Scout)

4.3.2. Live information

The live information icons on the system bar show current status information, for example about the network connection and connected USB devices. In addition, most of them offer quick access to the corresponding Configuration dialog (**Quick Config**).[1]

Whether the live information icons are displayed[2] and allowed for **Quick Config**[3] depends on the device configuration set by the Scout administrator (Advanced desktop settings).

Showing live information details

- Right-click[4] the relevant live information icon.

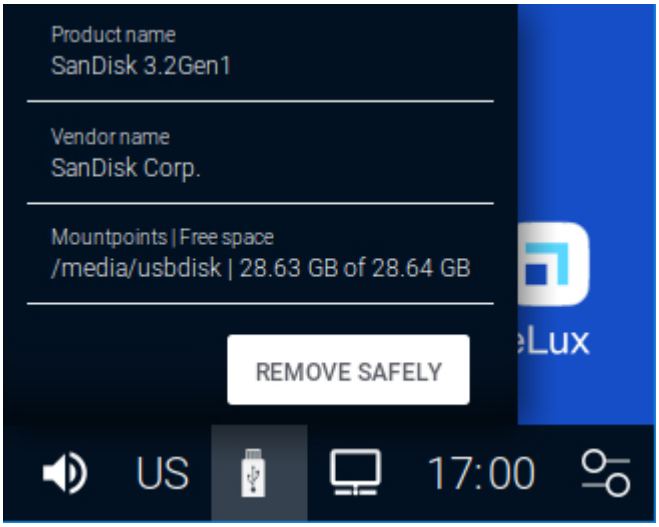
Jumping to Configuration dialog / Quick Config

- Click the relevant live information icon.[5]

The following section describes a few types of live information.

Connected USB devices

Note
Devices managed by Scout must be configured to allow local use of USB devices via mountpoints (**Device configuration > Hardware**). Otherwise, connected USB devices will not be displayed.



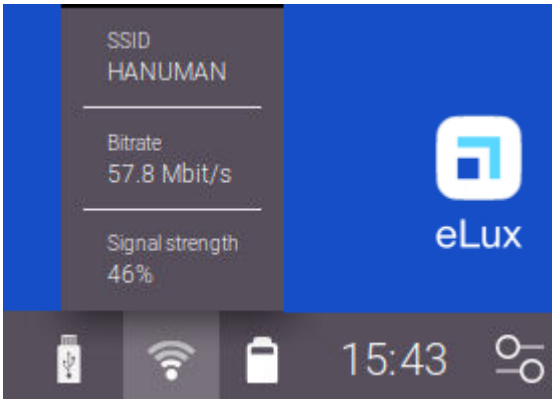
[1] from eLux RP 6.8
[2] from Scout 15.7 and eLux RP 6.7
[3] from Scout 15.8 and eLux RP 6.8
[4] for eLux RP 6.8 and later versions, for earlier versions left-click
[5] for eLux RP 6.8 and later versions

- Before you remove a USB device, click **Remove safely**. This is to ensure that all data are saved on the USB device.

> **Note**
> In the Scout Console, you can define a key combination that allows users to remove all connected USB mass storage devices safely. For further information, see Safe removal of USB devices in the **Scout** guide.

- To view the current free space at run-time, click the USB icon again.[1]

Current network connection



- Profile name of LAN, VPN, WWAN or SSID of the WLAN network
- Bitrate
- Signal strength (only WLAN and WWAN)

The network icon in the figure above shows a WLAN including approximate signal strength.

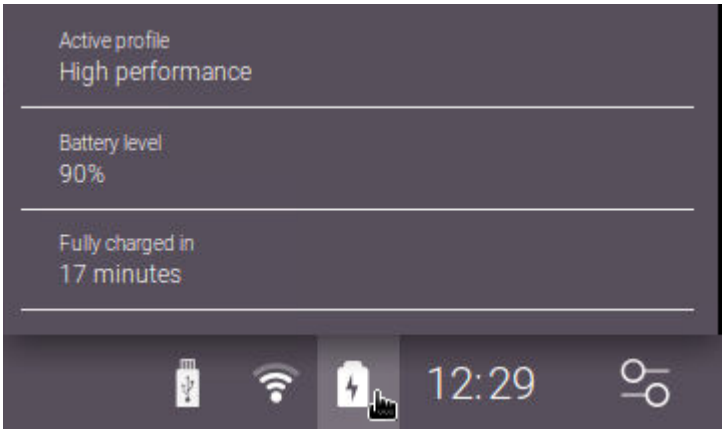
> **Note**
> If the network connection is interrupted, the network icon is displayed with an exclamation mark.

VPN connections

Each active VPN connection is displayed as a live information icon . Using the context menu, you can open the user interface of the VPN application or disconnect the connection.[2]

[1] for eLux RP 6.7 and later versions
[2] for eLux RP 6.10 and later versions

Battery level for mobile clients



Information	Description
Active profile	Shows whether the `High performance` or the `Power saver` (Eco) profile is active. If `Auto` is configured, the active profile depends on whether the device is connected to the power supply.
Battery level	Shows the current battery status in percent
Remaining time on battery (on battery power)	Shows the remaining minutes on battery power if the device is not connected to the power supply
Fully charged in (plugged in)	Shows the time in minutes until the battery is fully charged when the device is connected to the power supply.

The battery icon in the figure above indicates that the device is connected to the power supply. Without power supply, the icon shows the approximate battery status.

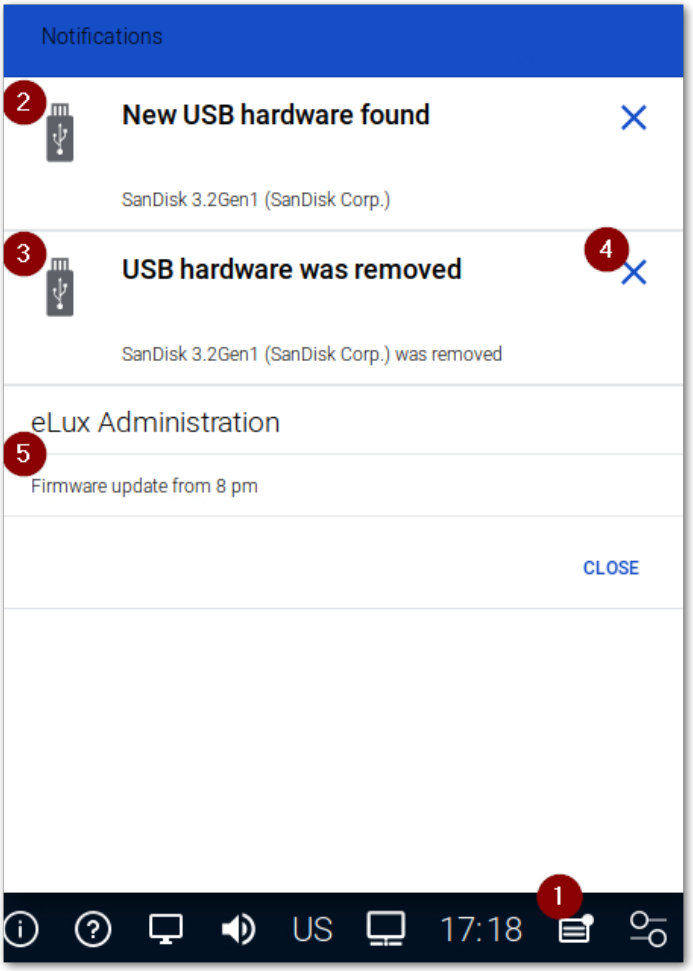
Locally connected printers

A live information icon is also shown for local printers.

4.3.3. Notifications

System notifications inform users about a changed network status or the connection or removal of peripheral devices, for example. Notifications are shown in a small message window at the bottom right of the screen and are removed after a few seconds.

To make it easier for users to read several messages, especially if they arrive at short intervals, an additional icon allows you to show all notifications in a separate panel.[1] This panel displays the notifications one under the other and remains active until you close it with a click.



1	To open the notification panel, click the respective icon which is displayed temporarily.
2	First notification
3	Second notification
4	To close a notification, click the **Close** field. The panel with further notifications remains open.
5	In addition to system notifications, the panel displays messages that the administrator sends to the users via the Scout command **Send message**.

[1] for eLux RP 6.7 and later versions

4.4. Configuration panel

You can show the Configuration panel in the right section of the screen. It is used for

- Device configuration
- Application definitions

Showing the Configuration panel

Requires
The option **Show Configuration panel** in **Desktop > System bar** is enabled.[1]

- On the System bar, click the  button. Alternatively, click the time or one of the live information icons.

  or

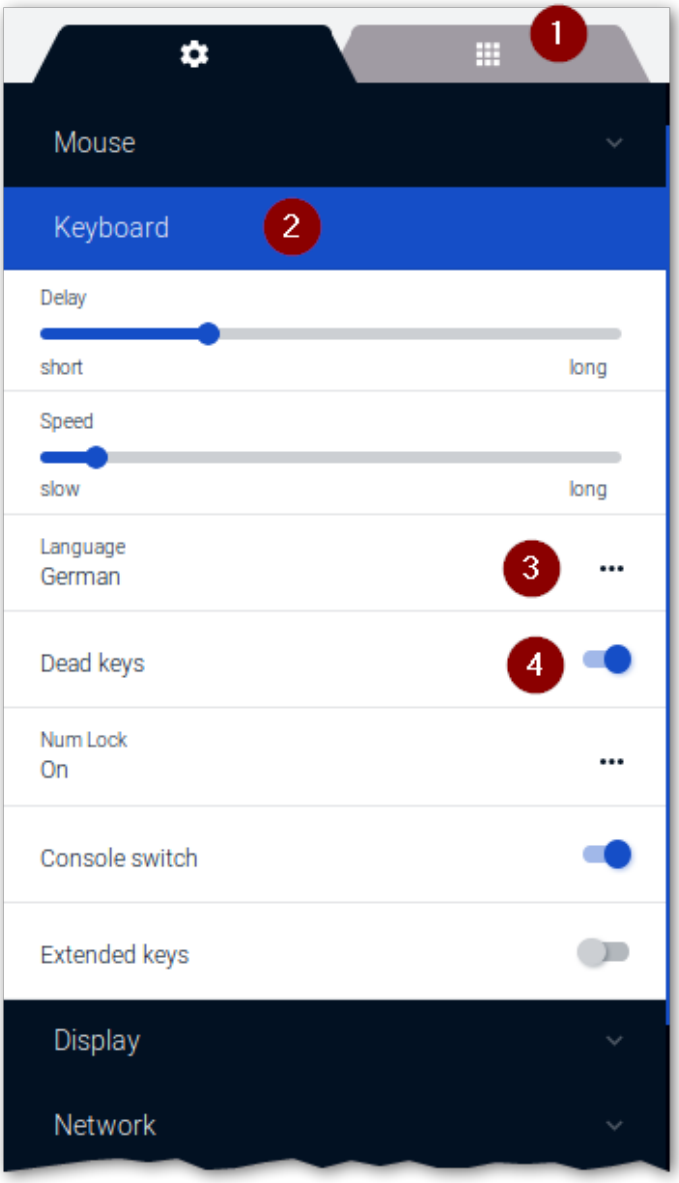
- On the keyboard, press WINDOWS+ALT+C.

  The Configuration panel with the Configuration dialogs is shown.

  The recently used Configuration dialog is opened. If you click the time or a live information icon, the corresponding dialog is opened.

The dialogs are displayed alphabetically[2] or sorted by content. Sorting can be defined in the Scout Console.

[1] for eLux RP 6.4 and later versions
[2] for eLux RP 6.9 and later versions



1	Switch to **Applications** tab
2	To open a dialog, click the dialog title. You can open only one dialog at a time.
3	Open a drop-down list or context menu
4	Enable or disable an option

Using the configuration and application dialogs

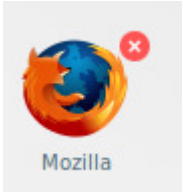
- To view all dialog titles or all dialog options, you might have to scroll down the frame.
- Many options are applied directly after you have set them. Some dialogs require you to click buttons such as **Apply** or **Cancel** before they are closed.
- When you enable an option, further entries might be required.
- Text fields are characterized by a line under the field.
- To pick a file from the file system, click .
- Mandatory fields are characterized by an asterisk* on the right. If you have missed to fill in a mandatory field, it is displayed in red.

For further information about the content of the dialogs, see

4.5. Applications in the eLux RP 6 interface

Starting applications

- In one of the desktop views, click an application icon.



At the top right of the application icon, a red close icon (x) is shown.

Disconnecting applications

- On the desktop, click the red close icon at the top right of the application icon.

  or

  On the system bar, right-click the open application and then click **Close**.

Note
To close a session completely, the user must log off. In addition, the administrator can define a timeout on the server to close any inactive sessions.

Searching for applications

1. Click into the search field and enter some characters of the application name you are looking for.
2. Press RETURN or click the magnifier icon.

The desktop displays only the matching applications.

- To deactivate the search filter, press ESC.

Sorting applications

- In the **All Applications** view, click the **AZ** button once or repeatedly.

  The applications are sorted alphabetically (ascending, descending, unsorted/free).

Free placing of applications[1]

- In the **Desktop** view, use a drag-and-drop operation to move an application icon to the position of your choice.

  The position of the application icons you have arranged is saved within the free positioning order  .

Switching between sessions/applications and the eLux Desktop interface

- Press the key combination STRG+ALT+D

Showing the desktop and minimizing application windows

- On the system bar, click the  icon.

For further information, see Defining applications.

[1] from eLux RP 6.7. From eLux RP 6.9, the user right **Sorting desktop icons** is required

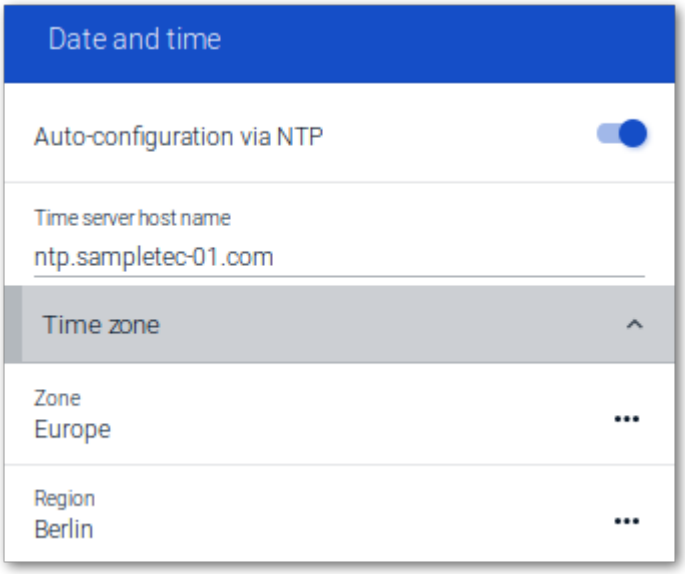
5. Device configuration

> **Important** If the client is managed by Scout, configuration is normally done centrally in the Scout Console. With inheritance enabled, local configuration changes on the client will be overwritten as soon as the client connects to Scout. For further information, see Device configuration in the **Scout** guide.

The local device configuration is located in the **Configuration panel** that you can show on the right of the screen.

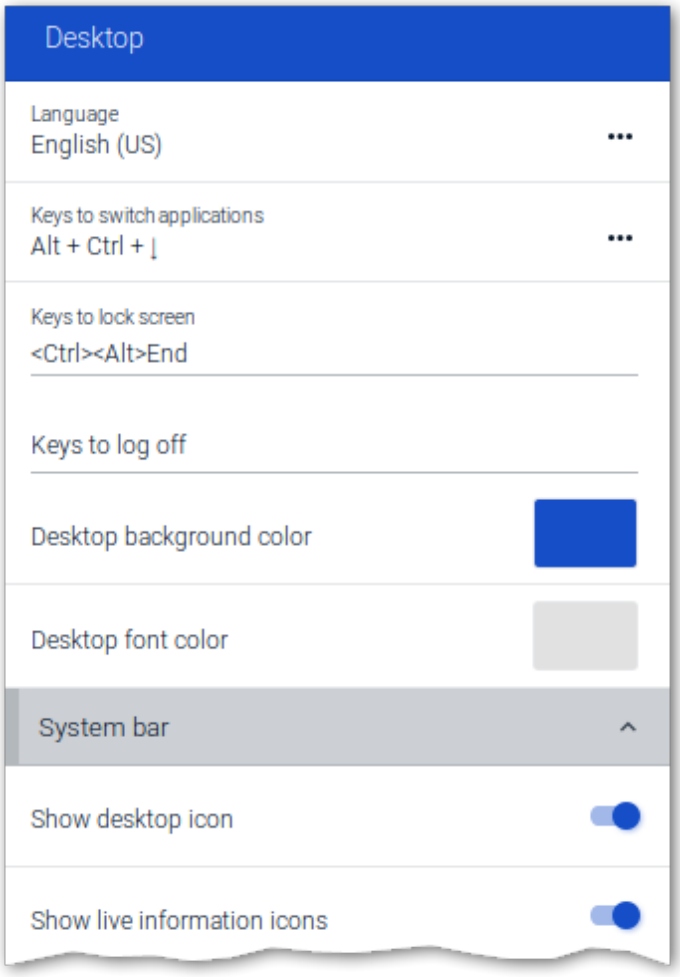
For further information on viewing and operating the Configuration panel, see Configuration panel.

5.1. Date and time dialog



Option	Description
Auto-configuration via NTP	Date and time are determined and displayed automatically via NTP (Network Time Protocol). The service runs on UDP port 123.
Time server	Host name of the NTP server
Time zone	For each level, select the time zone.

5.2. Desktop dialog



Option	Description
Language	Language for displaying desktop elements and configuration The following languages are supported: English, German, French[1] and Spanish[2] Applications are also started in the configured language but must be compatible with it in order to run correctly.
Keys to switch applications	Key combination to switch between applications or sessions The default is `ALT+CTRL+↑` to avoid conflicts with `ALT+TAB` which is used to switch between the tasks within a session.

[1] for eLux RP 6.9 and later versions
[2] for eLux RP 6.9 and later versions

Option	Description
Keys to lock screen[1] (AD users)	Key combination to activate password-protected screen saver Default: `<Ctrl><Alt>End`
Keys to log off[2] (AD users)	Key combination to log off current user The logon dialog is then displayed.
Desktop background color	Text field for the background color, can be entered as a hexadecimal value or as a CSS color name Example: `#FF0000` or `gold`
System bar	Display options for the system bar

> **Important** If you hide the Configuration panel, you cannot access the configuration any longer. Neither can you unlock the configuration panel with the device password. You need to synchronize the configuration data to the server-side settings or perform a factory reset. For further information, see eLux commands.

