SCOUT enterprise

Version 13.x.x

Management Tool for Thin Clients with eLux® NG, eLux® RT eLux® *RL*,*eLux*® *RP* Windows® CE XPe/WES7

Administrator's Guide

Build # 22

April 2013

Unicon Software GmbH

Contents

Figures

1 Introduction

1.1 Before you begin

This manual is for system administrators responsible for installing, configuring and using **Scout Enterprise** to manage Thin Clients.
Starting with this version Scout Enterprise supports the management of clients with

- **eLux® NG**
- **eLux® *RT***
- **eLux® *RL***
- **eLux® *RP***
- **Windows CE® 5.0**
- **Windows XP embedded**
- **WES7**

However, clients with eLux 1.x cannot be managed with this version any longer.

This manual assumes knowledge of:

- Installation, operation and maintenance of network and asynchronous communication hardware, including serial ports, modems and device adapters
- The operating system (OS) on the Thin Client

NOTE: No significant knowledge of Linux is needed, although Scout does manage Linux based clients.

1.1.1 Conventions

Convention	Description
>	Move to a menu, tab, screen element or folder.
⇨	Refers to a procedure.
" ..."	Quotation marks refer to screen text and text in pop-up messages.
ALL UPPERCASE	Represents keyboard keys (for example, ENTER, F4, CTRL).
Bold	Indicates boxes and buttons, column headings, command-line commands and options, dialog box titles, tabs, icons, lists, menu names and menu commands, directories, subdirectories and folders, and new terms.
`Courier New`	The Courier New font represents entries you can type at the command line or initialization files.
<*Italics*>	Indicate a placeholder for information or parameters that you must enter. As an example, if the procedure asks you to type <*IP address*>, you must type the actual IP address. Italics can also refer to book titles.

1.1.2 Glossary

Abbreviation	Description
BootP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
GUI	Graphical User Interface
ICA	Independent Computer Architecture
IP address	IP addresses are represented in four 3-digit groups separated by periods. *Example*: `192.45.85.1`
MAC address	Media Access Control address. The format of a MAC or hardware address is: xx:xx:xx:xx:xx:xx *Example*: `00:30:05:07:85:1A`
MSN	Multiple Subscriber Number
PING	Utility used to check whether an IP address is accessible or not.
RDP	Remote Desktop Protocol
SNMP	Simple Network Management Protocol
UTC	Coordinated Universal Time
VNC	Virtual Network Computing
wireless LAN	wireless local-area network
XDMCP	X Display Manager Control Protocol
ou	Organization Unit in the Scout Enterprise hierarchy

1.2 Finding More Information

This manual contains conceptual information, and installation and configuration steps for Scout Enterprise. Additional information is available from the following sources:

- The Scout Enterprise Administrator's Guide for previous versions of Scout
- The eLux NG and eLux *RL* Administrator's Guides for information on the Thin Client software.

This guide as well as other Scout documentation is available in Adobe PDF format. It can be found in the following locations:

- The documentation folder on your eLux CD-ROM
- The product documentation library at www.myelux.com (always the latest version!)

1.3 Scout on the World Wide Web

Unicon offers online technical support at www.myelux.com. This includes the following:

- PDF versions of the documentation
- Downloadable software
- The latest updates and hotfixes for download
- A list of supported hardware

To access the site you must complete a one-time, free registration.

1.4 What is Scout Enterprise?

Scout Enterprise is *the* Management Tool for large installations of Thin Clients or PCs running the operating systems eLux® NG, eLux® *RL* or Windows® CE, XPe/WES7. For installation of Scout Enterprise only small storage space on standard PC or Server architecture is needed. The administrator can manage the clients on 4 levels - firmware, device configuration, server connectivity and online commands. By supporting databases Scout Enterprise provides the default interface for data storage, allowing a smooth backup or recovery and optimizing scalability and performance. Domain users can be established as administrators, whose rights, such as access to certain organization units, can be set according to their responsibilities and tasks.

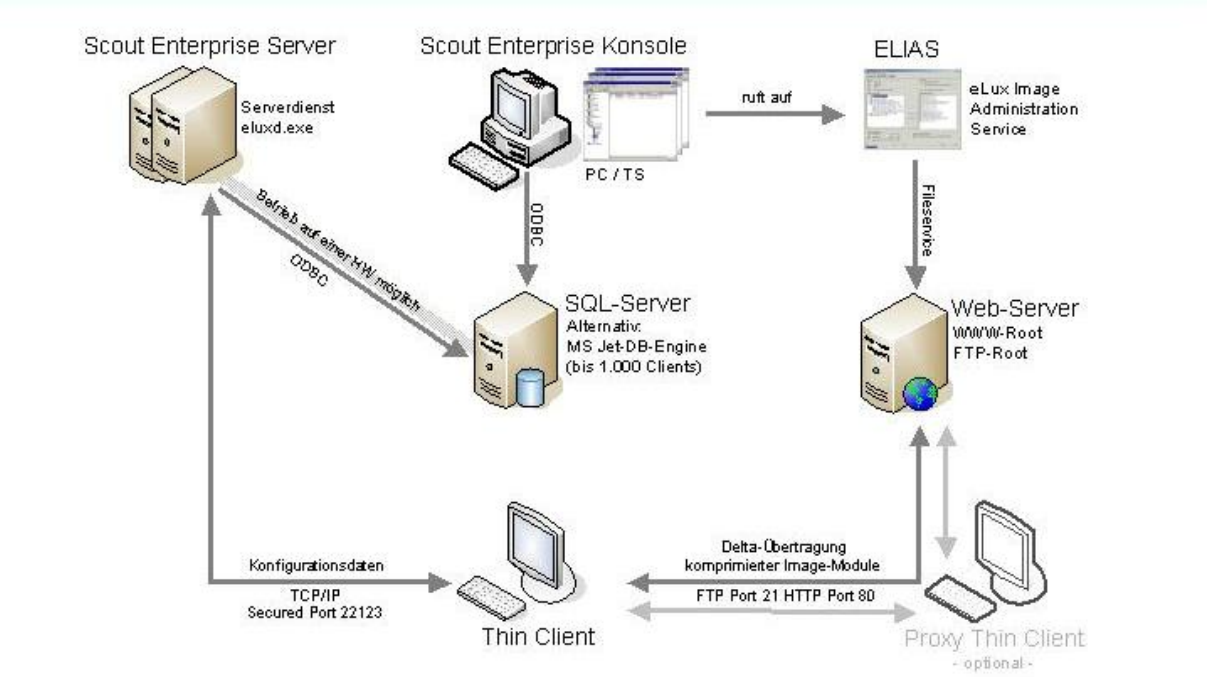


Figure 1: The Scout EnterpriseConcept

The Scout Enterprise software consists of the following components:

- **Scout Enterprise Server** The central component is a database that contains information on the devices currently being managed, their configuration, scheduled commands, past updates, and licenses. Generally, there is one instance in a network or network segment. The Scout Server service uses the database and runs constantly. It can support multiple administrator sessions (an administrator session is described below).
- **Scout Enterprise Console** Interface used to make changes to the Server. Can be installed on the same machine or on a remote machine. For security reasons, there are two sessions available: Administrator, which can make changes to the Server configuration; and Guest, who has help desk functionality and can enter licenses. Can be installed on multiple machines.
- **Container** Not just any software can be installed on the device – the software must be compatible with eLux. The container is a collection of software that can be installed on the terminal. With **eLux NG**: It is hardware-specific, which means every hardware platform has its own container. With **eLux *RL*:** there is only one container for every hardware platform!

ELIAS - eLux Image Administration Service - is available to owners of Scout Enterprise and allows the administrator to customize the software installed on the device to exactly satisfy end-user requirements. It is installed using the Scout Enterprise installation program, and is decribed in detail in this manual.

However, you can create your own packages – for example, to install a specific driver – using the **eLux Builder Kit** (EBKGUI). Advanced Linux knowledge is required. More information on this product as well as a user guide is available at the Web site www.myelux.com

1.4.1 Communication between Thin Client and Scout Server

It is **only** during the start of a Thin Client that this connects to its Scout Manager asking for new configuration data.

There are 3 options:

1. Thin Client reaches the Scout Server. The Scout Server has no new configuration data. Thin Client continues booting with the settings available so far.
2. Thin Client reaches the Scout Server, Scout Server reports new configuration data and transfers these to the Thin Client. If required, the Thin Client will restart with the new configuration.
3. Thin Client does not reach Scout Server, e.g. because of network or server problems, which results in a management timeout (see Configuration – Network > Advanced). The Thin Client keeps the latest stored settings.

During the operation of a Thin Client no data are exchanged between Scout Server and Thin Client . During the shutdown of the Thin Client it reports its status to Scout.

Exception: VPN Connections, see chapter 3.16 VPN.

1.4.2 Scout Functionality

Scout Enterprise offers the following features:

- **Easy Installation** The minimum requirements are described in chapter 2.1 System Requirements.
- **Silent (unattended) Installation**: The installation procedure is recorded and can be run at any time. For further information see chapter 2.8 Silent (unattended) Installation.
- **Easy device entry** Either remotely from Scout Enterprise Server (Client Discovery"), locally on the client (Reverse Discovery"), or automatically by configuring DNS server settings (ScoutSrv") or DHCP server settings (DHCP server vendor options"). Additionally, it is possible to customize the group list sent to the terminal during **First Configuration**, or set the Wizard parameters to the Scout Enterprise Server (SmartSrv").

- **Multiple Administrator Policy** Domain users can be added as administrators. Individual rights are set corresponding to their responsibilities and tasks. See chapter 10.
- **Database Support** By default we use the JET Database Engine (MDB) included in Windows; options are: Microsoft® SQL Server or MySQL® Server.
- **Application management** Applications can be easily created for an individual user or inheritedfrom the global application list, reducing configuration time for the administrator.
- **Easy firmware management** The firmware installed on the device can be automatically updated using the update scheduler.
- **Customizable scheduler** Schedule commands to occur at specific times and frequency. This reduces the impact of planned maintenance or configuration changes.
- **Licenses** Automatic software license distribution.
- **Security** Support of authentication servers during logon, including LDAP and ADS. This provides greater system entry security into networked environments by limiting user access to the system. In addition, password-protected groups to restrict unauthorized configuration access in the First Configuration Wizard. An essential objective of management is to prevent end users from making incorrect configurations. You can use Scout Enterprise to limit user rights. Smart card support for local authentication, user roaming, and Citrix ICA logon. SSH and virtual private networks are supported.
- **User variables** In conjunction with an authentication server, using user variables allows for configuration consolidation, reducing configuration time for the administrator and simplifying the configuration overall.
- **Hierarchical Structure** The managed clients are assigned to organization units on different hierarchical levels, thus replacing the former structure of locations and groups. Each organization unit contains applications and devices. Furthermore, Scout enables to set a global base configuration, global applications and the standard unit Lost&Found.
- **Server Transfer** In case the server hardware has to be replaced, just copy the database file and insert it to the installation directory of the new Scout Enterprise Server. You can be sure that all devices and their configurations as well as the licenses are available as before. To verify, please consult our separate Paper "**Scout – Migration & Server Transfer**" on www.myelux.com
- **Language** The console language can be changed from German to English directly in the Console, which avoids having to reinstall the Server.
- **Recovery Settings** The TFTP server, an integral component of the recovery procedure, can be configured using the Scout Enterprise Console. This avoids errors that can occur when the TFTP server configuration file is edited by hand and annoying troubleshooting during the recovery procedure.
- **Remote control of devices** For example, for scheduling maintenance or firmware updates.
- **Device monitoring** Display of remote device status (on/off, initializing desktop, performing update)
- **Troubleshooting** Access to update log for devices, Scout Enterprise Console and Scout Enterprise Server logs, adjusting default time-out values (update, device entry, time to contact manager, time to contact printer), factory reset to remotely delete the configuration and all locally-saved files, recovery installation to reformat the flash card or hard drive.
- **Help desk features** Interactive, real-time mirroring capabilities and sending messages to users.

2 Installing Scout Enterprise

2.1 System Requirements

The Scout Enterprise Server and Scout Enteprise Console both have the following minimum system requirements:

- Microsoft Windows Server 2003 SP1 or higher
  Windows XP Professional or higher
- 50 MB disk space
- Database System, e.g. the JET Database Engine (MDB) included in Windows; optional: Microsoft® SQL Server or MySQL® Server.
- You must have administrator rights on the PC and be connected to a TCP/IP network.

The container has the following requirements:

- FTP or HTTP server with write access, installed locally or available on a network drive
- Space requirements vary depending on the container for the hardware platform that is being installed and the software that is currently available for that container. Minimum for all containers at the time of publishing: 700 MB.

2.2 System Restrictions

No system restrictions are known for Scout Enterprise Server and Scout Enterprise Console. Other services, such as Citrix XenApp, can be running on the same PC.

For convenience, to view the server log, the Scout Enterprise Server and Scout Enterprise Console must be installed in the same directory.

2.3 Database Support

Scout Enterprise requires a database software. Using the Microsoft® JET Database Engine, no other database software is needed. The Microsoft® JET Database Engine is included in the operating system since Windows 2000. During installation Scout Enterprise then automatically creates the database file with the extension .mdb. Any file name can be assigned.

Alternatively, the database software Microsoft® SQL Server or MySQL® Server can be used. In this case the database must have been installed before. As above, the file name is arbitrary.

We recommend these database and driver versions:

- Microsoft SQL Server 2000 or higher
- MySQL Server for Windows V4.1.12a or higher
- MySQL Server for Unix V3.23.52 or higher
- My ODBC 3.51.11-1 (ODBC driver for MySQL)
- Microsoft Access (MDB)

Required memory space for the Scout database is 50 MB per 1,000 devices.

Starting with Scout Enterprise Version 9 there ist a **Database Connection Editor** integrated in the start menu, which allows you to define various database connections for the Scout Enterprise console. As a result one console system can connect to different databases.

The m**igration** from existing prior Scout installations to Scout Enterprise and the migration of the Jet Database Engine to Microsoft SQL Server 2000 as well as the procedure for **Servertransfer** is described in a separate manual **"Scout - Migration and Servertransfer"** in the download area "Manuals and Documentation" on www.myelux.com.

Note: In the setup > database dialog the name of the database can be entered now. That means that the database name need not necessarily be 'ScoutNG'.

When using MS-SQL as database type during setup, you can choose between the authentication method SQL-Server authentication and the Windows authentication.

SQL-Server authentication means:
User name and password to be entered must refer to a SQL-Server user.

Windows authentication – also called 'Trusted-Connection', means:
A program always logs on to the current 'credentials' SQL-Server.
No user or password are entered for the the logon to the SQL-Server.
However, in this case the Scout Enterprise service must be run within a specific user account.
Otherwise the service would run under the local system account which usually does not have the authorization in the SQL server.
The user name and password of the service accoung may also be entered in the dialog.

In addition there are two 'Browse' buttons which serve to show a list of the available SQL Server rsp. the available databases for you to select.

During setup the option 'Manuals' is stored in the Scout Enterprise section in the Windows start menu. Select from the available manuals.

2.3.1 Scout–Cluster

If Scout Enterprise uses an SQL or MySQL database, multiple servers can work on the database at the same time. Each server sends a list of all servers entered in the database to the clients, so that the Scout servers can be changed dynamically.

The clients must have the eLux NG BaseOS Version 1.24-1 or higher

2.3.2 Application Roles in MS SQL Server

In order to limit the authorization of the console to access the SQL Server tables, it is possible to define an MS SQL application role.

The name of the application role must be entered into the table "system" in the ScoutNG database.

Add a line with the ParamName='RName2' and ParamVal='<name of the role>' .

Add a line with ParamName='RPass2' and ParamVal='<password of the role>' .

During the start of the console these fields are read first and the applications role is set.

2.4 Encryption

The encryption between Scout Server and the eLux clients is based on the AES (Advanced Encryption Standard).

The clients must have eLux NG BaseOS Version 1.24-1 or higher.

Should a firewall be installed, Port 22123 must be unlocked.

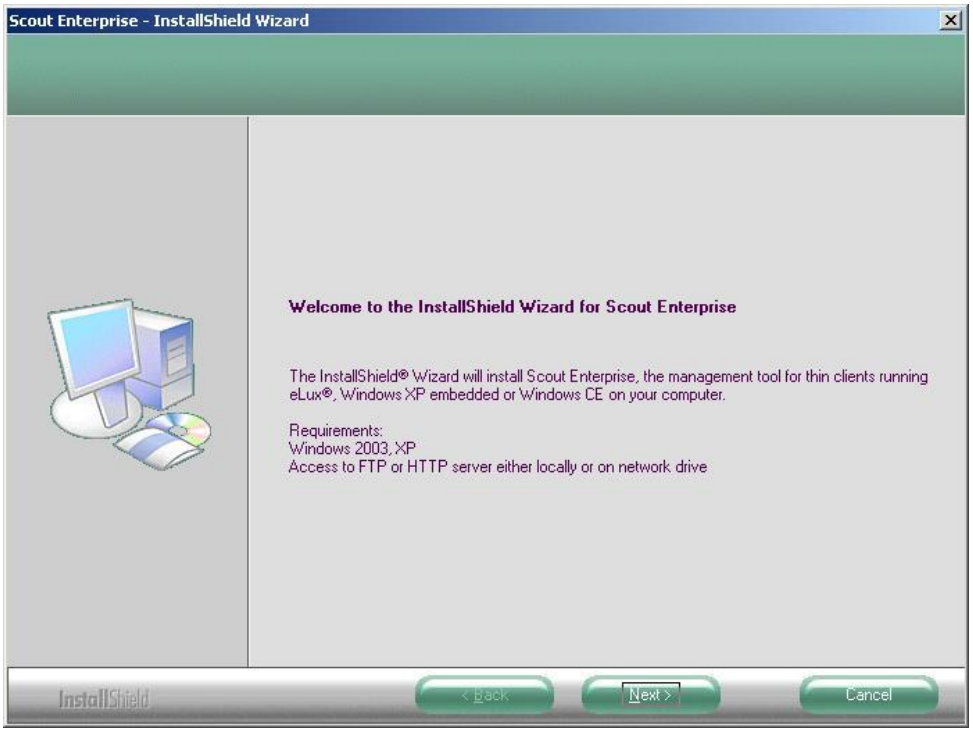
2.5 Installation Procedure

The Scout Enterprise setup program is available on the eLux NG rsp. eLux RL CD-ROM or can be downloaded from the Web site www.myelux.com.

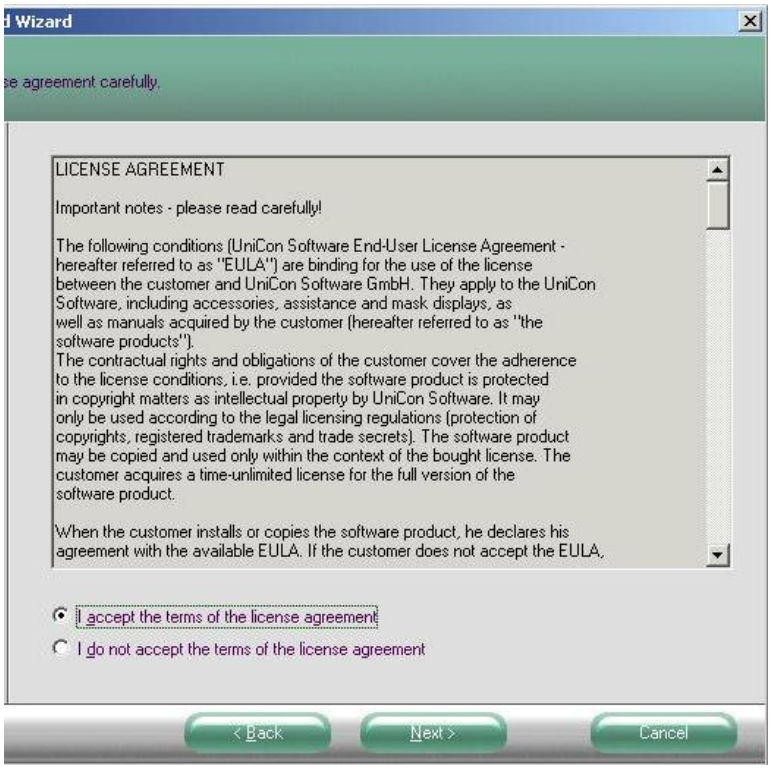
To begin the installation procedure, log on to your PC as administrator. If you are using a terminal server, please run the setup program from the applet **Add/Remove programs** in the Control Panel.

