unicon
SOFTWARE

eLux RT

Administrator´s Guide

Last edited: 2017-02-10

0. Legal information 3
1. Representation 4
2. Overview 5
   2.1. About the eLux RT guide 5
   2.2. Keyboard shortcuts 5
3. Installation 6
   3.1. First boot procedure 6
   3.2. First configuration 6
   3.3. Device password 7
   3.4. Self-administration on the client 7
4. Interface 8
   4.1. Task bar, start menu and systray 8
   4.2. Removing USB mass storage devices securely 9
   4.3. Control panel 10
5. Setup 12
   5.1. General tab 12
   5.2. Network tab 13
   5.3. Desktop 16
   5.4. Screen tab 19
   5.5. Mouse/Keyboard tab 19
   5.6. Firmware tab 21
   5.7. Security tab 25
   5.8. Multimedia 29

5.9. Drives tab 30
5.10. Hardware 31
5.11. Diagnostics tab 32
6. Defining applications 35
6.1. General 35
6.2. Connecting to a Citrix farm 36
6.3. Browser 53
6.4. Emulation 54
6.5. Local and user-defined applications 58
6.6. PNAgent application 60
6.7. Virtual Desktop 64
7. Applications 66
7.1. Starting an application 66
7.2. Disconnecting an application 66
8. Troubleshooting 67
9.1. Troubleshooting application definition 68
9.2. Troubleshooting device configuration 69
10. Appendix 73

0. Legal information

Information in this document is subject to change without notice. We disclaim all liability regarding correctness, completeness and topicality of the information contained herein and any errors or damage resulting from the information provided.

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

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

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

1. Representation

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

Representation	Description
Control element	All graphical user interface controls are displayed in **bold**
Menu > menu command	Whenever running a command involves clicking a series of menus, the single GUI controls such as menu commands or dialog tabs are linked by **>**.
`Value`	All data that have to be entered by the user or data that represent a field value are displayed in `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 (component of Scout Enterprise)
EPM	eLux package module (`.epm`, software package)
FPM	Feature package module (`.fpm`, part of a software package)
FQDN	Fully qualified domain name
GB	Gigabyte
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

2.1. About the eLux RT guide

eLux® RT is an operating system designed for clients based on the energy-efficient ARM architecture. This guide supports the system administrator in installation, maintenance and operation of devices running eLux RT, hereafter referred to as "eLux".

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 RT clients can be managed by Scout Enterprise Management Suite version 13.1 and later.

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

2.2. Keyboard shortcuts

Shortcut	Function
CTRL+ALT+↓	Switch between applications in use to the left.
CTRL+ALT+↑	Switch between applications in use to the right.
CTRL+ALT+←	Switch between different desktops to the left
CTRL+ALT+→	Switch between different desktops to the right.
CTRL+WIN	Open the start menu
WIN+ALT+I	Open the device information
CTRL+ALT+HOME	Unlock client configuration. Requests the local device password.
CTRL+ALT+END	Lock the client screen. If access authorization is active, the user password is required for unlocking.
CTRL+ALT+FUNCTION KEY	Switch between the consoles, if the **Switch consoles** option is active. For further information, see Advanced mouse and keyboard settings. The following consoles are available: F1: eLux desktop F4: message shell
ALT+CHARACTER KEY	In the control panel: Switch to the tab with the underlined character ALT+S opens the **Setup** tab.

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 Live Stick** image, available for download on our portal www.myelux.com and suited to create a live stick.
- 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 guides **eLux Live Stick** and **eLux Recovery procedures**.

3.1. 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 Enterprise Server, either DHCP or DNS must be configured for that. For further information, see Self-registration of devices in the **Scout Enterprise** guide.

c. Start the eLux operating system

If either DHCP or DNS has been configured for the Scout Enterprise server, the device is automatically entered in Scout Enterprise and receives a new configuration.

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

3.2. First configuration

During the first boot procedure, a wizard is launched supporting the first configuration process. You can choose to integrate the device into the management through the Scout Enterprise Console or to configure eLux manually, which means directly on the Thin Client.

If the client, during start-up, has received the IP address of a Scout Enterprise Server, the IP address is shown in the top section. Otherwise a default value is shown.

Going through the first configuration and connecting to Scout Enterprise

1. Select the keyboard language.
2. To manage the device via Scout Enterprise, click **Yes**.
3. Enter the IP address or the name of the Scout Enterprise Server.
   Optionally, enter further information.
4. Select the destination OU for the device in the Scout Enterprise Console.
5. Confirm with **Finish**.

The device is registered on the Scout Enterprise Server, added to the destination OU, and is restarted. The client contacts the Scout Enterprise Server and downloads the configuration and application definitions of the destination OU.

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

For further information on managing devices with Scout Enterprise, see the **Scout Enterprise** guide.

3.3. Device password

All Thin Clients managed by a Scout Enterprise 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 configuration.

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

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

3.4. Self-administration on the client

With administrator rights, you can change the configuration locally on the client or can completely disconnect from the management system. To prevent abuse, we recommend changing the device password and not releasing it.

Logging on with full access on the client

1. Press CTRL+ALT+HOME.
2. Enter the device password.

You are provided with full access rights on the client.

4. Interface

The eLux RT interface consists of the following elements:

1. Desktop
2. Taskbar
3. Start menu
4. Systray

4.1. Task bar, start menu and systray

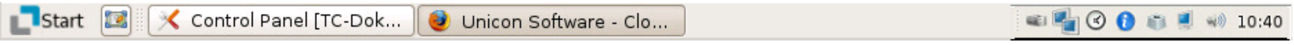
The task bar contains the following elements:

- Start menu
- Button to hide/show open applications (tasks) on the desktop

eLux RP 5 and eLux RT	
eLux RP 6	

- Active applications (tasks)
- Systray

The following figure shows the task bar of eLux RP 5:



You can configure how to display the task bar and systray in **Setup > Desktop > Advanced**.

The systray can show the following icons which provide access to configuration:

Icon	Description
Connected USB mass storage devices	Shows connected USB devices and their properties Removing USB devices safely
Network profile	Shows the network connections in use with status and options to Disconnect/Connect Definition in **Setup > Network**
Time settings	as in **Setup > Desktop > Date & Time**

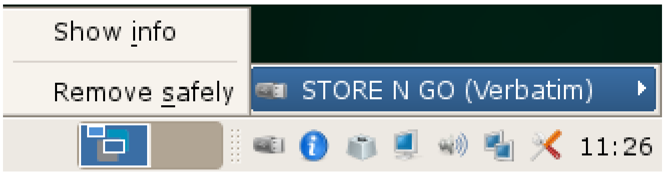
Icon	Description
Device information	Shows asset details as in **Setup > General** You can use the text boxes **Info1**, **Info2,**, **Info3** for additional information (and transfer them to the console if the **Client info** option in the software package `Desktop Tools` is active).
Mouse/Keyboard	as in **Setup > Mouse/Keyboard** Modifications become active immediately.
Screen settings	Connected screens are identified automatically. Any modifications are applied immediately. The **Info** tab shows all available screen resolutions supported by the monitor and further information. Use the **Resolution** tab to configure screen resolution and rotation. To disconnect one of the monitors, clear the **On** option. Use the **Layout** tab to configure multiple monitors and determine the the primary monitor (the one that shows the task bar).
Volume	Shows the active input and output devices You can control the sound level for input and output by using the slider bars as in **Setup > Multimedia**.
Time	Shows current time and current date

4.2. Removing USB mass storage devices securely

Important

To ensure that all data are saved on the USB device, remove any USB mass storage devices only after having clicked **Remove safely**.

1. On the systray, right-click the **USB device** icon.
2. Select **Remove safely**.



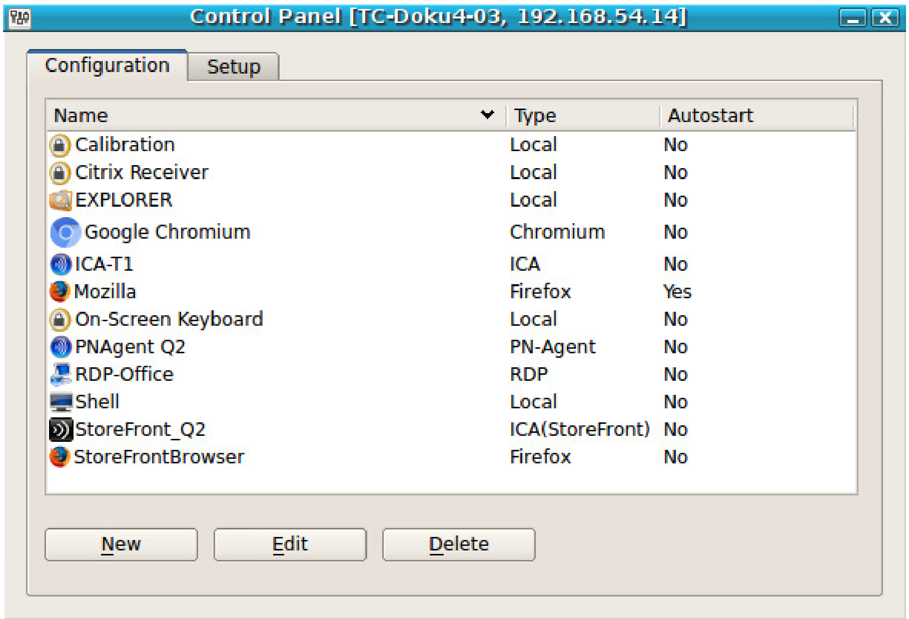
Note

In the Scout Enterprise Console, you can define a key combination that the users can press to remove all connected USB mass storage devices safely. For further information, see Key combination for safe removal of USB devices.

4.3. Control panel

The control panel provides the defined applications with their configuration (**Configuration** tab) and the device configuration (**Setup** tab). [1]

Depending on the defined user rights, the tabs or sub-tabs can be disabled.



Name	Type	Autostart
Calibration	Local	No
Citrix Receiver	Local	No
EXPLORER	Local	No
Google Chromium	Chromium	No
ICA-T1	ICA	No
Mozilla	Firefox	Yes
On-Screen Keyboard	Local	No
PNAgent Q2	PN-Agent	No
RDP-Office	RDP	No
Shell	Local	No
StoreFront_Q2	ICA(StoreFront)	No
StoreFrontBrowser	Firefox	No

Operation

- To open the control panel, use the Start menu (eLux RP 5) or the desktop icon Control Panel (eLux RP 6).