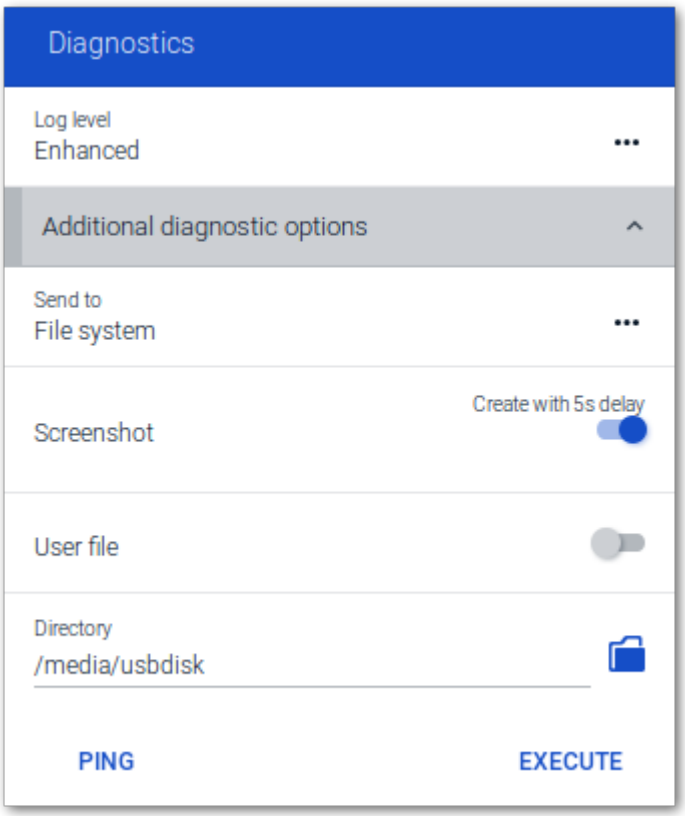
For further information on how to define keyboard shortcuts, see Defining keyboard shortcuts in the **Scout** guide.

[1] for eLux RP 6.9 and later versions
[2] for eLux RP 6.9 and later versions

5.3. Diagnostics dialog

The following diagnostic options are provided:

- Enhanced log level: Configuration and log files are retrieved to a greater extent
- Additional diagnostics by creating screenshots or adding further freely selectable files
- Display or send relevant files to FTP server, Scout Server or data medium
- Ping command to check connectivity and latency in your network



Option	Description
Log level	Choose between `Standard` and `Enhanced` for different amounts of configuration and log files. Use the `Enhanced` log level only temporarily, otherwise you risk exceeding the flash memory capacity of your Thin Client.

Option	Description	
Send to	Configure the destination: Where do you want to send the files?	
	Display	Opens the **Log Viewer** window in eLux showing various diagnostic files with their contents
	FTP address	The files are transferred to an FTP server Specify the address under **FTP address**.
	Scout Server	By default, the files are transferred to the Scout Server, to `%USERPROFILE%\Documents\UniCon\Scout\Console\Diag` **Note** A different destination server may be configured in the Scout Console.
	File system	The files are saved to a local data medium or USB device.

The following options are only visible after you have chosen a destination (except `Display`):

Screenshot (only if destination ≠ `Display`)	After you click **Execute**, with a 5 second delay, a screenshot is taken and transmitted with the diagnostic files. Screenshots are created as `.png` files under `/tmp`.
User file (only if destination ≠ `Display`)	Users can select a local file to be transmitted with the diagnostic files.
Directory / server address (only if destination ≠ `Display`))	File system directory or server address (Scout Server or FTP-Server) for transmission of the diagnostic files
Ping	Allows users to ping any host (IP address or FQDN)[1]
Execute	Displays or sends the selected amount of diagnostic files to the configured destination

If the destination is not `Display`, the diagnostic files are organized in directories such as `setup`, `var`, `tmp` and sent in a `.zip` file.

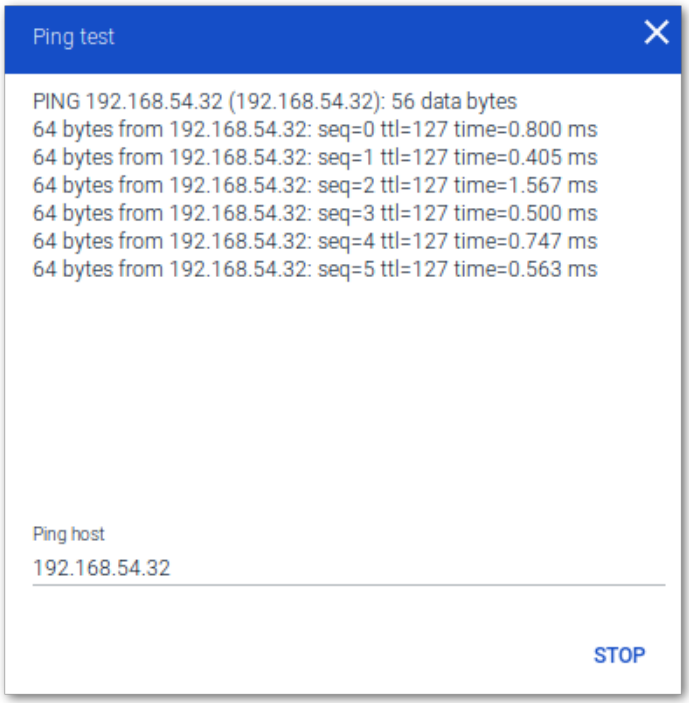
Note
The `systemd-journal.log` (Enhanced log level) logs network activities.[2]

[1] From Scout 15.7 and eLux RP 6.7, the user right for the ping command can be set independently of the other diagnostic functions.
[2] for eLux RP 6.4 and later versions

5.3.1. Performing a ping command

Requires
User right for executing the diagnostics feature / ping command[1]

1. Under **Diagnostics**, click **PING**.
2. In the **Ping test** window, type the name or IP address of the server you want to connect with.
3. Click **Start**.



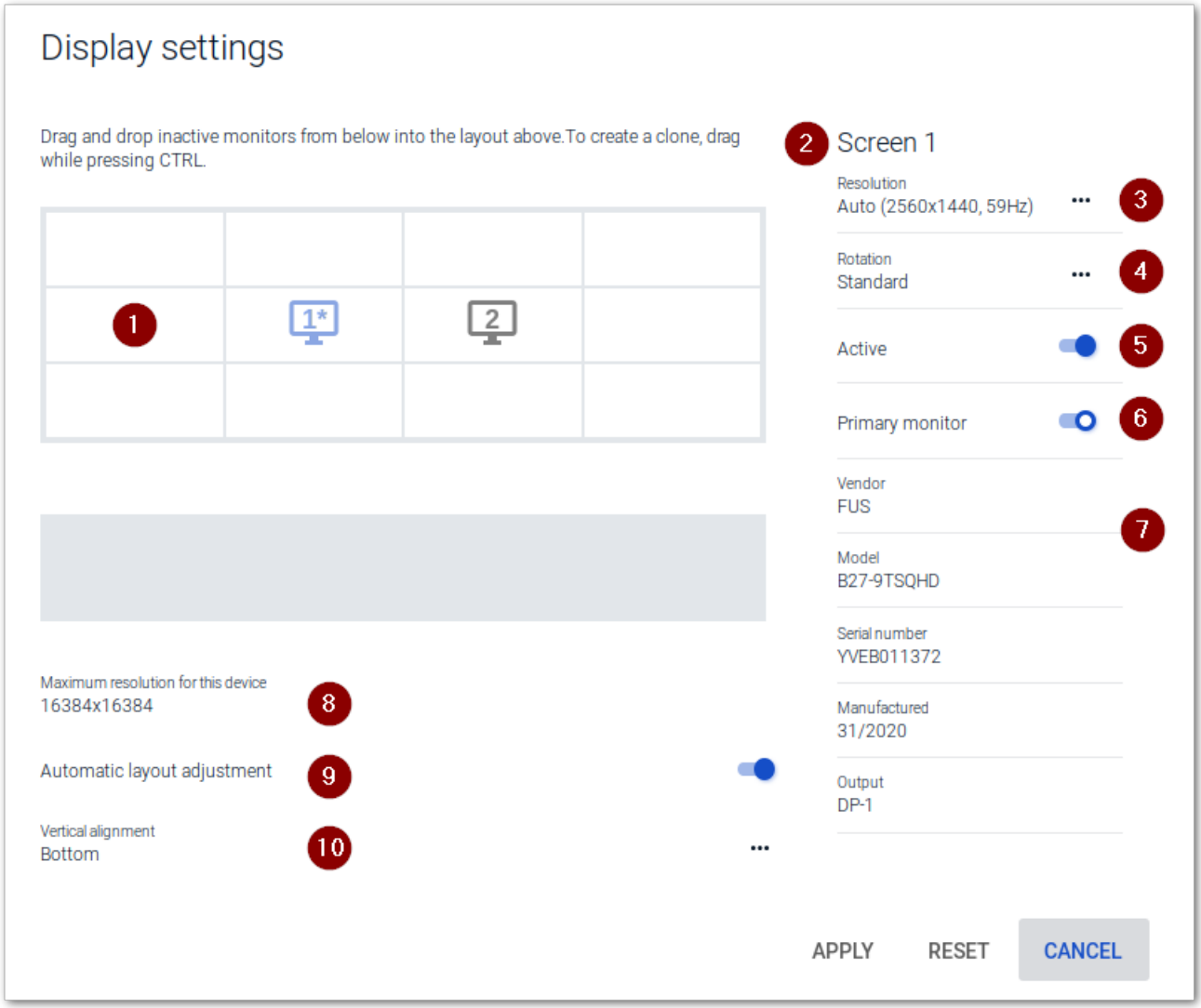
*The device connects to specified host and executes a ping command until you click **Stop**.*

4. Click **Stop**.

[1] From Scout 15.7 and eLux RP 6.7, the user right for the ping command can be set independently of the other diagnostic functions.

5.4. Display dialog

Note
Up to eLux RP 6.8, **Settings** and **Information** for all connected screens are displayed within the Config panel.



Legend to numbers	
1	All connected screens are displayed as monitor icons. The monitor icons can be moved freely via drag-and-drop operations.[1]
2	Options and details for the selected monitor
3	Selected monitor: All resolutions provided and supported by the screen are displayed and can be selected.

[1] for eLux RP 6.9 and later versions

Legend to numbers	
4	Selected monitor: The screen display can be rotated 270° (left), 180° (inverted) and 90° (right).
5	Selected monitor: Additional screens can be disabled.[1]
6	Selected monitor: Define as primary monitor screen
7	Selected monitor: Hardware details
8	Multiple monitors: Maximum supported resolution across all monitors
9	Multiple monitors: Automatic layout adjustment when a monitor is disabled.
10	Multiple monitors: Vertical alignment

5.4.1. Multiple monitors

Note
Up to eLux RP 6.8, you can organize multiple connected screens via options such as `Left of screen 2`. From eLux RP 6.9, a graphical solution with drag-and-drop operations is supported and described below.

If more than one monitor is connected, the following options are available:

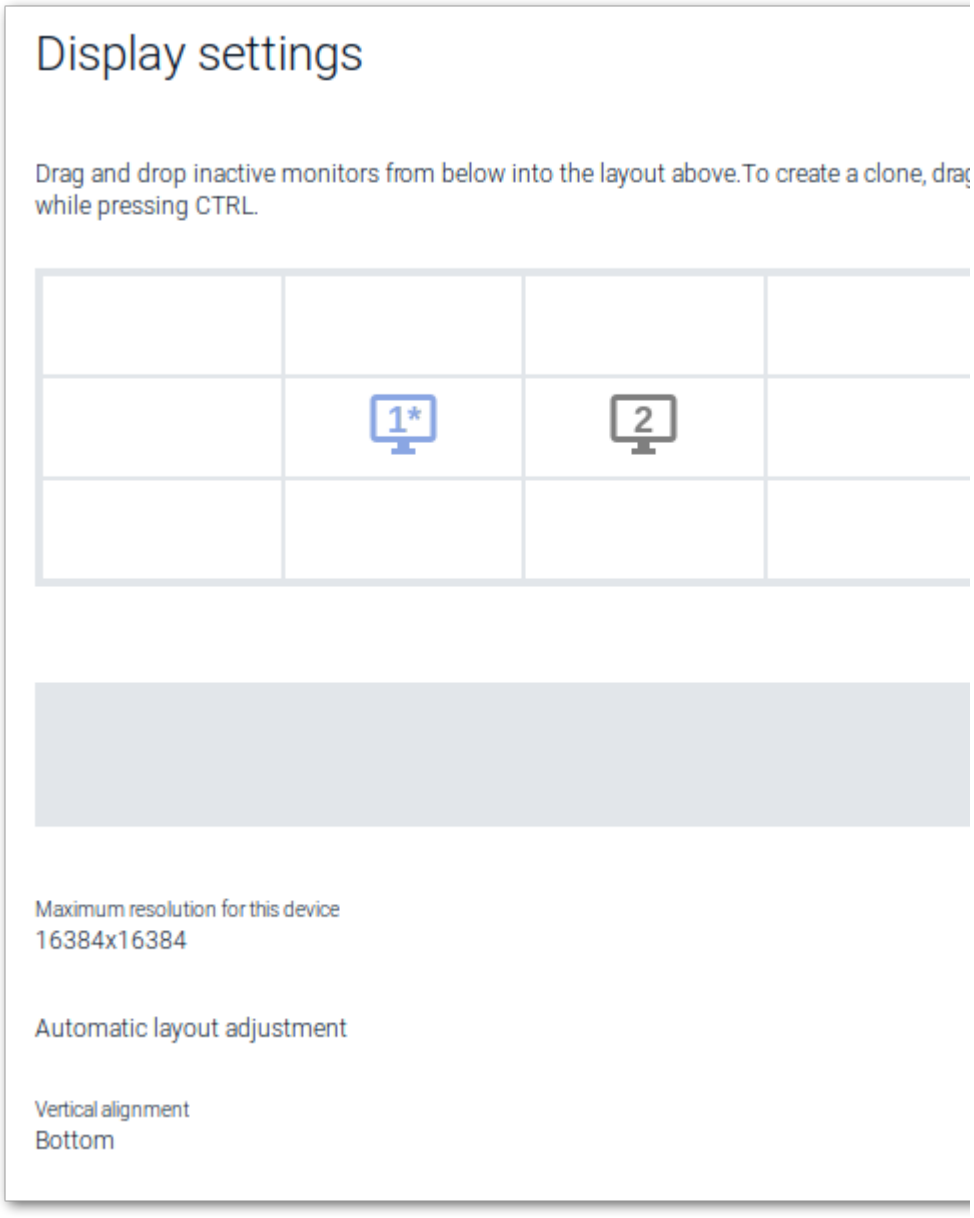
- Arranging monitors (Layout)
  - In the layout section (1), use a drag-and-drop operation to move the monitor icons to the position corresponding to the physical set-up.
    Valid positions are all four sides of an existing monitor icon.
    To place a monitor between two other monitors, drop the monitor icon on the middle line.[2]
- Cloning monitors (Clone mode),[3] see below
- Disabling monitors[4]
  - In the layout section, select a monitor icon. Then select the **Active** option for it.
    Alternatively, use a drag-and-drop operation to move the monitor icon to the section for inactive monitors (2).[5]
- Automatic layout adjustment when a monitor is disabled (4)
- Adjust vertical alignment (5)
  - From the list-field, choose between **Bottom** and **Top**.

[1] for eLux RP 6.9 and later versions
[2] from eLux RP 6.11
[3] from eLux RP 6.9
[4] from eLux RP 6.9
[5] from eLux RP 6.11

When multiple monitors are positioned side by side, all monitors are aligned at the bottom, for example. This feature allows you to manage your windows more easily and switch smoothly between monitors.

Note

The system displays the maximum resolution supported by the graphics card across all monitors (3) and ensures that this value cannot be exceeded by user actions such as cloning or changing resolutions.



1. Layout section: All connected and active monitors
   - Arrange monitors via drag-and-drop
   - Cloning monitors

   The selected monitor is displayed in blue.

   The primary monitor is indicated by an asterisk.
2. Section for inactive monitors
3. Maximum resolution supported across all screens
4. Automatic layout adjustment when a monitor is disabled
5. Vertical alignment

Cloning monitors

Create clone	▸ In the layout section, drag one monitor icon over another while holding down the CTRL key. *The two icons are merged into one monitor icon (clone). Both identifiers are displayed.* *An asterisk indicates whether the primary screen is included.* *The resolutions of all cloned monitors are changed to the greatest common resolution.* One clone may contain up to four monitors. Even monitor icons from the section for inactive monitors can be dragged over an icon in the layout section for cloning while you hold down the CTRL key.	
Show individual monitors of a clone	▸ Click a clon icon. *A pop-up window opens showing the individual monitor icons.* To show details for a screen, click a monitor icon in the pop-up window.	
Remove monitor from clone mode	▸ Drag the monitor icon from the open pop-up window to a free position in the layout section.	
Copy only rotation of a monitor	▸ In the layout section, drag monitor icon 1 over monitor icon 2. *The rotation of screen 2 is changed to the rotation value of screen 1.*	

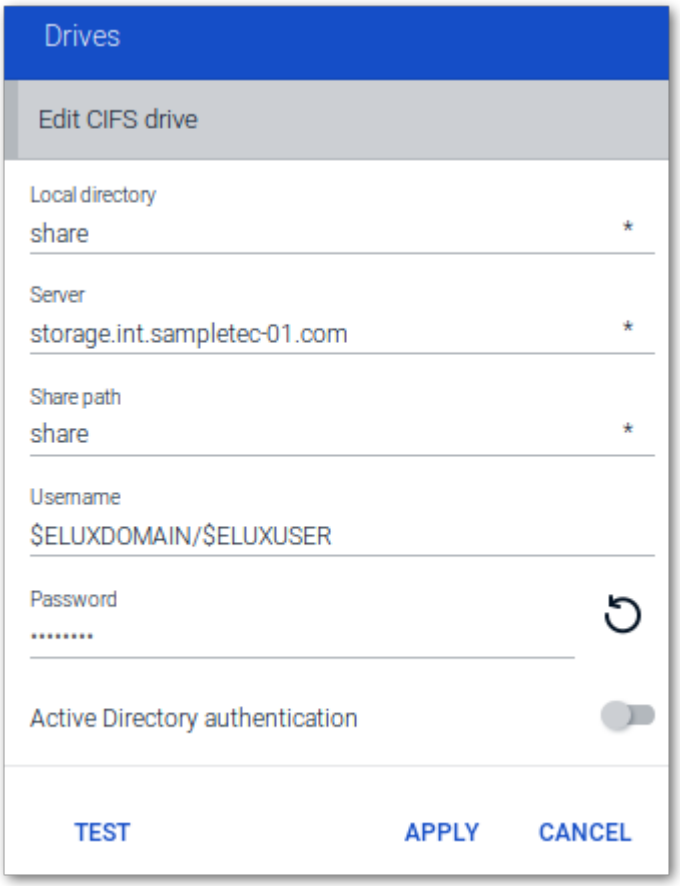
Number of supported monitors

The number of supported monitors depends on the device. If the maximum number of connected monitors is exceeded, eLux will disable the first monitor – or the exceeded number of monitors.[1] For example, if a notebook only supports one additional monitor (two in total) and you connect a second external monitor (three in total), eLux will disable the internal monitor.