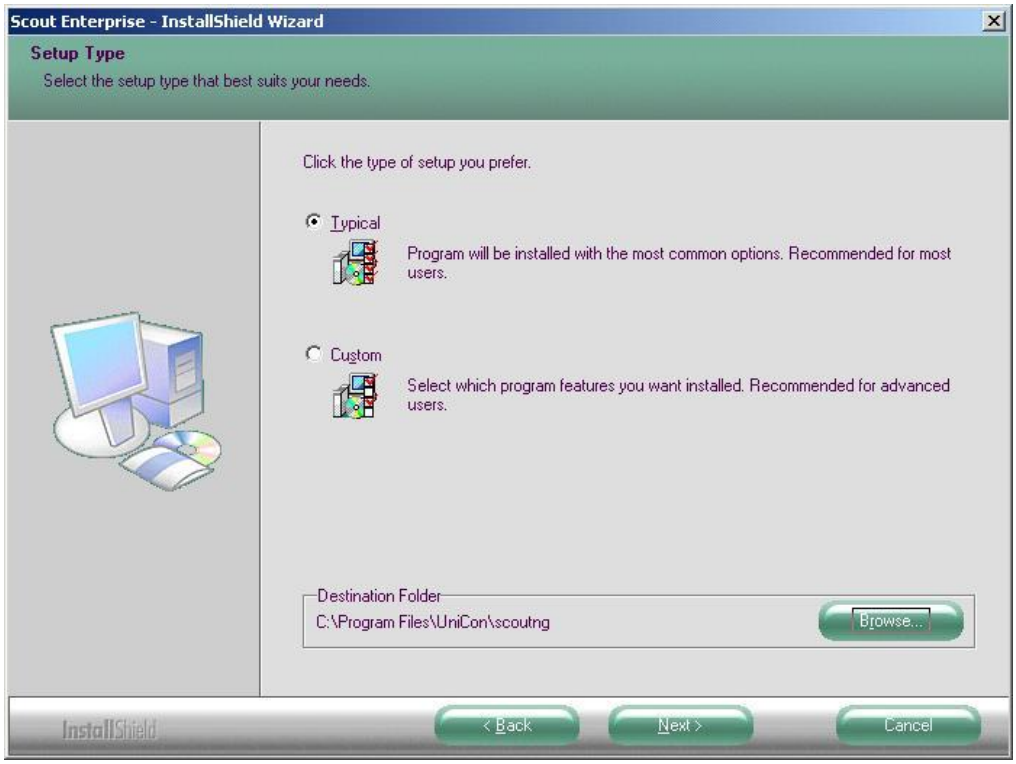
Choose the language you want for the installation procedure. This will also be the default language of the Scout Enterprise screen elements.

The InstallShield Wizard guides you through installation.



Please read the license agreement and accept the terms to continue.





1. Click **Typical** to install the three standard components mentioned above. All containers will be installed. You can also set the installation directory for Scout Enterprise (by default, c:\Program Files\Unicon\scoutng).
   To install a specific container only, click **Custom**.
2. Choose the type of server that will be used to access your container.
3. Enter the path of the FTP or HTTP server root directory (either locally or on a network drive) and the fully qualified URL to access the server (format: `[ftp/http]://<host>`). In addition, for FTP enter the logon information (anonymous" FTP is supported). Examples:

   HTTP server root directory.....\\server1\Inetpub\wwwroot\

   URL .....http://work.domain.com

   FTP server root directory ..... c:\Program Files\Inetpub\ftproot

   FTP..... ftp://ftp.domain.com

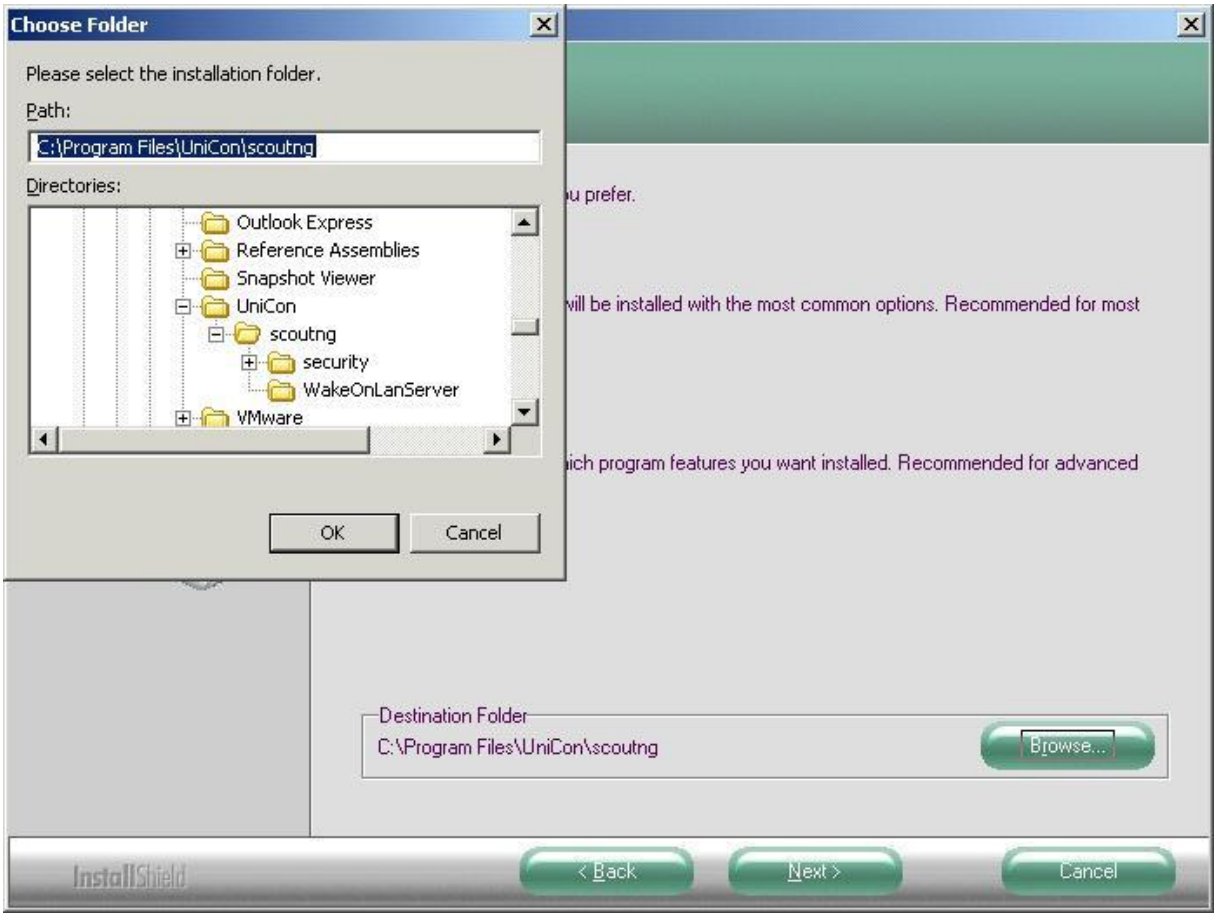
   User name..... anonymous

   Password..... eluxng@domain.com

   The setup program then attempts to verify the values you entered. Note: This may result in a delay – please do not click during this time.

   If there are problems contacting the server, an error message appears and you are prompted to change your parameters.
4. If the server was successfully reached, a summary of the components to be installed is displayed. Click **Next** to start copying files.

Select the installation folder:



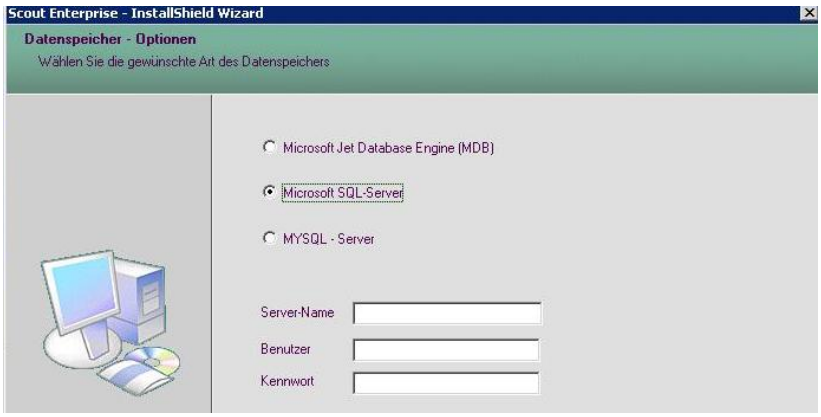
In the database option dialog please select on of the following databases:

- Microsoft Jet Database engine (MDB)
- Microsoft SQL Server
- MySQL Server.

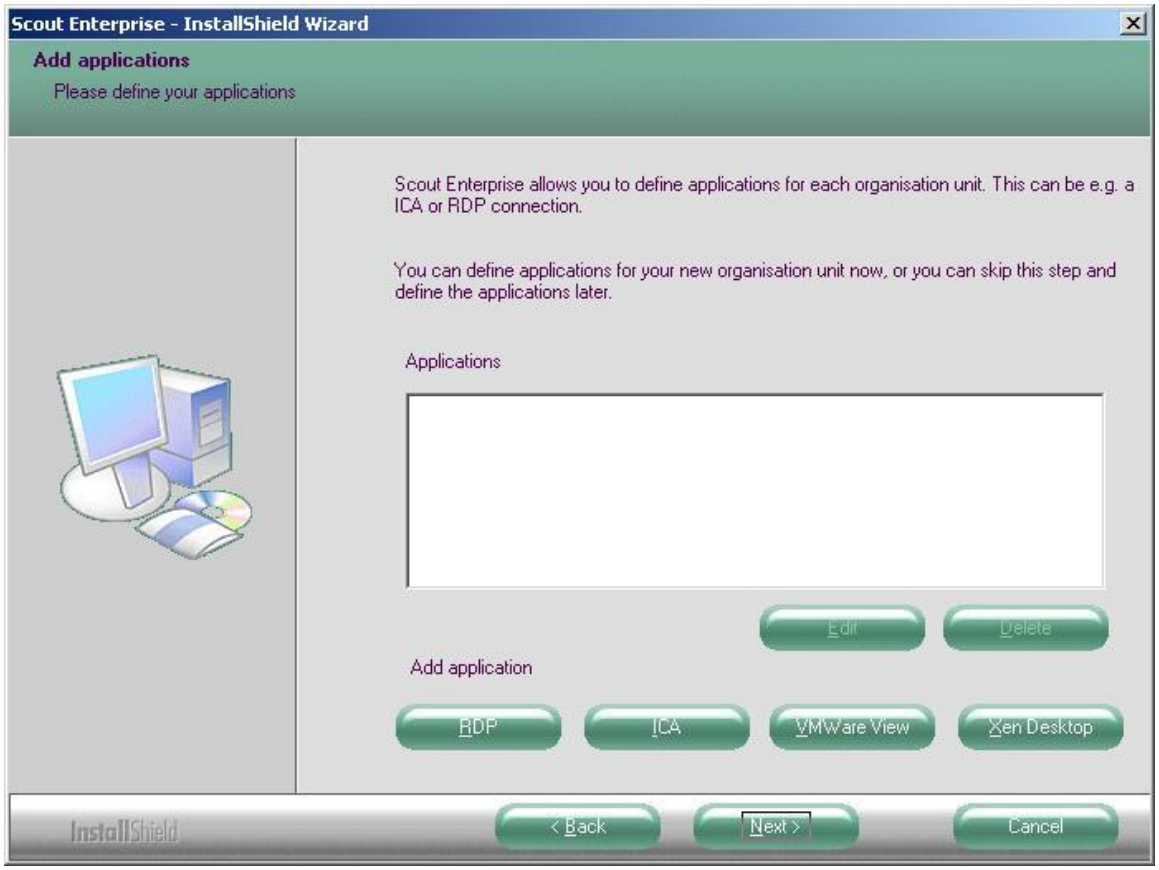
When choosing the Microsoft Jet Database engine (MDB) no further action is required.

However, when selecting Microsoft SQL Server or MySQL Server

- enter server name and a user who has access to the database,
- create an empty database named ‘ScoutNG’.



The next dialog offers to define applications, if you like.



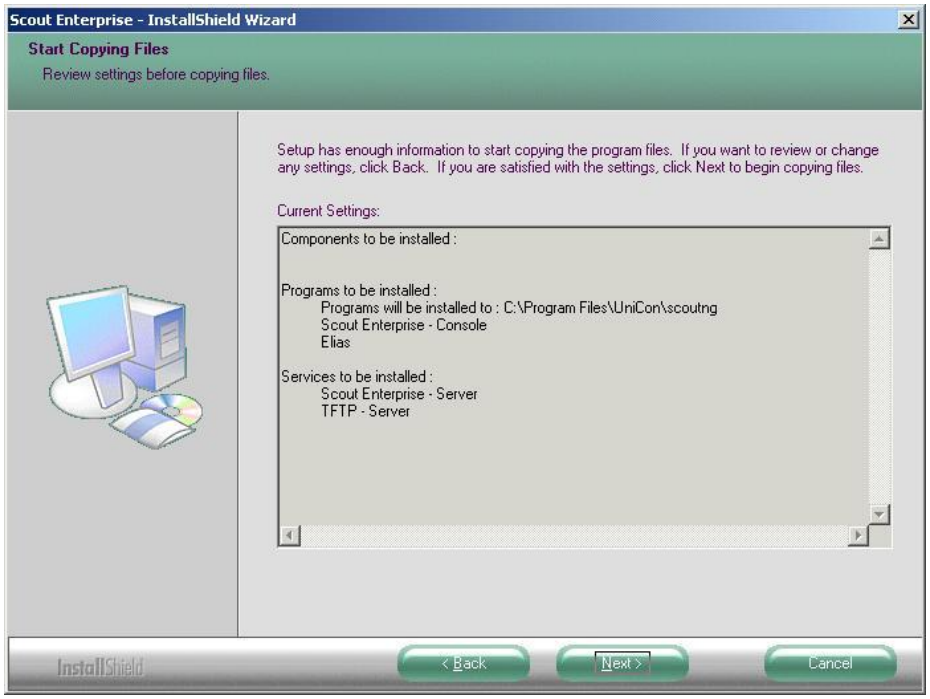
Defining a **RDP** application

Defining an **ICA** application

Defining a VMWare View application

Defining a XenDesktop application

The settings are displayed for checking purposes, click **Next** to start installation.



After the successful installation leave the wizard by clicking **Finish**. The Scout Enterprise console can be launched directly.

2.6 Changing installed Components

After installation, you can run the setup program at any time to change the components that are installed. Click **Modify** to add or remove single program components. The old setup program will be used. Click **Repair** to update the software.

2.7 Uninstall

To uninstall Scout Enterprise, click **Add/Remove Programs** in the Windows Control Panel. A list of installed software is displayed. Scroll down and highlight Scout Enterprise. Then click on the **Change or remove programs** button and follow the directions in the dialog. All program files are deleted.

2.8 Silent (unattended) Installation

In the first step the installation of Scout Enterprise must be recorded.

⇨ Recording the installation:

Initiate the install program by entering the following parameters:

`setup.exe /r /f1<Dateiname>`

- Parameter /r initiates the record mode of the installation.
- With the parameter /f1 you define the file the recorded data are to be saved in.
  z.B.: `setup.exe /f /f1C:\temp\scoutngsetup.iss`
- If parameter /f1 should not be defined, a file `setup.iss` will be created in the Windows directory.

⇨ Performing the silent installation

Start the install program with the following parameters:

`c:\>setup.exe /s /f1<Dateiname>` (c: is exemplary)

- Parameter /s initiates the execution of the installation (silent mode).
- Parameter /f1 is the same as during the recording of the installation.

3 Management on the Setup Level

This chapter contains information on how to set the Thin Client's desktop, hardware, network and security settings. This is done using the tabs in Setup.

3.1 Introduction

Scout Enterprise software organizes Thin Clients (devices") hierarchically. You can group individual devices into Organisation Units .

By default the global Setup, or base configuration, is applied to new devices that have not yet been configured. Elements can refer to the Setup of the next higher element in the hierarchy, the parent,or they can have an individualized Setup.

Locations, organization units and individual devices can be assigned individualized Setups. In addition, the "Use Parent" feature allows you to turn an individualized configuration off and revert to the base configuration, providing flexibility.

Organisation units and individual **devices** can be assigned individualized setups. In addition the Use Parent" feature allows you to turn an individualized configuration off and revert to the base configuration, providing flexibility.

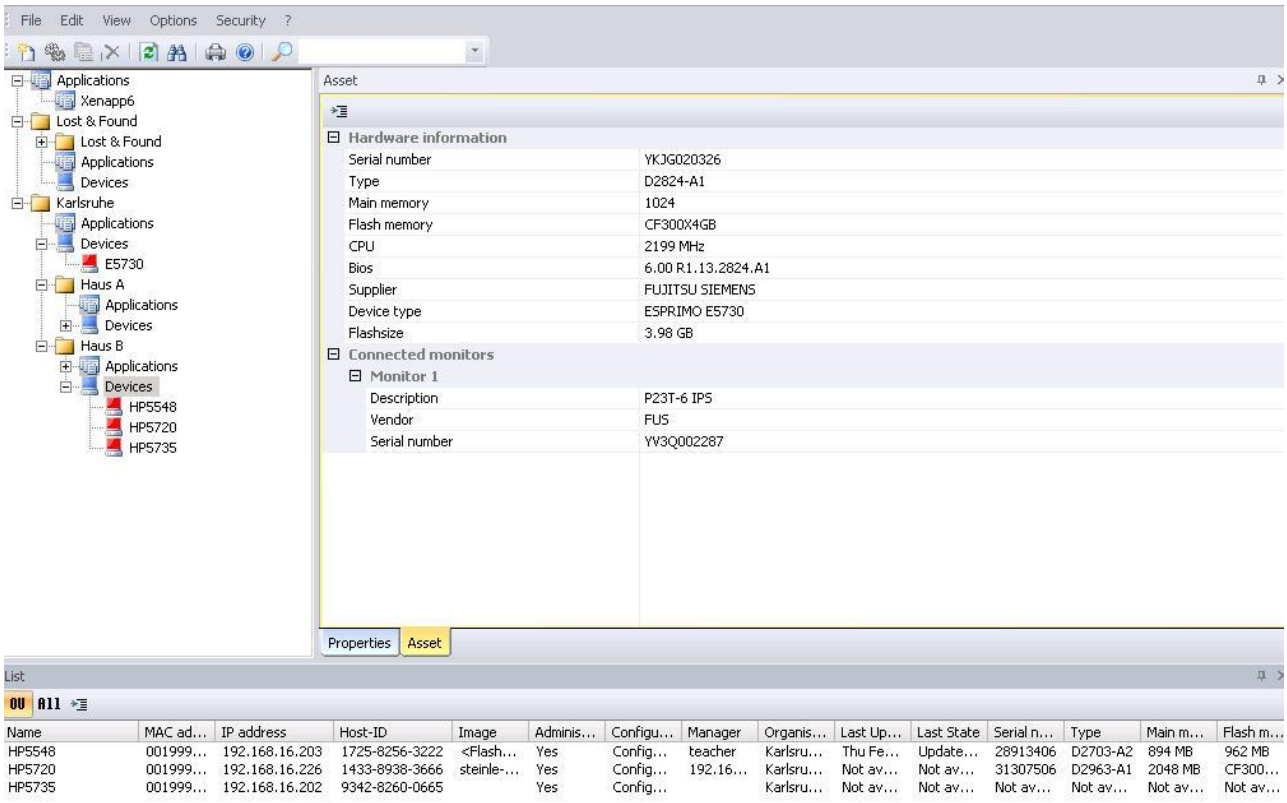


Figure 2: View > Main Window incl. List view and Asset window

- In the **View** menu → **Settings** you can define the time in seconds to refresh the display of the status of all visible devices.