The eLux control panel is designed for mouse operation. However, you can operate the desktop by using key combinations such as (`ALT + underlined letter`). For example, on the **Setup** tab, press ALT+ S to jump to the **Screen** tab.

The control panel can be closed by pressing ESC.

Application definition

With the appropriate user rights, you can define, edit or delete applications on the **Configuration** tab. If the device is managed by Scout Enterprise, the applications are defined in the Scout Enterprise Console. In addition to the application definition, the corresponding software packages must be installed in order to run an application.

[1] For eLux RP 5.x clients, the **Applications** tab is additionally provided that you can use to start applications from.

Device configuration

The **Setup** tab contains the device configuration. In initial state, some standard configuration is active. If the device is managed by Scout Enterprise, the device configuration is verified on each restart and might be updated to the status of the assigned OU.

The standard desktop language is English (US). For any other languages except German the desktop elements are shown in English. It is however important to select the relevant language in the desktop configuration to ensure that the local applications can be run correctly.

5. Setup

Local configuration of the client is done in the control panel on the **Setup** tab.

Important

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

The **Setup** tab contains the following sub-tabs:

Note

Most changes require a client restart. eLux will inform you after you have confirmed your changes by clicking **Apply**.

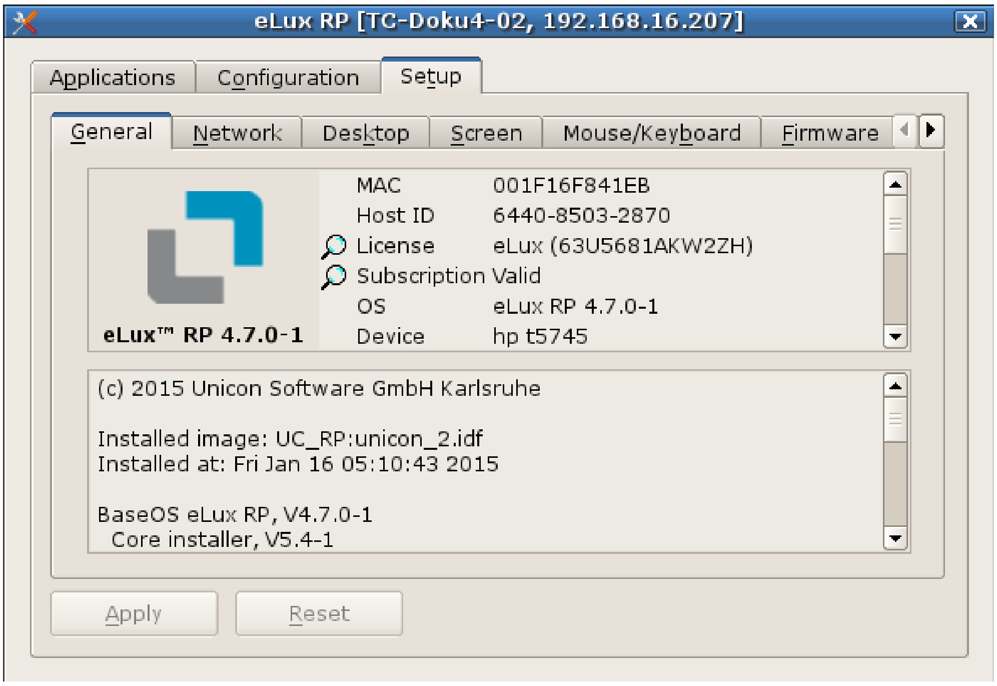
5.1. General tab

The **General** tab provides the following information:

- MAC address
- host id of the terminal
- eLux license[1] and Subscription
- eLux version
- information concerning the hardware in use for example CPU-clock, size of RAM, serial number and BIOS version.

The list below shows the installed software packages including version numbers and the installed IDF.

[1] for eLux RP 5 and earlier versions



MAC 001F16F841EB
Host ID 6440-8503-2870
License eLux (63U5681AKW2ZH)
Subscription Valid
OS eLux RP 4.7.0-1
Device hp t5745

(c) 2015 Unicon Software GmbH Karlsruhe

Installed image: UC_RP:unicon_2.idf
Installed at: Fri Jan 16 05:10:43 2015

BaseOS eLux RP, V4.7.0-1
Core installer, V5.4-1

5.1.1. License information

The eLux license key[1] and the current status of the Subscription are shown on the **General** tab. By double-clicking the magnifier icon, you can view more details.

Entering a new license[2]

1. In **Setup > General**, double-click the term **License**.
2. In the **eLux license information** dialog, in the **License key** field, enter the new License Base Key.
3. Confirm with **OK** and **Apply**.

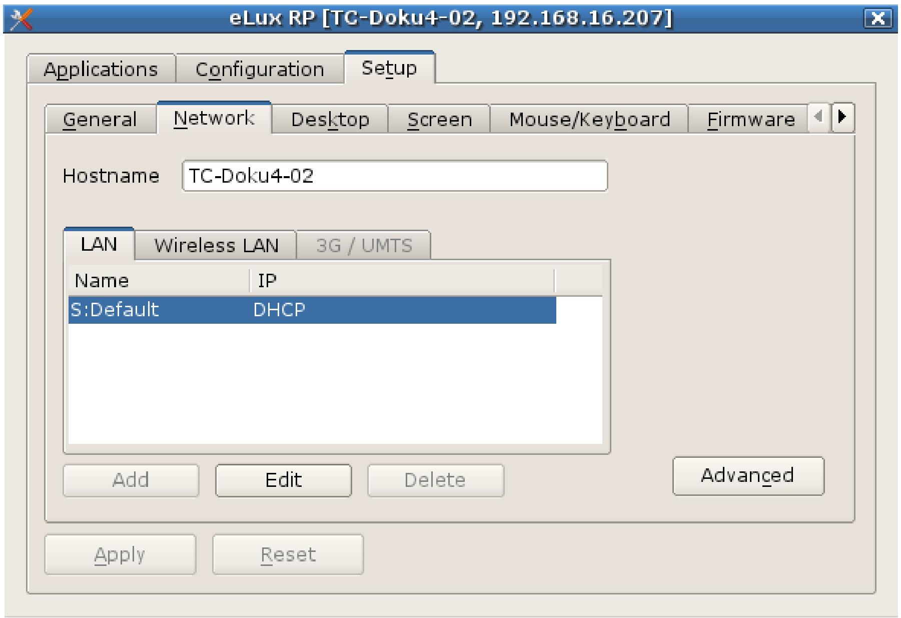
5.2. Network tab

Depending on the hardware installed, the **Network** tab shows some sub tabs:

- LAN
- Wireless LAN

The systray icon shows further information concerning the existing network connections.

[1] for eLux RP 5 and earlier versions
[2] for eLux RP 5 and earlier versions



Hostname: TC-Doku4-02

Name	IP
S:Default	DHCP

5.2.1. Defining a LAN profile

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

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

5.2.2. Defining a WLAN profile

The following configuration options are provided:

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

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

C. Corporate WLAN: A WLAN configuration can be distributed throughout the entire company network by using a WPA configuration file with and without 802.1X. This method requires configuring a dummy WLAN profile in the device configuration that can be hidden for the clients.[1]
For eLux RP 5.6 and later versions, users can create individual WLAN profiles locally on the cli-

[1] for eLux RP 5.6 and later versions

ent, on top. Configured WLAN networks can connect automatically depending on location and priority. For further information, see WPA support and Corporate WLAN.

Creating a WLAN profile in the Scout Enterprise device configuration

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

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

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

Option	Description
SSID	Service Set Identifier Name of the WLAN
Timeout	Time period in seconds waiting to connect
Channel	Selected automatically by default
Encryption	Authentication mode Select `WPA` or `WPA2` with pre-shared key (PSK). To authenticate via EAP (Extensible Authentication Protocol), use a WPA configuration file. For further information, see WPA support.

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

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

Displaying WLAN profile editor on the client

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

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

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

For further information, see Advanced file entries.

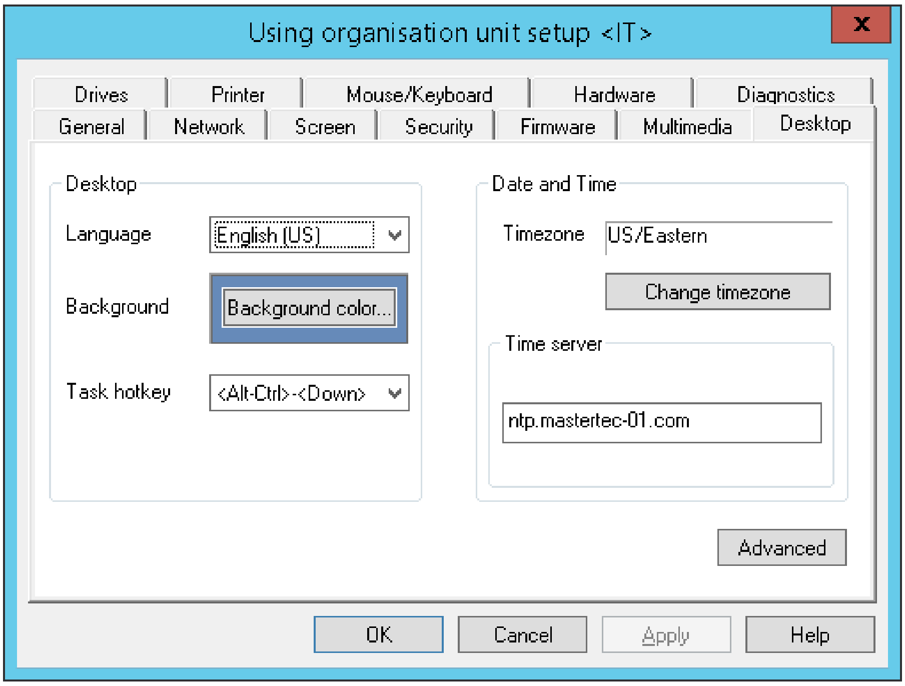
5.2.3. Adding a hostname by using DHCP

By using a DHCP request, the local hostname can be transferred to the DHCP server. The hostname will then be visible on the DHCP server.