[1] from eLux RP 6.9

5.5. Drives dialog

Define shared Windows network directories as drives that the client can access. These drives can be used as storage locations for browser files.



Option	Description
Local directory	Name for the directory
Server	Name of the server
Share path	Share path with Windows share name
Username	Windows domain and username to access the directory: `<Domain/User>` In the figure, user variables are used.
Password	Password to access the directory
Active Directory authentication	The Active Directory logon data are used to access the directory. The **Username** and **Password** fields are then hidden.

Note
To access network drives with AD authentication, the software package **Network drive share** and the included feature package **Linux Key Management Utilities** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

Test	Checks whether a connection can be established using the data specified

The directory path `/smb/` is automatically added in front of the directory name. The data are available on the local flash drive under `/smb/<Directory name>`.

Example: `/smb/share`

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

5.5.1. Browser home directory

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

1. In the tree view, for the relevant level, open the  **Applications** context menu and click **Software defaults...**

   For further information, see Defining software defaults.
2. 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.

5.5.2. 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.

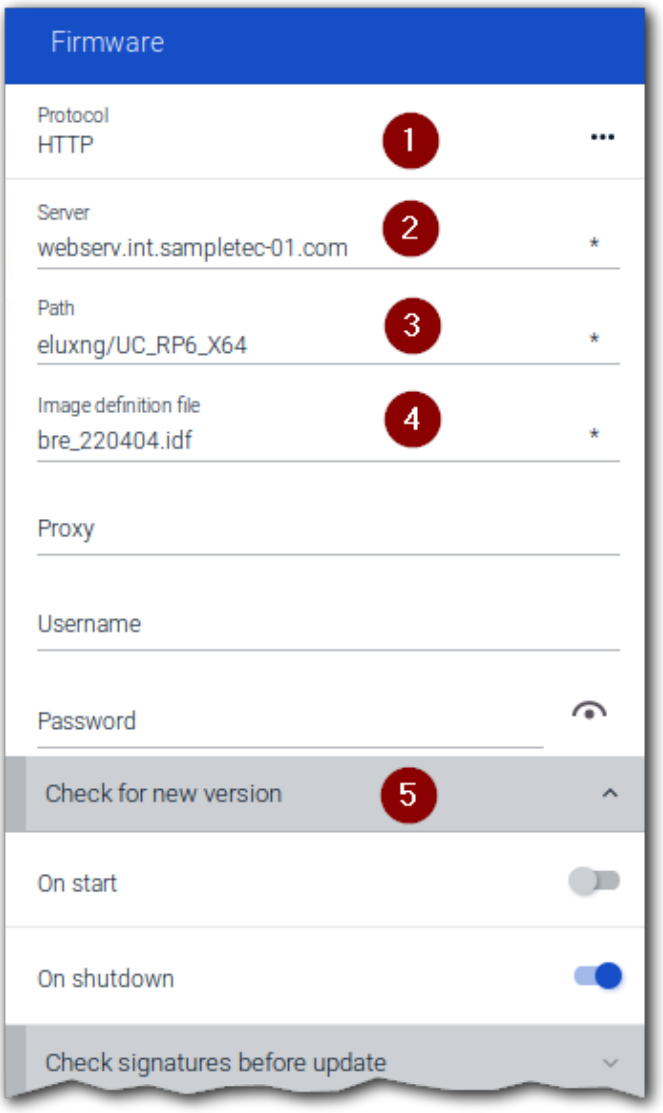
Mounted devices are shown as live information icons. For managed devices, the administrator can suppress the display of live information icons.

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

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

5.6. Firmware dialog

The **Firmware** dialog allows you to configure the firmware update settings for software updates of your device.



1	Protocol of the web server for transfer of the software packages
2	Web server that provides eLux software packages and image definition files
3	Directory path of the eLux software packages on the web server
4	IDF on the web server, defines the software packages for the firmware update
5	The device checks whether an updated IDF is available and triggers a firmware update if necessary.

For further information on performing a firmware update, see eLux commands.

5.6.1. 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 clients (`HTTP, HTTPS, FTP, FTPS`)
Server	Name (FQDN) or IP address of the web server containing the eLux software packages and the image definition file
2nd web server for VPN devices (optional)	Click ... to specify an alternative web server for devices connected via VPN:[1] Choose the protocol (`HTTP` or `HTTPS`)[2] 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)	Static (Consumer): IP address and port number (3128) of the proxy server Format: `IP address:port` Example: `192.168.10.100:3128` Dynamic: Within the subnet, one of the devices is automatically used as a proxy client. Note that for the definition of a static proxy device, from Scout 15 2204 the entry `None` must be selected. For further information, see Static proxy.
User and Password (optional)	Username and password (if required) to access the eLux software container of the web or FTP server

[1] from Scout 15 2107 and eLux RP 6 2204
[2] from Scout 15 2204

Option	Description
Path	Directory path of eLux software packages on the web server Use slashes / to separate directories. Example: Use `eluxng/UC_RP6` to refer to the IIS web server directory `W:\inetpub\wwwroot\eluxng\UC_RP6\` If you use ELIAS 18, specify the path name defined during the ELIAS 18 installation. Example: `elias/UC_PR6_X64` To distinguish by installed eLux major versions, use the container parameter.
Image file	Name of the image definition file (IDF) on the web server which is used for firmware updates Depending on the object rights, an IDF name can be entered or an IDF is selected from the list-field. For further information, see Protecting firmware configuration. To define an alternative image for specific hardware models, use the Release parameter.
Check for new version on start / shut-down	The device checks during start or shutdown whether any firmware updates are available and necessary. To allow users to decline an update, select **User must confirm update**.
Elias... button	Starts the ELIAS tool and opens the image definition file indicated in the **Image file** field
Security... button	The **Security settings** allow you to define a signature check before update through the client. Signature checks can be performed for the image definition files and/or eLux software packages.
Reminder... button	The **Reminder Settings** allow you to define whether a user is allowed to defer a firmware update and for how long. Moreover, you can specify time intervals for the update reminder. For further information, see Update deferment by user.

3. Test the **Firmware** settings on a client. To do so, on the eLux RP 6 device, on the **Command panel**, click **Update**. For further information, see Updating the firmware in the eLux guide.

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

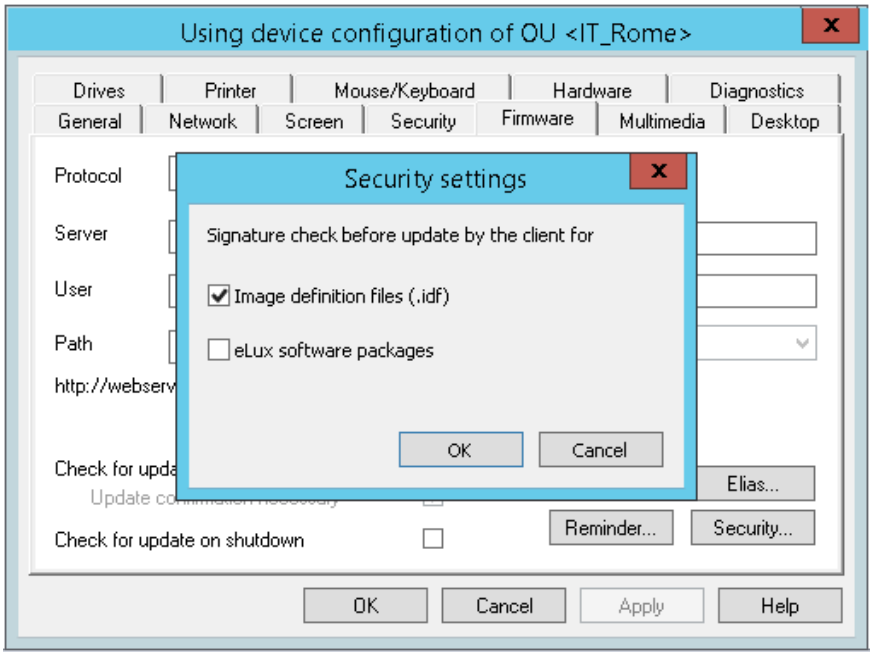
5.6.2. Firmware security through signature

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

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

Activating signature check

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



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

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

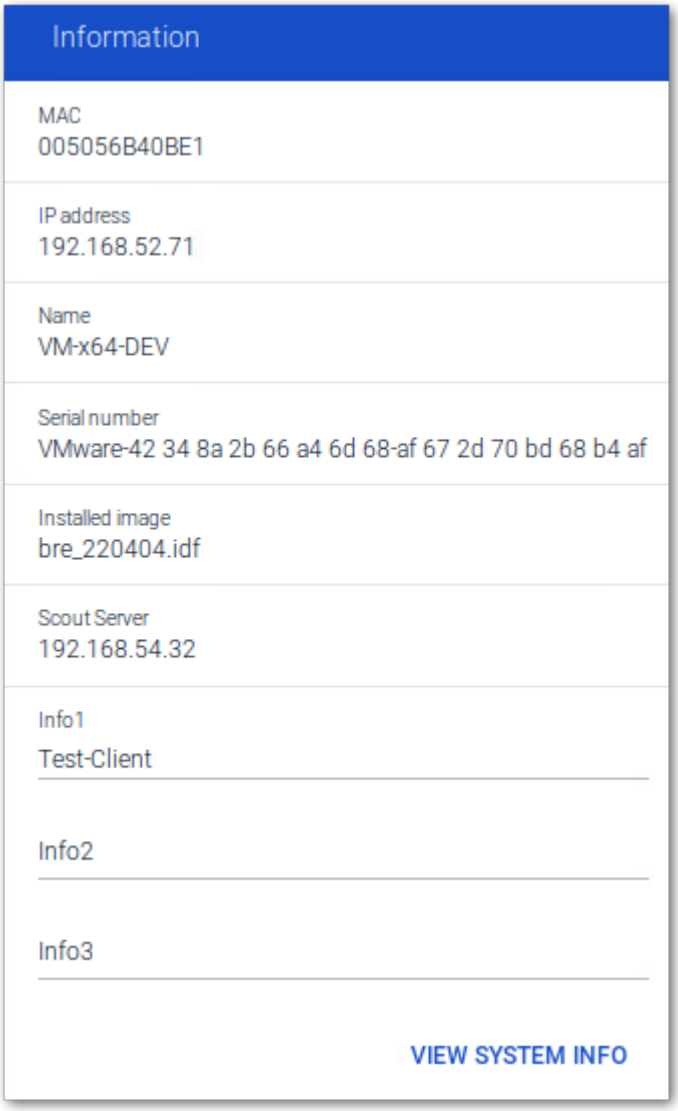
Certificates

Verifying the IDF signature on the client side requires the root certificate, but also the signature certificate in the local client directory `/setup/cacerts`. If you use own certificates for signing IDFs or individually composed eLux packages, 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.

5.7. Information dialog



Option	Description
MAC address	MAC address of the device
IP address	IP address of the device
Name	Host name of the device
Serial number	Serial number of the device
Installed image	Name of the currently installed IDF
Scout Server	Scout Server that manages the device
Info1-3	The **Info** fields can be edited by the users if they have the relevant user right. They are already provided in the First Configuration Wizard.

Option	Description
Logged-on user (with AD user authentication)	Username of the logged-on user
View system info	• Host ID • Current status of Subscription Double-click the magnifier icon to view details on the license lease (if managed through Scout). • eLux version • Hardware information such as CPU clock speed , RAM size and BIOS version • Installed software packages including version numbers

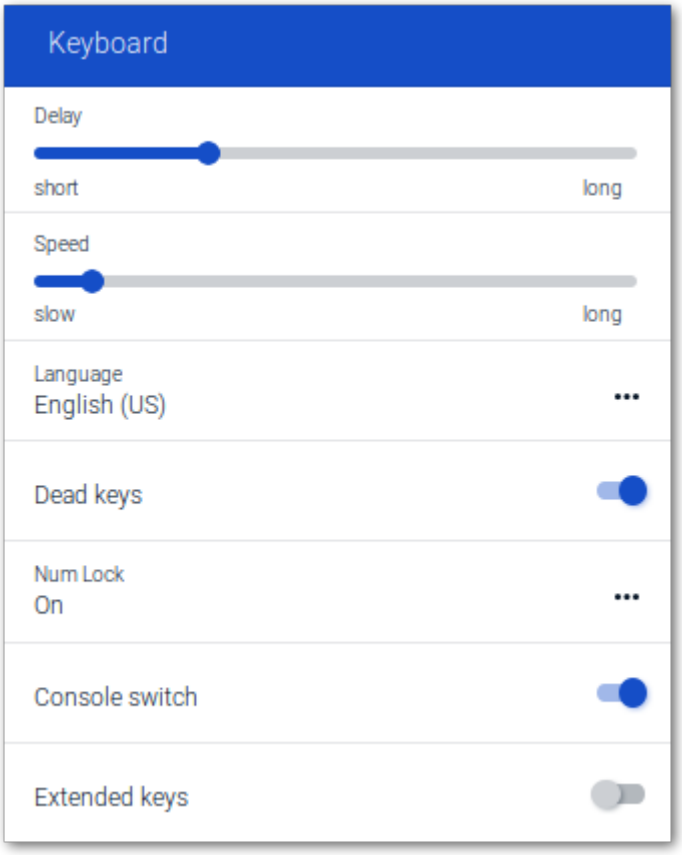
Opening the Information dialog via key combination

- Press WINDOWS+ALT+I.

Note
The **Information** dialog can be hidden via the user rights.[1]

[1] from eLux RP 6.5

5.8. Keyboard dialog

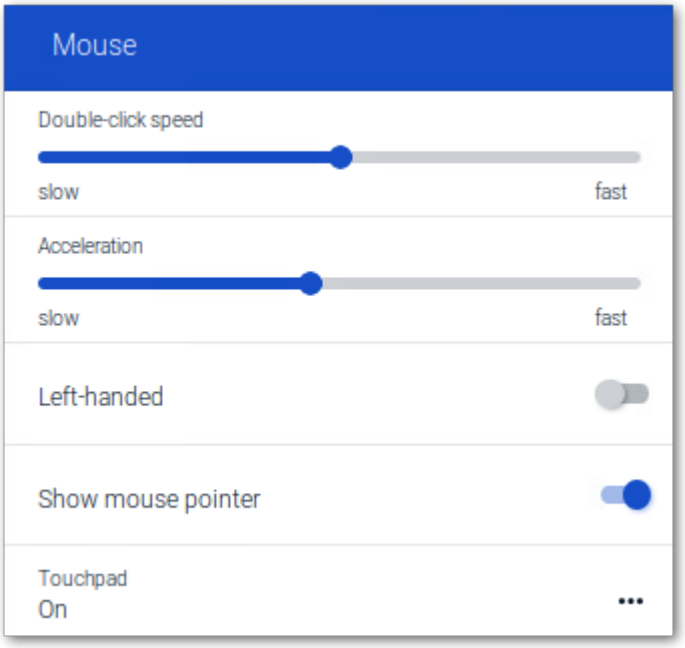


Option	Description	
Delay	Controls how long a key needs to be pressed until the letter is retyped	
Speed	Controls how fast a letter is retyped when a key is pressed	
Language	Keyboard language	
Dead keys	Dead keys only produce visible output when they are followed by a second key-stroke. For example, accent keys are dead keys as they need to be pressed before you press a character key (`+ A => à). Note: Some hardware platforms and some applications do not support this option.	
Num Lock	On	Enables the numeric keypad of the client keyboard on device start (default)
	Off	Disables the numeric keypad of the client keyboard on device start
	Auto[1]	Enables the numeric keypad on mobile devices and disables it on other devices

[1] for eLux RP 6.4 and later versions

Option	Description
Console switch	Users can use key combinations to switch between consoles. If this option is not selected, console 1 (eLux desktop) is shown. For further information, see Shortcuts.
Extended keys	Enables multimedia and other keys with special keyboard functions

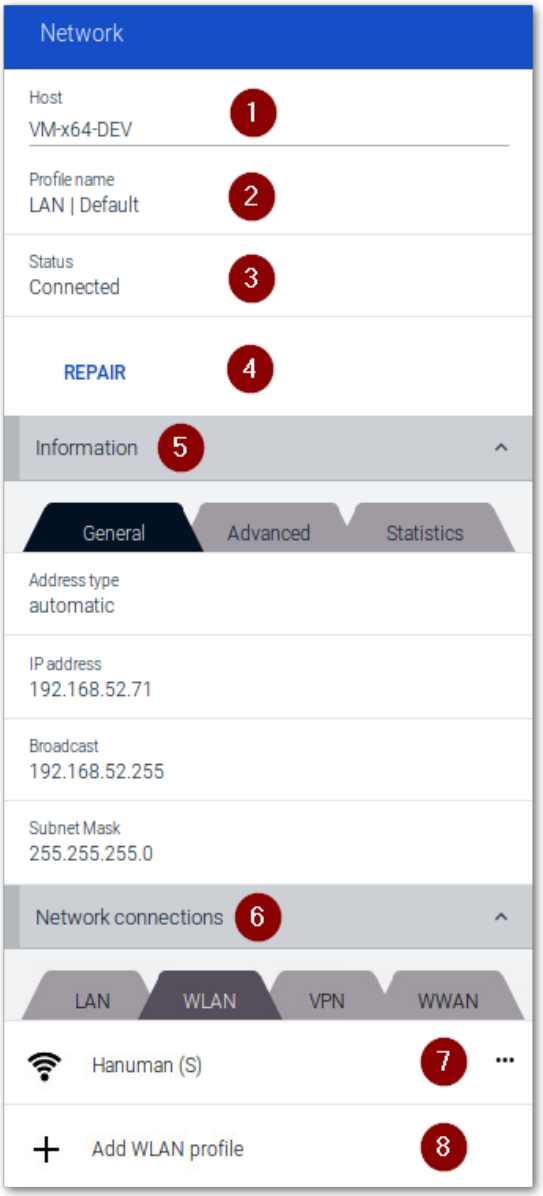
5.9. Mouse dialog



Option	Description	
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.	
Left-handed	Switches primary and secondary mouse buttons	
Show mouse pointer	Determines whether the mouse pointer is shown	
Touchpad[1] (für mobile Geräte)	On	Enables touchpad (default)
	Off	Disables touchpad
	Auto	Disables touchpad when a mouse is plugged in

[1] from eLux RP 6 2103

5.10. Network dialog



1	The host name of a device can be set by the Scout Console, by the First Configuration wizard, or by eLux (`elux-xxx`). If configured, you can change the host name locally (and send it to the DHCP server).
2	Shows the active network connection with network type and profile name
3	Shows the status of the active network connection
4	Use this button to check the status of the active network profile and establish a connection.
5	Under **Information**, network-related data such as IP address and MAC address of the device are shown, as well as statistics. This segment can be hidden via the user rights.[1]
6	Under **Network connections**, depending on the hardware installed, up to four tabs are shown for different network types.
7	An existing network profile can be connected / disconnected, edited or deleted via menu. Click ...
8	Create a new network profile

The following network types are available:

- LAN (only one profile, cannot be deleted)
- Wireless LAN
- VPN
- Wireless Wide Area Network (Mobile Internet)[2]

[1] for Scout 15.5 and later versions
[2] for eLux RP 6.5 and later versions

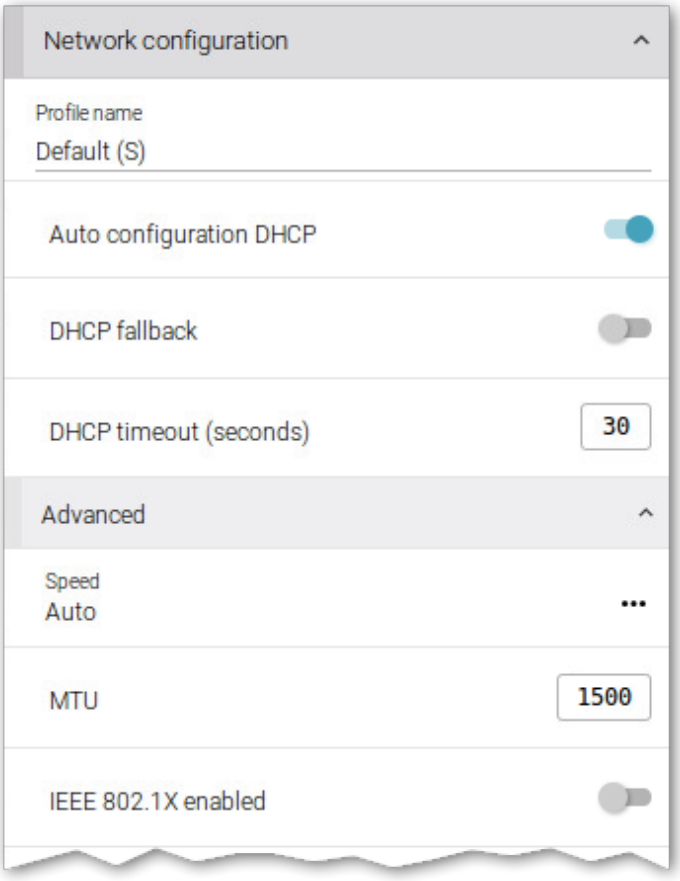
Note
In addition to Internet Protocol Version 4 (IPv4), **IPv6** is supported for local applications.[1] For further information, see Internet Protocol version 6 (IPv6) in the **Scout** guide.