If the two parameters are disabled the refreshing of the display can be initialized directly on the console. by the shortkey CTRL-F5 thus refreshing the display of the visible devices. By pressing the F5 key the display of all devices is being refreshed.

Further the dialog **Settings** in the **View** menu offers the option to **Check independent configurations**. This option checks for all subordinate, independent configurations after a configuration has been modified. The independent configurations will be shown in a dialog and you have the choice

- not to apply the modifications to other orginazation units,

- to apply the modifications to all independent configurations,

- to select individual configurations which the modifications are to be applied to.

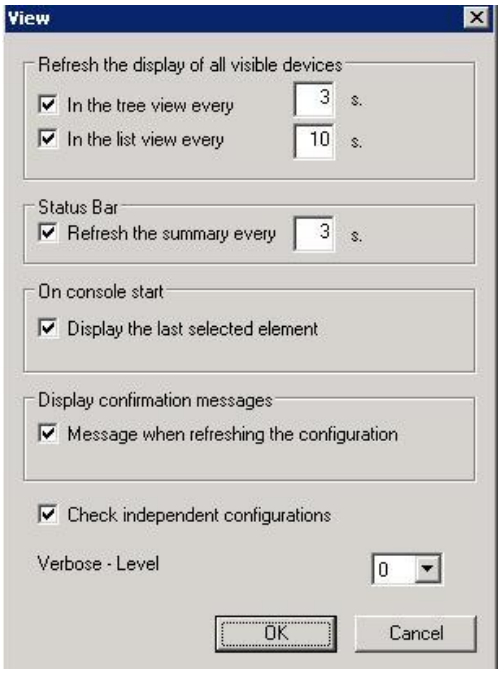
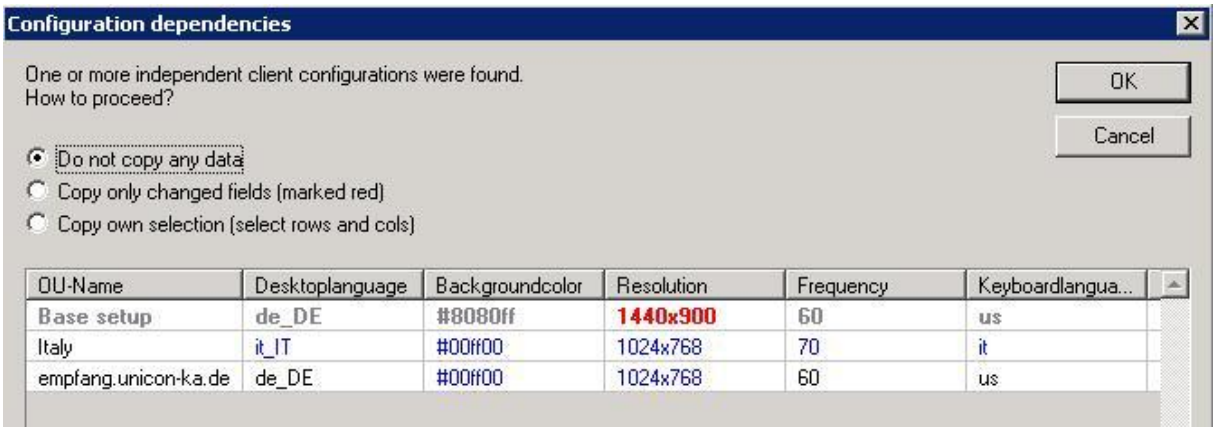


Figure 3: View → Settings



Note: This can only be done directly after the modification of a configuration.

Updating Locked Fields

Normally, when the configuration has changed in Scout Enterprise, the entire device configuration will be sent to the client the next time the client boots.

If tabs have been blended out, either for security reasons or to prevent the user from configuring them locally (see section 3.4.1), it is possible to update the locked tabs only.

In the **Options** menu, select **Advanced**. The **Advanced options** dialog box appears.

In the Update of fields area, click to select Only locked fields are updated on the client.

The next time the desktop configuration is sent, only the locked tabs will be updated. The local configuration the user has made in unlocked tabs will not be overwritten.

3.2 General

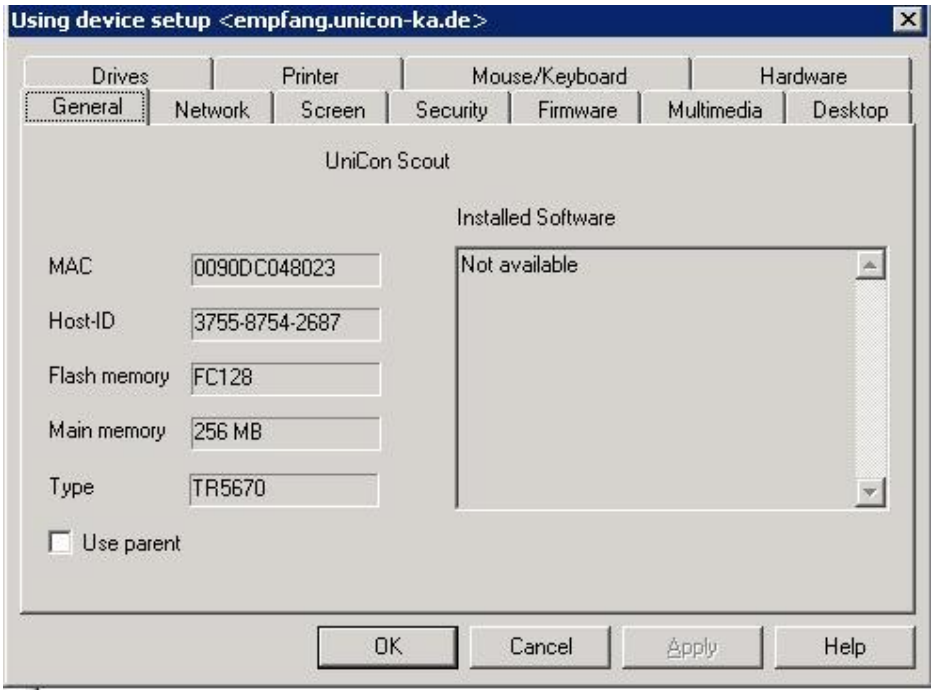


Figure 4: Setup > General tab (individual device)

The **General** tab lists hardware information, as shown in the figure above. Because this information is device-specific, it is only displayed in the individual device Setup.

- **MAC address** The hardware Media Access Control address of the device.
- **Host ID** Host ID assigned to the device. This is required for the eLux NG licensing procedure.
- **Flash memory** A short description of the flash local storage type and size.
- **Main memory** Size of the main memory in megabytes.
- **Type** Product description as set by the hardware supplier (a string).

In addition, the **General** tab contains **Use parent.** Select this check box to use the Setup of the next higher element in the hierarchy: The individual device will refer to the Setup of thenext higher organisation unit and so on.

When this check box is selected, the remaining tabs in this Setup are disabled.

Note Because network and system information is device specific, it is only displayed in an individual device Setup, and not in the Setup of an organisation unit or the base configuration.

Starting with Scout V 12.x and eLux RL 3 the configuration of network profiles offers more flexibility.

In earlier versions only 1 network profile could be defined at a time, now different profiles can be configured simultaneously, e.g. Ethernet, WLAN, UMTS. The profiles are available at the client, where you can select between them easily in the systray of the client, too.

In particular, this improvement provides higher flexibility for mobile clients.

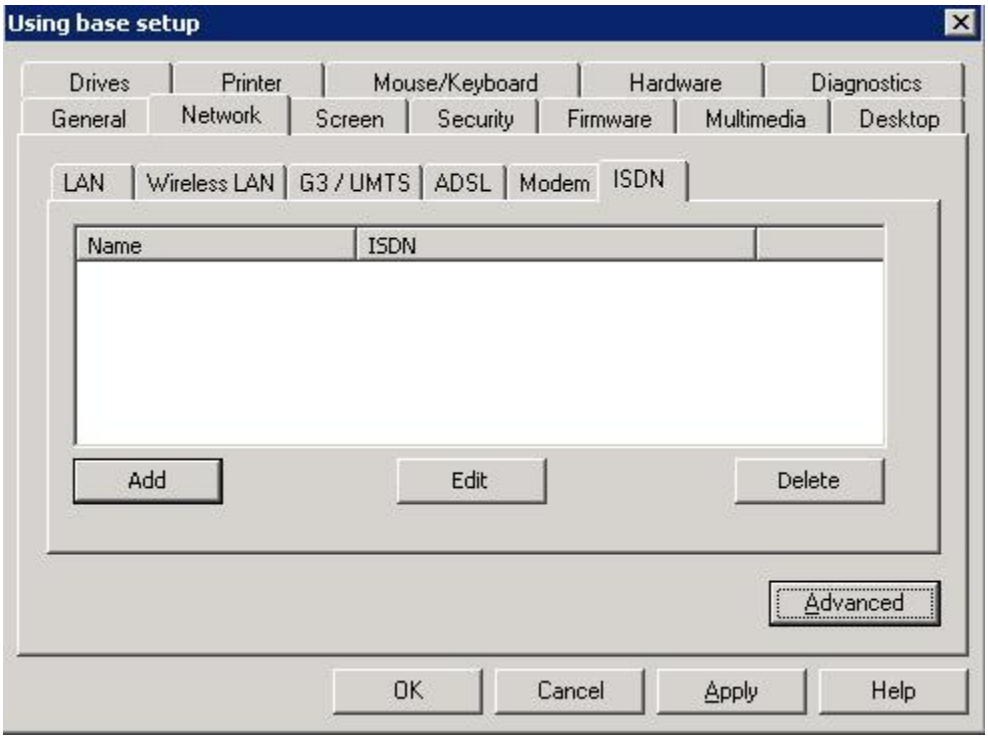


Figure 5: Setup > Network

The **Network** tab consists of the subtabs

- LAN
- Wireless LAN
- G3/UMTS
- ADSL
- Modem
- ISDN

Each can be created by clicking the **Add** button, can be edited (**Edit** button) or deleted (**Delete** button).

3.2.1 LAN

If you install an external Ethernet card please deactivate the LanOnBoard function. Further, please consider that Wake-on-LAN will not work in this case.

Click your Ethernet speed from the **Speed** list.

- **1 Gbit**: Only available for the gigabit Ethernet network card Broadcom Tigon 3 (BCM570x). Other card parameters will be automatically configured.
- **BNC**: Only available for 3Com Combo cards.
- **AUI**: Only available for 3Com Combo cards.

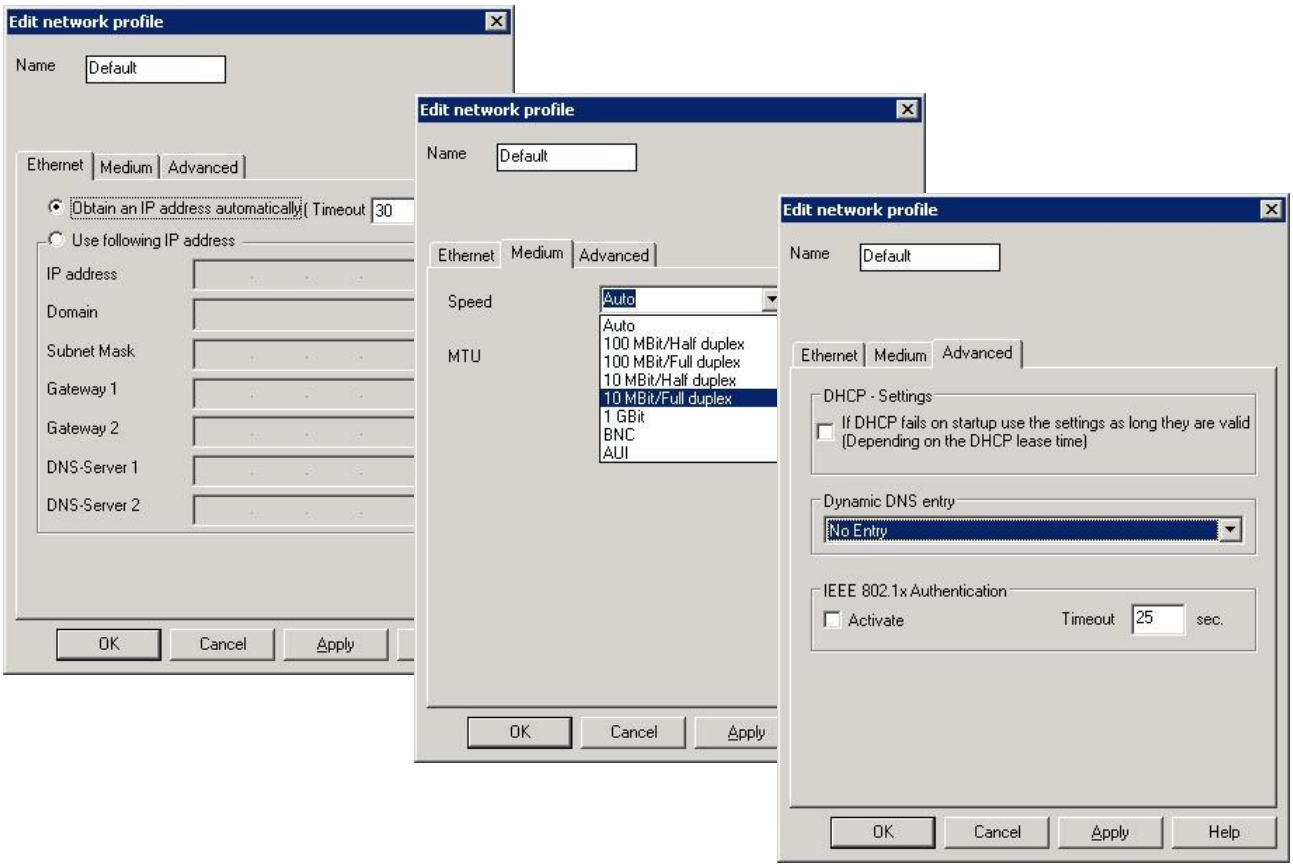


Figure 6: Network > LAN

IEEE 802.1x Authentication can be activated in the subtab **Advanced**. The subject is described in chapter 3.3.8.

A **Timeout** parameter can be entered to define after how many seconds the attempt to connect to the manager can be cancelled.

The Smardtcard domain is described in chapter 3.15 Smartcard.

3.2.2 Wireless LAN

Note:

On www.myelux.com > **eLux Software Packages** → Click the column Released Packages of the relevant client → **Supported Hardware Components** you find an up-to-date list of the Wireless LAN products which are supported by eLux.

The following settings are possible for Wireless LAN. Please check with your administrator which setting is the proper one for your environment.

(1) WEP
(2) WPA (PSK)
(3) WPA2 (PSK)
(4) WPA2 (EAP)
(5) IEEE 802. 1x (LEAP)

The fields differ depending on the defined mode.

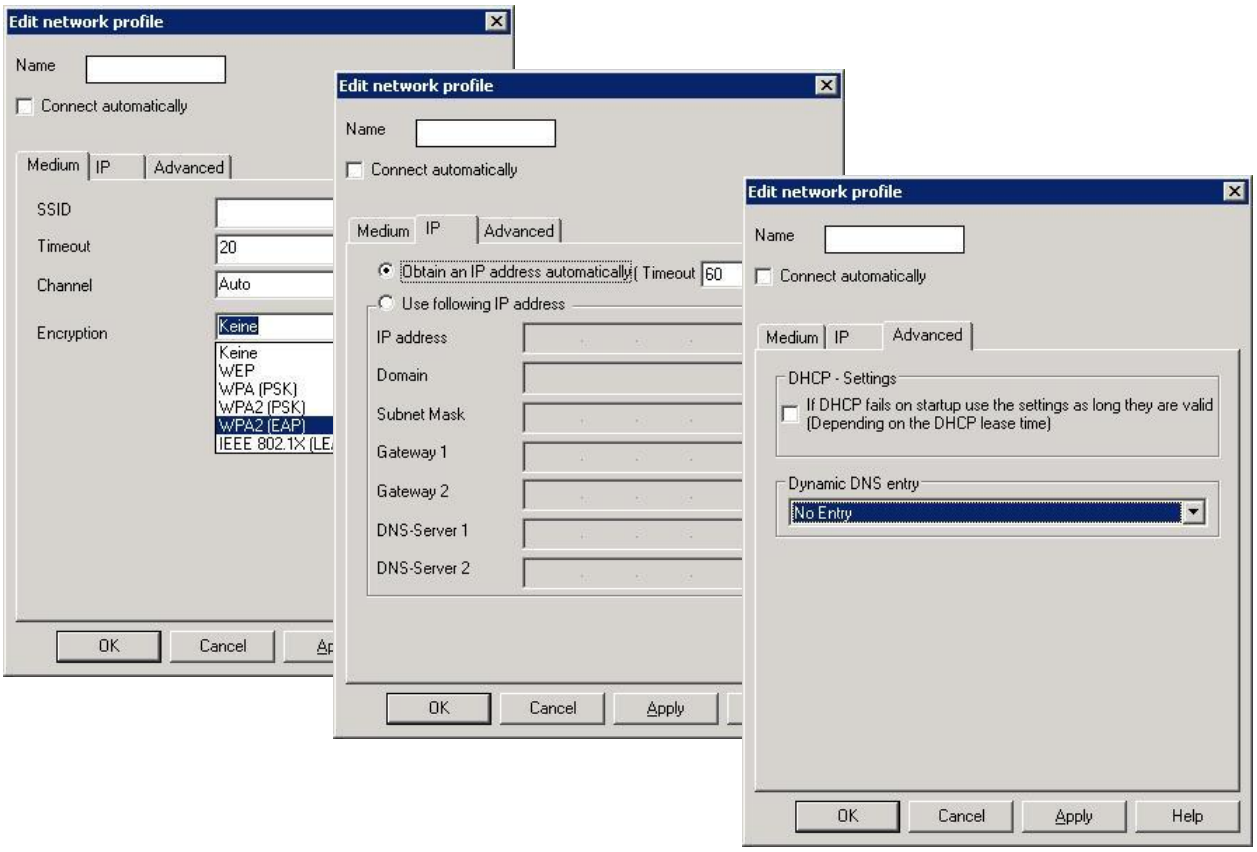


Figure 7: Network > WLAN

Dynamic DNS entry

The advanced network profile settings offer to define whether a client is to inform dynamically the name server about the name, so that the name server can issue the entry in the Forward rsp. Reverse Lookup zone.