- In **Setup > Network**, in the field **Hostname**, enter the host name of the particular Thin Client and click **Apply**.

5.3. Desktop

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



Using organisation unit setup <IT>

Desktop

Language: English (US)

Background: Background color...

Task hotkey: <Alt-Ctrl>-<Down>

Date and Time

Timezone: US/Eastern

Time server: ntp.mastertec-01.com

5.3.1. Configuring desktop

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

Note

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

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

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

Note

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

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

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

5.3.2. Advanced desktop settings

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

Option	Description
Interactive Desktop	Icons displayed on the desktop
Desktop writable	Users are allowed to place icons on the desktop.
Classic Desktop	The eLux Modern User Interface is deactivated. The **Background colour** selected on the **Desktop** tab is shown.
Window manager	If the **Animated Windows** option is selected, the windows' content is displayed while moving them. If the **Maximize/Fullscreen**option is selected, and you have connected multiple monitors, you can assign each application (ICA and RDP) to a dedicated monitor.[1]
Taskbar	Settings for the taskbar at the bottom of the screen

[1] only for eLux RP 5. For eLux RP 6, the functionality is available by default.

Option	Description
Quick Setup (Systray)	Systray icons to be displayed in the taskbar. **Multimedia**: Selecting input and output devices, Volume control, Test sound **Mouse/Keyboard**: Mouse and keyboard speed, left-handed mouse, keyboard language **Screen**: Information, resolution, alignment **USB mass storage devices**: Information about USB devices **Show network status**: LAN/WLAN, network information, disconnect/connect, configuration **Device information**: MAC, IP, name, serial number, free information fields **Date/Time**: Display and configuration of date, time and time zone
Background image (only Scout Enterprise)	There are two options to define background images: • In the **Server file** field, type the picture file name including its path relative to the Scout Enterprise Server directory (`...\UniCon\Scout\Server`) • Click **Load** to browse and select the picture file. The picture file is imported into the database. This option has precedence over a file referenced in the file system. Click **Delete** to remove the current background image from the database. Files that you import into the database are saved with the SQL database backup. Files that you reference in the file system provide the opportunity to be replaced by other content as long as the file name remains. The background image is not reloaded on each restart, but after changes have been made in the file configuration or in the files themselves.
	Note Make sure to have enough space on the client flash card. The background image is stored in the `/setup` directory of the flash card.
Autostart	The control panel is started after the system start with the defined delay in seconds
Work spaces	Number of desktops

5.3.3. Time zone and time server

In **Desktop > Date and time**, you can select a time zone and specify a time server.

Option	Description
Time zone	Click **Change time zone** and select the required time zone from the list..
Time server	Under **Time server**, specify the relevant server name or IP address..

The time server must comply with the Network Time Protocol (RFC 1305) or the Simple Network Time Protocol, a simplified form of NTP. Microsoft Windows operating systems include the **W32Time** service which communicates via SNTP in older versions such as Windows 2000, and uses NTP in later versions. The time service is started automatically.

The service runs on port 123 and uses the UDP protocol.

On the eLux client, the user then can synchronize the current time with the time server by using the **Synchronize** button.

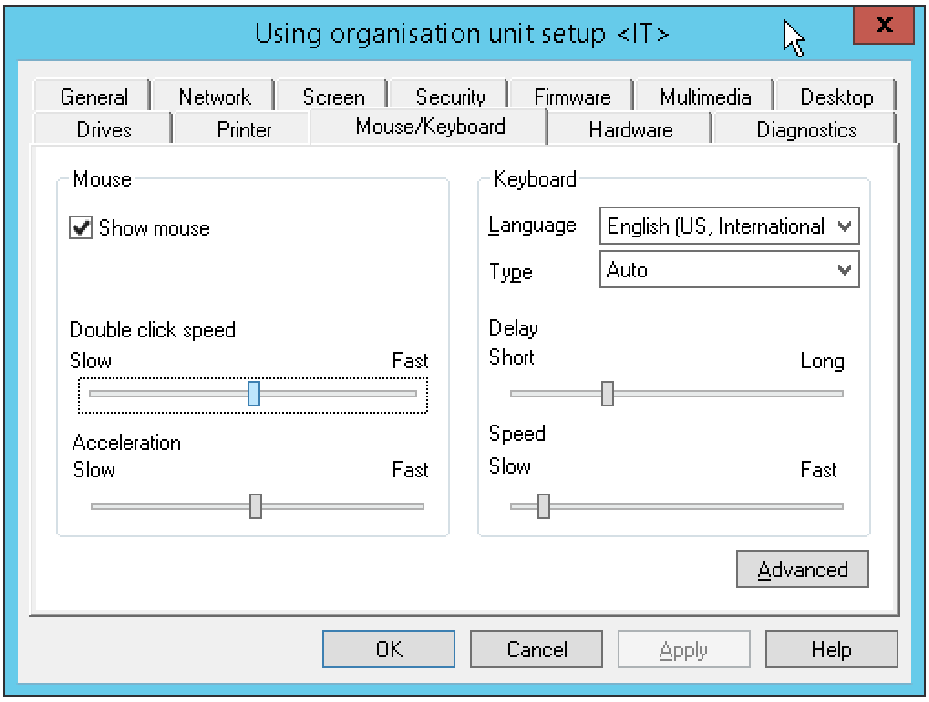
For further information on the Windows Time Service, see the Microsoft documentation.
For further information on NTP, see http://www.ntp.org.

5.4. Screen tab

- Screen resolution and rotation
- Layout for multiple monitors
- Power save mode
- Screen saver

Note
To modify the screen resolution settings, instead of the control panel, use the systray icon because it shows the resolution values supported by the individual monitor.

5.5. Mouse/Keyboard tab



☑ Show mouse

Language: English (US, International

Type: Auto

5.5.1. Configuring mouse settings

1. On the **Mouse/Keyboard** tab, under **Mouse**, to hide the mouse pointer, clear the **Mouse** option.

   The type of the mouse is recognized automatically.[1]

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

2. To increase the speed of the mouse pointer, under **Double click speed**, move the slider to the right.

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

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

   The faster the mouse pointer, the smoother the movements.

5.5.2. Configuring the keyboard

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

   The type of the keyboard is identified automatically.

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

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

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

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

5.5.3. Advanced mouse and keyboard settings

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

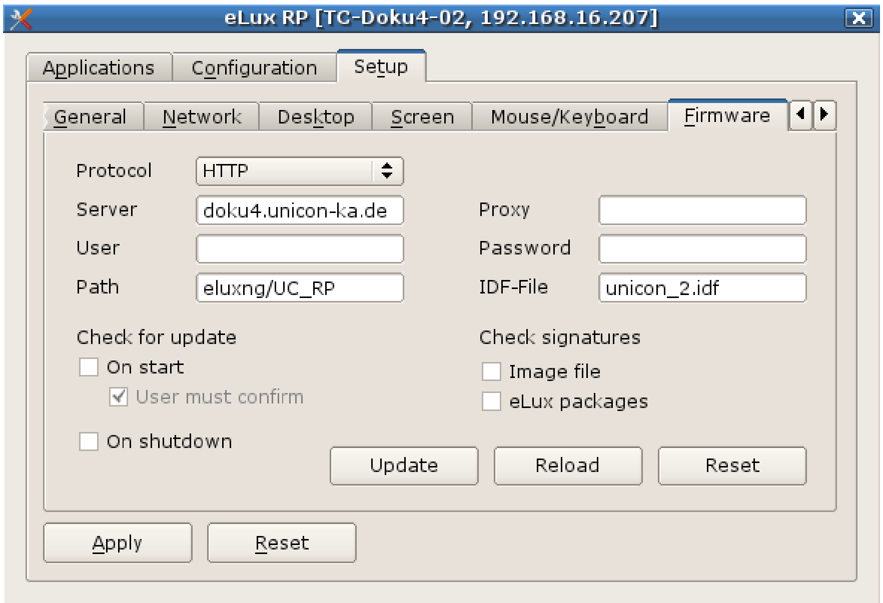
Option	Description
3 button emulation	Emulates the third mouse button for 2-button mice: Press the left and right mouse button simultaneously.
Left-handed	Reverse mouse buttons
Dead Keys	Dead keys only produce visible output when they are followed by a second keystroke. Accent keys are dead keys as the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

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

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

5.6. Firmware tab

On the **Firmware** tab, you configure the firmware update settings for software updates of your device.



Protocol: HTTP

Server: doku4.unicon-ka.de

User:

Path: eluxng/UC_RP

Proxy:

Password:

IDF-File: unicon_2.idf

Check for update

□ On start

☑ User must confirm

□ On shutdown

Check signatures

□ Image file

□ eLux packages

5.6.1. 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. On the **Firmware** tab, ensure that the fields **Protocol**, **Server**, **Path** and **Image file** are configured correctly. For further information, see Configuring firmware update.
2. Click **Update** to start comparing.

   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.
3. If an update is required, start the update process with **Yes**.

The firmware update is performed and the client is restarted.

Note
Before starting the update you can display the components to be updated by clicking **Details**.

5.6.2. Resetting Thin Client to factory status

Important

If you reset the client to factory status, all settings are set back to default.

Resetting a client can be useful, for example, if the local configuration does not work correctly.

The configuration of the client firmware is set back to the factory status, application definitions and locally stored data are deleted. The license information is retained.

- On the **Firmware** tab, click **Reset**.

The client is set back to factory settings.

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

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

5.6.3. Synchronizing configuration

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

- On the Firmware tab, click **Reload** and confirm with **Yes**.