[1] for eLux RP 6.6 and later versions

5.10.1. Configuring the LAN profile

1. In the configuration panel, open the **Network** dialog, and under **Network connections**, select the **LAN** tab.
2. Click the displayed LAN connection (Default) or the ... button next to it. Then, on the context menu, click **Edit**.

   *The **Network configuration** dialog opens:*



3. Edit the following fields:

Option	Description
Profile name	Name of the LAN profile For profiles defined in the Scout Console, the character string `(S)` is appended.
Auto-configuration DHCP	Integration into existing network via DHCP If you do not use DHCP, use the provided fields to configure IP address, net mask, gateway and name server manually.
DHCP fallback	If DHCP fails, the defined settings are used as long as the lease is valid.
DHCP timeout	Timeout in seconds for the DHCP request
Speed	Data transfer rate in MBit/s
MTU	Maximum transmission unit
IEEE 802.1X enabled	Enables authentication via IEEE 802.1X
IEEE 802.1X allow without authentication[1]	Specify whether a connection may be set up if a timeout or authentication error for 802.1X occurs. The option is active by default as soon as you enable 802.1X authentication.[2] If the option is cleared, you can only connect after successful 802.1X authentication.
IEEE 802.1X number of connection retries[3]	Number of connection retries before aborting
IEEE 802.1X number of logon retries[4]	Number of authentication retries for a successful connection before authentication is aborted
IEEE 802.1X timeout	Time period in seconds before an authentication try is aborted

[1] from eLux RP 6.9.1000
[2] from eLux RP 6.9.1000 and eLux RP 6.11
[3] from eLux RP 6.9.1000
[4] from eLux RP 6.9.1000

Option	Description
Use proxy[1]	The proxy setting you define here is used by the `System proxy` option in the browser application definition. For further information, see Proxy configuration.
Internet connection test[2]	Each time a connection is set up, the system can check whether addresses on the Internet can be reached. For further information, see "Adding a WLAN profile" on the next page.

4. Confirm with **Apply**.

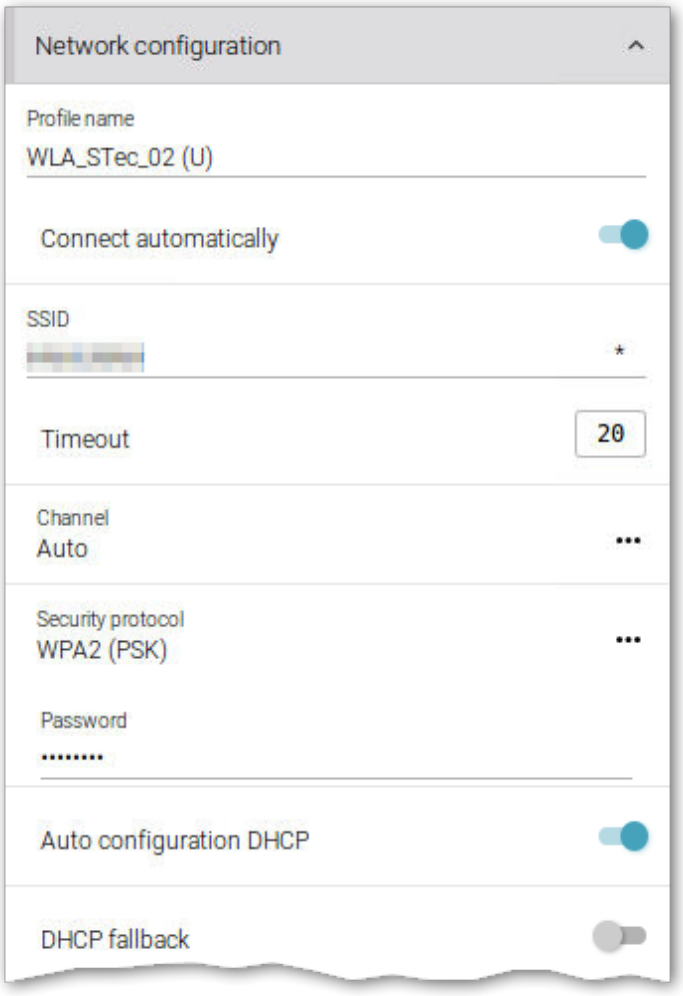
[1] for eLux RP 6.5 and later versions
[2] from Scout Enterprise Management Suite 15.9

5.10.2. Adding a WLAN profile

1. In the configuration panel, open the **Network** dialog. Then under **Network connections**, select the **WLAN** tab.
2. Click **+ Add WLAN profile**.

   The WLAN networks active at the site are displayed with their SSID.
3. Select the WLAN you want to connect to, or click **Manual**.

   *The **Network configuration** dialog opens:*



4. To configure a WLAN profile manually, edit the following fields:

Option	Description
Profile name	Name for the new WLAN profile The character string `(U)` is appended to a user-defined profile. For profiles defined in the Scout Console, the string `(S)` is appended.

Option	Description
Connect automatically	If the signal strength is sufficient, the device automatically attempts to connect to this WLAN.
SSID	Name of the WLAN
Hidden SSID[1]	Select this option if the SSID of the WLAN is not shown.
Timeout	Time period in seconds for establishing the connection
Channel	Is selected automatically by default
Security protocol	Authentication type
Password	Password or security key
Auto-configuration DHCP	Integration into existing network via DHCP
DHCP fallback	If DHCP fails on start-up, the settings are used unless the lease has expired.
DHCP timeout	Time period in seconds for the DHCP request
Use proxy[2]	The proxy setting you define here is used by the `System proxy` option in the browser application definition. For further information, see Proxy configuration.
Internet connection test[3]	Each time a connection is set up, the system can check whether addresses on the Internet can be reached. Without connectivity, the system then checks for the existence of a captive portal and, if available, redirects to it. For `automatic` (default), the connection test is performed unless a central system proxy is defined. Whether the option is displayed depends on the corresponding dedicated user right.[4]

5. If you connect to an existing WLAN, most of the information is read-only. To connect, enter the password or security key.
6. Confirm with **Apply**.

When connected to a WLAN, the system bar shows a WiFi icon  which roughly reflects the signal strength.

[1] from eLux RP 6.11
[2] from eLux RP 6.5
[3] from Scout Enterprise Management Suite 15.9
[4] from Scout Enterprise Management Suite 15 2101

- Click the WiFi icon to display further information.

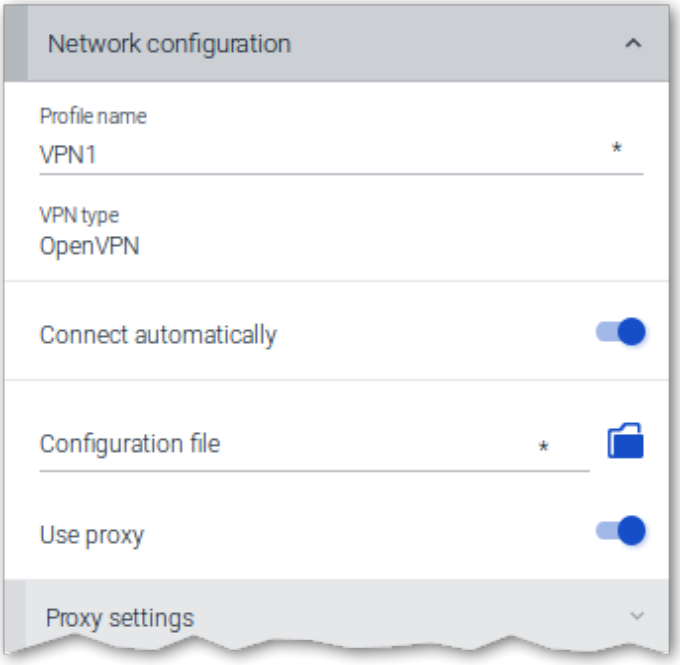
For further information, see Live information.

5.10.3. Adding a VPN profile

Note
The **VPN** tab is only shown if the relevant software is installed on the device.

As VPN clients Cisco AnyConnect and OpenVPN are supported.

1. In the configuration panel, open the **Network** dialog. Then under **Network connections**, select the **VPN** tab. [1]
2. Click **+ Add VPN profile**.



[1] for eLux RP 6.4 and earlier versions in a separate dialog

3. Edit the following options:

Option	Description
Profile name	Name of the new VPN profile The character string `(U)` is appended to a user-defined profile. For profiles defined in the Scout Console, the string `(S)` is appended.
VPN application type	Select `Cisco AnyConnect` or `OpenVPN`
Connect automatically	The VPN client is started automatically on each device restart.
Configuration file	Depending on the VPN application used, the client devices must have a configuration file. Select the relevant configuration file.
Use proxy[1]	The proxy setting you define here is used by the `System proxy` option in the browser application definition. For further information, see Proxy configuration.

4. Confirm with **Apply**.

For further information, see VPN in the **Scout** guide.

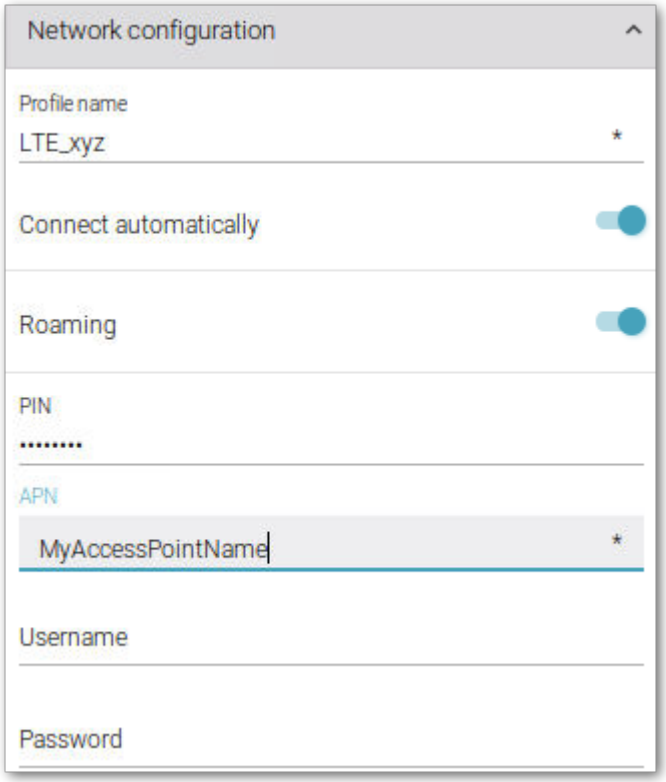
5.10.4. Adding a WWAN profile

- for eLux RP 6.5 and later versions -

If your mobile device has an appropriate SIM card, you can connect to a wireless wide area network. This can be cellular data networks such as LTE or UMTS.

1. In the Configuration panel, open the **Network** dialog. Then under **Network connections**, select the **WWAN** tab.
2. Click **+ Add WWAN profile**.

[1] for eLux RP 6.5 and later versions



3. Edit the following options:

Option	Description
Profile name	Name of the new WWAN profile The character string `(U)` is appended to a user-defined profile. For profiles defined in the Scout Console, the string `(S)` is appended.
Connect automatically	If the signal strength is sufficient, the device automatically attempts to connect to the WWAN.
Roaming	The cellular data connection stays on when your device is outside your mobile operator's network.
PIN	PIN of the SIM card (if used) If you leave the field empty and the SIM card requires a PIN, the PIN will be requested on each connection setup.[1]
APN	Access Point Name: Address used to connect to the Internet when using your cellular data connection
Username	Username for your mobile account
Password	Password for your mobile account

4. Confirm with **Apply**.

[1] To define PIN settings for your SIM card, use a mobile device such as a smart phone.

When connected to a WWAN, the system bar shows a WWAN icon  which roughly reflects the signal strength.

- Click the WWAN icon to display further information.

For further information, see Live information.

5.10.5. Proxy configuration

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

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

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

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

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

Option	Description
No proxy	No proxy server is used
Manual (Proxy:Port)	Specify fixed proxy server with port number Example: `proxy.sampletec-01.com:3800` To define destinations that you do not want to access via proxy, in the **Proxy exception list**, enter the relevant network addresses separated by semicolons.

Auto (URL)	Proxy auto-config (PAC): Determines the appropriate proxy for each URL
	Examples:
	`http://proxy.sampletec-01.com/proxy.pac`
	`http://wpad.sampletec-01.com/wpad.dat`

Pass-through logon for proxy (with AD user authentication)[2]	If a central **system proxy** is configured with AD authentication, the AD logon data are used for authentication. Proxy authentication may be required if you use browser content redirection under Citrix.
Proxy username[3]	Username for authentication on the system proxy

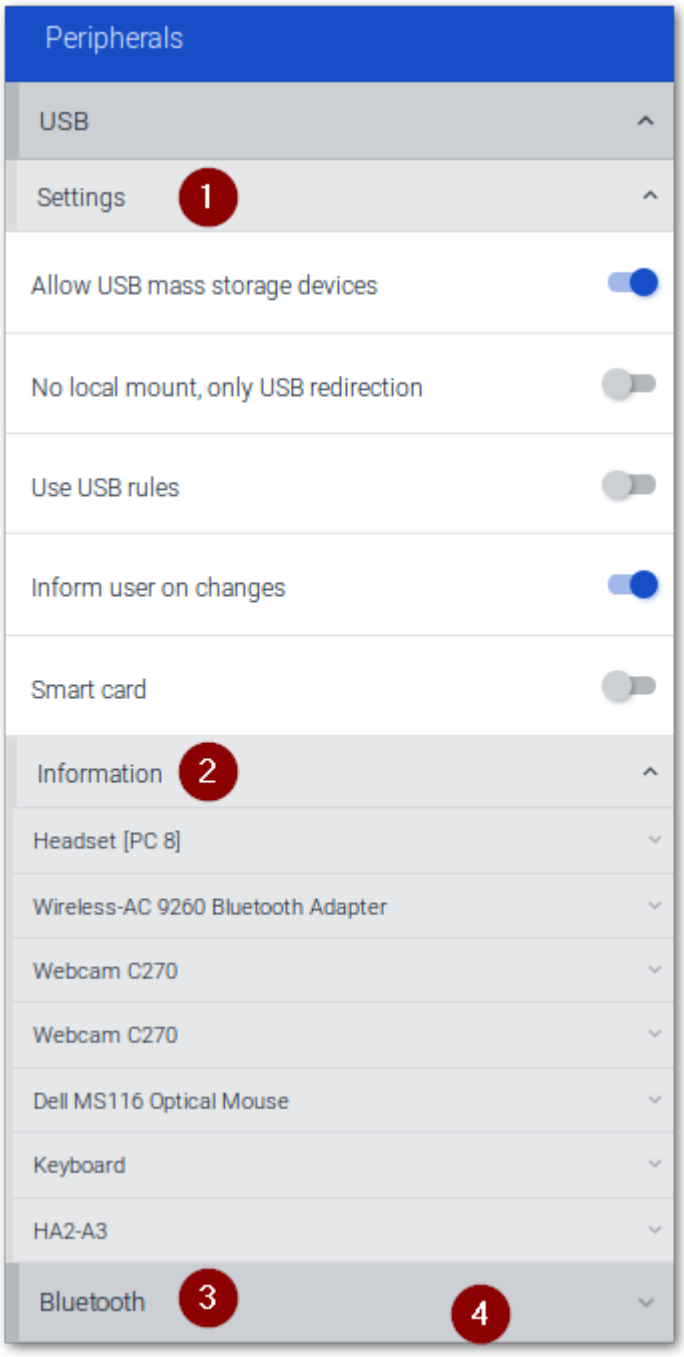
[1] for Scout 15.5 and later versions
[2] from Scout Enterprise Management Suite 15.8 and eLux RP 6.7
[3] from Scout Enterprise Management Suite 15.8 and eLux RP 6.7

Option	Description
Proxy password[1]	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.