WindowsCE Clients may issue only one entry in the Forward Lookup zone.

3.2.3 UMTS

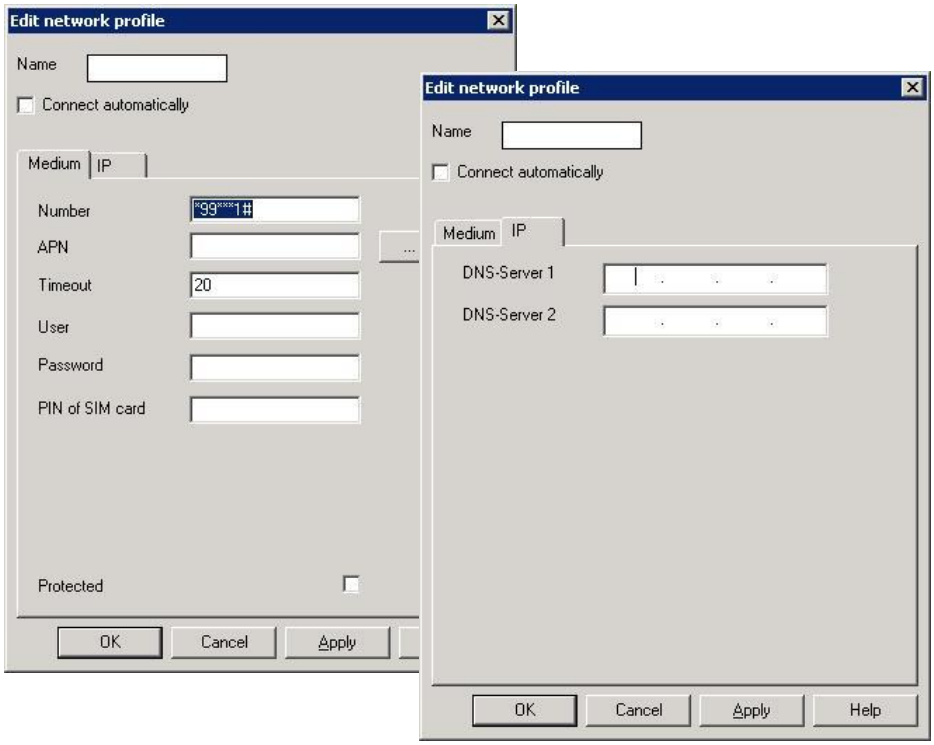


Figure 8: Network > UMTS

Name:	Name of UMTS profile, e.g. the name of your provider
APN:	Website of your provider
Timeout:	Enter a value for the idle time (in seconds). After this specified amount of inactivity, eLux disconnects the UMTS connection.
User:	user name assigned by your provider
Password:	password assigned by your provider
PIN of SIM card	The PIN assigned to your SIM card by your provider
Protected:	(optional) Security feature. Prevents the local user from making configuration changes to the profile. See chapter for more on security.

When you are done entering information, click **OK** in the **Network Profile** dialog box.

3.2.4 ADSL

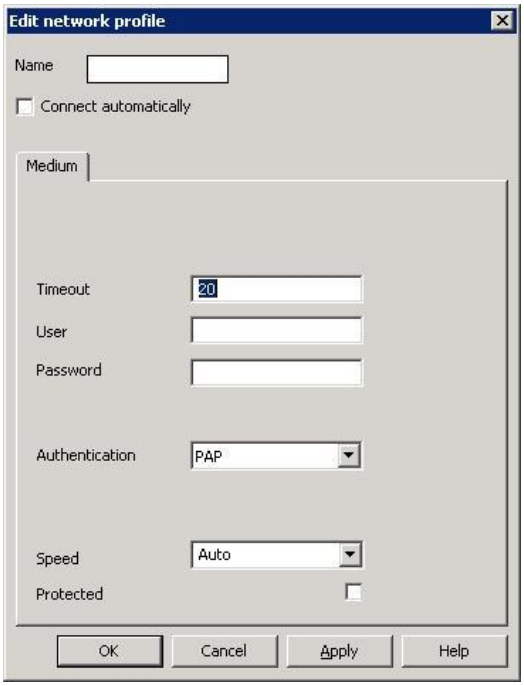


Figure 9: Network > ADSL

Click a profile from the **Profile** drop-down list. Otherwise click **Edit**. This opens the **Profiles** dialog box. Click **New** to create a new profile or **Edit** to modify an existing one. This opens the **Network Profile** dialog box.

Name:	Enter a name for the profile, such as the name of your provider.
Timeout:	Enter a value for the idle time (in seconds). After this specified amount of inactivity, eLux NG disconnects the connection.
User name:	Enter the user name assigned by your provider.
Password:	Enter the password assigned by your provider.
Authentication:	Click the method assigned by your provider.
Protected:	(optional) Security feature. Prevents the local user from making configuration changes to the profile. See chapter for more on security.

When you are done entering information, click **Apply** in the **Edit Network Profile** dialog box. Repeat until you have created / edited the desired profiles.

eLux supports dynamically changing IP addresses for ISDN, modem and ADSL.

3.2.5 Modem

Select the Modem tab and click **New** to configure the profile.

Click the baud rate of your modem from the **Speed** list. It must be greater than the actual maximum modem baud rate.

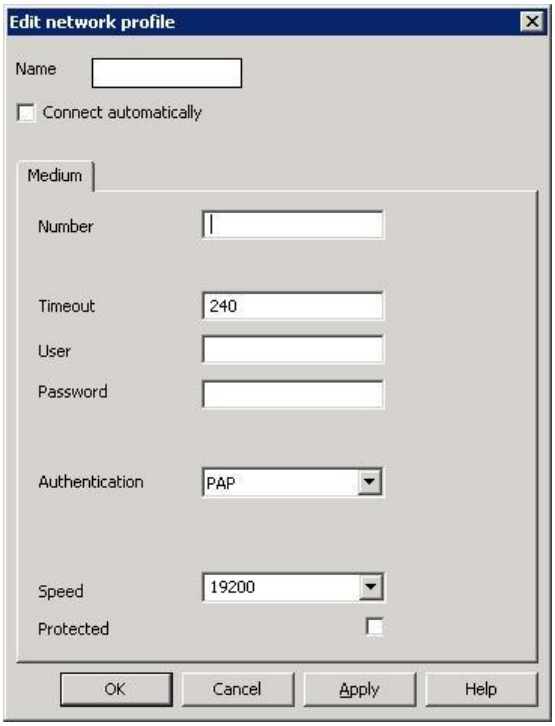


Figure 10: Network > Modem

When you are done entering information, click **Apply** in the **Edit Network Profile** dialog box.

3.2.6 ISDN

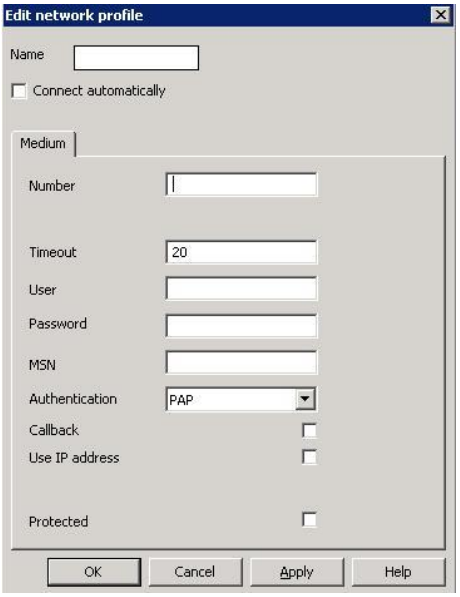


Figure 11: Network > ISDN

Click **Add** to open the dialog Edit network profile and create a new profile. Otherwise click **Edit**.

Name:	Enter a name for the ISDN profile, such as the name of your provider.
Number:	Enter the access number of your provider.
Timeout:	Enter a value for the idle time (in seconds). After this specified amount of inactivity, eLux NG disconnects the ISDN connection.
User name:	Enter the user name assigned by your provider.
Password:	Enter the password assigned by your provider.
MSN:	Multiple Subscriber Number. If you use the callback function, enter the phone number of your terminal (without the area code). If you don't use the callback function, enter zero.
Authentication:	Click the method assigned by your provider.
Callback:	Click the check box if your provider supports the callback feature (usually unchecked for commercial providers).
Use IP address:	Click the check box if your provider reserves a static IP address for your eLux NG terminal (usually unchecked for commercial providers).
Protected:	(optional) Security feature. Prevents the local user from making configuration changes to the profile. See chapter for more on security.

When you are done entering information, click **OK** in the **Network Profile** dialog box. Repeat until you have created / edited the desired profiles.

eLux supports dynamically changing IP addresses for ISDN, modem and ADSL.

3.2.7 Advanced Network Settings

Host entries:

If your network does not contain a domain name server (DNS), the Thin Client can still resolve host names locally.

⇨ To set a hosts list when no name server is present

1. In the **Network** tab click **Advanced**. The **Advanced network settings** dialog box appears.

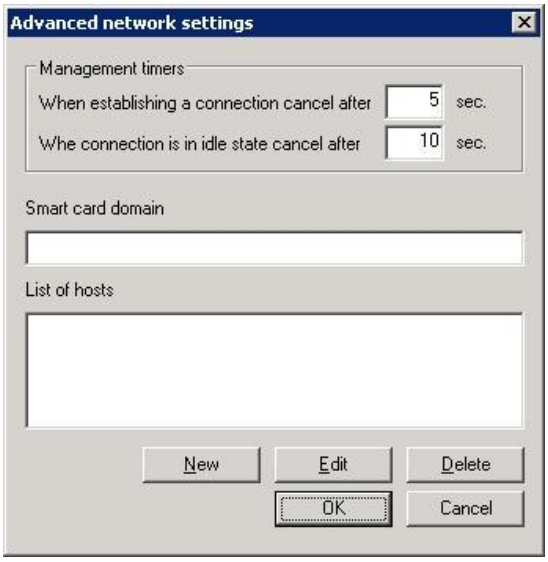


Figure 12: Advanced network settings

2. Click **New**. Enter the desired IP addresses and IP names of the hosts.
3. Save your settings.

The list is transferred to the Thin Client the next time the Thin Client starts.

3.2.8 IEEE 802.1x Authentication (Xsupplicant)

802.1x is an IEEE Standard, which specifies the port-based network access control (on level 2 in the ISO/OSI reference model) for IEEE 802 networks. The network access in 802 LANs is realised via ports (physical port in a switch). IEEE 802.1x enables to protect the network from being accessed by illegal devices by means of controlled ports and the authentication to a RADIUS server implementation (RADIUS = Remote Authentication Dial-In User Service).

IEEE 802.1x Activation

Installation of the Xsupplicant Firmware

Using the XSupplicant service requires the eLux RL Base-OS Version 2.6.0 or higher. Proceed as follows to install the xsupplicant functionality:

- Start ELIAS and add the following software package to your image definition file (idf):
  - **Xsupplicant Version >= 1.2.8.1-1**. Activate this package.
- Save the idf and exit ELIAS.
- Install the software at the Thin Client by performing a firmware update with the idf just modified.

Activating the Xsupplicant package

Go to the Setup tab of the eLux® *RL* control panel and open the tab **Network > Advanced**.

Enable the **Activate** checkbox in the area **IEEE 802.1x authentication**. Click **OK.** Back on the **Network** tab click **Apply**. The client needs to be restarted.

The configuration file xsupplicant.conf
xsupplicant is configured in the file /setup/xsupplicant.conf.
Within the file parameters such as the type of authentication, transfer of user names, EAP settings and the path for the certificates can be defined.

Management of 802.1x
During the initial installation certificates are distributed in a separate, privat, non-secured network ("quarantine" network).
For this purpose Standard or Vendor Tags (VendorID = ELUXNG) are defined on the DHCP server. These serve to transfer the requested certificates and configurations to the client. Requirement: Microsoft IAS Server.

1. These are the tags to be defined:

Standard Tag 226 / Vendor TAG 6
CERT_URL, enter the URL for the user certificate,
e.g. http://www.mydomain.com/cert/TC__MAC__/.pfx
When exporting the certificate the private key must also be exported to create a .pfx file. This format will automatically be converted to the PEM format required by eLux. Alternatively the PEM format can be used.

Standard TAG: 227 / Vendor TAG 7
XSUP_CONF: enter the URL for the xsupplicant configuration.
A template is availabe on every eLux client in /setup/xsupplicant/xsupplicant.conf.cert,
e.g: http://www.mydomain.com/cert/xsupplicant.conf
Example:

```
network_list = all
default_netname = default

logfile = /tmp/xsupplicant.log

default
{
  allow_types = all
  identity = "__IDENTITY__"
  force_eapol_ver = 1

  eap_tls {

    user_cert = /setup/cacerts/TC__MAC__.pem
    user_key  = /setup/cacerts/TC__MAC__.pem
    user_key_pass = "__PHRASE__"

    root_cert = /setup/cacerts/root-ca.pem

    chunk_size = 1398
    random_file = /dev/urandom
    session_resume = yes

  }
}
```

You can use the following macros in the configuration file to make it valid for all clients.
__MAC__ for the MAC address
__IDENTITY__ the identity if the Windows account name
__PHRASE__ the password for the private key as defined during the export of the PFX file.
The macro __MAC__ may also be used in the identity TAG.

Standard TAG: 228 / Vendor TAG 8
CERT_PHRASE: the password of the PFX file is stored here.
The password may be the same for all tags and only serves to import the certificate.

Standard TAG: 229 / Vendor TAG 9

XSUP_IDENTITY: the Windows account name is entered here.

e.g. TC__MAC__@mydomain.com. Also, the __MAC__ macro can be used here. If a Radius server should be used in Linux, the identity corresponds to the CN of the certificate.

Standard TAG: 230 / Vendor TAG 10
ROOT_CERT: URL with the Root CA certificate
e.g. http://www.mydomain.com/cert/root-ca.cer.
Since the Root certificate does not include a private key, the default Windows format can be used.

2. Initial installation

Once all the TAGs have been defined, during the first boot of a new client the data are loaded, converted and imported. Then the client is prepared for the oepration on a 802.1x Switch and is switched off. The basic configuration (ex-factory) remains with the client. The certificates and the 802.1x configuration remain stored even after a reset to the factory configuration.
All certificates must reside on the web server for every client. If errors occur during this procedure, a message will appear and the client is shut down. To repair the error so erscheint ein entsprechender Hinweis und der Client schaltet sich nicht wieder ab. For troubleshooting the client is to be restarted completely and must be reset after the detection and correction of the configuration error.

3. Operation

The client can now be run on the productive network. Authentication is performed via 802.1x and – if successful – the First Configuration Wizard appears.

4. Update

The configuration is verified during each boot procedure, i.e. all TAGs are checked for modifications and ,if necessary, the configuration is recreated. All files are being synchronized with the web server, whereby only the date of the file is verified.

The certificates must be renewed on the web server in due time. Approximately 8 days before expiration of the certificates a message appears. This period of time can be set in the termina.ini via Scout Enterprise.
[Network]
Dot1xDays=8

3.3 Screen

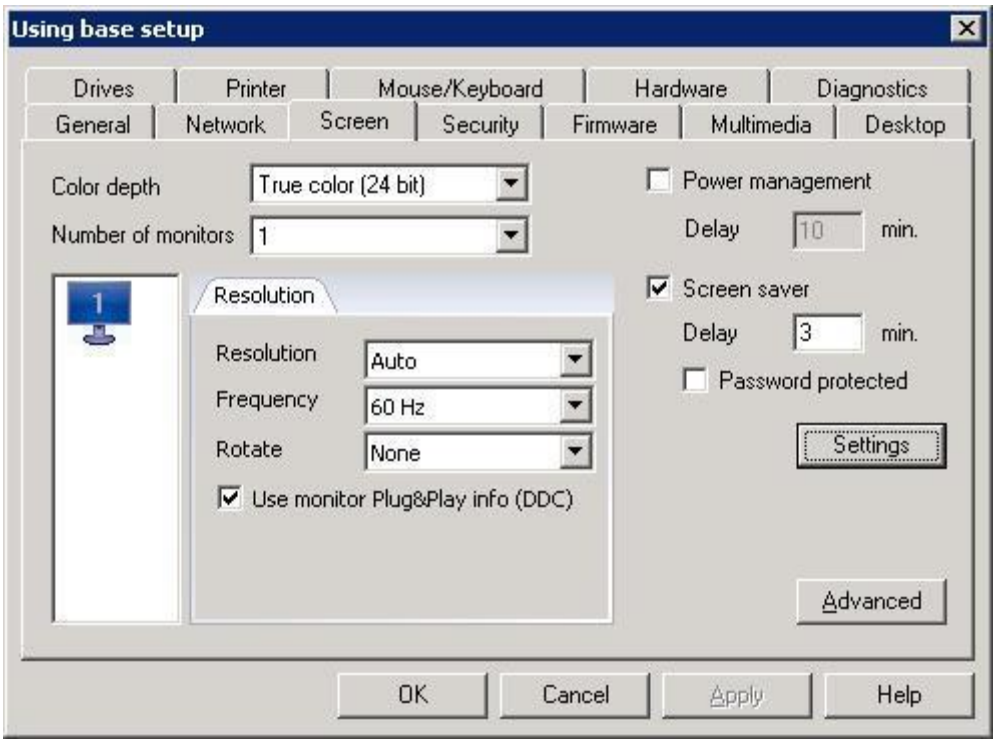


Figure 13: Setup > Screen

Use the **Screen** tab to set the resolution, frequency and color depth. High resolution and high color use more main memory. Therefore, the Thin Client's system resources limit the total number of applications that can be used at the same time.

Possible screen resolutions now include the **wide screen** resolution: 1440*900, 1680*1050, 1920*1200.

eLux NG comes equipped with a screen saver to prolong monitor life. The screen saver starts after the idle time you enter in **Delay**. The user can close the screen saver by pressing a key. If you enter a password, the screen saver becomes a security feature that can only be turned off by entering the correct password or restarting the Thin Client. On the Thin Client, the keyboard combination to start the locked screen saver: CTRL + ALT + END.

Note If an authentication server is active, (see 3.5.3 Access Authorization), for convenience the screen saver password is preset to $ELUXPASSWORD.

In addition, you can enter an idle time (in minutes) for power management delay, an energy saving feature that shuts the monitor off after a specified time. Moving the mouse or pressing a key reactivates the monitor.

Starting with Scout **V 9.4.0** the field "**Rotate**" allows to define, whether the monitor contents are to be turned 90° right or 180° or 90° to the left. Requirements at the client: BaseOS **V 1.36-1** or higher.

Starting with Scout **V 9.6.1** the option "**Use Monitor Plug&Play Info**" allows to define, whether you want to use the monitor information as to frequency and resolution or not.
By default the option is enabled which corresponds to **"no ddc=false"** (ddc= Display Data Channel).
When using display ports the option "**Use Monitor Plug&Play Info**" should be enabled.

3.3.1 Screensaver Settings

Click on **Settings** on the **Screen** tab opens the dialog to select and set the screensaver.