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

5.6.4. Configuring firmware updates

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

Option	Description
Protocol	Network protocol of the web server for the software package transfer to the clients (`HTTP, HTTPS, FTP, FTPS`)
Server	Name (FQDN) or IP address of the web server containing the eLux software packages and the image definition file
Proxy (optional)	IP address and port number (3128) of the proxy server Format: `IP address:port` Example: `192.168.10.100:3128`

Option	Description
User and Password (optional)	Username and password (if required) to access to the eLux software container of the web server
Path	Directory path of the eLux software packages on the web server / FTP server Use slashes `/` to separate directories. Example: `eluxng/UC_RP5` corresponds to the IIS web server directory `C:\inetpub\wwwroot\eluxng\UC_RP5\` To handle different eLux versions the container directory can be parametrized by the container macro.
Image file	Name of the image definition file (IDF) on the web server which is used for firmware updates Depending on the permissions, an IDF name can be entered or an IDF is selected from the list-field. For further information, see Allocation of the image definition file. If you have both, UEFI devices and non-UEFI devices, use the Base System macro within the IDF name.
	Note The fields **Protocol**, **Server**, **Path** and **Image file** are used to build a URL-address, which is used by the clients when starting the transmission of Image Definition file and eLux software packages for a firmware update. The URL address is displayed below the **Path** field.
Check for update on boot / shutdown	The Thin Client checks during start or shutdown, if there are firmware updates available and necessary. You can set the option **Update confirmation nesessary** to let the user decline the update, if required..
Elias... button	Starts the ELIAS tool and opens the Image Definition file indicated in the **Image file** field.
Security... button	The **Security settings** let you define signature check before update through the client. Signature check can be performed for the Image Definition files and/or for the eLux software packages.
Reminder... button	The **Reminder Settings** let you define if a user is allowed to defer a firmware update and for how long. Moreover, you can specify time intervals for the update reminder. For further information, see Update deferment by user.

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

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

Note

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

5.6.5. Firmware security through signature

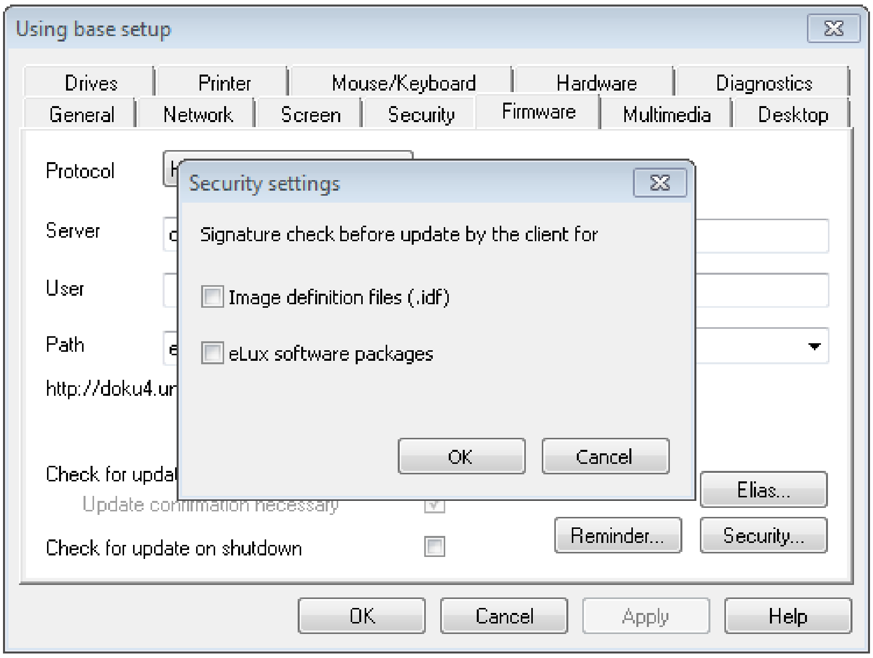
You can configure Scout Enterprise to make the client check signatures each time before an update is performed. In this case, an update is performed only if the signature of the image definition file (IDF) and/or the signature of the eLux software packages have been verified successfully. The update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

Important

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

Activating signature check

1. In **Setup > Firmware**, click **Security...**...



Security settings

Signature check before update by the client for

□ Image definition files (.idf)

□ eLux software packages

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 on the **Firmware** tab..

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

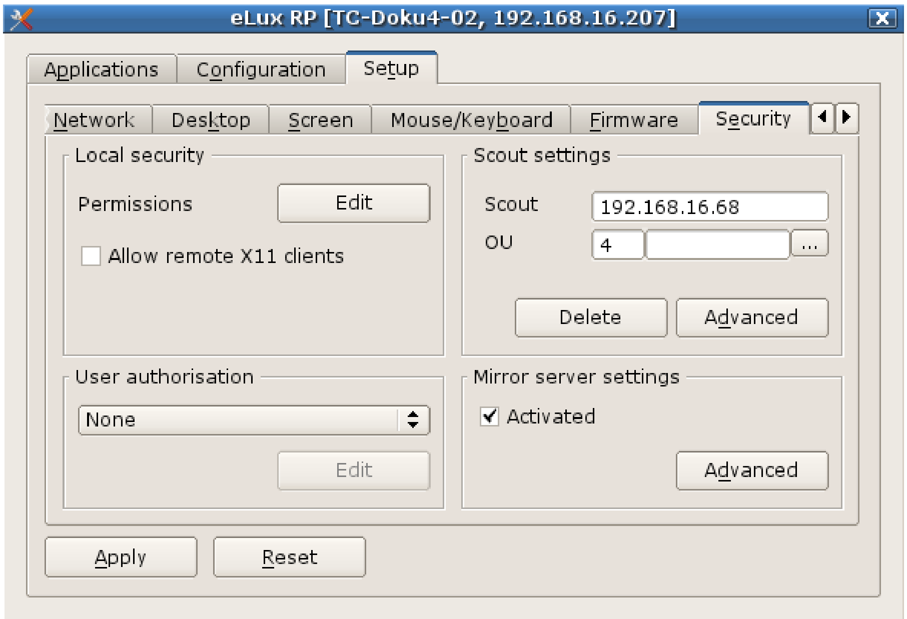
Certificates

Verifying the IDF signature on the client side requires the root certificate, but also the signature certificate in the local client directory `/setup/cacerts`. If you use own certificates for signing IDFs or individually composed eLux packages, you can configure their transfer by using the Scout Enterprise command **Options > Advanced options... > Files**. For those eLux packages provided by Unicon, all required certificates are included in the BaseOS.[1]

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

5.7. Security tab

On the **Security** tab, you can edit user permissions, access authorization, Scout Enterprise Server settings as well as the mirroring settings.



☐ Allow remote X11 clients

None

Scout 192.168.16.68

OU 4

☑ Activated

5.7.1. Changing user rights

The eLux control panel provides a **Configuration** tab containing the application definitions for the installed applications, and a **Setup** tab containing the device configuration. To prevent users from configuring defective or unwanted settings locally on the client, for both tabs, you can deactivate or restrict the user rights related to the features shown there. Additionally, some general features such as **Logoff** are provided. Each feature can be allowed or locked.

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

[1] for eLux RP 4.7.0 or later versions

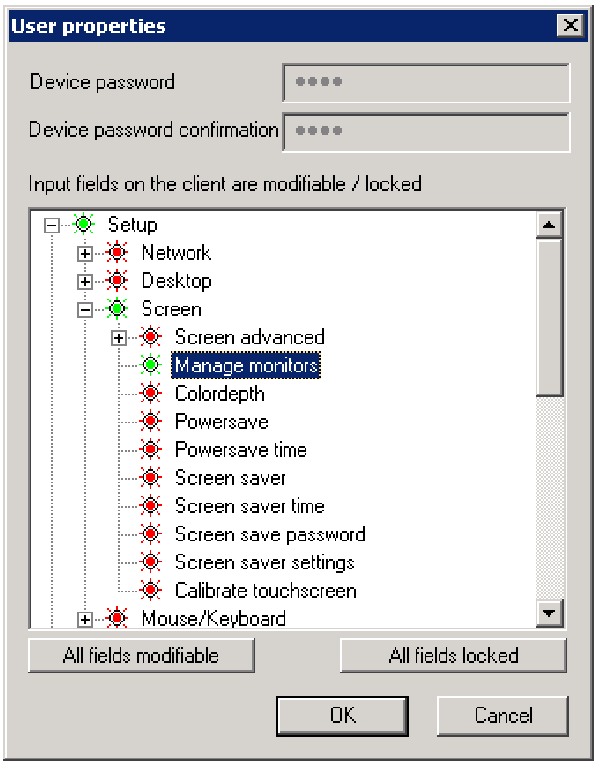
Note

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

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

Modifying user rights for device configuration

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



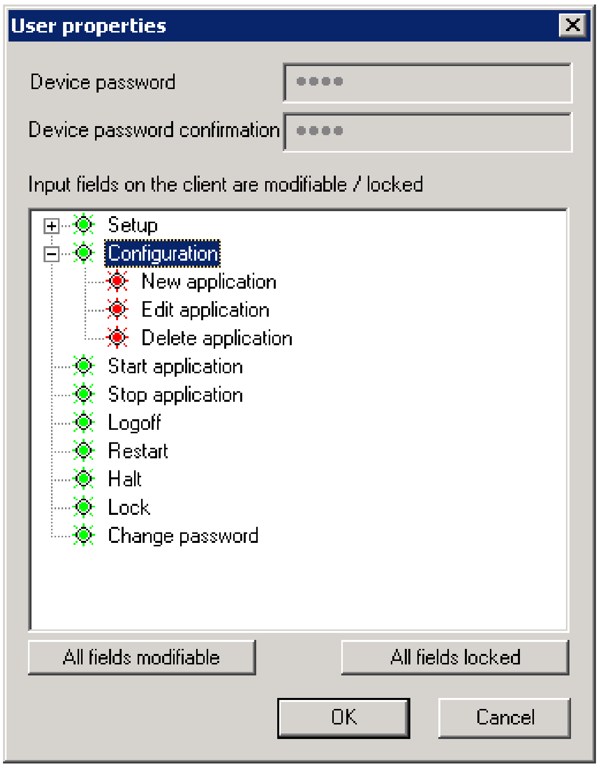
*The **Setup** node refers to the device configuration and its structure corresponds to the tabs and fields of the eLux control panel.*

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

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

Modifying user rights for application definitions

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



User properties

Device password: ●●●●

Device password confirmation: ●●●●

Input fields on the client are modifiable / locked

- 🟩 Setup
- 🟩 Configuration
  - 🟥 New application
  - 🟥 Edit application
  - 🟥 Delete application
- 🟩 Start application
- 🟩 Stop application
- 🟩 Logoff
- 🟩 Restart
- 🟩 Halt
- 🟩 Lock
- 🟩 Change password

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

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

Note

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

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

5.7.2. Allowing remote connections to X11 clients

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

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

Important

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

5.7.3. Scout Enterprise connection

On the **Security** tab, under **Scout Enterprise** settings, the data required to connect to the Scout Enterprise Server are shown or can be entered:

- IP address of the Scout Enterprise Server
- ID of the OU the client is assigned to

OUs can be protected by passwords that will be requested when a client is assigned to them.