[1] from Scout Enterprise Management Suite 15.8 and eLux RP 6.7

5.11. Peripherals dialog



1	The **USB** section is divided into **Settings** and **Information**.[1] The individual USB settings are described below.
2	View all connected USB devices ▸ Expand an entry to view the Product name, Vendor name, Product ID, Vendor ID and USB type.
3	Display Bluetooth audio devices[2]
4	Further down, settings for COM ports such as speed, parity, stop bits are shown

[1] for eLux RP 6.4 and later versions
[2] for eLux RP 6.6 and later versions

Option	Description
Allow USB mass storage devices	Allows the use of connected USB mass storage devices If the local use of USB devices via mountpoints is allowed, connected USB devices are shown on the system bar as live information.[1] To remove a USB device safely, click the live information icon 
No local mount, only USB redirection	Restricts the use of USB mass storage devices to USB redirection within configured sessions on a backend. There are no mount points provided for using USB mass storage devices locally on the eLux client.
Use USB rules	Restricts the use of USB mass storage devices according to defined rules: Using USB mass storage devices can be restricted to devices with specified VID (Vendor ID) and/or PID (Product ID) such as an individual USB stick model. Moreover, the USB rules can be applied to further USB device classes such as smart card readers. USB rules are defined in the Scout Console. For further information, see USB rules in the **Scout** guide.
Inform user on changes	When a USB mass storage device is connected, a systray message is displayed.
Smart card	Enables card readers

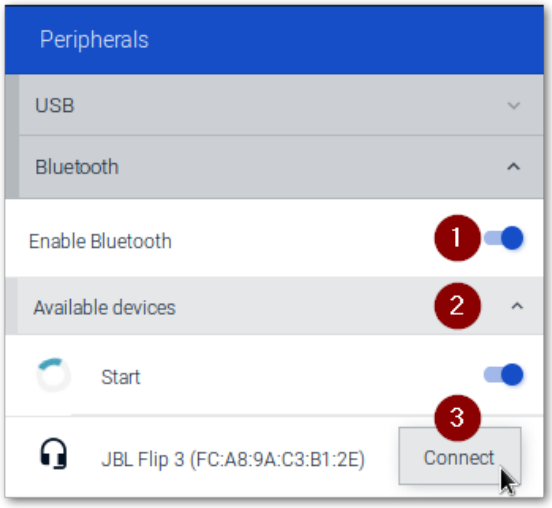
Note
To use smart card readers, the relevant middleware must be installed on the clients. For further information, see USB mass storage devices and card readers in the **Scout** guide.

Webcams

Webcams are shown under **USB > Information** even if they are built in. In order for users to receive a preview of one or more cameras, an app must be defined to display it.[2] For further information, see Webcamsin the **Scout** guide.

[1] for eLux RP 6.4 and later versions
[2] from eLux RP 6 2107

5.11.1. Connecting Bluetooth audio devices



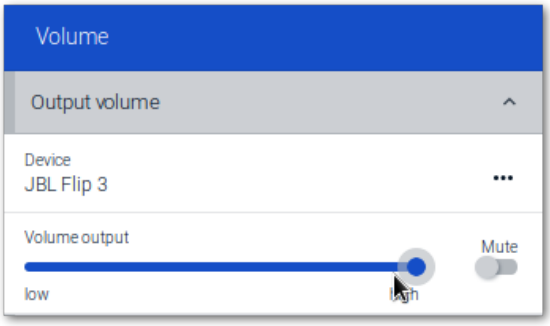
1. In the **Peripherals** dialog, under **Bluetooth**, select the **Enable Bluetooth** option (1).

   The devices paired via Bluetooth are displayed.

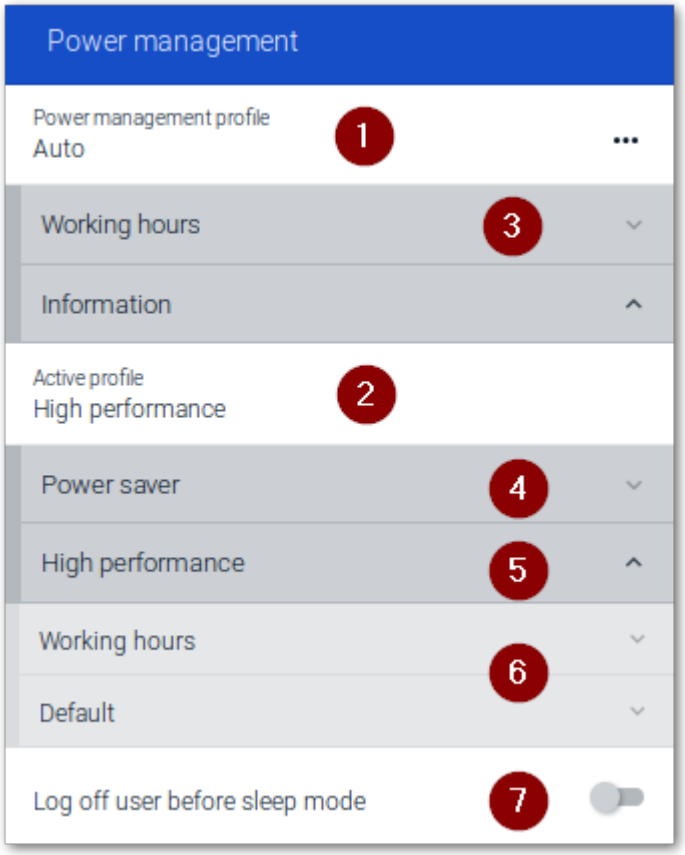
2. To start searching for Bluetooth devices, expand the **Available devices** dialog with ⌄ (2).
3. For the Bluetooth device you want to connect, click **Connect** (3).

   The Bluetooth device is connected and added to the paired devices.

4. To adjust the volume of a connected Bluetooth audio device, use the **Volume** dialog.



5.12. Power management dialog



1	Selecting one of the options, enables the relevant profile: `High performance` profile or `Power saver` profile or `Auto` option `Auto` enables `High performance` if the device is plugged in and `Power saver` if the device is on battery power.
2	Shows the currently active profile
3	In order to distinguish between inside and outside working hours in the profiles, the working hours must be defined.[1]
4	Settings for the **Power saver** profile
5	Settings for the **High performance** profile (expanded in the screenshot)
6	Click to view options for working/non-working hours (default) within **High performance**
7	When the computer wakes from sleep, the user must log on again.[2]

Using profiles, you can pre-define settings for the power management of 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 the computer's performance and the screen brightness

You can either explicitly activate one of the power management profiles or you can let the system choose by using 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.

To further distinguish between working hours and non-working hours, a total of four profiles are available, provided you have specified your working hours (3).[3] If you do not define any working times,

[1] for eLux RP 6.8 and later versions and Scout 15.8
[2] for eLux RP 6.7 and later versions
[3] for eLux RP 6.8 and later versions and Scout 15.8

the **Default** profile is always active for **Power Saver** and **High Performance**. Any values under **Working hours** within a profile (6) are then not applied.

Note
The sleep mode corresponds to **Suspend to RAM (S3)**. For further information, see Sleep mode (Suspend) in the **Scout** guide.

For mobile clients, the System bar shows a battery icon.

- Click the battery icon to display more information.

For further information, see Live information.

5.12.1. Options of a power management profile

- To edit the options, open the **Power saver** or **High performance** profile.
  If available, then select the subprofile **Working hours** or **Default** (non-working hours).[1]

Option	Description
Screen brightness	Screen brightness in percent for the selected profile
Turn off the display - after	Determines whether, after a specified number of minutes (**after**), 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 (**after**), the screen saver is enabled when the user is not using the device (idle state)

On idle
- after
- after (User logged off)[2]
- action
	Determines whether, when the device is not used (idle state), after a specified number of minutes (**after**), the selected **action** is performed:
	`Shut down`
	`Sleep mode`
	This option can be specified for both states: user logged on and user logged off

Action on 'Closing the lid'	Action that is performed when users close the lid:
	`No action`
	`Turn the display off`
	`Shut down`
	`Sleep mode`

[1] for eLux RP 6.8 and later versions and Scout 15.8
[2] from eLux RP 6.10

Option	Description

Action on 'Pressing the power button'	Action that is performed when users press the power button:
	`No action`
	`Turn the display off`
	`Shut down`
	`Sleep mode`

Action on 'Pressing the Power/Sleep key' [1]	Action that is performed when user press the Power/Sleep key on their keyboard (requires a suitable keyboard):[2]
	`No action`
	`Shut down`
	`Sleep mode`[3]

Note
The sleep mode corresponds to **Suspend to RAM (S3)**. For further information, see Sleep mode (Suspend) in the **Scout** guide.

[1] for eLux RP 6.5 and later versions
[2] If this key is not available, the configuration has no effect.
[3] Default

5.12.2. Definition of working hours

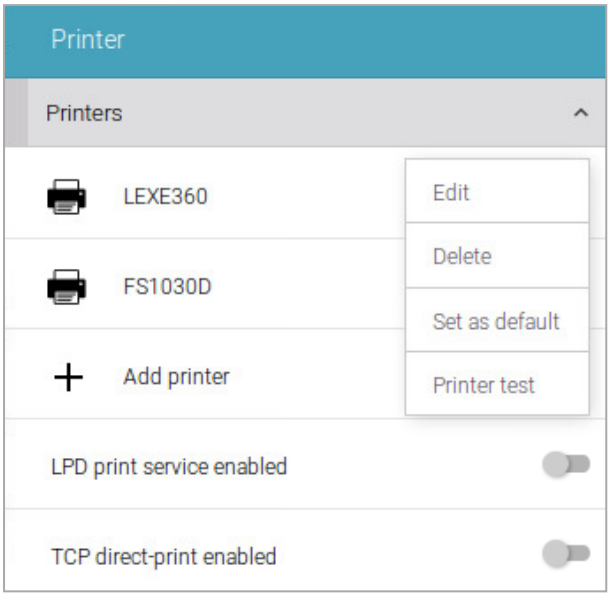
- for eLux RP 6.8 and later versions and Scout 15.8 -

Requires
User right **Define working hours**

- To define your working times, open the Configuration Panel and select **Power management > Working hours**.

Option	Description
Monday to Sunday	Specify for each day of the week whether it is a working day.
Start time	Earliest time for the start of work, effective for all specified working days
End time	Latest time for the end of work, effective for all specified working days

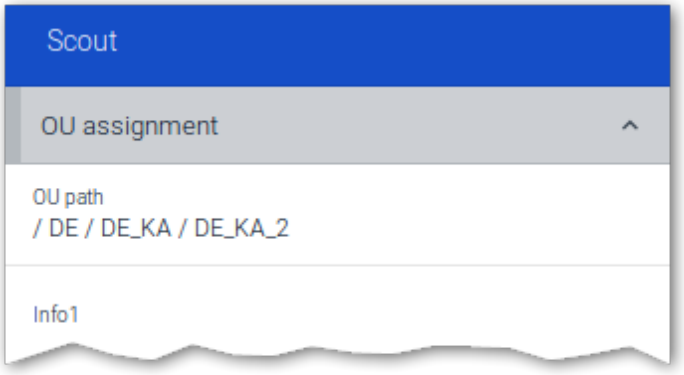
5.13. Printer dialog



Option	Description
Edit (defined printer)	Opens the **Editing printer** dialog for the selected printer
Delete (defined printer)	Deletes the selected printer
Set as default (defined printer)	Defines the selected printer as the default printer
Printer test (defined printer)	A test page is printed on the selected printer.
+ Add printer	Opens the **Adding new printer** dialog For further information on configuring printers, see Printer configuration in the **Scout** guide.
LPD print service	Allows you to share defined printers with other systems via LPD (within the network)
TCP direct print	Select to receive the print data directly via TCP/IP and send it to the printer port (no print formatting, no spooling of print jobs)

5.14. Scout dialog

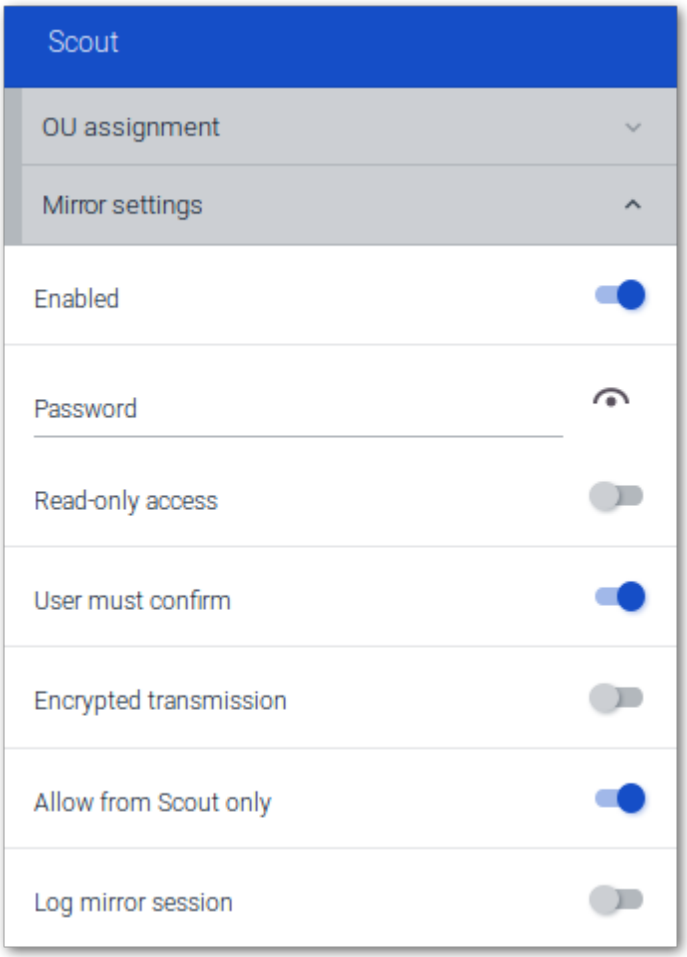
Under **OU assignment**, you configure the connection to an OU of the managing Scout Server. The Scout Server address can be found in the **Information** dialog.



Option	Description
OU path	OU the device is assigned to
Password	If an OU is password-protected, you must enter the password before you can assign a device to it.
Info 1-3	Information on the device

5.14.1. Mirror settings

The settings for mirroring are part of the device configuration and can be found in the configuration panel under **Scout**. As always, they are only shown with the relevant user rights granted.



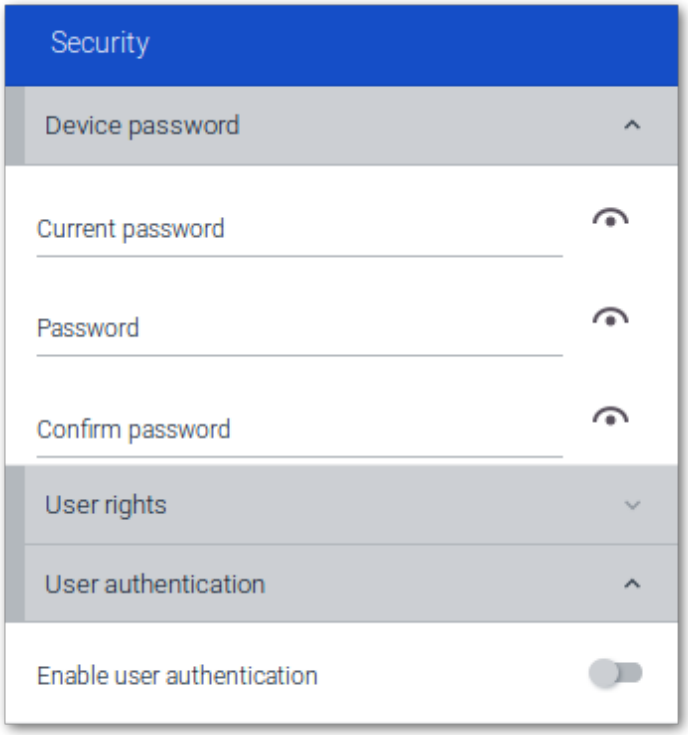
Option	Description
Enabled	Mirroring must be enabled before a mirror session can be started.
Password (optional)	If you define a mirror password, the administrator will need to enter it at the beginning of a mirror session. The device can only be mirrored by persons who know the password. The password must have 6 characters minimum and 8 characters maximum.
Read-only access	Allows the mirroring administrator to read only, not to write
User must confirm	Before a mirror session can be started, the user must confirm.
Encrypted transmission	The mirroring data are transferred using an encrypted connection.

Option	Description
Allow from Scout only	Mirroring is only allowed if the Scout Console is used.
Log mirror session	Each mirror session is logged.

Note
The user can cancel a mirror session at any time. During the entire session, a message is shown to inform the user about the current mirror session.

6.1. Security dialog

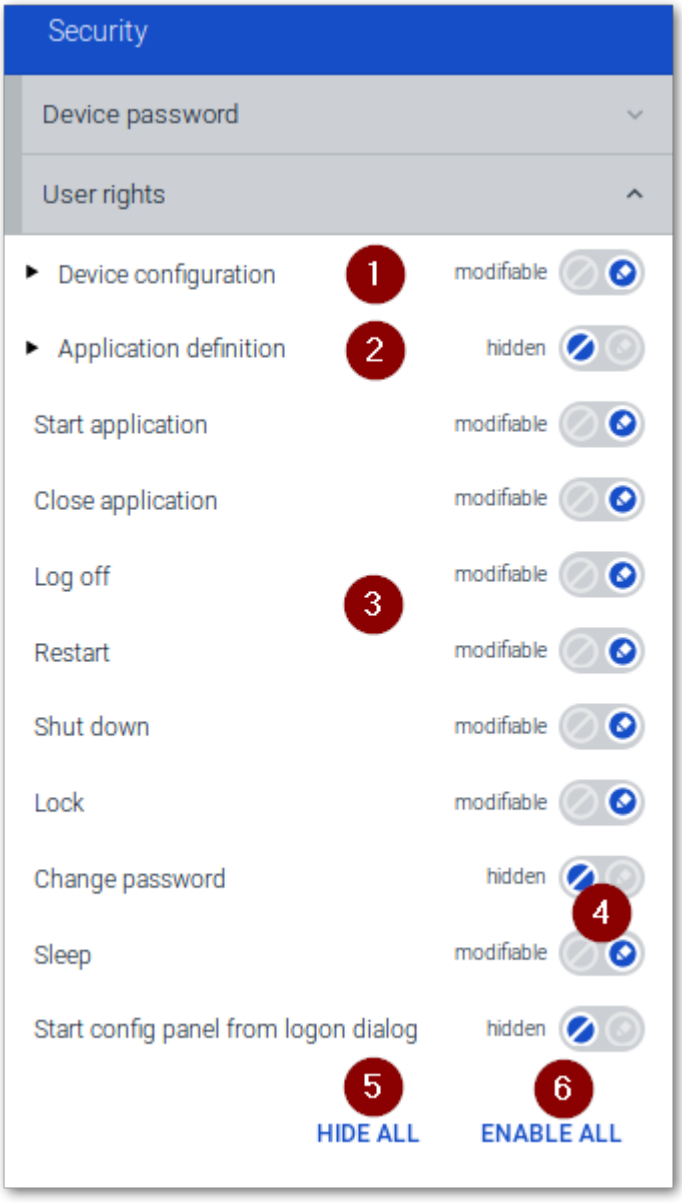
In the **Security** dialog, you can change the device password, configure user rights and set user authentication – provided you have the relevant user rights.