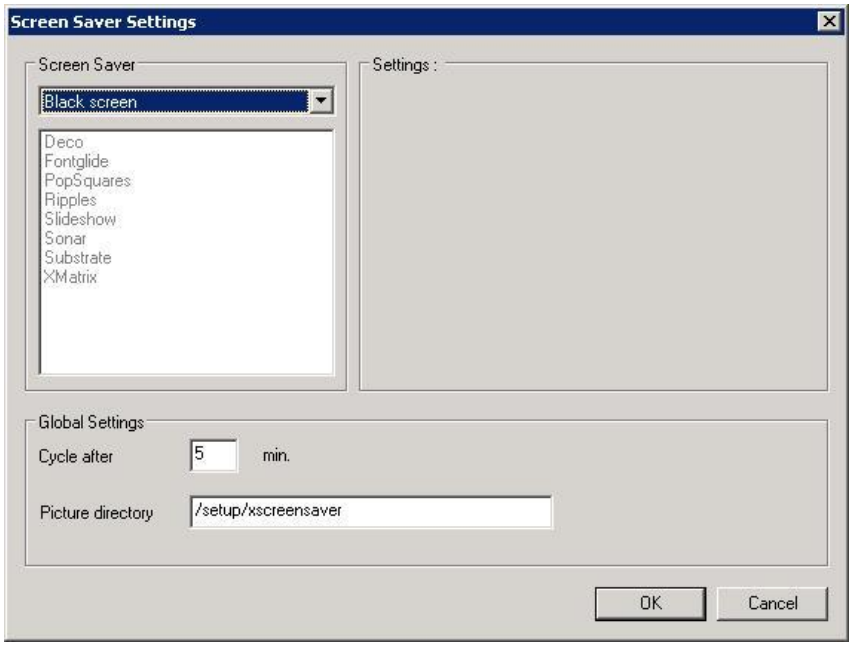


Figure 14: Screensaver Settings

3.3.2 Advanced Screen Settings

NOTE: In general Advanced Settings are prior to the configuration!

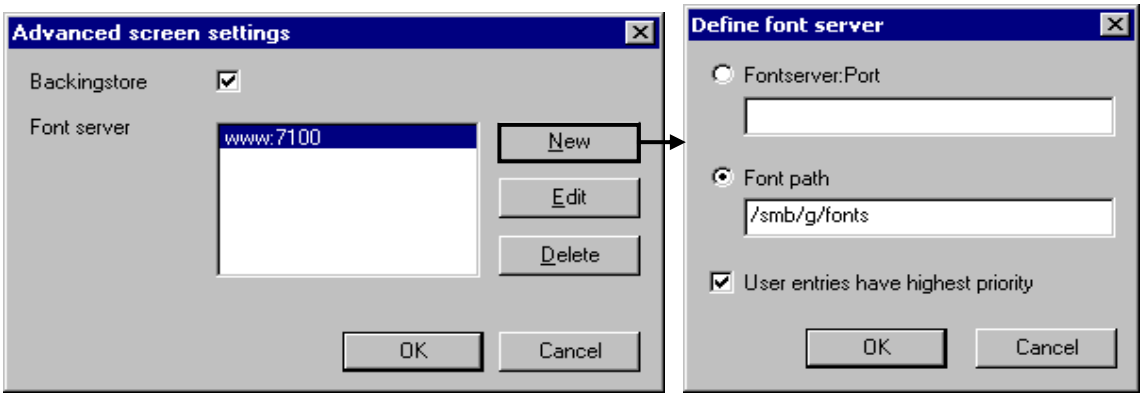


Figure 15: Advanced Screen Settings

Front server

To set a font server, click **Advanced** and **New**. The **Define font server** dialog box appears. Enter the font server and port number in the following format: *<font server name or IP address>*:*<port number>*. Otherwise enter the font path. By default, local fonts have precedence. Select the **User entries have highest priority** check box to give the font server (or font path) precedence.

The font server is available to both the eLux desktop and XDMCP sessions.

Backingstore

Saves screen information to the local X11 server on the thin client. The picture (pixmap) of every window will be stored in the local X server, regardless of whether the pixel is visible or not. The purpose of the function is to avoid transferring screen information from the server to the thin client every time a window is selected,meaning it moves to the foreground. Instead, data is saved locally to the X server, which is then used to refresh the screen. The individual pixmaps are saved to main memory, meaning the X server becomes larger. This increases the screen refresh speed when the network connection is slow, and is especially recommended for a slow ISDN connection.

However, memory requirements are large. Minimum recommended main memory: 128 MB. Otherwise memory constraints depend on how many windows will be displayed and the monitor settings (24 bit requires more memory than 16 bit, for example).

Screen modifications entered in Scout Enterprise take effect the next time the remote desktop restarts.

Attention If you set resolution, frequency and color depth to values the Thin Client's monitor does not support (the screen image will be highly distorted), turn off the Thin Client monitor to prevent damage and revise settings.

In addition, the resolution, frequency and color depth can now be set in the **Properties** window of a **device** or **Organisation unit.** Rightclick to open the Properties and set the values in the **Screen** tab. **These settings are prior to the values set in the configuration.**

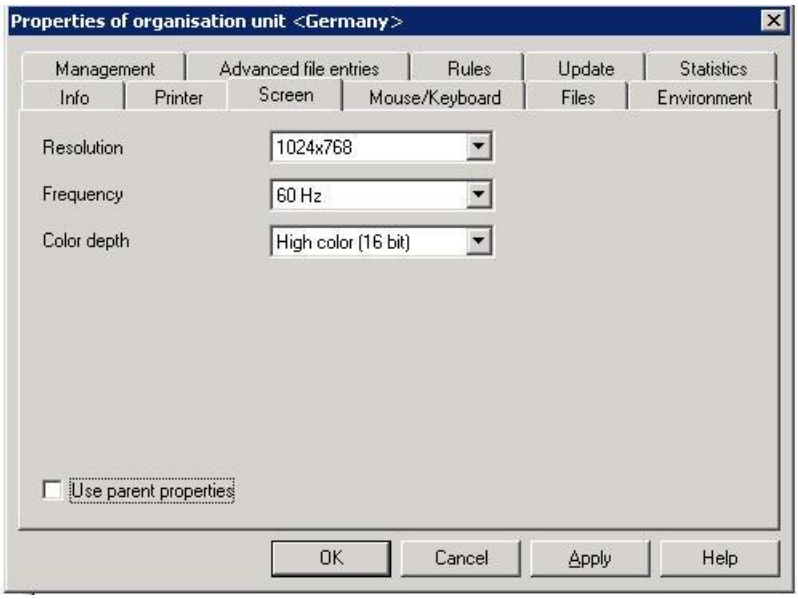


Figure 16: Properties > Screen

3.4 Security

In the **Security** tab you set local user rights, the thin client password, activate an authorization server and define user variables.

Mirroring settings are discussed in chapter 6.5.

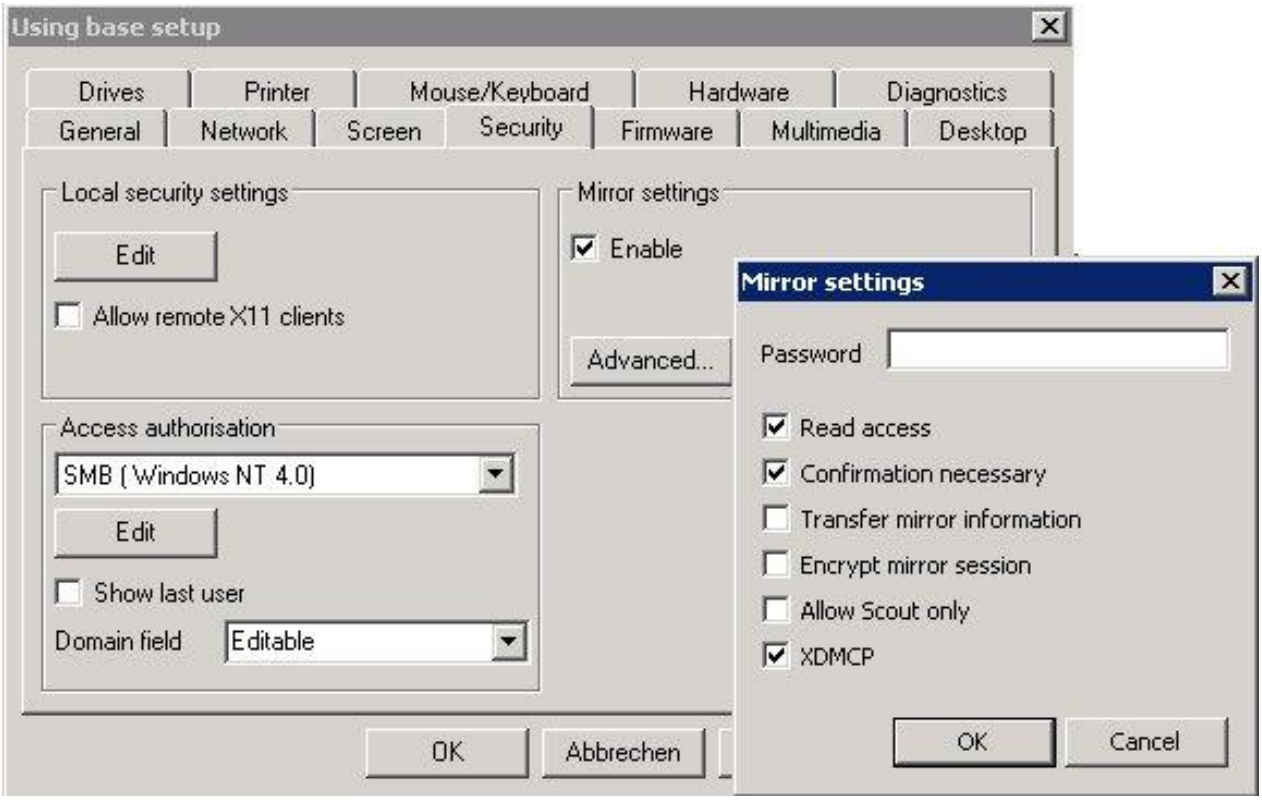


Figure 17: Security tab

3.4.2 Local User Rights

An essential objective of the Scout Enterprise remote management tool is to prevent local users from making incorrect configurations. One way to do this is to disable local configuration.

The Scout Enterprise **Security** tab allows you to give the local user full or limited configuration rights, or to forbid access. Click on **Edit**. The **User properties** dialog box appears. The configuration parameters are displayed in a branching tree-like structure. Upon restart, the user can only access the functions that you enabled.

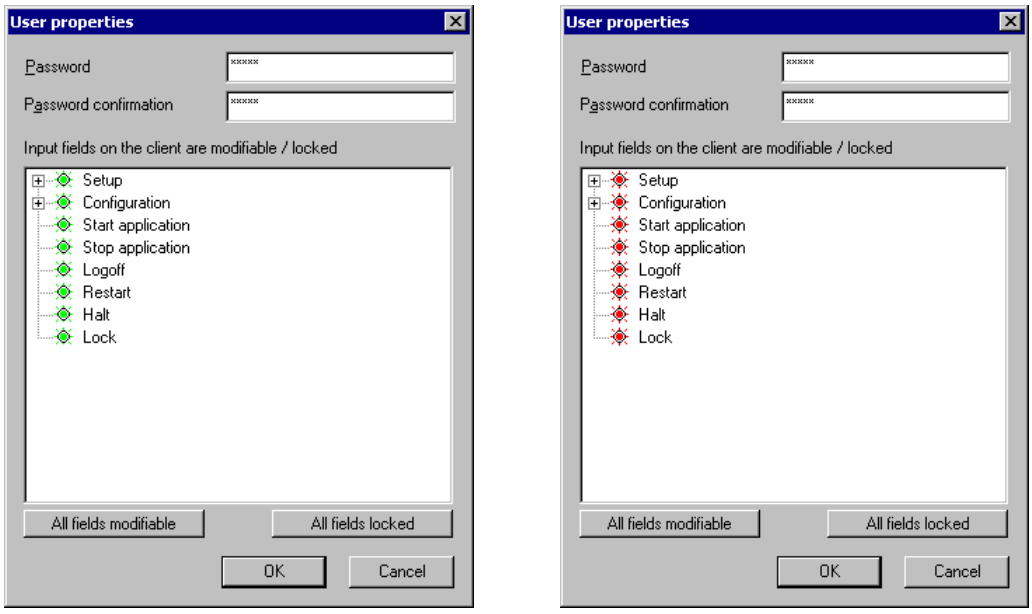


Figure 18: Examples of "All fields modifiable" (left) and "All fields locked" (right)

1. **All fields modifiable** Click to enable local configuration of all fields. The color green indicates that a field is unlocked.
2. **All fields locked** Click to disable local configuration of all fields. The color red indicates that a field is locked.

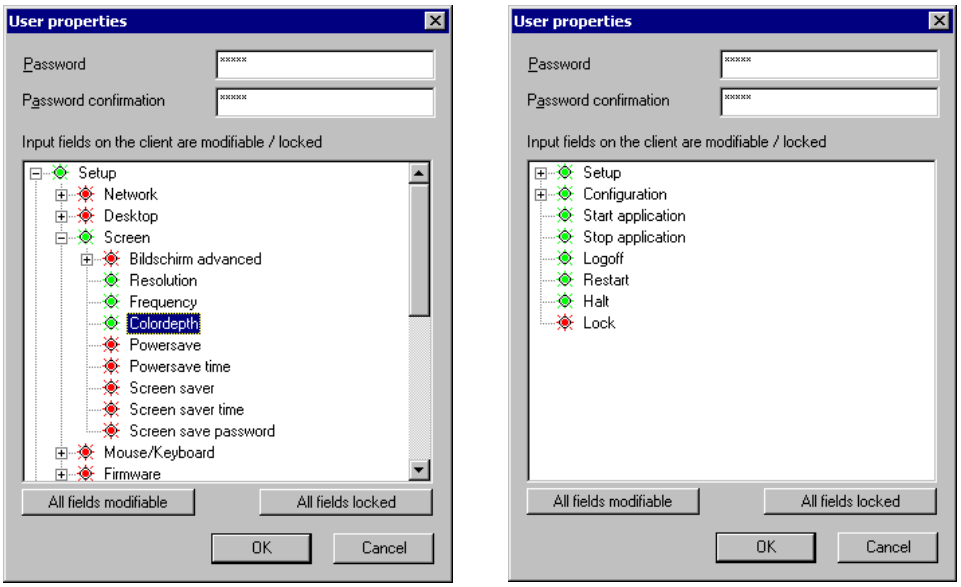


Figure 19: Examples of fields in the Setup tab (left) and Applications tab (right)

The configuration parameters are displayed in a tree-like structure. Click the plus to expand the element. Click the minus to collapse the element. Double click with the left mouse button (keyboard equivalent: space bar) to change a field's status: red = locked, green = unlocked (local configuration allowed).

3. **Setup** To allow users to access the **Setup** tab and modify user settings, expand Setupand set the desired fields to green.
4. **Configuration** Allows you to restrict local access to the **Configuration** tab and local access to application profiles.
5. The remaining top-level parameters refer to options in the **Applications** tab (see Figure 52, right).

   Start application and Stop application refer to the Connectand Disconnect" options.

   Logoff, Restart, Halt and Lock refer to the shutdown options.
6. When you are done configuring local access, click **OK** in the **Local security settings** dialog box and **Apply** in the **Security** subtab.

In addition, the option Allow remote X11 clientsin the **Security** tab allows remote X11 clients to connect to the local Thin Client.

When the desktop configuration is transferred to the device, it is possible to update the locked fields only. In the **Options** menu, select **Advanced**. The **Advanced options** dialog box appears. In the **Update of fields** area, click to select **Only locked fields are updated on the client.** The next time the desktop configuration is sent, only the locked tabs will be updated. The local configuration the user has made in unlocked tabs will not be overwritten.

In addition, local configuration of network hardware profiles (ISDN, ADSL, modem) can also be disabled. See chapter 0 ISDN > Protected option,page 27.

Thin Client users can remove themselves from management by using the hot key CTRL – ALT – HOME and entering the Thin Client password in the dialog box to regain configuration rights, going to the **Setup** > **Security** tab in eLux NG, removing the management address in **Management**, and changing the password of LocalLogin (click **Apply**). If you do not want users to be able to remove themselves from management, do not share the device password.

3.4.3 Client Password

All Thin Clients managed by a Scout Enterprise server receive the same client password. It is not possible to set multiple Thin Client passwords. The password can only be modified in the base configuration.
The client password is used to authenticate at the Scout Enterprise Server, i.e. no other Scout server could manage these clients.

Client password changes are made on those Thin Clients that have **Management** turned on. Password changes are not made on those Thin Clients with **Management** off.

To change the Thin Client password from the default (recommended), open the base configuration. In the **Setup** > **Security** tab click Local security settings" > **Edit**. The **User properties** dialog box appears.

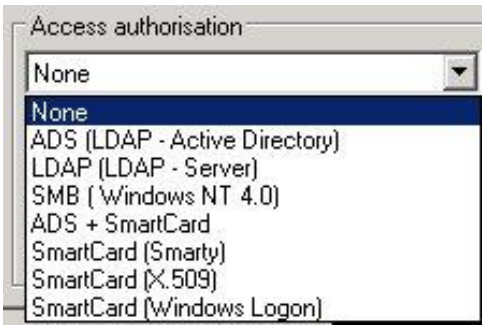
Enter a password in **Local password**. Repeat it in **Password confirmation** to check for typing errors. The default is `elux` (all lowercase) Click **OK**.

When you save the Scout Enterprise configuration, the password is updated immediately for Thin Clients that are currently turned on. It is updated the next time the Thin Client starts for Thin Clients that are currently turned off.

Note the device password can only be set in the base configuration!

3.4.4 Access Authorization

eLux supports an authorization server. The installation of the "User authorisation modules" package is required. Settings are made in the **Setup** > **Security** tab. When activated, the user enters his or her logon data (username, password and domain) once at device start.



⇨ To activate user authentication

1. Under "Access authorization", select the type of authorization server from the drop-down list:

   None: To disable user authorization

   ADS: For an Active Directory® server (Windows® 2000)
   If this authentication method is chosen, you can define, whether the client data should be stored on a server (starting with Scout Version 9.6.1).

   LDAP: For a Lightweight Directory Access Protocol server

   SMB: For a Windows NT® 4.0 domain controller
2. Click **Edit**. The **Access configuration** dialog box appears. Here is where you set server settings. The parameters differ depending on the type of authorization server you selected. They are described in detail below.
3. Click **OK** and then **Apply** in the **Security** tab.

The user must now enter a user name and password when the Thin Client starts.

Active Directory Server

The directory service for Windows 2000 is called Active Directory. The structure is different from Windows NT: there are no longer PDCs and BDCs. PDCs and BDCs are given up in favor of a peer model, where all domain controllers (DC) in a Windows forest are equal.