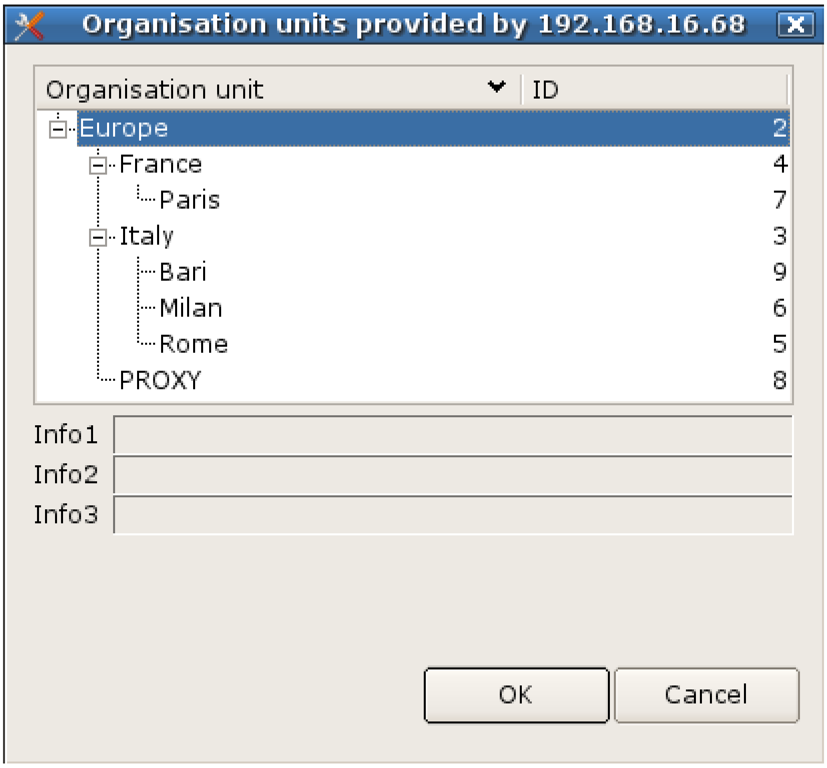
To connect a client to the relevant Scout Enterprise Server, use the **Reverse Discovery** feature.

Executing the Reverse discovery

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

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

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



Organisation units provided by 192.168.16.68

Organisation unit	ID
Europe	2
France	4
Paris	7
Italy	3
Bari	9
Milan	6
Rome	5
PROXY	8

Info1

Info2

Info3

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

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

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

Disconnecting from the Scout Enterprise Server

- On the **Security** tab, under **Scout Enterprise settings**, click **Delete**.

The device is set back to initial state. All settings and all data are deleted, including the connection data for the Scout Enterprise Server.

Note
If the client is not connected to a Scout Enterprise Server, you can use the **Reverse Discovery** feature to search for the relevant server and add the client to the client infrastructure.

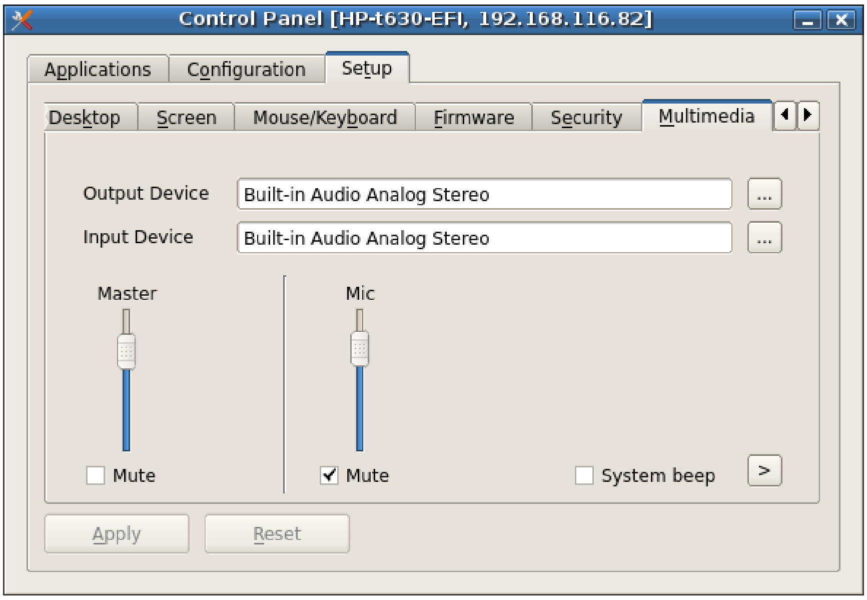
5.8. Multimedia

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

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

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

On the client, the connected devices are shown in list-fields.



Output Device: Built-in Audio Analog Stereo

Input Device: Built-in Audio Analog Stereo

Option	Description
Volume (output)	Slider to control the playback sound level for the selected device class (0 to 100)
Microphone (input)	Slider to control the level of sensitivity for recording for the selected device class (0 to 100)
Mute (output and input)	No sound is reproduced / recorded
System beep	Acoustic feedback signal when switching off the client

5.9. Drives tab

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

5.9.1. Browser home directory

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

If you define a browser home directory on the network, browser settings such as bookmarks can be saved and made available to the user after each client restart. Use a network share that you have configured for access:

Requires
Configured Windows network share (**Defined drive**).
Example: `/smb/share`
For further information, see Defining a network drive.

Defining browser home directory

Note
The following information refers to Scout Enterprise Management Suite 15.0 and later versions. Documentation for earlier versions can be found in the **Archive** section of the PDF downloads page.

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

   For further information, see Defining software defaults.

2. In the list-field, select the relevant browser and click **Edit**.
3. In the **Browser home directory** field, enter the name of one of the defined drives in **Device configuration > 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.

5.9.2. Mount points

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

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

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

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

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

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

5.10. Hardware

On the **Hardware** tab, you can enable or disable USB mass storage devices, configure smart card readers and COM ports.

If you click the icon of the systray, you can see all available USB mass storage devices, and you can also remove them securely.

5.10.1. USB mass storage devices and card readers

Option	Description
Allow mass storage devices	Allows using the connected USB mass storage devices

Option	Description
No local mount, only USB redirection[1]	Restricts the use of USB mass storage devices to USB redirection within configured sessions on a backend. There are no mount points provided to use USB mass storage devices locally on the eLux client.
Use rules	Restricts the use of USB mass storage devices according to defined rules: Using USB mass storage devices can be restricted to devices with specified VID (Vendor ID) and/or PID (Product ID) such as an individual USB stick model. Moreover, the USB rules can be applied to further USB device classes like smart card readers.
Edit	Opens the USB rules dialog: Define rules to explicitly allow or deny individual device models.
Card reader	Enables a card reader on the selected port
Inform user	When a USB mass storage device is connected, a systray message is displayed.
COM port settings	Set particular COM port settings such as speed, parity, stop bits
Write filter (only Windows Embedded)	The user is not allowed to store local data on their Windows Embedded client.

Note

– only for eLux 5.4 clients and Scout Enterprise 14.7 or earlier versions:

To use USB rules, for the relevant clients, in **Advanced settings > Advanced file entries**, define the following entry:

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

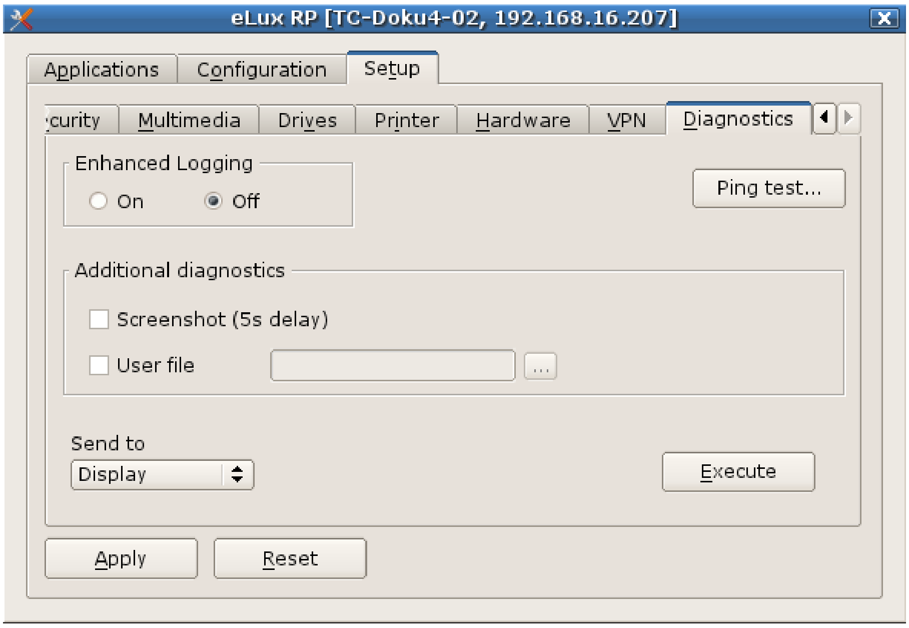
For further information, see Advanced file entries.