Option	Description
Device password	Important: If you change the device password locally, the device can no longer be managed through the Scout Console.
User rights	Configure eLux user rights for device configuration, application definition and some general eLux functions
User authentication	Configure access rights for example via AD

7.0.1. User rights

In most cases, the administrator defines user rights centrally in the Scout Console. However, with the relevant user right, the user can also change user rights locally.



1	The user rights of the device configuration correspond to the dialogs of the Configuration panel. Example: The user right to modify the key delay is located under **Device Configuration > Mouse/Keyboard**.
2	User rights to define new applications or modify/delete existing applications
3	User rights for general functions
4	Switch status between `hidden` and `modifyable`
5	Attention: All user rights are hidden and thus deactivated with a single click.
6	Allow all user rights with a single click

Changing user rights

Requires
User right **Edit user rights**

1. Open the Configuration panel and select **Security > User rights**.
2. To edit user rights for the device configuration or application definition, expand the relevant node and navigate to the desired function.
3. To modify the status of a function, use the control on the right and click `hidden` or `modifiable`.

   The current status of a function is also displayed textually.

   > **Important** If you hide the **Device Configuration** node, the entire Configuration panel will no longer be displayed. Also, you will no longer be able to access the user rights.

4. Confirm with **Apply**.

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

Note: If the device is managed by Scout, normally the device configuration defined in the Scout Console and thus the user rights defined there have priority. The administrator can define exceptions and support (protect) local device configurations.

For further information, see User rights in the **Scout** guide.

7.0.2. User authentication

Users whose devices are managed via Scout are normally connected to a user management such as Active Directory.

If the user(s) of a device are not yet configured via the central device configuration, the relevant settings can be made locally on the device. As with other functions, be aware that the centrally maintained device configuration may overwrite the local configuration on the next contact with the Scout Server.

Note
The eLux package **User authentication modules** must be installed on the device.

Activating user authentication

1. In the Configuration panel, open **Security > User authentication**.
2. Select the option **Enable user authentication**.
3. Select the **authentication type** such as `Active Directory`.

4. Specify one or more servers or domains.
5. Confirm with **Apply**.

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

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

For further information, see Configuring user authentication and Additional options for AD users in the **Scout** guide.

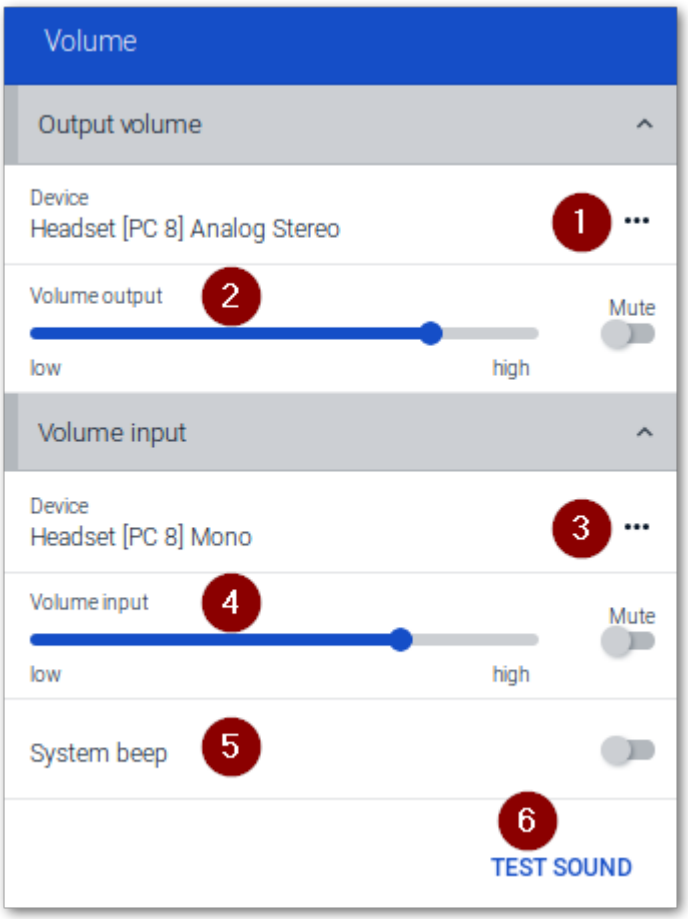
8.1. Volume dialog

The output and input devices are grouped in classes depending on their connector. For each device class, you can control the volume level (Volume output) and sensitivity (Volume input).

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

By default, the priority is defined as follows: USB - Analog - Digital. Priority can be changed in the Scout Console. For further information, see Multimedia tab in the **Scout** guide.

All connected input and output devices are shown.



1	Choose ouput device (class)
2	Control the playback sound level for the selected device class
3	Choose input device (class)
4	Controls the level of sensitivity for recording for the selected device class
5	Acoustic feedback signal when switching off the client
6	Plays a sample sound with the defined volume level

Use the **Mute** option to ensure that no sound is reproduced (output) / recorded (input).

9. Applications

eLux provides two kinds of applications

- Applications providing access to back-end systems (server-based remote applications)
- Local applications

Thin Clients are mainly used as terminals in server-based computing. **Remote** means that the applications such as Windows applications run on a remote server. Still, client-side software is required to initiate and maintain a session.

By nature, the Thin Client has limited resources, meaning the majority of applications are server-based. However, in addition to server-applications, eLux also offers a variety of local applications. **Local** means the application runs locally on the Thin Client. Local applications include browser software, a local shell (XTerm), and desktop tools.

Usually, applications are defined centrally in the Scout Enterprise Management Suite and made available to the clients. Applications can also be defined locally on the client.

The following topics describe how to configure both, applications for connecting to back-end systems and local applications. In addition, further configuration may be required in the application itself. For further information on configuring terminal sessions, please consult the manufacturer's product documentation.

9.1. Defining applications

Applications can be defined locally on the eLux device, the relevant user rights provided.

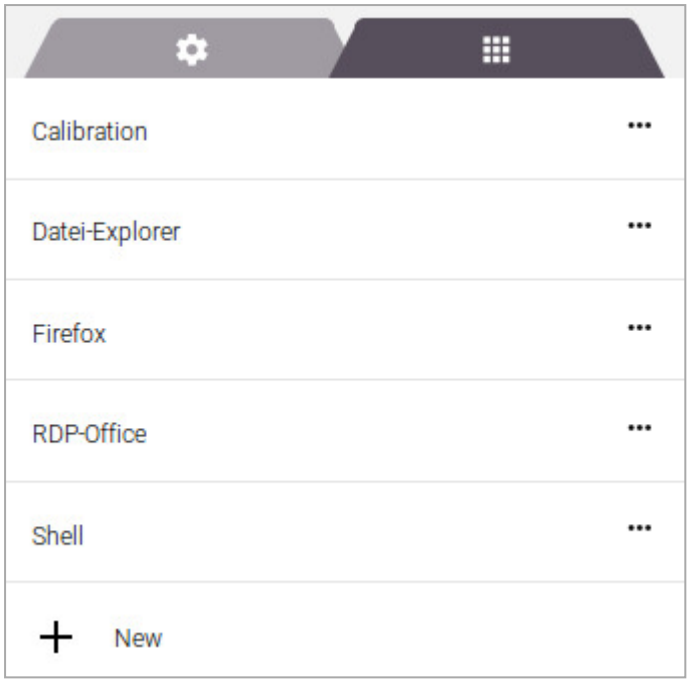
Applications are defined in the Configuration panel.[1]

Defining new applications

1. Open the configuration panel. For further information, see Configuration panel.
2. Click the **Applications** tab  .

   The already defined applications are shown in the configuration panel.

[1] from eLux RP 6.3, for versions in the control panel



3. Click **+ New**.
4. In the **Add new application** dialog, click **Application type**. From the list, select the required application type.

   Note
   If the relevant application entry is missing, the corresponding software package is not installed on the device.

5. Configure the application.

   Under **Properties**, further options are available. For further information, see Application properties.

   If you define a local application, under **Properties**, select the application type.
   For further information on the definition of individual application types, see Application definition in the **Scout** guide.

   For further information on operating, see Configuration panel.

6. Confirm with **Apply**.

Note
The application types `ICA`, `Emulation` and `XenDesktop` cannot be used to for defining applications locally on the eLux RP 6 device. To make these applications available on the device, define them in the Scout Console

Editing applications

1. Open the configuration panel and select the **Applications** tab.
2. Click the application you want to edit.

3. On the context menu, click **Edit**.

   *The **Edit application** dialog opens.*

4. Edit the application and confirm with **Apply**.

Deleting applications

1. Open the configuration panel and select the **Applications** tab.
2. Click the application you want to delete.
3. On the context menu, click **Delete**.
4. Confirm with **Apply**.

9.2. Application properties

The following options are provided for most applications:

Option	Description
Name	Name of the application, shown in the control panel and on the start menu
Server	Name of the server the application connects to
Login	The user is automatically logged on to the terminal server by using predefined credentials (username, password, domain).
Pass-through login	The values of the local user variables `$ELUXUSER`, `$ELUXPASSWORD` and `$ELUXDOMAIN` 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).
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 (except for PNAgent) For eLux RP 6, the desktop icon is also shown in the personal desktop view.

9.3. Connecting to a Citrix farm

Users can connect to sessions running on a Citrix back-end. Once the connection has been made, the user can access published desktops and applications.

Connecting the Thin Client to a Citrix back-end is performed by one of the following applications:

- by a StoreFront application to a StoreFront server
- by the Citrix Self-Service user interface to a StoreFront server
- via browser to a StoreFront server or Web Interface server
- by a PNAgent application to a StoreFront server (XenApp Services Support must be enabled on the Citrix farm) or Web Interface server
- by an ICA application to a virtual desktop or published applications

---

Note
Access via the **ICA** application type is deprecated and only supported by Citrix up to XenApp version 6.x.

Requirements

- The eLux package **Citrix Workspace app for Linux** or **Citrix Receiver for Linux** must be installed on the clients.
- To connect via HTTPS, for the application types **Storefront**, **Self Service** and **PNAgent**, the relevant root and intermediate certificates must be available on the clients.
  - Root certificates must be transferred to `/setup/cacerts`.
  - Intermediate certificates must be transferred to `/setup/cacerts/intcerts`.

  For further information, see Certificates in the **Installation** guide.
- To connect via HTTPS, for the application type **Browser**, the relevant root and intermediate certifcates must be available on the clients.
  - Firefox: Root certificates and intermediate certificates must be transferred to `/setup/cacerts/firefox`
  - Chromium: Root certificates and intermediate certificates must be transferred to `/setup/cacerts/browser`
- The eLux taskbar should be enabled on the clients if published applications are provided as **seamless applications**. Seamless applications behave like local applications and users can only restore them from minimized window size by using the taskbar. For further information, see Advanced desktop settings.

9.3.1. StoreFront application

By using the application type **StoreFront**, users can connect to a Citrix StoreFront server. Virtual desktops and published applications are aggregated and provided through stores. The Citrix products mainly used are XenApp and Citrix XenDesktop. StoreFront sites can be accessed via HTTP or HTTPS.

The StoreFront application enables users to access Citrix resources of one or more stores together with other configured applications, such as **RDP** or **Browser** sessions by using only one interface – the eLux RP 6 User Interface. For further information, see eLux RP 6 User Interface.

Defining a StoreFront application

Note
HTTPS connections require the relevant SSL certificates on the device.

1. Add a new application and select the application type **StoreFront**.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Console
Use Provisioning File (.cr)[1]	Enter the Citrix store provisioning file name without the file name extension. The Provisioning file must be located on the client in the directory `/setup/ica/`. For further information, see StoreFront / Store provisioning file. This option excludes the specification of Store URLs (next option).
Stores	Specify the URL of one or more stores ▸ Click **Add** and replace the automatically created default value by your individual value (double-click or F2) Example: (`https://CtrXd76.sampletec-01.com/Citrix/Store33/discovery`) This option excludes the use of a Provisioning file (previous option).
Logon	The user is automatically logged on to the store by using the specified credentials (username, password, domain).

[1] for Scout 15.5 and later versions

Option	Description
Pass-through logon	The user is logged on to the store via single sign-on. The AD user credentials are used. If AD users log on via smart card, and if Citrix Receiver for Linux 13.4.x or later versions are used, the authentication method **Domain pass-through** on the Citrix server must be disabled.

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

For further information, see StoreFront / Authentication.

Show last user	The user credentials (except for password) of the last logon are displayed in the XenApp logon dialog. This option has no effect if you specify fix user credentials for automatic logon under **Logon**.
Autostart	Specify the names of those StoreFront applications you want to have started automatically. Make sure to spell the names exactly as in StoreFront. Separate multiple application names by semicolon. Example: `MyApp1;MyApp2` If only one resource is defined for a store, alternatively use the free parameter `AutostartUniqueResource=true`[1]
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters.

3. To delete an entry from the **Stores** list, select the entry and click **Delete**.
4. To configure further settings, click **Advanced** and edit the following fields:

Option	Description
Windows properties	Desktops can be launched in full-screen or window mode.

[1] for eLux RP 6.4 and later versions (Citrix Workspace app)

Option	Description
Timed logoff	To enable automatic logoff from the StoreFront server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last StoreFront application has been closed.
Application reconnection	Determine the actions to be done on a reconnect to the StoreFront server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.
Manual logoff	Determine the actions to be carried out upon logoff from the StoreFront server **Logoff only server**: Logoff is performed only from the StoreFront server **Logoff server and applications**: Logoff is performed from the StoreFront server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the StoreFront server but the virtual desktop session is only disconnected. This enables the user to reconnect later on.

Note
Access to the advanced settings can be defined via the object rights.[1]

5. Confirm with **Apply** and **OK**.

After users have logged on to a StoreFront server or Web Interface server, they can show all provided resources by double-clicking the **StoreFront** *icon on the eLux desktop.*

[1] for Scout 15.5 and later versions

9.3.2. Self-Service user interface

The Self-Service user interface (UI) replaces the configuration manager **wfcmgr** and allows access to Citrix services providing published ressources. After users are set up with an account, they can subscribe to desktops and applications, and then start them.

Defining Citrix Self-Service as local application

Note
The eLux package **Citrix Workspace app for Linux**[1] and the included feature package **Self-service** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

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

Option	Description
Name	Name for the application
Local application	Select `Custom`.
Parameter (manatory)	Enter the following program name to start the application: `selfservice`

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

Note
The `selfservice` application cannot be configured individually. To use configuration options, alternatively use the Self-Service UI with extensions (`ucselfservice`) for eLux RP 5 clients. For eLux RP 6.2 and later versions, you can use the see Citrix Self-Service UI in kiosk mode.

9.3.3. Browser session to access published resources

Users can access applications and desktops that have been published through a store on the Citrix StoreFront server or through Citrix Web Interface by using a local browser.

Defining a browser application to access published resources

Note
To provide the users with a browser application to be used directly on the client, the relevant software package for Firefox or Chromium must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

[1] formerly Citrix Receiver for Linux

Note
HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and select the application type **Browser**.
2. Edit the following fields:

Option	Description
Name	Name for the browser session
Browser type	Firefox or Chromium

Called page	URL of the Web Interface homepage or StoreFront store.
	Examples:
	`https://<Servername>/Citrix/StoreWeb`
	`https://<Servername>/Citrix/XenApp`

3. For the remaining parameters, see Defining a browser application.

The local user starts the browser and is forwarded to the defined page. After successful logon to the StoreFront server or Web Interface server, the published applications, desktops and contents available are shown in the browser window.

9.3.4. PNAgent application

An application of the type **PNAgent** (Program Neighborhood Agent) enables users to access published resources through a server running a XenApp Services site. Published resources can be published applications, published desktops, or published contents (files).

Customizable options for all users are defined in the configuration file `config.xml` which is stored on the Web Interface server (by default in the directory `//Inetpub/wwwroot/Citrix/PNAgent`). When a user starts one of the published programs, the application reads the configuration data from the server. The configuration file can be configured to update the settings and user interface regularly.

The `config.xml` file affects all connections defined by the XenApp Services site. For further information, see the Citrix eDocs on http://support.citrix.com.

Defining a PN Agent application

Note
HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and select the application type **PNAgent**.
2. Edit the following fields:

Option	Description
Name	Name of the application

Server	Specify the address of the configuration file on the Web Interface server (URL).
	If you use the default directory and port 80, the server address is sufficient.
	
	Examples:
	`https://CtrXd.sampletec-01.com/Citrix/PNAgent/config.xml`
	`https://192.168.10.11:81`

Login	The user is automatically logged on to the Web Interface server by using the specified credentials (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: Kerberos authentication is no longer supported with Citrix Receiver for Linux 13.x.and later versions.

Option	Description
Autostart application/folder	Specify the names of those applications you want to have started automatically. Alternatively, you can specify an autostart folder containing the relevant published applications. The folder must have already been created on the Web Interface server.
Show last user	The user credentials (except for password) of the last logon are displayed in the PNAgent logon dialog. This option has no effect if you specify fixed user credentials for automatic logon under **Logon**.
Allow cancel	Allows the user to close the PNAgent logon dialog.
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start Example: `PNATimeout=60` brings Citrix Workspace app[1] to try for 60 seconds to enumerate the published applications and desktops. To configure dual-monitor mode, you can also use the **Free parameters**, see below. For further information, see Defining free application parameters.

3. To configure further settings, click **Advanced** and edit the following fields:

Option	Description
Window properties	For resolution/window size, color depth and audio output, select **Use default** (server settings) or select one of the values from the list-field.
Timed logoff	To enable automatic logoff from the Web Interface server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last PNAgent application has been closed.

[1] formerly Citrix Receiver

Option	Description
Application reconnection	Determine the actions to be done on a reconnect to the Web Interface server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.
Manual logoff	Determine the actions to be carried out upon logoff from the Web Interface server **Logoff only server**: Logoff is performed only from the Web Interface server **Logoff server and applications**: Logoff is performed from the Web Interface server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the Web Interface server but the virtual desktop session is only disconnected. This enables users to reconnect later on.

Note
Access to the advanced settings can be defined via the object rights.[1]

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

Program Neighborhood variables

For example, variables can be used to define a unique client name for a Citrix XenApp session. To log on to a Web Interface server with Program Neighborhood, you can use the following variables:

`$ICAUSER`	Username
`$ICADOMAIN`	Domain for this user
`$ICAAPPLICATION`	Name of the PNAgent application definition

Creating a domain list

For PNAgent applications, you can create a domain list from which the user can select a domain.

[1] for Scout 15.5 and later versions

1. Create the text file `icadomains` without file name extension.
2. Enter the required domain names, one domain per line.
3. Save the file to the Scout installation directory.
4. Transfer the file to the `/Setup` directory on the Thin Client by using the Scout feature Files.

If some of the configuration data are missing when a PNAgent application is started, the missing data are requested by a Citrix Web Interface logon dialog. The defined domains are listed in a drop-down list.