The configuration depends on the system your Thin Clients are running:

- eLux NG version 1.7 or higher
- eLux NG before 1.7 or eLux 1.1

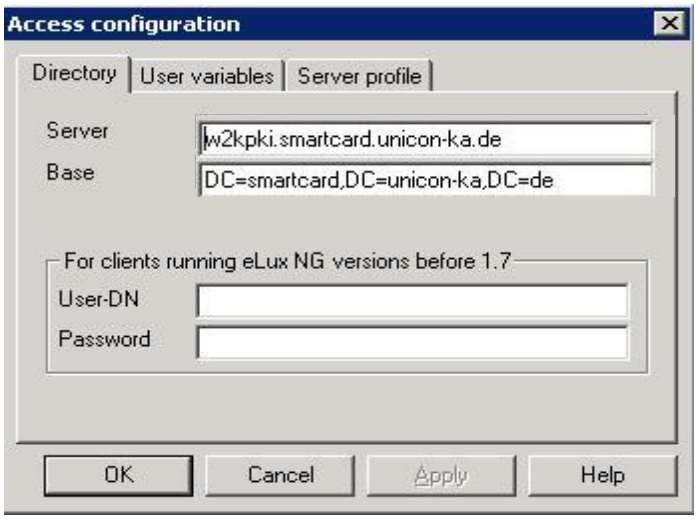


Figure 20: Access Configuration

For authorization using Active Directory, enter the following parameters:

- **Server**: Enter the IP address/name of the domain controller. Multiple servers can be entered, separated with a blank. If the server is in a different subnet than the Thin Client, use the fully qualified domain name.
- **Base**: The search base indicates where in the hierarchy to begin the search. The branch point to use as a starting point when searching for a user, for example, ou=users,dc=mydomain,dc=com".

  eLux NG version 1.7 or higher If you know the domain controller, you can use a Thin Client running eLux NG version 1.7 or higher to easily determine the search base. See Determining the search base using Thin Client" in this section.
- User ID

  eLux NG version 1.7 or higher Leave blank

  eLux NG before 1.7 or eLux 1.1 Enter the distinguished name for the user allowed to initiate the authorization call.
- Password

  eLux NG version 1.7 or higher Leave blank

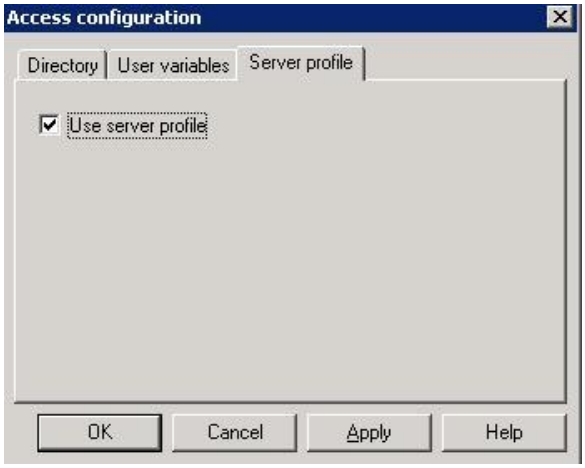
  eLux NG before 1.7 or eLux 1.1 Enter the password for the above user
- **User variables**: See the section User Variables in this chapter.

See your administrator for more information on search base, user DN and authorization server parameters.

eLux supports changing the ADS password. When the password on the ADS server expires, the user will be requested to enter a new password in the logon dialog box.

New function starting with eLux V1.44 / Scout Enterprise V 9.6.0:

When setting user authorisation via **ADS** there is now the option to use the server profile. By enabling this option several user data are packed during Logoff and are stored on a defined directory on the server. During Logon the data are restored from the server directory. Thus each user gets his individual data (such as locally defined setup data or bookmarks in the browser) independent from the client he/she logs on to.
Note: Only setup data are stored which are **not** managed by Scout.



The profile directory must be predefined as UNC in the ADS entry (attribute profilePath) of the user. The macros $ELUXUSER, $ELUXDOMAIN and %USERNAME% and %USERDOMAIN% can be used.

Further, the relevant feature in the eLux BaseOS (starting with V1.44) must be install

ADS+Smartcard

To logon with smartcard (certificate X509) you need to enter the server address (see above figure) and the root certificate to check for the user certificate. Select the root certificate in the tab **Certificates**, so that this will be transferred to the client. Further certificates may be added and selected.

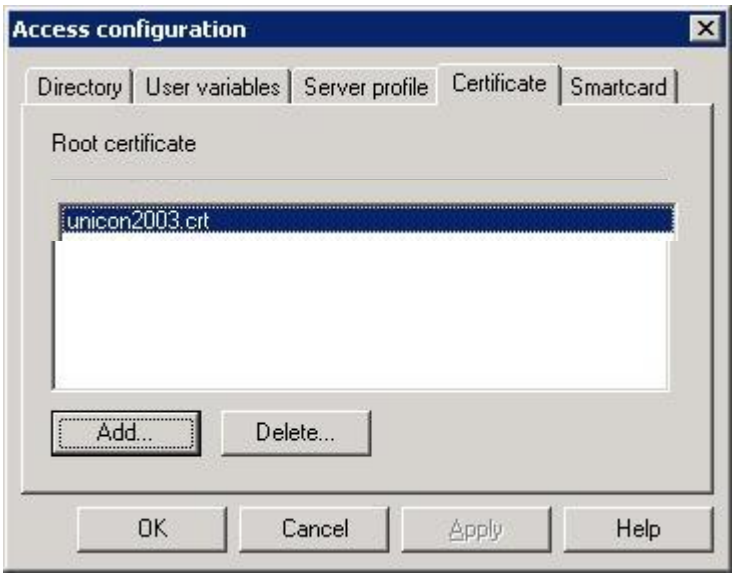
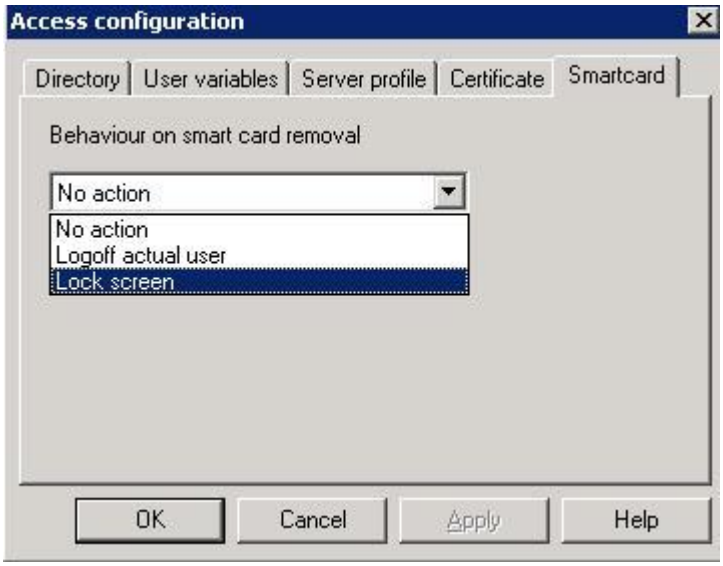


Figure 21: Access Configuration – ADS+Smartcard

The setting in the **Smartcard** tab defines the behaviour when the smartcard is removed. Select ***Lock screen***, and please consider to enable the option **Password protected** in Setup > Screen.



Smarty

With the Smarty solution the smartcard stores

- user name
- password
- domain

instead of a certificate.

Figure 22: Access Configuration – Smarty

One option is to give these data to the corresponding server connection directly as $ELUX variables.

Else ADS or LDAP can check for the user name, password and domain, if the option **Additional ADS authorization through… ADS or LDAP** has been enabled. If the password changes (group directive) the dialog for changing the password will appear at the client. The new password will then be written to the smartcard automatically.

To personalize the smartcard a tool is available for download on www.myelux.com.

The tool enables to enter an initial PIN – e.g. 1111 – and to leave the password field blank.
The user is then requested to enter his own new PIN and initial password. PIN and password will be stored on the smartcard.

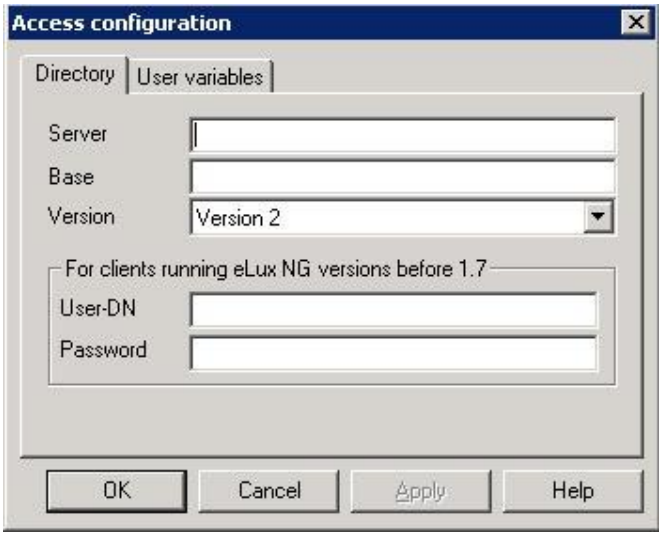
The tool Smarty also allows to define the PIN Policy, which, however, must not be identical with the initial PIN – as mentioned above: 1111.

Allow user/password logon
This option allows to configure that - when using a smartcard – you can switch to logon with user/password by pressing the ESC key.

Lightweight Directory Access Protocol

LDAP is a TCP/IP based protocol that defines a standard method for accessing directory services.

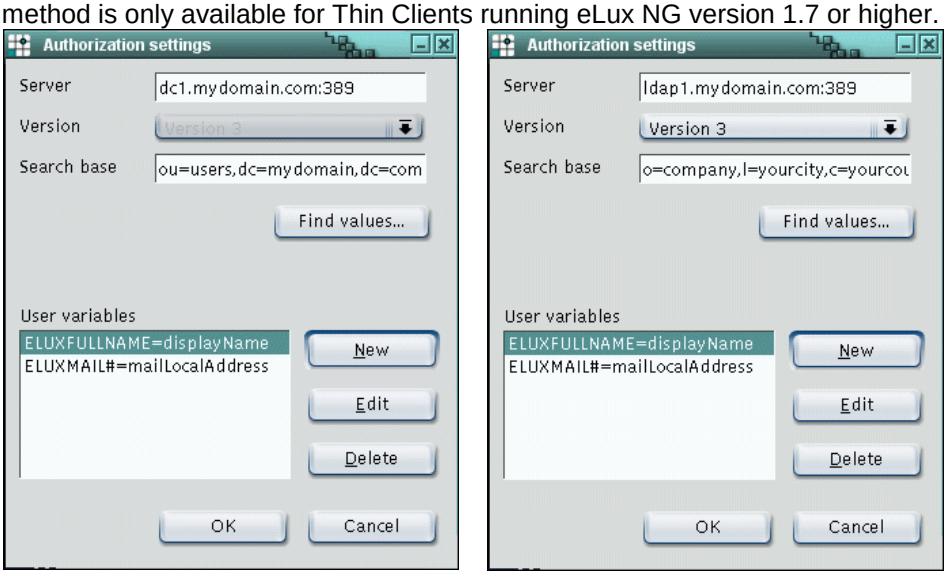
For authorization using an LDAP server, enter the following parameters:



- **Server**: Enter the IP address/name of the LDAP server. Multiple servers can be entered, separated with a blank. If the server is in a different subnet than the Thin Client, use the fully qualified domain name.
- **Base**: The search base indicates where in the hierarchy to begin the search. The branch point to use as a starting point when searching for a user, for example, o=<*company*>,l=<*your city*>,c=<*your country*>. See your LDAP server administrator for this parameter. Alternatively, if you know the LDAP server name, you can use a Thin Client running eLux NG version 1.7 or higher to easily determine the search base. See Determining the search base using Thin Client" in this section.
- **Version**: the LDAP version to use
- **User variables**: See the section User Variables in this chapter.

Determining the search base using the Thin Client

This method is only available for Thin Clients running eLux NG version 1.7 or higher.



On the Thin Client, go to **Setup** > **Security**. In the User authorizationarea, select **LDAP server** or **Active Directory Server** from the **Authorization** drop-down list. Click **Edit**.

In the **Server** field, enter the IP address or name of the LDAP server or ADS domain controller. If the server is in a different subnet, use the fully qualified name.

Click **Find values**. The Thin Client will search for the server and automatically fill in the **Search base** field. Enter this parameter in Scout Enterprise

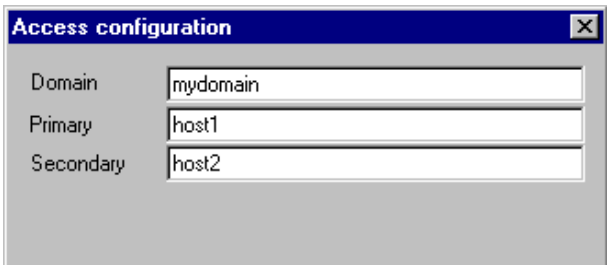
SMB (Windows NT 4.0)

In a Windows NT domain the user accounts are administrated by a Primary Domain Controller (PDC). When a user logs on to the PDC, he or she is authenticated using the user database. User account

information must no longer be entered on every workstation within the domain. User information must only be entered once. Due to redundancy, load sharing or optimizing WANs, user information can be replicated using a Backup Domain Controller (BDC). Authorization takes place using this server if the PDC cannot be reached.

For authentication using a Windows NT computer, enter the following parameters:

- **Domain**: Enter the NT domain.
- **Primary**: Enter the IP name of the Primary Domain Controller (PDC). Each domain has one and only one PDC. An IP address is not allowed.
- **Secondary**: Enter the IP name of the Backup Domain Controller (BDC). An IP address is not allowed. While a domain can have more than one BDC, only one entry is allowed.



The NetBIOS name of the PDC must be identical to the IP name. This is also true for the BDC.

Help! I'm locked out!

Directory service settings are made on the Scout Enterprise server. If the device is managed, to change incorrect settings connect to the Scout Enterprise server, change the settings, save your changes, and restart the device remotely.

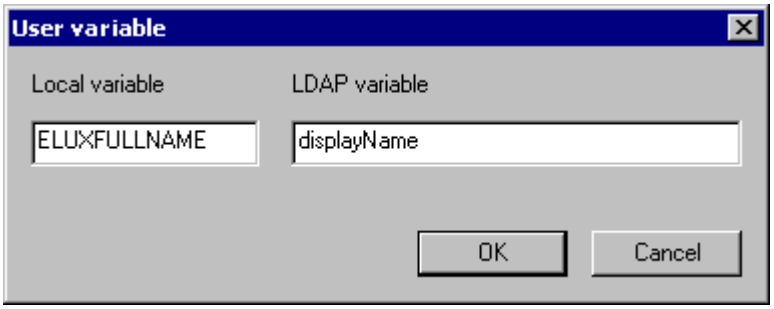
If the device is not currently managed, the administrator can still log on to the Thin Client locally using the login name LocalLogin" and the Thin Client password (see section 3.4.1) and correct the settings by going to **Setup** > **Security**.

User Variables

User variables are variables whose values are read from the authorization server when the Thin Client makes its authorization call. The variables can be used in certain fields in the configuration fields.

When directory services is active, the default ELUX variables ($ELUXUSER, $ELUXDOMAIN and $ELUXPASSWORD) are automatically set when the user logs on.

If you use the authorization server LDAP or Active Directory, you can also set customized user variables.



⇨ To set customized user variables (ADS or LDAP)

1. In the **Access configuration** dialog box for ADS or LDAP click on **New**. The **User variable** dialog box appears.
   - **Local variable**: Enter a name for the variable. The name must begin with the prefix ELUX" and without the initial $".
     End with the #character to transfer more than one value, for example, ELUXMAIL#=mailLocalAddress. If more than one mail account address resides on the server, they will be transferred using the nomenclature $ELUXMAIL_1, $ELUXMAIL_2, etc. In this case, the variable $ELUXMAIL_0 contains the number of mail addresses that were read.
   - **LDAP variable**: Enter the name of the attribute that the LDAP or Active Directory should assign the variable. As an example, the LDAP/Active Directory schema can contain the attribute displayName". If you assign this attribute to the variable ELUXFULLNAME, it will be assigned the value of this attribute during the next user authorization call.
2. Click **OK** in the **User variable** dialog box and **Apply** in the **Security** tab.

See the following section for helpful hints on where to use user variables.

Application Possibilities

When user authorization is active, user variables can be entered in Setup just like normal parameters. In this case, start each variable with the $character. For example, in an ICA application definition you can enter $ELUXUSER, $ELUXPASSWORD and $ELUXDOMAIN for the user login data. The variables will be replaced with their assigned values when the application is called.

Following is a list of fields in which you can use user variables.

Applications Tab

Field	Function	User Variable
Shut down > **Lock**	Manual activation of the screen saver lock	Preset with the value of $ELUXPASSWORD

Setup Tab

Subtab	Field	User Variable
Drives	**Username**	$ELUXUSER
	Password	$ELUXPASSWORD
	Directory, Server, Share	Every $ELUX variable
	Browser home directory	Every $ELUX variable
Screen	**Screen saver password**	$ELUXPASSWORD

Configuration Tab

Application	Field	User Variable
ICA/RDP	**Server**	Every $ELUX variable
	Username	$ELUXUSER
	Password	$ELUXPASSWORD
	Domain	$ELUXDOMAIN
Browser	**Proxy, Proxy port**	Every $ELUX variable
Tarantella	**Server**	Every $ELUX variable
Local > Customized Commands		
Application possibility: Programs that can be executed using the command line.		
Example: `rdesktop -u $ELUXUSER -p $ELUXPASSWORD` *<machine>*		
	Parameter	Every $ELUX variable

3.5 Firmware

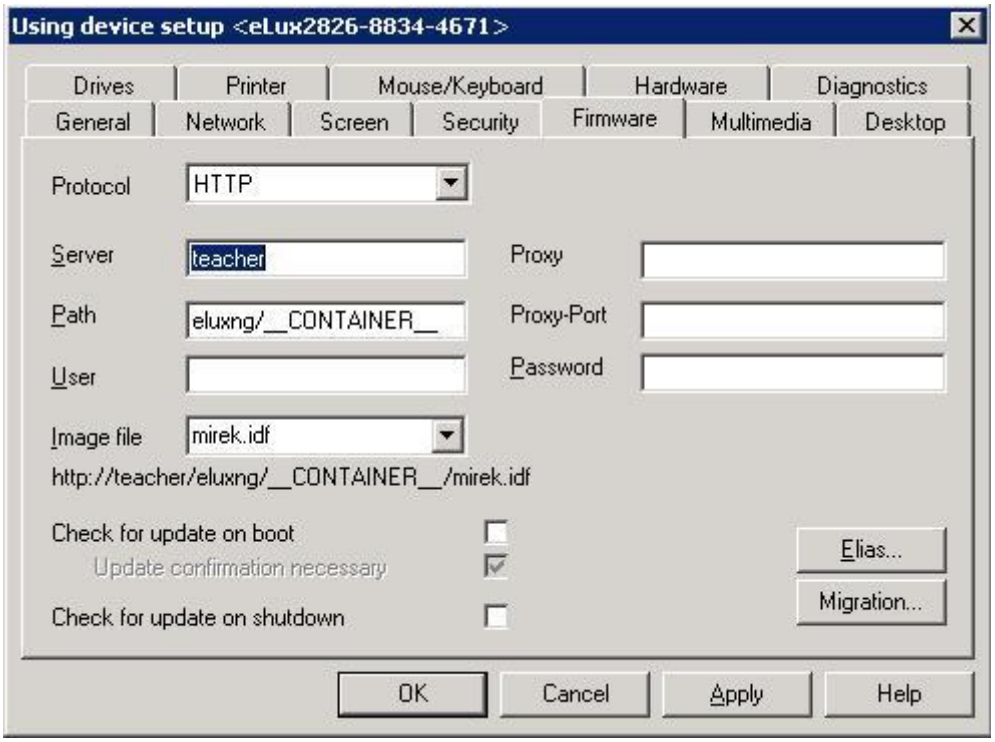


Figure 23 Setup > Firmware

The Image Definition File Die image(IDF) defines the specific software to be installed on the Thin Client.
The **Firmware** tab contains any required information to access the IDF.