5.11. Diagnostics tab

The following diagnostic options are provided:

- Enhanced logging to retrieve configuration and log files to a greater extent
- Additional diagnostics by creating screen shots and additional diagnostic files
- Displaying or sending relevant files to FTP server, Scout Enterprise Server or disk
- Ping test to check connectivity and latency in your network

[1] for eLux RP 5.4 and later versions



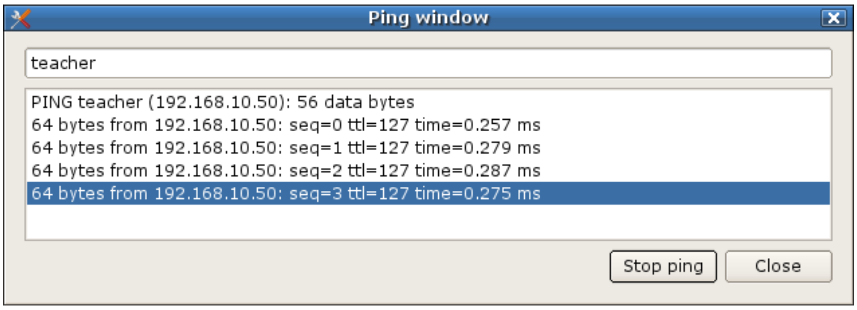
Enhanced Logging
○ On ● Off

Additional diagnostics
□ Screenshot (5s delay)
□ User file

Send to
Display

5.11.1. Running ping test

1. On the **Diagnostics** tab, click **Ping test...**.
2. In the **Ping window**, in the field on top, type the name or IP address of the server you want to connect with.
3. Click **Start ping**.



teacher

```
PING teacher (192.168.10.50): 56 data bytes
64 bytes from 192.168.10.50: seq=0 ttl=127 time=0.257 ms
64 bytes from 192.168.10.50: seq=1 ttl=127 time=0.279 ms
64 bytes from 192.168.10.50: seq=2 ttl=127 time=0.287 ms
64 bytes from 192.168.10.50: seq=3 ttl=127 time=0.275 ms
```

The client connects to the server and, in the bottom windows section, the ping command is executed unless you stop.

4. Click **Stop ping**.

5.11.2. Starting diagnostics

1. On the **Diagnostics** tab, enable **Enhanced logging**.
2. To save an additional screenshot, select the **Screenshot** option.
3. To add an additional file, select the **User file** option and select the file from the file system.

4. Under **Send to**, select where the diagnostic files should be sent to:

Option	Description
Disk	Files are saved to local data medium
FTP server	Files are saved to an FTP server
Scout Enterprise	Files are saved to the Scout Enterprise folder `%USERPROFILE%\Documents\UniCon\Scout\Console\Diag`
Display	Opens the **Log Viewer** window in eLux which shows a couple of diagnostic files and their content.

5. Click **Execute**.

6. Defining applications

6.1. General

eLux provides two kinds of applications

- Server-based remote applications, mostly providing access to back-end systems
- Local applications

Thin Clients are mainly used as terminals in server-based computing. **Remote** means that the application such as a Windows application runs 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.

The following topics describe how to configure both, local and server-based applications. In addition, further configuration may be required in the application itself. For further information on configuring session clients such as a Citrix client, please consult the manufacturer's product documentation.

6.1.1. Adding applications

1. In the eLux control panel, select the **Configuration** tab.
2. Click **New**.

*The **Application definition** dialog opens. This dialog provides several tabs, each of them relating to a particular application type.*

3. Click the tab relating to the application you want to define.

   If the relevant application tab is missing, the software package is not installed on the Thin Client.

4. Configure the application.
5. Confirm with **Apply** and **Finish**.

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).

Option	Description
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 PN Agent)

6.1.2. Editing applications

1. In the eLux control panel, select the **Configuration** tab.
2. Select the application you want to edit.
3. Click **Edit**.

*The **Application definition** dialog opens. Depending on the application, different properties can be configured.*

6.1.3. Deleting applications

1. In the eLux control panel, select the **Configuration** tab.
2. Select the application you want to delete. To select more than one application, press the CTRL key.
3. Click **Delete**.
4. Confirm with **Yes**.

The application is deleted.

6.2. Connecting to a Citrix farm

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

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

- by a StoreFront application to a StoreFront server
- by the Citrix Self-Service user interface to a StoreFront server
- via browser to a StoreFront server or Web Interfaceserver

- by a PNAgent application to a StoreFront server (XenApp Services Support must be enabled on the Citrix farm) or Web Interfaceserver
- 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 Receiver for Linux, V13.5.x** must be installed on the clients. .
- To connect via HTTPS, for the application types **Storefront**, **Self Service** and **PNAgent**, the relevant root and intermediate certifcates must be available on the clients.
  - Root certificates must be transferred to `/setup/cacerts`.
  - Intermediate certificates must be transferred to `/setup/cacerts/intcerts`.

  For further information, see Certificates 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.

6.2.1. StoreFront application

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

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

Defining a StoreFront application

Note

HTTPS connections require the relevant SSL certificates on the client.

1. Add a new application and click the **StoreFront** tab.
2. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console
Stores	Specify the URL of one or more stores ▶ Click **Add** and replace the automatically created default value by your individual value (double-click or F2) Example: (`https://CtrXd76.sampletec-01.com/Citrix/Store33/discovery`)
Logon	The user is automatically logged on to the store by using the specified credentials (username, password, domain).
Pass-through logon	The user is logged on to the store via single sign-on. The AD user credentials are used. If AD users log on via smart card, and if Citrix Receiver for Linux 13.4.x or later versions are used, the authentication method **Domain pass-through** on the Citrix server must be disabled.
	Note For pass-through logon, the eLux package **Citrix Receiver Extensions** and the included feature package **Dialog Extension** must be installed on the clients.
Show last user[1]	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 StroreFront applications you want to have started automatically. Make sure to spell the names exactly in the way they are in StoreFront. To separate more than one application name, use a semicolon. Example: `MyApp1;MyApp2`
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters.

[1] for Scout Enterprise 14.7 and later versions

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

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

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

Smart card authentication for StoreFront

If you use smart card authentication for StoreFront, you can configure the behavior of the smart card when it is removed.

Note

Using a smart card requires the smart card middleware to be installed on the client. In addition, smart card authentication must be enabled on the Citrix farm. If Citrix Receiver for Linux identifies smart card middleware on the client, smart card logon has precedence over logon with username and password by default.

- Define the following entry by using the Scout Enterprise feature Advanced file entries:

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

Controlling the authentication method via eLux[1]

The logon can be changed to username and password regardless of the smart card packages installed.

- Define the following entry by using the Scout Enterprise feature Advanced file entries:

File	`/setup/sessions.ini`
Section	`ICADefaults`
Entry	`StoreFrontLogOnWithPassword`
Value	`true`| `false` (Default: `false`)

Access to published resources

After users have logged on to a StoreFront server or Web Interface server, they can access the provided resources through the eLux Start menu or through the control panel and the **Applications** tab: The **StoreFront** node can be expanded to view the resources provided on the server.

6.2.2. Self-Service user interface

The Self-Service user interface (UI) replaces the configuration manager **wfcmgr** and allows access to Citrix services providing published ressources. After 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 Receiver for Linux** and the included feature package **Self-service** must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

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

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`).

6.2.3. Self-Service user interface with extensions

The Citrix Self-Service user interface (UI) can also be used in an extended version with further functionality[1]

- Configuration of the stores
- Logoff and reconnect options
- Dialog and window layout

Defining Citrix Self-Service UI with extensions

– Steps for eLux RP 5 –

Note

The eLux package **Citrix Receiver for Linux 13.5.** or later must be installed on the clients.
The eLux package **Citrix Receiver Extensions 2.x** or later must be installed on the clients.
Depending on the desired features, the following included feature packages must be installed on the clients:
Self-service wrapper
Dialog Extension (for modifications on the Citrix dialog design)
Self-service dialog themes (for modifications on the Citrix dialog design)

This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

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

[1] for eLux RP 5.6 CR and later versions

Option	Description
Free parameters	Define StoreFront URLs for all stores you want to provide as Free application parameters as shown below: `StoreUrl1=`*<URL to store1>* `StoreUrl2=`*<URL to store2>* `StoreUrl3=`*<URL to store3>* Alternatively, you can provide the users with a range of predefined stores to choose from.[1] For further information, see Self-Service user interface with multistore option.

3. Optionally, define further parameters and values for window properties and connection options. For further information, see Parameters for the Self-Service extension (ucselfservice).
4. Confirm with **Apply** and **OK**.
5. If you want to change the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries**. For further information, see Parameters for the Self-Service extension (ucselfservice).

6.2.4. Self-Service user interface with multistore option

The Citrix Self-Service user interface with extensions can also be used with a different option allowing to provide users with a range of predefined stores. The users then can select one of the provided stores to connect to when they log in.[2]

Defining Citrix Self-Service UI with extensions and multistore option

– Steps for eLux RP 5 –

Note

The eLux package **Citrix Receiver for Linux 13.5.** or later must be installed on the clients.
The eLux package **Citrix Receiver Extensions 2.1** or later must be installed on the clients.
Depending on the desired features, the following included feature packages must be installed on the clients:
Self-service wrapper
Dialog Extension (for modifications on the Citrix dialog design)
Self-service dialog themes (for modifications on the Citrix dialog design)

This may require modifications of the image definition file on the web server by using ELIAS.

[1] for eLux RP 5.5.1000 LTSR CU and later versions

[2] for eLux RP 5.5.1000 LTSR CU and later versions

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

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

Free parameters	Configure access to the stores you want to provide for the users to choose from. use the Free application parameters as shown below:
	`Stores=<number of store entries>`
	`Store1=<store display name>,<store url>`
	`Store2=<store display name>,<store url>`
	...
	`Domains=<number of domain entries>`
	`Domain1=<domain display name>,<domain>`
	`Domain2=<domain display name>,<domain>`
	...
	`ShowLastUser=<0|1>`
	Note: You can predefine multiple stores and multiple domains using the format shown above.

3. Optionally, define further parameters and values for window properties and connection options. For further information, see Parameters for the Self-Service extension (ucselfservice).
4. Confirm with **Apply** and **OK**.
5. If you want to change the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries**. For further information, see Parameters for the Self-Service extension (ucselfservice).