Note
In the PNAgent application definition, you can predefine a specific domain.
Example: `work.sampletec-01.com`.

Settings for dual monitor mode

For PNAgent sessions, you can configure a dual-monitor mode by using one of the following methods. The Citrix session can be transferred to the first monitor, to the second monitor, or to both of them.

Method 1:

- Use the **Advanced file entries** feature of the Scout Console and modify the ICA software defaults:

File	`/setup/sessions.ini`
Section	`ICADefaults`
Entry	`Xinerama`
Value	`-1|0|1`

For further information, see Advanced file entries.

Method 2:

- In the Scout Console, in the application definition, set the following **Free parameters**:

```
Key=Xinerama
Value=-1|0|1
```

For further information, see Free parameters.

The values mean the following:

`-1`	both monitors
`0`	first monitor
`1`	second monitor

9.3.5. Citrix Connection Center

By means of the Citrix Connection Center, users can see all current server connections and can log off, disconnect or close them without operating the application. In addition, the connection transport statistics can be viewed which might be helpful for slowing connections.

The Connection Center is provided as a desktop application.[1]

Defining the Citrix Connection Center

Note
If you use **Citrix Receiver for Linux**, the eLux package **Citrix Receiver Extensions** and the included feature package **Connection Center** must be installed on the clients. If you use the later **Citrix Workspace app**, the included feature package **Utilities and tools** must be installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.

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

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

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

[1] formerly as a systray icon on the taskbar

9.4. 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.

9.4.1. Defining an RDP Windows desktop session

1. Add a new application and select the application type **RDP**.
2. Edit the following fields:

Option	Description
Name	Name for the RDP application
Server	IP address or name of the server
Application	Leave the field empty.
Working directory	Leave the field empty.
Logon	The user is automatically logged on to the server by using the specified credentials (username, password, domain).
Pass-through login	The user is logged on via single sign-on. The AD user credentials are used.

Free parameters	Allows to define any parameters supported by **eluxRDP** in the format:
	`FreeRDPParams=<Parameter> <Parameter> <Parameter>...`
	Separate multiple parameters by spaces.
	Examples:
	`FreeRDPParams=/microphone:sys:pulse +fonts /cert-ignore`
	To view the allowed parameters, enter the `eluxrdp` command in a shell.
	For further information, see Defining free application parameters.

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**.

9.4.2. Defining an RDP application

To configure an individual application via RPD, the Windows desktop definition requires additional data about the relevant application.

1. Add a new application and select the application type **RDP**.
2. Edit the following fields:

Option	Description
Name	Name for the RDP application
Server	IP address or name of the server

Application	Name of the Windows application including path name
	System variables are allowed.
	Examples:
	`c:\Program Files\Microsoft Office\Office\EXCEL.EXE`
	`%SystemRoot%\system32\notepad.exe`

Working directory (optional)	Working directory of the Windows application
Logon	The user is automatically logged on to the server by using the specified credentials (username, password, domain).
Pass-through logon	The user is logged on via single sign-on. The AD user credentials are used.

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

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

9.4.3. Advanced application settings / RDP and VMware

The settings described below apply to the following applications:

- RDP applications
- VMware applications

  If you select a protocol other than RDP, some options are not available.

Accessing advanced application settings

Note
Access to the advanced settings can be restricted via the object rights.[1]

- 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 `Full-screen`, select if you want to display on one specific or all monitors. Up to eight monitors are supported.[2]
Colors	Color depth for the session (8-32 Bit)

Note
If you use multiple monitors but wish to display content on only one of them, under **Device configuration>**[3] **> Desktop > Advanced > Windowmanager**, the **Maximize/fullscreen to single monitor** option must be selected.

Local Resources tab

Note
- for terminal servers supporting RDP protocol version 5.2 or later -
The settings take effect only if, on the **Advanced** tab, the value of the **Protocol** field is not set to `RDP V4`.

[1] for Scout 15.5 and later versions
[2] for Scout 15.0 and later versions
[3] formerly Setup

Option	Description

Drive mapping	Select drive, mount point and drive letter that you want to show in the RDP/VMware session.
	The mount points correspond to the local access paths of the resources and are provided by eLux.
	
	For USB devices the mount points are
	`/media/usbdisk`
	`/media/usbdisk0`
	and so on.
	For further information, see Mount points.

Connect printer	Up to four printer definitions can be created automatically for a session. The printers must be configured on the Printer tab in the eLux device configuration and have the correct driver name as defined on the server (case-sensitive!). The first four profiles can be used with drivers. To define a default printer, choose **Set as default** in the eLux printer configuration.
Sound	**Play local** reproduces the sound locally on the client. **Play remote** causes play-back on the remote server.
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)	Enables you to set the RDP protocol to version 4 or 5 Normally, the protocol is recognized automatically.
Keyboard language	Defines the keyboard layout within a session The default is **Auto** which corresponds to the keyboard setting of the eLux device configuration.

> **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. 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. By default, the option is disabled.

Show connection bar on full screen	Shows connection list in full-screen mode
Bandwidth	Choose between `standard`, `modem`, `broadband` or `LAN`.

9.4.4. Running RDP client from eLux command line

You can run the RDP client within a local shell on the client.

1. Start a local shell.
2. At the command prompt, enter the following command:
   `eluxrdp /v:<server>`

Note
To view the provided command line parameters, enter the command **eluxrdp** without parameters. You can use these parameters to define an RDP session as local application.

9.4.5. Configuring RemoteFX

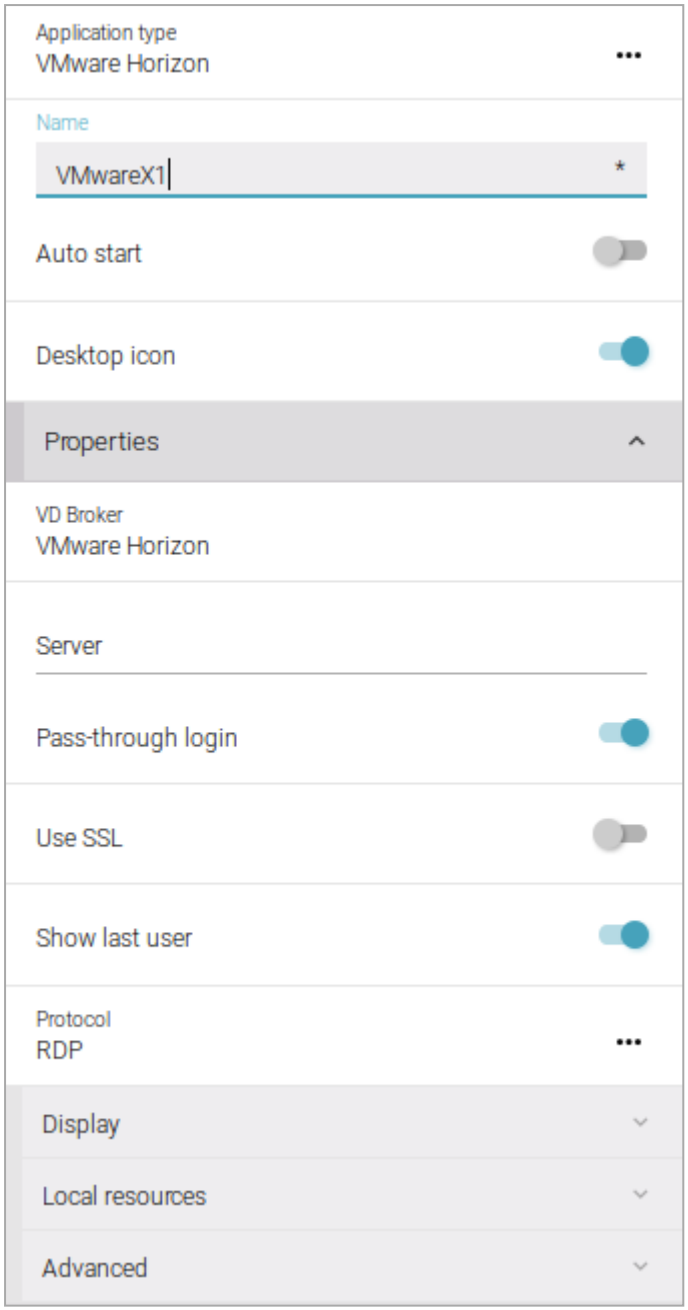
Microsoft RemoteFX™ offers comprehensive functionality for Virtual Desktop Infrastructure (VDI) by providing a virtual 3D adapter, intelligent codecs and the ability to redirect USB devices to virtual machines.

Note
RemoteFX only works if the server supports RemoteFX and is configured in the right way. The only parameter to be configured on the client is bandwidth.

1. For your **RDP** application, open the **Application properties** dialog and click **Advanced**.
2. On the **Advanced** tab, in the **Bandwidth** field, select `LAN`.
3. Confirm with **Apply** and **OK**.

9.5. VMware Horizon

Note
This application type is available only on the eLux RP 6 device. In the Scout Console, choose the `Virtual desktop` application type and, under **VD broker**, select `VMware View`.



Option	Description
Name	Name for the application
Auto-start	The application starts automatically after eLux has been started.
Desktop icon	Provides a desktop shortcut on your personal desktop
VD broker	VMware Horizon
Server	IP address or name of the server
Pass-through logon	The user is logged on via single sign-on. The AD user credentials are used.

Option	Description
Username, Password, Domain	The user is automatically logged on to the server by using the specified credentials.
Use SSL	Forces the connection via HTTPS Note that HTTPS connections require the relevant SSL certificates on the client.
Show last user	The user credentials (except for password) of the last logon are displayed in the logon dialog

Protocol	Choose between the following protocols:
	`RDP`
	`PCoIP`
	`VMware Blast`[1]

For information on **Display**, **Local resources** and **Advanced** settings, see Advanced application settings.

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

- With the help of VMware documentation,[2] create the file `view-userpreferences`. Transfer the file via the Scout feature Files configured for transfer to the clients to `/setup/elux/.vmware/view-userpreferences`

Note
The configuration on the Scout or eLux interface has precedence over the configuration file and will overwrite values of the configuration file.

[1] for Scout 15.2 and later versions
[2] Installation guide for VMware Horizon Client for Linux

9.6. Browser

Supported browsers are Mozilla Firefox and Google Chromium.

In addition, the Builtin Browser is available as a slimmed-down browser.[1] The Builtin Browser is based on the WebKit2 engine which is part of the **Desktop environment**[2] package. By default, the Builtin Browser is run without address and navigation bar. These and some more features can be configured for the kiosk mode.

Note
If you use Chromium, we recommend that you equip your Thin Clients with 2 GB of RAM.

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

9.6.1. Defining a browser application

1. Add a new application and select the application type **Browser**.
2. Edit the following fields:

Option	Description
Name	Name of the browser shown in the Scout Console
Browser type	Select `Firefox`, `Chromium` or `Builtin Browser`.[3]
Start page	Web page (URL) that opens when you click **Home**
Called page	Web page (URL) that opens after starting the browser
Proxy type	■ `No proxy`: No proxy server is used ■ `Manual (Proxy:Port)`: Specify a proxy server and port number ■ `Auto (URL)`: Use a proxy configuration file ■ `Use system proxy` (default):[4] 'System-wide' proxy setting defined in the device configuration under **Network > Advanced** per network profile Note that the setting behind `System proxy` can also be `No proxy`). For further information, see Proxy configuration.

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

[1] for Scout 15.4 / eLux RP 6.5 and later versions
[2] formerly MATE Desktop
[3] for Scout 15.4 / eLux RP 6.5 and later versions
[4] for Scout 15.5 and later versions

Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start see Defining free application parameters

3. To enable the **Kiosk** mode for Firefox, see Configuring kiosk mode.
4. Confirm with **Apply** and **OK**.

Note
By default, all browser files (cache, history, bookmarks, etc.) are saved temporarily to the flash memory but are deleted with each restart. We recommend that you configure the browser home directory on a network drive. For further information, see Browser home directory.

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

Preferences Chromium

Preferences Firefox

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 client:

Mozilla Firefox	`/setup/cacerts/firefox` for eLux RP 6.4 and earlier versions `/setup/cacerts/browser` for eLux RP 6.5/Firefox 60.5 and later versions[1]
Google Chromium	`/setup/cacerts/browser`

  For further information, see Files configured for transfer.

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

9.6.2. Kiosk mode for Firefox

- for Firefox up to version ESR 52.8 [2] and from version 71.0 -

[1] The certificates can be located in either directory.
[2] included in eLux RP 6.4

Note
For eLux RP 6.5 and later versions, you can use the Builtin Browser in kiosk mode. For further information, see Builtin Browser in kiosk mode.

The kiosk mode starts the browser in full-screen mode and with limited user rights. The user cannot open other windows and cannot exit the browser.

By default, the browser window is displayed without address bar and navigation buttons. So users are forced to stay on the predefined web page and cannot exit.

Kiosk mode is suitable if the users are supposed to see only one website and not use further applications on the Thin Client. For correct use of the kiosk mode, we recommend that you disable related functions of the Thin Client such as restarting the device and opening the control panel. For further information, see Device configuration > Security.

Configuring kiosk mode

Note
Firefox supports kiosk mode again starting with version 71.0, but without configuration options. With Scout 15 2110, the Firefox application definition is adapted and offers only the option **Enable kiosk mode**.

1. In the application properties of your browser application, click **Advanced**.
2. On the **Kiosk mode** tab, edit the following fields:

Option	Description
Enable kiosk mode	Activates the kiosk mode
Display navigation bar[1]	Allows using browser tabs despite kiosk mode Users can view multiple web pages of the defined web site concurrently
Add print button[2]	Allows using browser tabs and provides a **Print** feature despite kiosk mode
Add address bar[3]	Allows using browser tabs and provides the address bar including navigation buttons despite kiosk mode

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

On the next restart, the Firefox browser opens in kiosk mode.

[1] up to Scout 15 2107
[2] up to Scout 15 2107
[3] up to Scout 15 2107

9.7. 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.

9.7.1. Defining predefined local applications

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

Option	Description
Name	Name of the application shown in the Scout Console
Local application	In the list-field, select a predefined application.
Parameter (optional)	Command-line parameters for application start
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start see Defining free application parameters.

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

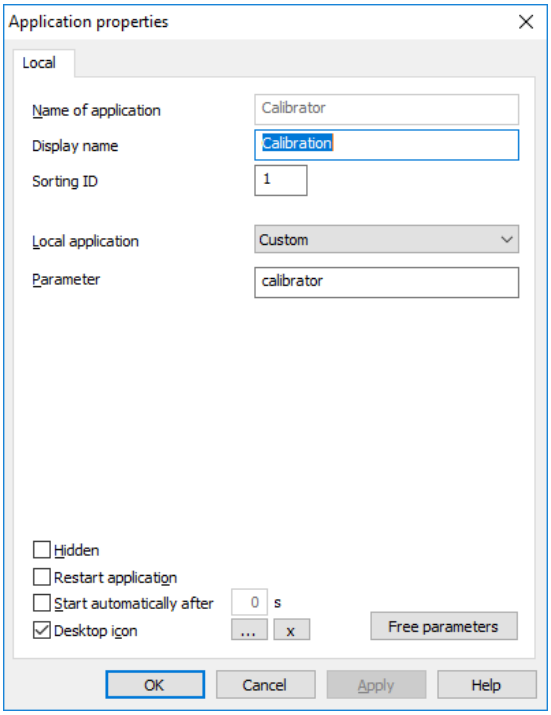
9.7.2. Defining custom applications

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

Option	Description
Name	Name of the application shown in the Scout Console
Local application	Select `Custom`.

Option	Description
Parameter (mandatory)	Enter the program name required to start the application. If required, add start parameters. Example: `calibrator` calls the **Calibrator** tool `squid` calls the **Squid** application `squid /tmp/mycache` calls **Squid** using the specified cache directory
Hidden	The application is not shown on the **Application** tab of the client control panel. The option **Start automatically** or **Application restart** must be active.
Application restart Start automatically Desktop icon	See Adding applications.
Free parameters (optional)	Individual parameters for application start see Defining free application parameters

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



The figure shows the application definition for the calibration tool **Calibrator**. After the next client restart, the **Calibration** application is provided on the client and can be started via the control panel, start menu, or desktop icon (provided that the **Calibrator** tool is included in the image).

9.7.3. Defining Ekiga SIP Softphone

Ekiga is a free software application for audio and video telephony (VoIP) that supports the SIP protocol. Configuration is based on a SIP account.

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

Option	Description
Name	Name for the application
Application	`Custom`
Parameter	`ekiga`

3. Click **Free parameters** and then **Add** to define the following free parameters:

Variable	Value
account	*<Name of the SIP account>*
server	*<server URL>*
user	*<SIP username>*
password	<password>
outbound_proxy	*<proxy URL >*

   Example: `password=424242`
   For further information, see Using free application parameters.
4. In the **Free application parameters** dialog, right-click the variable name `password` and click **Encrypt**.
5. Confirm with **Apply** and **OK**.

9.7.4. Defining Zoom for Linux

The native Zoom client for Linux is a Video Conferencing and Web Conferencing service and offers high-quality video, audio, and screen-sharing experience.

The video and audio devices are configured via the application interface.

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

Option	Description
Name	Name for the application
Application	`Custom`
Parameter	`zoom`

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

10. eLux commands

Die following eLux commands are provided to the user depending on the configured user rights.

- Open the Command panel and click the relevant command.

10.1. Updating the firmware

You can check anytime if the current software status of a Thin Client does match with the available IDF on the server and, if required, initiate a firmware update on-demand.

1. Check if the firmware settings of the device configuration are configured correctly. For further information, see Configuring firmware update.
2. Show the Command panel of the System bar.
3. Click the **Update** button.

   The client firmware is compared to the specified IDF on the web server. A message will inform you, if the IDF on the web server contains updated packages and hence requires a firmware update.

   Note
   Before starting the update, click **Details** to view the components that require an update.

4. To perform the firmware update, click **Yes**.

The firmware update is performed and the client is restarted.

10.2. Synchronizing configuration

After having modified the device configuration or application definitions locally on the client, you can reset the configuration data to the server-side defined settings anytime.

1. Show the Command panel of the System bar, and then, click the **Configuration** button.
2. Confirm with **Yes**.

The current device configuration and application definitions for the device or OU are loaded from the Scout Server and are available on the client on the next restart. Local configuration settings are overridden, unless they are protected.

10.3. Resetting a client to factory status

> **Important** A factory reset causes the system to reset local configuration data.

Resetting a client to factory status can be useful for troubleshooting, for example, if the locally defined device configuration does not work correctly.

1. Show the Command panel of the System bar, and then, click the **Factory reset** button.
2. Confirm with **Yes**.

The device configuration of the client firmware is set back to the factory status,[1] local application definitions and locally stored configuration data are deleted.