The IDF is created using the companion program ELIAS, included on the CD-ROM or available for download at www.myelux.com (registration required).

We recommend accessing an FTP server using a user account. However, anonymousFTP is supported.

When **Check for update on boot** is selected, an update check is performed when the Thin Client boots. When **Update confirmation necessary** is selected, a confirmation box appears on the Thin Client before an update takes place, allowing the user to cancel.

Click on the button **Elias** to edit the image definition file. **Note**: For ELIAS to open the image definition file automatically, you must set the correct container path in the **ELIAS – Settings** dialog box (**Options** menu > **ELIAS Settings**).

For detailed information on ELIAS, firmware settings, and performing an update, see chapter 5 Management on the Firmware Level.

Double-check that your firmware parameters are correct, as incorrect parameters could cause problems. A quick and easy method to check the validity of firmware parameters is to perform an update using one Thin Client as described below.

To Test Firmware Parameters

On a Thin Client, go to the eLux NG main screen. In **Setup** tab > **Firmware** enter the firmware parameters you are testing and click **Update**. If you get a message saying an update is necessary, a connection to the image file server and image file was made and the parameters are correct. Cancel the update. If you get an error message, locate and revise the incorrect parameter(s). Once you have verified the parameters, you can use Scout to perform a general update.

3.6 Multimedia

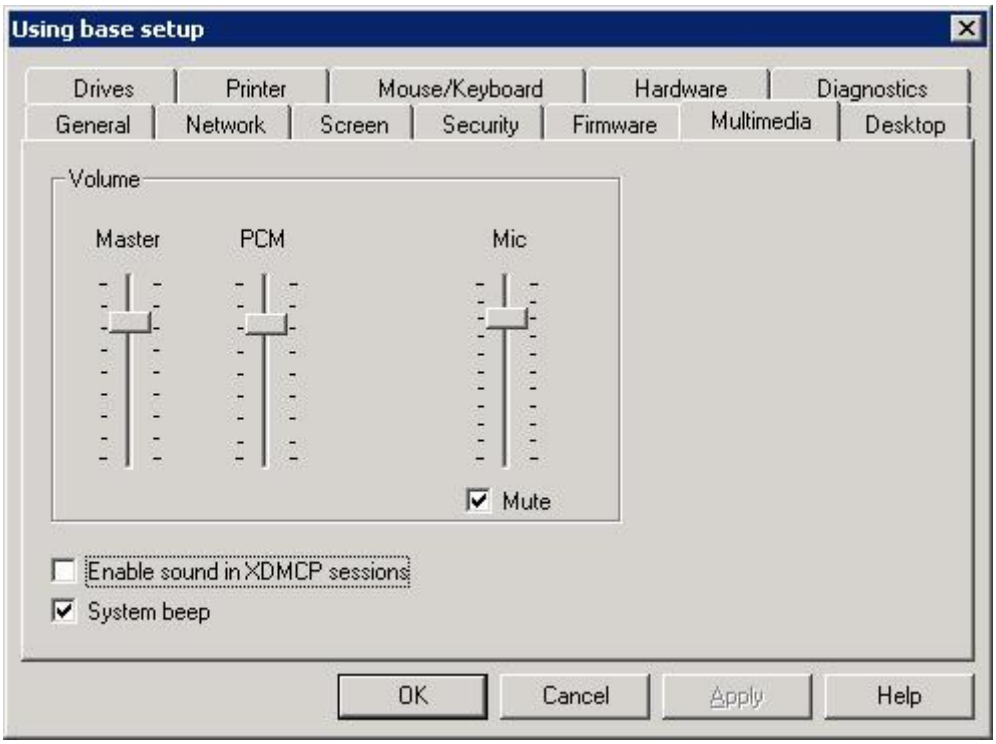


Figure 24: Setup > Multimedia

To adjust the volume for Master or PCM, move the slider up or down and click **Apply**.

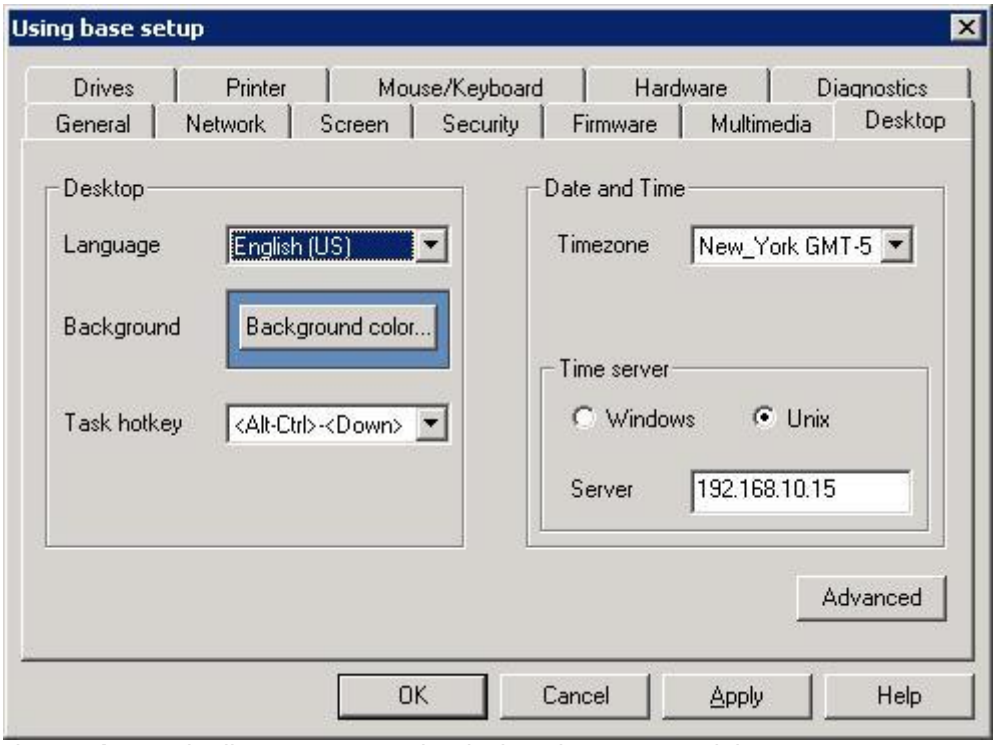
The sound of the microphone can also be switched to mute.

To enable sound in XDMCP sessions, click to select **Enable sound in XDMCP sessions**.
Note: The application must be e-sound system compatible.

If **System beep** is enabled the user is prompted an audio signal when pressing the "Power off" button at the Thin Client.

3.7 Desktop

Figure 25: Setup > Desktop



The **Desktop** tab allows you to set the desktop language and time zone.

Language

Select the desktop language. This sets the language for the eLux NG main screen and for applications running locally on the Thin Client – browser, Acrobat® Reader®, etc. (assuming required language software has been installed).

- The default language of eLux NG screen elements (tabs, lists, etc.) is English (US).
- The eLux NG screen elements themselves can only be displayed in English or German. However, your country's language must be set for local applications to work correctly.

Background Color

Click this button to open the **Color** dialog box, where you can set the desktop background color using hexadecimal values or the color palette.

Task Hotkey

Choose the key combination the local user will use to switch between current open applications, or tasks. The hotkey not only switches between applications, such as between a local browser and an ICA application, but also between eLux NG screens, such as the main eLux NG screen and a dialog box. Default is CTRL + ALT + <*cursor*>.

- CTRL + ALT + ↓: Left selection in the Applications bar
- CTRL + ALT + ↑: Right selection in the Applications bar

Time Zone

Choose your time zone from the drop-down list.

Time Server

In addition to time zone, the time must be set on the Thin Client for proper use. This can, of course, be done locally on the Thin Client. However, due to its better accuracy we recommend using a time server.

You have the option of entering a time server running on either a UNIX or Windows machine.

Note Please read the entire section for a complete overview of all possibilities!

Windows

Enter the IP address or name of a computer running Windows 2000 (or later).

If you select this option, the time server must conform to Simple Network Time Protocol as described in RFC 1305. The Windows Time Service (W32Time), which is installed by default on computers running Windows 2000 or later, is SNTPv4 compliant.

The W32Time service starts automatically on computers that are joined to an Active Directory domain. For computers that are not joined to a domain, you must start the time service manually.

The Windows NT time service does not support SNTP. To use NT, you must install third-party software. See the following section Unix" for more information.

For more information on SNTP, see the Knowledge Base article 224799 (Basic Operation of the Windows Time Service"), 216734 (How to Configure an Authoritative Time Server in Windows 2000") or the white paper Windows Time Service(http://www.microsoft.com/windows2000/docs/wintimeserv.doc).

The forerunner of SNTP is Network Time Protocol as described in RFC 1305. The two protocols are interchangeable. Thus, you can alternatively enter an NTP-compliant machine. Many UNIX servers have xntpd, which is NTP compliant. The service must be started.

For more information on NTP, see www.ntp.org.

This service operates on port 123 with the UDP protocol.

Unix

Enter the IP address or name of a UNIX machine running a RFC 868 time service.

If you select this option, the time server must conform to Internet standard RFC 868 (Time protocol"). This type of time service is a standard component on UNIX machines as an internal service of inetd. It can be activated in the file /etc/inetd.conf.

There are several products on the market that allow you to install a time server conform to RFC 868 on a Windows machine, for example, the free time server for Windows NT from Roberson Computer Consulting, Inc., available at www.rccinc.com.

The service operates on port 37 with the TCP and UDP protocols.

For more information on RFC 868, see www.faqs.org.

Note If using the GUI is not an option (rare), you can set the Thin Client's system time in BIOS Setup. See the Appendix.

3.7.1 Desktop - Advanced

The eLux desktop consists of the taskbar, the starter (control panel) and workspaces. These areas can be configured in the **advanced** settings..

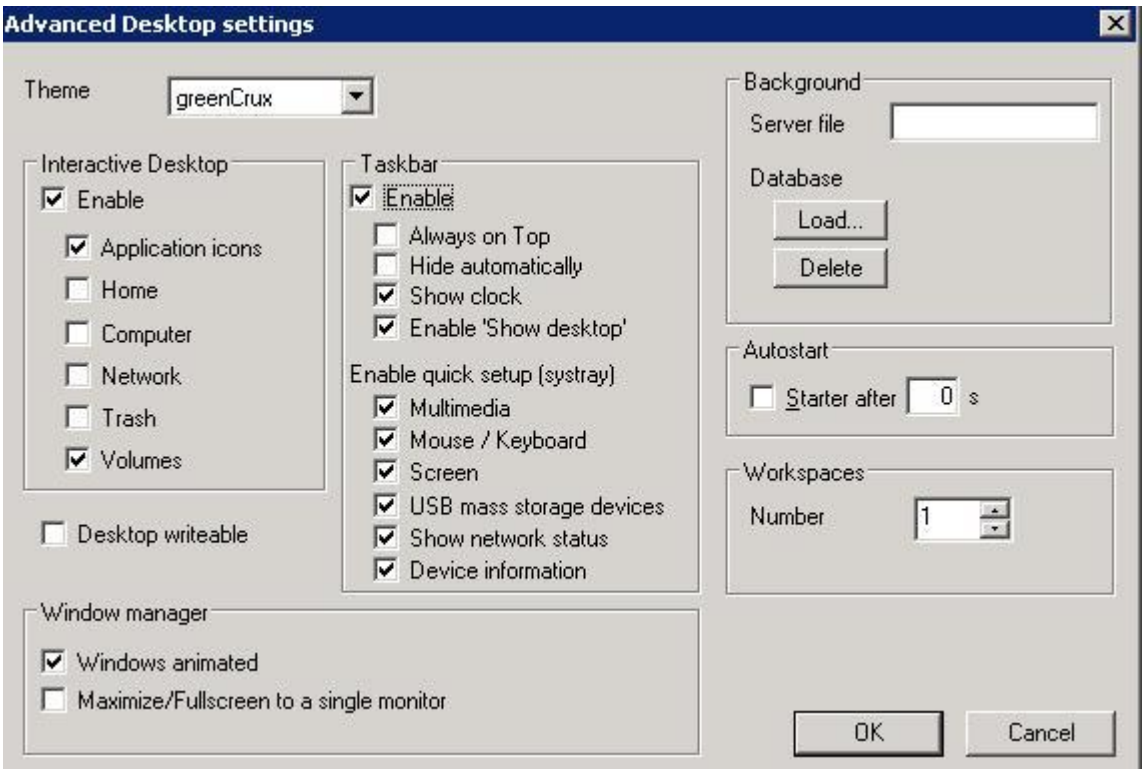


Figure 26: Desktop – Advanced

Desktop Themes

eLux *RL* offers options for an interactive desktop, so that you can select here which icons to put on the desktop.

Taskbar

The taskbar allows application windows to be minimized. Users click on the buttons that appear on the taskbar to switch between running programs/workspaces. The taskbar appears at the bottom of the local user's desktop.

In the **Desktop** tab click **Advanced**. Here you can set the taskbar options (Always on top", Hide automatically") or blend out the taskbar by deselecting the **Taskbar** check box. In addition, you can choose to blend out the clock.

Starting with Scout **V 9.6.1** the area "**Enable quick setup (systray)**" allows to define whether to display an applet in the systray for the client settings of mouse/keyboard, multimedia and USB mass storage devices.

Window manager

By enabling the option "**Maximize/Fullscreen to a single monitor**" it is possible to configure applications to that effect that in dual screen mode the fullscreen mode applies to one defined monitor only.

Background image

There are 2 options to define the background image:

1. Enter an image file into the field**Server file**.

or

2. Click the button **Load** to select a file and import it to the data base. This option is prior to a file entered in the field **Server file**, if there is any.

Just one click on the **Delete** button will remove the background image.

The next time the Thin Client boots, the background image will automatically be transferred. You can restart the device or desktop immediately using the context menu or the Command Scheduler (**View** menu > **Schedule**).

Please be aware of the following:

- The image will be centered. In order to correctly fit the desktop, the background image must match the resolution setting of the monitor. If it is smaller than the desktop, a border will appear in the current background color.
- eLux NG does not support wallpaper or tiled images.
- To reduce network traffic, the image will not be transferred upon Thin Client boot, except when:
- (1) the Desktop settings in Scout Enterprise have changed and
- (2) the image does not already exist on the Thin Client or
- (3) the image was changed.
- You can force Scout Enterprise to transfer the image by using the REFRESH SETTINGS command. The image will not be transferred if it is not in the Scout Enterprise installation directory or subdirectory.
- Please be aware that there must be enough space for the image on the Thin Client (saved to `/setup` on the flash card).
- To remove a background image, delete the file name in the **Server file** field rsp click the button **Delete** to remove it from the database.
- The background image files can also be deleted from a Thin Clilent by selecting "Remote Factory Reset" on the Scout console.
-

Control Panel (=Starter in eLux NG)

The starter is a screen on the terminal that contains three tabs with the following functions:

- **Setup** Configuring eLux settings.
- **Configuration** Defining applications.
- **Applications** Starting applications and shutdown options.

When the device is not managed, user settings are made in the starter.

By default, the starter runs automatically when the devices starts. To deactivate this feature, in the **Desktop** tab click **Advanced**. Deselect the **Starter** check box. You can run the starter from the eLux NG desktop at any time by clicking the Run starter button in the taskbar or using the hotkey CTRL-<Win key>.

Workspaces

Workspaces have been integrated into eLux . In the **Desktop** tab click **Advanced**. Select the desired number of workspaces from the **Number** list. You can set up to four. Default is one.

3.8 Diagnostics

The **Diagnostics** tab allows to define the log level, and an URL can be entered to send the log files to.

Figure 27: Setup > Diagostics

In the context menu of individual devices in Scout **files** can be requested for diagnostic purpose.

Request files: Opens a dialog which allows the administrator to define a list of files and the contents of a script file. Click on **Request files** and all the files having been defined in the field **File list** are added to an archive of the device.

#System is a template the name of which cannot be changed. If required, additional templates can be created.

The contents of the field **Additional Script** will be run as script. The output of this script file are also added to the archive of the device.

Example:
The field **File list** contains:
/setup/terminal.ini
/setup/user.ini
/tmp/eluxd.log
The field **Additional Script** contains:
#!/bin/bash
echo DDCXINFO
echo PS...

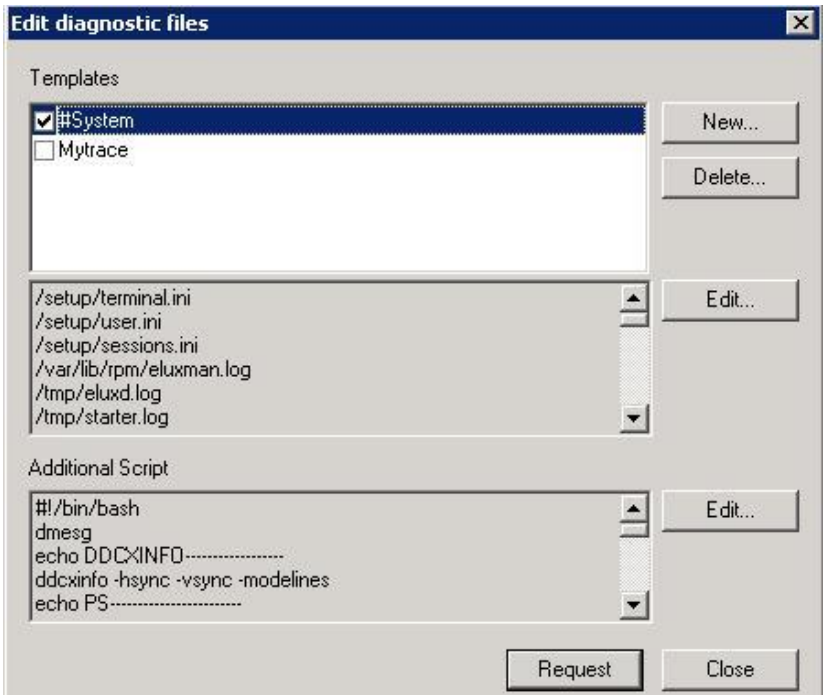


Figure 28: Diagnostic > Request files

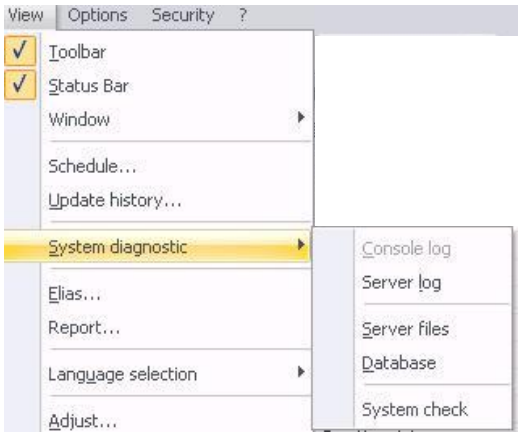
The client sends these data to the Scout server in a zip file. The data are stored in the subfolder **'diag'** of the Scout server installation.

Up to Scout version 11.1: in the directory C:\Programme\Unicon\scoutng\diag.

Starting with Scout version 11.2:
in the directory C:\Dokumente und Einstellungen\All Users\Dokumente\Unicon\Scout\Server\diag

The format of the file is:
devicename_IPAdress_TT_MM_YY_HHMMSS_diag.zip, e.g.:
myDev_217.160.115.92_11_02_08_095241_diag.