6.2.5. Parameters for the Self-Service extension (ucselfservice)

Parameters for window properties and connection options

- In the application properties, define the following options as free parameters (Steps for eLux RP 5):

Parameter	Description	Origin
`SharedUserMode=`<*true*|*false*>	**Shared User Mode** allows to use one system user account for multiple users. When users log off or close the UI, the user data are removed.	Citrix
`FullscreenMode=`<*0*|*1*|*2*>	0 Not full-screen 1 Full-screen 2 Maximized and undecorated, taskbar remains visible This can be useful as users can launch seamless applications. Default: 0 (not full-screen)	Citrix
`SelfSelection=`<*true*|*false*>	Used to disable the search box and the self-selection panel Disabling prevents users from subscribing to extra applications. Default: false	Citrix
`ReconnectOnLogon=`<*true*|*false*>	Tries to reconnect to all sessions, for a given store, immediately after logon to that store	Citrix
`StoreGateway=`<*store gateway*>	If required, specify a gateway	Citrix
`ReconnectOnLaunchOrRefresh=`<*true*|*false*>	Tries to reconnect to all sessions when an application is launched or the store is refreshed	Citrix
`SessionWindowedMode=`<*true*|*false*>	true: Display desktops windowed false: Display desktops in full-screen	Citrix
`UseLogoffDelay=`*<0|1>*	To activate automatic logoff, set `UseLogoffDelay=1`.	Unicon
`LogoffDelay=`<*seconds*>	Delay in seconds for automatic logoff	Unicon
`ForcedLogoff=`*<0|1>*	1 Logoff timer is started with logon 0 Logoff timer is started when the last Citrix app is closed.	Unicon

Parameter	Description	Origin
`LogoffInfoTimeout`=<*seconds*>	During logoff (selfservice restart), an info dialog can be shown to the user for some seconds.	Unicon

For further information, see Defining free application parameters.

Important

To provide the stores for the users, you can either predefine them as fix values or predefine a range of stores the user can choose from in a pre-logon dialog.[1] For further information, see

- Self-Service user interface with extensions or
- Self-Service user interface with multistore option

Parameters for the design of the Citrix dialogs

- If you want to modify the design of the Citrix dialogs for all Citrix connections, use the Scout Enterprise feature **Advanced file entries** to set the following entries:

File	Section	Entry	Value
/setup/sessions.ini	ICADefaults	UiDialogTheme	`ucselfservice`
/setup/sessions.ini	ICADefaults	UiDialogDecorated	<`true|false`>
/setup/sessions.ini	ICADefaults	UiDialogKeepAbove	<`true|false`>
/setup/sessions.ini	ICADefaults	UiDialogKeepBelow	<`true|false`>
/setup/sessions.ini	ICADefaults	UiDialogColorHover	<*color*> Example: `#b0b0b0`
/setup/sessions.ini	ICADefaults	UiDialogColorUnselected	<*color*> Example: `#a0a0a0`
/setup/sessions.ini	ICADefaults	UiDialogColorSelected	<*color*> Example: `#c0c0c0`

For further information, see Advanced file entries.

Note

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

[1] for eLux RP 5.5.1000 LTSR CU and later versions

6.2.6. Browser session to access published resources

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

Defining a browser application to access published resources

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

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

1. Add a new application and click the **Browser** tab.
2. Edit the following fields:

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

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

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

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

6.2.7. 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 click the **PNAgent** tab.
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.
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

Option	Description
Free parameters (optional)	Individual parameters for application start Example: `PNATimeout=60` brings Citrix Receiver to try for 60 seconds to enumerate the published applications and desktops. To configure dual-monitor mode, you can also use the **Free parameters**, see below. For further information, see Defining free application parameters.

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

Option	Description
Window properties	For resolution/window size, color depth and audio output, select **Use default** (server settings) or select one of the values from the list-field.
Timed logoff	To enable automatic logoff from the Web Interface server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last PNAgent application has been closed.
Application reconnection	Determine the actions to be done on a reconnect to the Web Interface server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.
Manual logoff	Determine the actions to be done on logoff from the Web Interface server **Logoff only server**: Logoff is performed only from the Web Interface server **Logoff server and applications**: Logoff is performed from the Web Interface server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the Web Interface server but the virtual desktop session is only disconnected. This enables the user to reconnect later on.

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

Program Neighborhood variables

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

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

Creating a domain list

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

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

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

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

Settings for dual monitor mode

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

Method 1:

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

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

For further information, see Advanced file entries.

Method 2:

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

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

For further information, see Free parameters.

The values mean the following:

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

6.2.8. Defining an ICA application

Note

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

1. Add a new application and click the **ICA** tab.
2. Edit the following fields:

Option	Description
Name	Name of the application
Published application	Configures direct access to a published application To provide access to complete desktops, clear the option.
Server	IP address or name of the Citrix server (terminal server)
Application	Only relevant if you have selected the **Published application** option Name of the Windows application including path (see Citrix server) Note: The **Browse** option applies to the Citrix farm but is no longer supported.
Working directory (optional)	Only relevant if you have selected the **Published application** option Working directory for the application

Option	Description
Login	The user is automatically logged on to the Citrix server by using the specified credentials (username, password, domain).
Pass-through logon	The user is logged on to a Citrix server via single sign-on. The AD user credentials are used. Note: Kerberos authentication is no longer supported with Citrix Receiver for Linux 13.x.
Smart card logon	The client uses a smart card for logon.
Application restart Start automatically Desktop icon	See Adding applications
Free parameters (optional)	Individual parameters for application start For further information, see Defining free application parameters.
Connection options Advanced (eLux)	Opens the configuration dialog of Citrix Receiver for Linux (`wfcmgr`) Edit the relevant options. The Citrix Receiver configuration is saved to the file `/setup/ica/wfclient.ini` on the Thin Client and can be viewed from the Scout Enterprise Console by using the **Diagnostic files** feature.

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

A published application is displayed on the eLux client in the same way as local applications.

6.2.9. ICA Connection Center

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

The Connection Center is provided as systray icon on the taskbar.

Defining the Citrix Connection Center

Note

The eLux package **Citrix Receiver Extensions** and the included feature package **Connection Center** must be installed on the clients. This may require modifications of the image definition file on the web server by using ELIAS.

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

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

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

6.3. Browser

Supported browsers are Mozilla Firefox and Google Chromium.[1]

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.

6.3.1. Defining a browser application

1. Add a new application and click the **Browser** tab.
2. Edit the following fields:

Option	Description
Name	Name of the browser shown in the Scout Enterprise Console
Browser type	Select `Firefox` or `Chromium`[2].
Start page	Web page (URL) that opens whenyou click **Home**
Called page	Web page (URL) that opens after starting the browser

Proxy type	● `No proxy`
	● `Manual (Proxy:Port)`: Proxy server and port
	Example: `proxy.sampletec-01.de:3800`
	For manual proxy type, you can specify exceptions[3] in the **Advanced browser settings**.
	● `Auto (URL)`: Proxy configuration file
	Examples:
	`http://www.wpad.sampletec-01.com/wpad.dat`
	`http://www.proxy.sampletec-01.com/proxy.pac`

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

[2] Chromium is provided with Scout Enterprise Management Suite 14.8 and later versions

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

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

3. For the manual proxy type, to define destinations that you do not want to access via proxy, click **Advanced > Proxy exception list**, and then enter the relevant addresses.

4. To enable **Kiosk** mode, see Configuring Kiosk mode.

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

Note
By default, all browser files (cache, history, bookmarks, etc.) are saved temporarily to the flash memory but are deleted with each restart. We recommend 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 in the Scout Enterprise guide:

Preferences Chromium

Preferences Firefox

Deploying SSL certificates for the browser

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

Mozilla Firefox	`/setup/cacerts/firefox`
Google Chromium	`/setup/cacerts/browser`

For further information, see Advanced settings > Files.

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

6.4. Emulation

The following emulations are available:

Emulation	Description
PowerTerm InterConnect	PowerTerm® InterConnect from Ericom® Software is an emulation suite that allows you to connect to IBM mainframes, IBM AS/400, Unix, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000 and Data General. The **PowerTerm InterConnect** (powerterm) package is required for installation. PowerTerm InterConnect is a licensed product and available from our distribution partners.
eterm	eterm is a terminal emulation suite including the following emulations: Siemens 97801 (7 & 8 bit), ANSI, AT386, BA-80, VT320. The **Eterm 97801 terminal emulation** (eterm) package is required for installation. eterm is included in licensed eLux software free of charge. For information on configuration and how to modify the key mapping, see the **eterm** guide, available in the Archive on the uDocs Download page.
Virtual Network Computing	Virtual Network Computing (VNC) is a remote display system which allows you to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. The remote machine to be viewed must have a VNC server installed and the local machine a VNC viewer. In the **Emulations** dialog, you can configure the VNC viewer, which is open source and included free of charge in the eLux software. The **VNC client** (vnc) package of the **X Org** eLux package is required for installation. For further information, see Mirroring in the **Scout Enterprise** guide.
X11	The X Window System (X11) is the de facto standard graphical engine for the UNIX and Linux operating systems. It provides common windowing environment bridging heterogeneous platforms. It is independent of the operating system and hardware. The X11 server developed by The XFree86 Project, Inc (www.xfree86.org) is included in the **Xorg** package and is part of the BaseOS.
Tarantella	Tarantella allows users to access their applications over a Web-based interface. The **Tarantella Client** (tarantella) package is required for installation. The server version is licensed, the client version is free of charge. For further information, see www.tarantella.com.

For further information, see Configuring PowerTerm InterConnect and Configuring X11 application in the Scout Enterprise guide.

6.4.1. Defining an X11 application

1. Add a new application and click the **Emulation** tab.
2. In the **Emulation type** list, select **X11**.
3. Edit the following fields:

Option	Description
Name	Name of the application shown in the Scout Enterprise Console Do not use blanks within the name.
Server address	Enter the IP address or name of the UNIX server.
Username	Enter the name of the user registered on the UNIX system.
Application	Enter the application name including its complete path.
Use SSH	The X11 session is started via Secure Shell (SSH) protocol. Public key authorization only

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

6.4.2. Configuring PowerTerm InterConnect

The configuration of PowerTerm InterConnect is carried out in two steps:

- Defining a PowerTerm application on a reference client and transferring the created configuration files
- Defining a PowerTerm application for all clients by using the configuration files created on the reference client

Defining a PowerTerm InterConnect application for a reference client

Note

The **PowerTerm** software package must be installed on the client. This may require modifications of the image definition file on the web server by using ELIAS.

1. On the reference client or in the Scout Enterprise Console, define a PowerTerm application containing only the application name (for details see below).
2. Start the PowerTerm application on the reference client and configure the application manually.