The following data are retained:

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

On the next restart, the client acts like a device in initial operation and can be connected to a Scout Server via the following methods:

- DNS alias `ScoutSrv`
- DHCP options 222 and 223
- Local First Configuration Wizard on the client
- Searching for the device by using the **Discovery** feature of the Scout Console

10.4. eLux Command Scheduler

The eLux Command Scheduler can schedule and execute recurring time-based commands. In contrast to the Scout commands initiated on the server side, the commands are executed according to the local time zone of the devices.

Commands to be scheduled must first be defined through an `.ini` file by the administrator. For further information, see eLux Command Scheduler in the **Scout** guide.

[1] From Scout 15.7 and eLux RP 6.7, local user configuration data in unlocked fields can be configured by the Scout administrator to be retained.

11. Troubleshooting

11.1. Troubleshooting locally on the device

Problem	Reason	Solution
After changes in the **Configuration panel** in **Security > User authentication**, you are locked out by the system.	The user authentication has been enabled by using incorrect values.	Log on locally by using the `LocalLogin` account with the device password (default:`eLux`). You will be provided with full access rights and can modify the relevant settings.
Local configuration changes are required but the user rights are restricted.	-	The administrator can unlock the **Configuration panel** locally: Press the key combination STRG+ALT+POS1 and enter the device password.
After configuration changes, the screen does not work correctly.	The combination of resolution, frequency and color depth defined is not supported by your monitor.	1. Switch off the device. Have the device password ready. 2. Restart, and after the BIOS has been run through, press and hold the ESC key. 3. Select the **Factory reset** option to bring the device back to initial state.

Printing problems	Reason	Solution
PostScript-file – PostScript printer (Filter = `None`)	Some local applications generate PostScript output. To check the file format, in the **Print** dialog, select **Print to file**, save to a network drive or the local `tmp` directory and open the `.prn` file. If the first line starts with `%!`, the file is PostScript.	To print PostScript files with PostScript printers, set the filter to `None`. If your printer prints a lot of ASCII text, use `PCL format`.
PostScript-file – PCL printer (filter should be set to `PCL2`)	To show this filter option, the **Print Environment** package with FPM **Filter** must be installed on the client.	Install the required package and set the filter to `PCL2`.
Does the printing problem affect just one device?		Try printing to other printers and accessing the network. If the connection works fine, check if the print job reaches the printer (most printers have a status line). If it does, the problem is most likely the file format (see above).
Communication problem		If the printer has an IP address, try to communicate with the printer via a local shell on protocol level. If communication is not successful and multiple clients are concerned, you might have a network problem.
Performance problem	The Thin Client stores printer data temporarily in the main memory. The memory size may not be adequate compared to the print file, and delays may occur if the printer is not ready. Graphics and color enlarge the file, PostScript files are often much larger than the original file is.	Provide the device with more main memory.

11.2. Troubleshooting application definition

Error / problem	Reason	Solution
Missing firmware	The required software is not installed on the Thin Client	Install the software on the Thin Client. For further information, see Creating an IDF in the ELIAS guide and Firmware update.
Doubled names	Two applications have the same name. This causes conflicts because applications are identified by their names.	Use unique names.
Hidden application cannot be executed	Applications are invisible for the user when they run in hidden mode. This option is available for applications of the **custom** type.	Enable the option **Start automatically** or **Application restart** to start hidden applications on start or to run them non-stop, respectively.
Problems with certificates in combination with VMware server	Server problem occurred: After successful installation, the VMware server uses a self-signed certificate. If a Thin Client is configured correctly, it will not accept. The reason is that the **FQDN** (fully qualified domain name) is mandatory for server certificates.	Create a server certificate in the **Windows-CA** with **FQDN**. If you use **mmc**: Create a server certificate using the Snap-In **Certificates (Local computer)**. The key must be exportable. The display name of the server must be **vdm**. The name must be unique in the certificate store **Local computer / Personal**.

Error / problem	Reason	Solution
COM port redirection in RDP session does not work	Communication errors such as high latencies in the network between your serial device and the virtual desktop do not allow serial communication.	Use the **permissive** mode for the RDP application. This parameter causes communication errors to be downgraded to warnings, and communication becomes more tolerant of timeouts. Define a free parameter in your RDP application definition with the **permissive** option. Example: `FreeRDPParams=/serial:COM1,/dev/ttyS0,Serial,permissive` For further information, see Defining free application parameters.

11.3. Troubleshooting device configuration

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

Error / problem	Reason	Solution
When you use **USB multimedia devices** such as headsets or web-cams, the screen freezes or the window cannot be focused.	The USB operating elements register themselves as keyboard or mouse devices in the system.	Prevent the registration as input devices by defining a `terminal.ini` entry. The basic functionality of the operating elements is not affected. For further information, see Preventing registration of USB multimedia components.
Multimedia USB devices, connected via **DisplayPort to eLux RP 5 devices with an AMD processor**, do not play back sound.	Sound reproduction via DisplayPort is disabled.	Enable sound reproduction by defining a `terminal.ini` entry. To do so, use the Scout feature Advanced file entries: File: `/setup/terminal.ini` Section: `Screen` Entry: `Radeon.Audio` Value: `true` Alternatively, use a separate audio cable.

Error / problem	Reason	Solution
Monitor via DisplayPort with AMD GPU: After changing to lower resolution the monitor brings an **Out of range** error message.	The resolution on this monitor interferes with the configured sound reproduction via DisplayPort.	Disable sound reproduction via DisplayPort. This will fix the monitor error. To do so, use the Scout feature Advanced file entries: File `/setup/terminal.ini` Section `Screen` Entry `Radeon.Audio` Value `false`
When you use a **touch screen**, the location of a fingertip touch is not recognized precisely.	The monitor has not been calibrated precisely enough.	To calibrate the monitor, configure a custom application by using the parameter `calibrator`. Then start the application.
Only eLux RP 5.7.x: In **dual monitor mode**, if the second monitor is configured to **vertical**, the desktop icons are not displayed (correctly).	For some resolutions, the desktop icons on the primary monitor cannot be displayed when the second monitor is vertically aligned and the lower screen area is referenced.	For eLux RP 5.7.3000 and later versions: Use a new parameter to configure the vertical alignment to the upper screen area (`top`). To do so, use the Scout feature Advanced file entries: File `/setup/terminal.ini` Section `Screen` Entry `VerticalAlignment` Value `top` The default value is `bottom`.

Error / problem	Reason	Solution
Display/general **graphics issues**	The feature package for hardware acceleration **HwVideoAccDrivers** is not installed.	Activate the **HwVideoAccDrivers** FPM within the **XOrg** package in the IDF.

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

AD logon to eLux RP 6.x does not work.	Port 389 is configured for the authentication server.	Do not define a particular port for the authentication server.

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

12. Appendix

12.1. eLux partitions

A thin client's flash memory is generally divided into three or four partitions when eLux is installed. Each partition is reserved for a dedicated purpose and is only touched when you perform special tasks that are related to this partition.

All partitions are created during a recovery installation.

Partition	Requires	Purpose	Recreated with	Other
System		Reserved for the firmware (software packages)	Scout **Update** command with option **Format system partition before update**	Size for eLux RP 6 2104 LTSR and earlier versions: 1,77 GB / 1,84 GB with/without encryption Size for eLux RP 6 2107 and later versions: 2,35 GB / 2.41 GB with/without encryption
Boot	only UEFI and USB	Boot section	-	
Setup		Device configuration Local application definitions	Factory reset command	Does not affect the system partition with installed firmware
Update	4 GB flash memory	Software delivery in advance (before firmware update) via Scout command or notification Signature check for eLux software packages Devices with update partition can be used as Dynamic Proxy (Provider) for firmware updates.	Scout **Delivery** command with option **Format update partition before delivery**	The size of the update partition complies with the storage space provided. The update partition is no larger than the storage space provided. Devices with less than 4 GB flash memory are not provided with an Update partition.

Note
In the Scout Console, in the Properties window of a device, the system, setup and update partitions are listed including their sizes.

Extended system partition starting with eLux RP 6 2107

When you perform an update installation or a new installation (recovery) to eLux RP 6 2107 or later, the system partition is created with 2,35 GB / 2.41 GB (with/without encryption) instead of the previous almost 2.0 GB. This creates more space for the firmware and allows larger images to be used.

- **Update installation**

  An update installation (firmware update) is still based on the previous partition sizes. The image size is thus still limited to the earlier values. Afterwards, the extended system partition is available and you can install images that may be up to 2.35 GB / 2.41 GB in size. This means, to install larger images on the freshly resized partition of the devices, a second firmware update is required.

- **Recovery installation**

  Provided an up-to-date recovery system is available, with a PXE or USB recovery installation the system partition can be partitioned to the new size directly during the installation process and a larger image with up to 2.35 GB / 2.41 GB can be written in the same process. A new installation or recovery installation thus allows the partition to be resized and used in one step.

Downgrade

> Important To downgrade devices with the extended system partition (eLux RP 6 2107 or later) to an earlier version that only supports the previous system partition with less than 2 GB, you will have to go back to eLux RP 6 2104 LTSR.

We therefore recommend that you update test devices to eLux RP 6 2107 or later as the first step to thoroughly test functionality.

12.2. IP ports

eLux / required ports

Port	Type	Description	How to deactivate	In/Out
	ICMP	**ping** must be supported to verify the status of the eLux devices		In/Out
80	TCP	Firmware update by using HTTP (and proxy port, if used)		Outgoing
443	TCP	Firmware update via HTTPS/TLS		Outgoing

Port	Type	Description	How to deactivate	In/Out
5900	TCP	Mirroring eLux desktop	In **Config**[1] **> Security**, 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) [2]		In/Out
22129	TCP	VPN		Outgoing

eLux / optional ports

Port	Type	Description	How to deactivate	In/Out
	ESP	VPN (data transfer)	Uninstall package `VPN System`	In/Out
21	TCP	Update via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	5250 emulations and telnet sessions		Outgoing
53	TCP, UDP	DNS server		Outgoing
67	UDP	DHCP server	Configure a local IP address (**Config > Network**)	Outgoing
68	UDP	DHCP client (or: BootP client)	Configure a local IP address (**Config > Network**)	Incoming
69	UDP	TFTP server (only used during PXE recovery)		Outgoing
88	TCP, UDP	AD authentication (Kerberos)		Outgoing

[1] Device configuration, formerly Setup
[2] for Scout 15.1 / eLux RP 6.1 and later versions

Port	Type	Description	How to deactivate	In/Out
111	TCP, UDP	TCP port mapper - RPC internal use only Works with lockd (random) UDP port mapper - drive access on NFS servers Works with NFSD drive access (port 2049) and mountd (random)	Uninstall `Network Drive Share` package	In/Out
123	UDP	Windows Time server (NTP)	Do not configure a time server (**Config > Desktop**)	In/Out
139	TCP, UDP	SMB drive mapping, (NetBIOS) and SMB user authentication (CIFS)	Uninstall `Network Drive Share` package and `User authentication modules` package	Outgoing
161	UDP	SNMP	Uninstall `SNMP Environment` package	In/Out
162	UDP	SNMPTRAP	Uninstall `SNMP Environment` package	Outgoing
177	UDP	XCMCP protocol		Outgoing
389	TCP	AD authentication with user variables		Outgoing
443	TCP	VPN (connecting) via HTTPS/TLS	Uninstall package `VPN System`	In/Out
464	TCP, UDP	AD authentication (Kerberos) / Set password		Outgoing
514	TCP	Shell, X11 applications		Outgoing
515	TCP	Printing via LPD	Uninstall package `Print environment (CUPS)`	In/Out
631	TCP, UDP	CUPS (IPP) print client	Uninstall package `Print environment (CUPS)`	Outgoing
636	TCP	LDAPS authentication with user variables		Outgoing
2049	UDP	NFSD drive access NFS	Uninstall FPM `NFS Support` in `Network Drive Share` package	Outgoing

Port	Type	Description	How to deactivate	In/Out
6000	TCP	Remote X11 application	In **Config > Security**, clear **Allow remote X11 clients** option	Incoming
7100	TCP	Font server can be assigned in (**Config > Screen > Advanced**		Outgoing
8080	TCP	Firmware update via Dynamic proxy (Provider and Consumer)	Set **Config > Firmware > Proxy-Typ** to `None`	In/Out
9100	TCP	Printing directly to parallel port can be assigned in (**Config > Printer**)	In **Config > Printer**, clear **TCP direct print** option	Incoming
9101	TCP	Printing directly to USB port can be assigned in (**Config > Printer**)	In **Config > Printer**, clear **TCP direct print** option	Outgoing
20000	UDP	Wake On LAN		In/Out
22124	TCP	Scout Statistics		Outgoing

Scout Server

Port	Type	Description	In/Out
	ICMP	**ping** must be supported to verify the status of the eLux devices	In/Out
1433	TCP	MS SQL Server	Outgoing
1434	UDP	MS SQL Server (Browser service)	In/Out
22123	TCP	Clients (Scout Manager / secure)	In/Out
22124	TCP	Scout Statistics	Incoming
22125	TCP	Clients (Scout Manager / TLS 1.2) [1]	In/Out

Scout Console

Port	Type	Description	How to deactivate	In/Out
1433	TCP	MS SQL Server		Outgoing

[1] for Scout 15.1 / eLux RP 6.1 and later versions

Port	Type	Description	How to deactivate	In/Out
1434	UDP	MS SQL Server (Browser service)		Outgoing
5900	TCP	Mirroring the eLux desktop	In **Config > Security**, disable mirroring or uninstall `VNC server` in `X.Org` package	Outgoing

Scout Dashboard

Scout Dashboard can be installed with HTTP or HTTPS.

Port	Typ	Description	How to deactivate	In/Out
80	TCP	Dashboard service / web server via HTTP		Incoming
443	TCP	Dashboard service / web server via HTTPS/TLS		Incoming
5901	TCP	Mirroring the eLux desktop	In **Config > Security**, disable mirroring or uninstall `VNC server` in `X.Org` package	Outgoing

Scout Cloud Gateway

Port	Typ	Description	In/Out
22125	TCP	Scout Server (Scout Manager / TLS 1.2)	In/Out
22129	TCP	VPN	Incoming

12.3. SNMP

SNMP (Simple Network Management Protocol) is a network protocol for monitoring and controlling network devices.

For eLux RP 5 and eLux RP 6, version SNMPv3 is used.

Note
The command line program **snmpget** is not included in the software package. To query SNMP status information, please use third party software.

12.3.1. Configuring SNMP

1. From our portal **www.myelux.com**, under **eLux Software Packages**, for your eLux version, under **Add-On**, download the package **SNMP Environment** and deploy it to the clients.
2. If there is no `/setup/snmp/snmpd.conf` on the clients, transfer the configuration file `snmpd.conf` to the clients to `/setup/snmp/snmpd.conf` by using the Scout feature Files.

   Or:

   Modify the `terminal.ini` file by using the Advanced file entries feature of Scout. Example:

File	`/setup/terminal.ini`
Section	`SNMPD`
Entry	`rocommunity`
Value	`secret`

3. Optionally, to define further SNMPD Configuration Directives, use the Advanced file entries feature and modify the `terminal.ini` file under `SNMPD`. Examples:

   ```
   syscontact=contact@sampletec.com
   syslocation=testcenter
   doDebugging=1
   ```

   For further information on SNMPD Configuration Directives, see http://www.net-snmp.org.

The section `SNMPD` of the `terminal.ini` file is evaluated by the client and the file `/setup/snmp/snmpd.local.conf` is created. An existing `/setup/snmp/snmpd.conf` will be overwritten.

If the configuration file does not exist, the file `/setup/snmp/snmpd.local.conf` is created with default values.

Notes on configuring SNMP v3

- When you define users (**createUser**), set a password with at least 8 characters.
- For the authentication method, define `authPriv` or `authNoPriv`.

Note
For SNMP v2, you can use `noAuthNoPriv` as the authentication method.

12.3.2. SNMPD and SNMP Configuration Directives

The following table refers to the software package **snmp-5.6.1.1-2** for eLux.
For further information on using SNMP with eLux, see SNMP.

For further information on SNMP commands, see http://www.net-snmp.org.

Application	Command
authtrapenable	1 | 2 (1 = enable, 2 = disable)
trapsink	host [community] [port]
trap2sink	host [community] [port]
informsink	host [community] [port]
trapsess	[snmpcmdargs] host
trapcommunity	community-string
agentuser	agentuser
agentgroup	groupid
agentaddress	SNMP bind address
syslocation	location
syscontact	contact-name
sysservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1|v2c|usm security
access	name context model level prefx read write notify
view	name type subtree [mask]
rwcommunity	community [default|hostname|network/bits] [oid]
rocommunity	community [default|hostname|network/bits] [oid]
rwuser	user [noauth|auth|priv] [oid]
rouser	user [noauth|auth|priv] [oid]
swap	min-avail
proc	process-name [max-num] [min-num]
procfix	process-name program [arguments...]
pass	miboid command

Application	Command
pass_persist	miboid program
disk	path [minspace | minpercent%]
load	max1 [max5] [max15]
exec	[miboid] name program arguments
sh	[miboid] name program-or-script arguments
execfix	exec-or-sh-name program [arguments...]
file	file [maxsize]
dlmod	module-name module-path
proxy	[snmpcmd args] host oid [remoteoid]
createUser	username (MD5|SHA) passphrase [DES] [passphrase]
master	pecify 'agentx' for AgentX support
engineID	string
engineIDType	num
engineIDNic	string

SNMP Configuration Directives

Application	Command
doDebugging	(1|0)
debugTokens	token[,token...]
logTimestamp	(1|yes|true|0|no|false)
mibdirs	[mib-dirs|+mib-dirs]
mibs	[mib-tokens|+mib-tokens]
mibfile	mibfile-to-read
showMibErrors	(1|yes|true|0|no|false)
strictCommentTerm	(1|yes|true|0|no|false)
mibAllowUnderline	(1|yes|true|0|no|false)
mibWarningLevel	integerValue
mibReplaceWithLatest	(1|yes|true|0|no|false)
printNumericEnums	1|yes|true|0|no|false)
printNumericOids	1|yes|true|0|no|false)
escapeQuotes	(1|yes|true|0|no|false)

Application	Command
dontBreakdownOids	(1|yes|true|0|no|false)
quickPrinting	(1|yes|true|0|no|false)
numericTimeticks	(1|yes|true|0|no|false)
suffixPrinting	integerValue
extendedIndex	(1|yes|true|0|no|false)
printHexText	(1|yes|true|0|no|false)
dumpPacket	(1|yes|true|0|no|false)
reverseEncodeBER	(1|yes|true|0|no|false)
defaultPort	integerValue
defCommunity	string
noTokenWarnings	(1|yes|true|0|no|false)
noRangeCheck	(1|yes|true|0|no|false)
defSecurityName	string
defContext	string
defPassphrase	string
defAuthPassphrase	string
defPrivPassphrase	string
defVersion	1|2c|3
defAuthType	MD5|SHA
defPrivType	DES (currently the only possible value)
defSecurityLevel	noAuthNoPriv|authNoPriv|authPriv