   The configuration is saved to the local client directory `/setup/PowerTerm/` *in the following four files*
   `ptdef.pts`
   `ptdef.ptc`
   `ptdef.ptk`
   `ptdef.ptp`
3. Close the PowerTerm application.
4. Copy the four configuration files via network or USB stick and make them available to Scout Enterprise Console.
   Or:
   Transfer the files from the client to the Scout Enterprise Console remotely by using **Request diagnostic files** with an individual template. For further information, see Configuring diagnostic files.

The configuration files for the PowerTerm configuration are provided. The second step can be carried out.

Defining a PowerTerm InterConnect application for all clients

1. In the Scout Enterprise Console, add a new application for the relevant OU.
2. On the **Emulation** tab, in the **Emulation type** list, select `PowerTerm`.
3. Edit the following fields:

Option	Description
Name of application	Enter an appropriate name without using blanks.

Option	Description
Parameters	Optional starting parameters for the PowerTerm application: `-fullscreen` full screen `-maximize` maximized window `-no-menu-bar` no menu bar `-no-tool-bar` no toolbar `[myName].pts` name of an individual PowerTerm configuration file of the client Example 1: `-fullscreen -no-menu-bar -no-tool-bar` Example 2: `-fullscreen ptconfig001.pts`
Terminal setup file	Select the relevant `.pts` file of the reference client from the file system.
Communication file	Select the relevant `.ptc` file of the reference client from the file system.
Keyboard file	Select the relevant `.ptk` file of the reference client from the file system.
Power PAD file	Select the relevant `.ptp` file of the reference client from the file system.
x button	Delete previously selected configuration file from the Scout Enterprise database if required. To delete the file physically from the client you need to perform a factory reset.

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

PowerTerm InterConnect is available for all clients of the relevant OU on the next restart.

6.5. 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 by using the `Custom` option of the **Local Application** list-field.

Error messages will not be shown. If your command does not include an X client application, no messages are shown during execution. For this reason, we recommend running the command first within an XTerm session for testing purposes.

6.5.1. Defining predefined local applications

1. Add a new application and click the **Local** tab.

2. Edit the following fields:

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

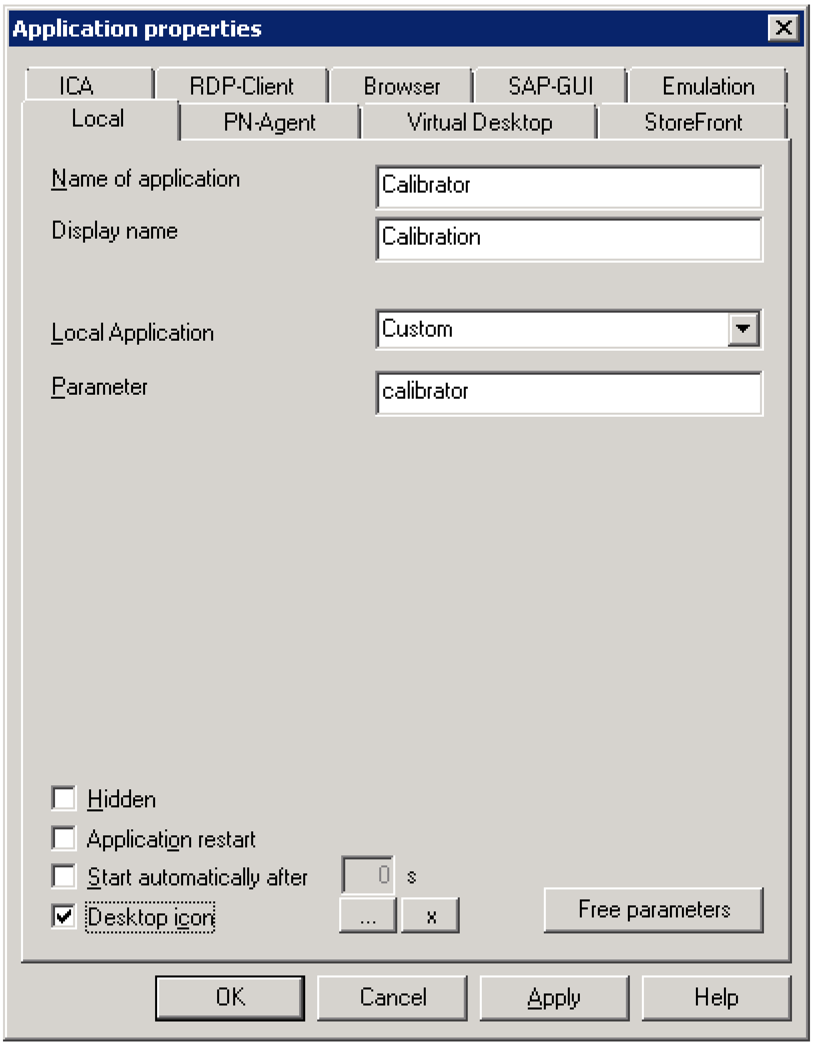
3. Confirm with **Apply** and **OK**.

6.5.2. Defining custom applications

1. Add a new application and click the **Local** tab.
2. Edit the following fields:

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



Name of application: Calibrator

Display name: Calibration

Local Application: Custom

Parameter: calibrator

☐ Hidden

☐ Application restart

☐ Start automatically after 0 s

☑ Desktop icon

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

6.6. 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 click the **PNAgent** tab.
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.
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

Option	Description
Free parameters (optional)	Individual parameters for application start Example: `PNATimeout=60` brings Citrix Receiver to try for 60 seconds to enumerate the published applications and desktops. To configure dual-monitor mode, you can also use the **Free parameters**, see below. For further information, see Defining free application parameters.

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

Option	Description
Window properties	For resolution/window size, color depth and audio output, select **Use default** (server settings) or select one of the values from the list-field.
Timed logoff	To enable automatic logoff from the Web Interface server, select the **Logoff after** option and specify a delay in seconds. Automatic logoff does not affect the launched desktop. Alternatively, automatic logoff can be configured to be performed after the last PNAgent application has been closed.
Application reconnection	Determine the actions to be done on a reconnect to the Web Interface server **Do not reconnect**: The connection to the desktop or the published applications is not restored (default). **Disconnected sessions only**: The connection to a disconnected session is restored. **Active and disconnected sessions**: The connection to a disconnected or active session is restored.
Manual logoff	Determine the actions to be done on logoff from the Web Interface server **Logoff only server**: Logoff is performed only from the Web Interface server **Logoff server and applications**: Logoff is performed from the Web Interface server and from the virtual desktop or published applications. **Logoff server and disconnect session**: Logoff is performed from the Web Interface server but the virtual desktop session is only disconnected. This enables the user to reconnect later on.

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

Program Neighborhood variables

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

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

Creating a domain list

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

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

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

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

Settings for dual monitor mode

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

Method 1:

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

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

For further information, see Advanced file entries.

Method 2:

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

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

  For further information, see Free parameters.

The values mean the following:

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

6.7. Virtual Desktop

The **Virtual Desktop** tab helps you define Citrix or VMware connections with with a VD broker. For Citrix XenDesktop, the logon data is defined according to an ICA connection.

6.7.1. Defining a virtual desktop

1. Add a new application and click the **Virtual Desktop** tab.
2. Edit the following fields:

Option	Description
Name	Name for the application
VD Broker	Choose the desired Broker from the list
Server	Enter the IP address (or the name) of the server
Logon Pass-through logon	See Adding applications
Protocol (VMware View only)	Choose between `RDP` and `PCOIP`

3. To configure further settings, click **Advanced**. For further information, see depending on the broker or protocol selected
   - Advanced XenDesktop settings or

- Advanced RDP settings

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

7. Applications

In the eLux control panel, on the **Applications** tab, all defined applications are shown along with their type of application and information on their status (active or inactive).

7.1. Starting an application

1. In the eLux control panel, click the **Applications** tab.
2. Select the relevant application.
   To start more than one application, select them one by one while pressing CTRL.
3. Click **Connect**.

Or:

▶ Double-click the relevant application.

7.2. Disconnecting an application

1. In the eLux control panel, click the **Applications** tab.
2. Select the relevant application.
   To disconnect more than one application, select them one by one while pressing CTRL.
3. Click **Disconnect**.

When the user turns off the device, the remote session and application remains active on the server.

If you want to have the sessions closed completely before the devices are turned off , either the administrator can define a timeout on the server to close any inactive sessions, or the user logs off from a session instead of disconnecting.

8. Troubleshooting

9.1. 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 View Server	Server problem occurred: VMware View Server, after successful installation, is using 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.

9.2. Troubleshooting device configuration

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

Error / problem	Reason	Solution
When you use USB multimedia devices such as headsets or webcams, the screen freezes or the window cannot be focused.	The USB operating elements register themselves as keyboard or mouse devices in the system.	Prevent the registration as keyboard or mouse devices by defining a `terminal.ini` entry. To do so, use the Scout Enterprise feature Advanced file entries: File `/setup/terminal.ini` Section `Xorg` Entry `IgnoreUsbInput` Value `VendorID_1:ProductID_1,VendorID_2:ProductID_2` Example: `0b0e:034c,047f:c01e` The basic functionality of the operating elements is not affected.
Multimedia USB devices, connected via DisplayPort, do not play back sound.	Sound reproduction via DisplayPort is disabled.	Enable sound reproduction by defining a `terminal.ini` entry. To do so, use the Scout Enterprise feature Advanced file entries: File `/setup/terminal.ini` Section `Screen` Entry `Radeon.Audio` Value `true` Alternatively, use a separate audio cable.

Error / problem	Reason	Solution
When you use a touch screen, the location of a fingertip touch is not recognized precisely.	The monitor is not calibrated exactly.	To calibrate the monitor, configure a custom application by using the parameter `calibrator`, and then start the application.
Display/graphics issues	The feature package for hardware acceleration **HwVideoAccDrivers**[1] is not installed.	Activate the **HwVideoAccDrivers** FPM[2] within the **XOrg** package in the IDF.

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

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

Error / problem	Reason	Solution

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

AD login 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, one more client restart might be required to enable the new setting.

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

[2] for eLux RP 5.6 and later versions

10. Appendix