In the **View** menu open **System diagnostics** to display information for diagnostic purposes:



Example of a **server log**:

Figure 29: View > Log files > Server log

System check:

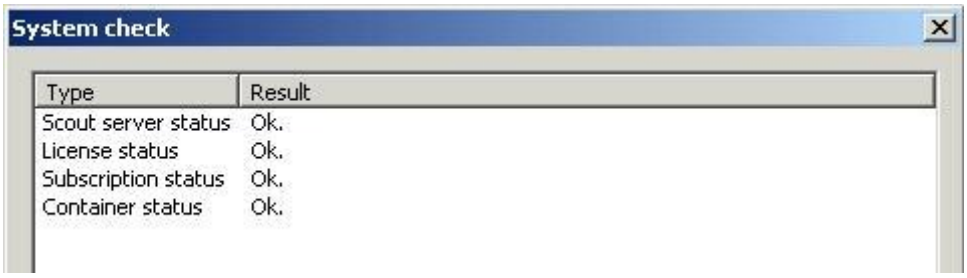


Figure 30: View > Log files > System check

This is to check if

- the Scout server runs
- all devices have a management license
- ssubscription is available
- the file container.ini exists in the configurable container paths.

The system check can be closed by pressing the ESC key.

Examples for the directory in which the logged **server files** are stored:

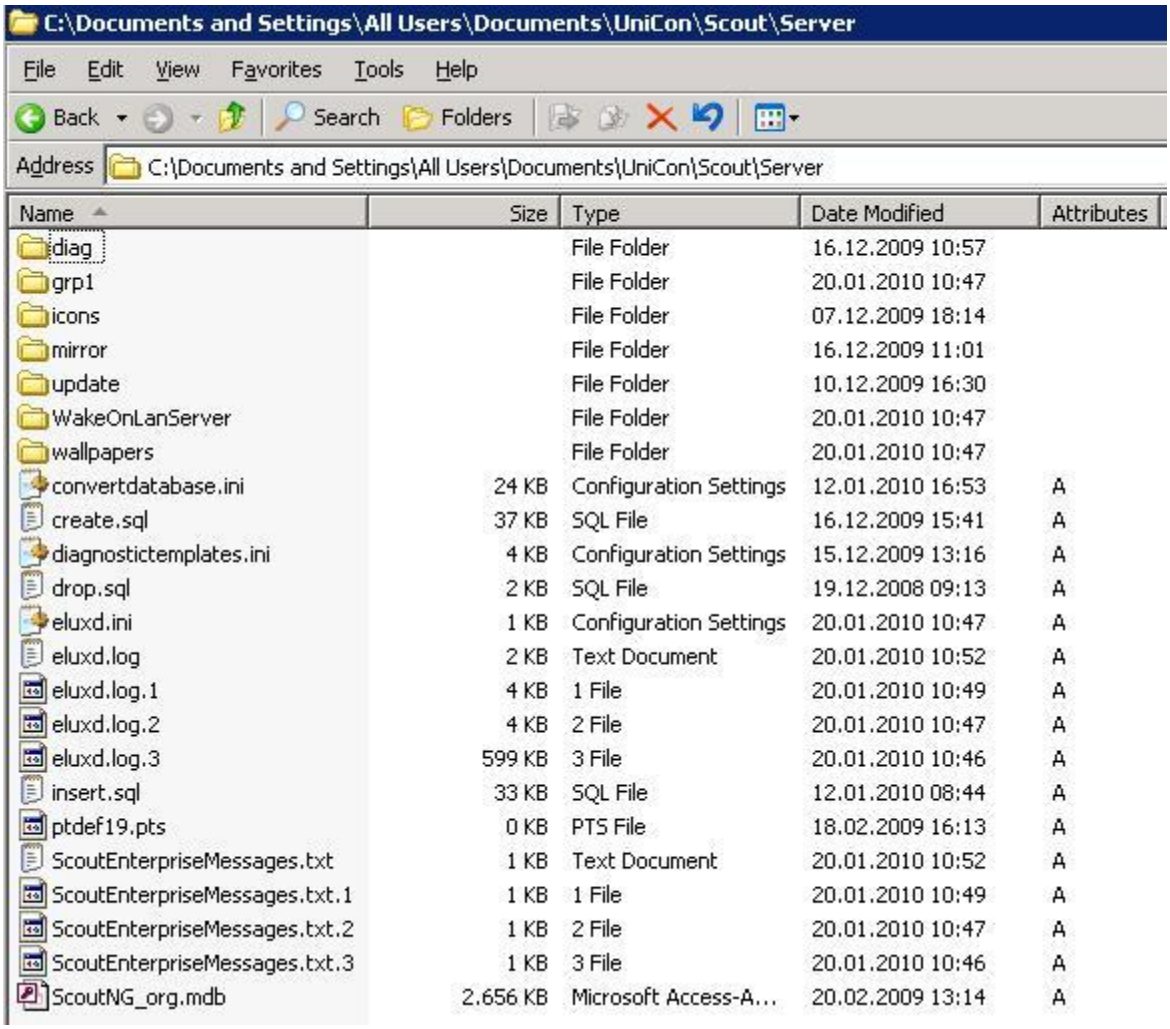


Figure 31: View > Log files > Server files

Examples of the directory in which the logged **database** (.mdb) is stored:

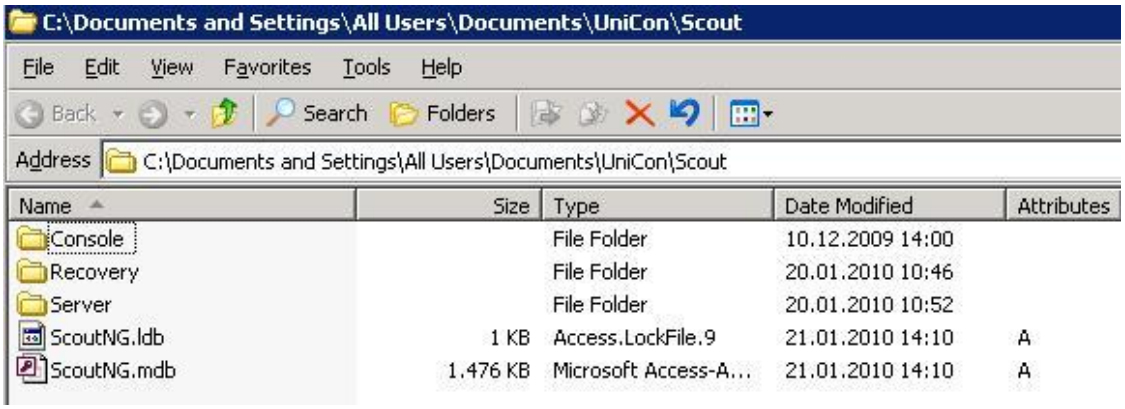


Figure 32: View > Log files > Database

The paths are by default, they may change dynamically, however.

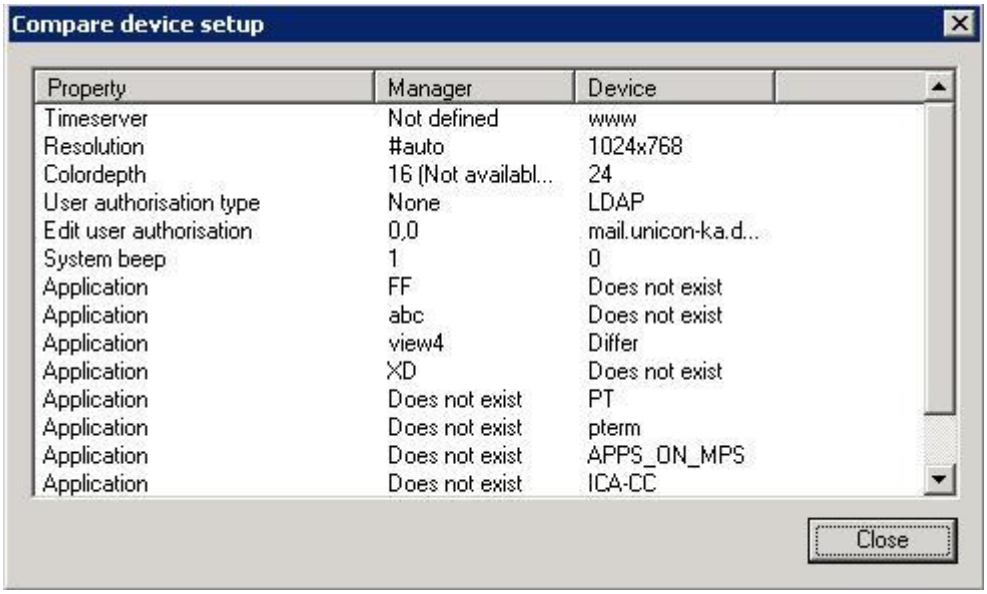
Another option available in the context menu **Diagnostic** is:

Setup comparison

This allows the administrator to compare the settings, configurations and applications on the client with those defined in Scout for the specific client.

If, for example, software packages do not exist on the device, but in Scout, the reason may be that a due update has not been performed.

Figure 33: Diagnostic > Setup comparison



3.9 Drives

The following drives are available:

- Samba
- Network File System
- internal drives (CD-ROM, floppy)
- Universal Serial Bus

Note The **Drives** tab is exclusively for mapping SMB drives! All other drive types are mapped automatically.

This section describes how the user can access the various drives.

3.9.1 Samba

Samba is an implementation of the Session Message Block (SMB) protocol that allows Linux and Windows computers to share files and printers over the network. Network drives for a Windows NT or Samba server must be explicitly defined.

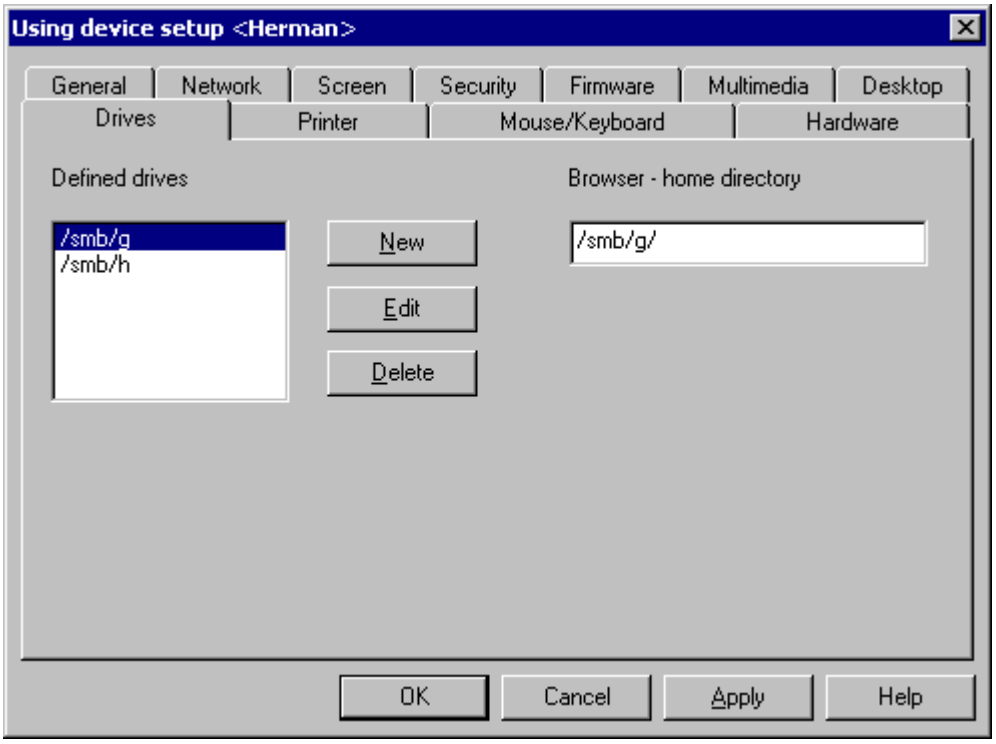
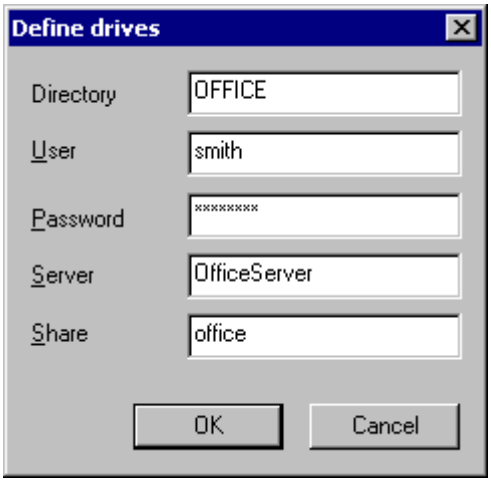


Figure 34: Setup > Drives tab > SMB drive

⇨ **To set a network drive using Windows NT or Samba Server**



Click **New** to open the **Define Drives** dialog box.

Directory: Enter the directory name.

Scout automatically adds `/smb/` to the directory name. The data can then be accessed locally on the thin client in the directory `/smb/`*<directory name>*. See section 0 Mountpoints for more information.

User name: Enter the user name on the server.

Password: Enter the password on the server.

Server: Enter the name of the server.

Share: Enter the export name of the shared drive.

3.9.2 Network File System

eLux NG comes equipped with Network File System (NFS) drive capability. No additional settings modifications are required to use a network drive shared via NFS on the Thin Client.

To use a network drive shared via NFS, the user uses the following format:

`/nfs/`*<hostname>*

or

`/nfs/`*<IP address>*

When the Thin Client accesses an NFS drive, all shared NFS directories on this host are displayed.

Attention All Thin Clients have access to the server as nobody.There is no privacy. Each client has the same access rights to the other clients' files. Therefore, we strongly recommend that you permit write-protected drives only.

3.9.3 Internal Drives

If the device contains an internal (IDE) CD-ROM or floppy drive, the user can access it without further configuration. It is also automatically mapped in a Citrix ICA session.

To access it locally, use the mount point. See section 0

Mountpoints.

3.9.4 USB Drives

More than one USB port can be in use at the same time. For a description of supported USB peripherals, see section 3.12.1 USB Port Activation.

Due to security reasons, by default the USB port for mass storage is disabled. To enable the port, select one of the **USB** check boxes in the **Hardware** tab.

A pop-up message appears locally when the peripheral is successfully connected to the Thin Client.

To access a USB peripheral connected to the Thin Client, the user should use the mount point. See section 0

Mountpoints.

To access it from within a Citrix ICA session, it must be mapped. See section .

3.9.5 Mountpoints

eLux is Linux based. For this reason, to access a drive from a local application, you must use a prefix in your drive path. This prefix is the so-called mount point." The drive prefixes are:

-
- Samba /smb
- NFS /nfs
- Internal Floppy /media/floppy
- Internal CD-ROM /media/cdrom
- USB peripheral /media/usbdisk rsp. 0...7

All mount points are fixed, except for USB. For USB, the mount points are distributed chronologically starting with /media/usbdisk, i.e. the first USB device gets the mountpoint /media/usbdisk, the second /media/usbdisk0 etc.

This information is displayed in the systray of the client, if the option has been enabled in the tab **Desktop** > **Advanced.**

For security reasons, the USB port for mass storage devices must be enbled before use (**Hardware** tab).

3.9.6 Browser – Home Directory

To set a home directory, from the **Drives** tab in Setup enter the netdrive path in the **Browser – Home Directory** field. The path must have been defined in a superior directory, for example,

`/smb/g/user/paul` or `/nfs/hal2001/users/paul`

If no home directory is defined, the folder `/tmp` will be used.

Attention The `/tmp` folder resides on a RAM disk and is automatically deleted when the Thin Client is turned off.

3.10 Printer

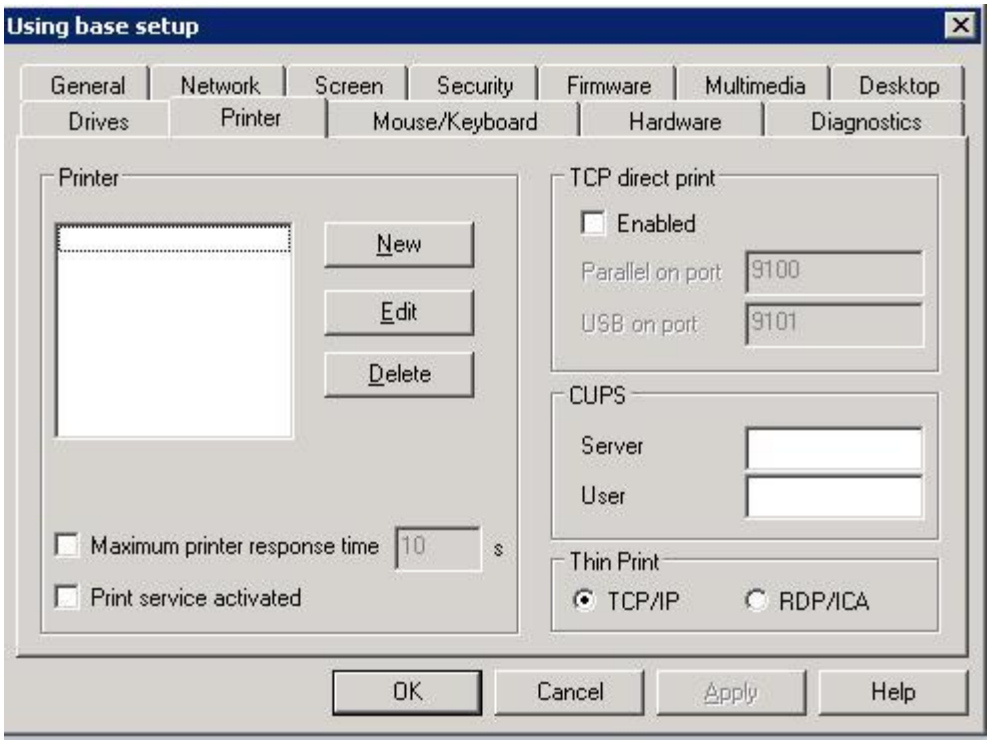


Figure 35: Setup > Printer tab

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

You can use **Setup** > **Printer** > **New** in Scout Enterprise to configure and assign logical names to local printers (most useful in the individual device Setup), which can then be managed from within the network.

The option **Print service activated** defines that the print service is to be startet at the client.

Further, when printing via **CUPS** server, the server and user name can be predefined.

For printing with **ThinPrint** you can define whether to use the TCP/IP protocol or print via RDP/ICA channel. This setting applies for WindowsCE clients only.

3.10.1 Local Printer

Local printers can be connected to the parallel, serial (COM1) or USB interface. COM2 is not available. It is reserved for the card reader.

To configure a local printer, click **New**. The **Define Printer** dialog box appears.

Enter the printer name, connection type and baud rate (serial connection only). To set COM port settings, see 3.12.3.

Select the **Text filter** check box to print from a local shell
(print shell command: `lpr -P` *<printer name>*).

The **Driver name** field is left blank unless you are using the Citrix ICA autocreated printer function.

Click **OK**. The name appears in the **Defined Printer** list.

3.10.2 Network Printer

To configure a network printer, click **New**. The **Define Printer** dialog box appears.

Enter the printer name. Choose `Network` for connection type.

Select the **Text filter** check box to print from a local shell
(print shell command: `lpr -P`*<printer name>*).

Enter the printer's name (or IP address) and the name of the printer queue.

The **Driver name** field is left blank unless you are using the Citrix ICA autocreated printer function. See the next section.

Click **OK**. The name appears in the **Defined Printer** list.

The Thin Client uses the standardized Line Printer Daemon Protocol (BSD spool) as defined in RFC 1179 to communicate with network printers.

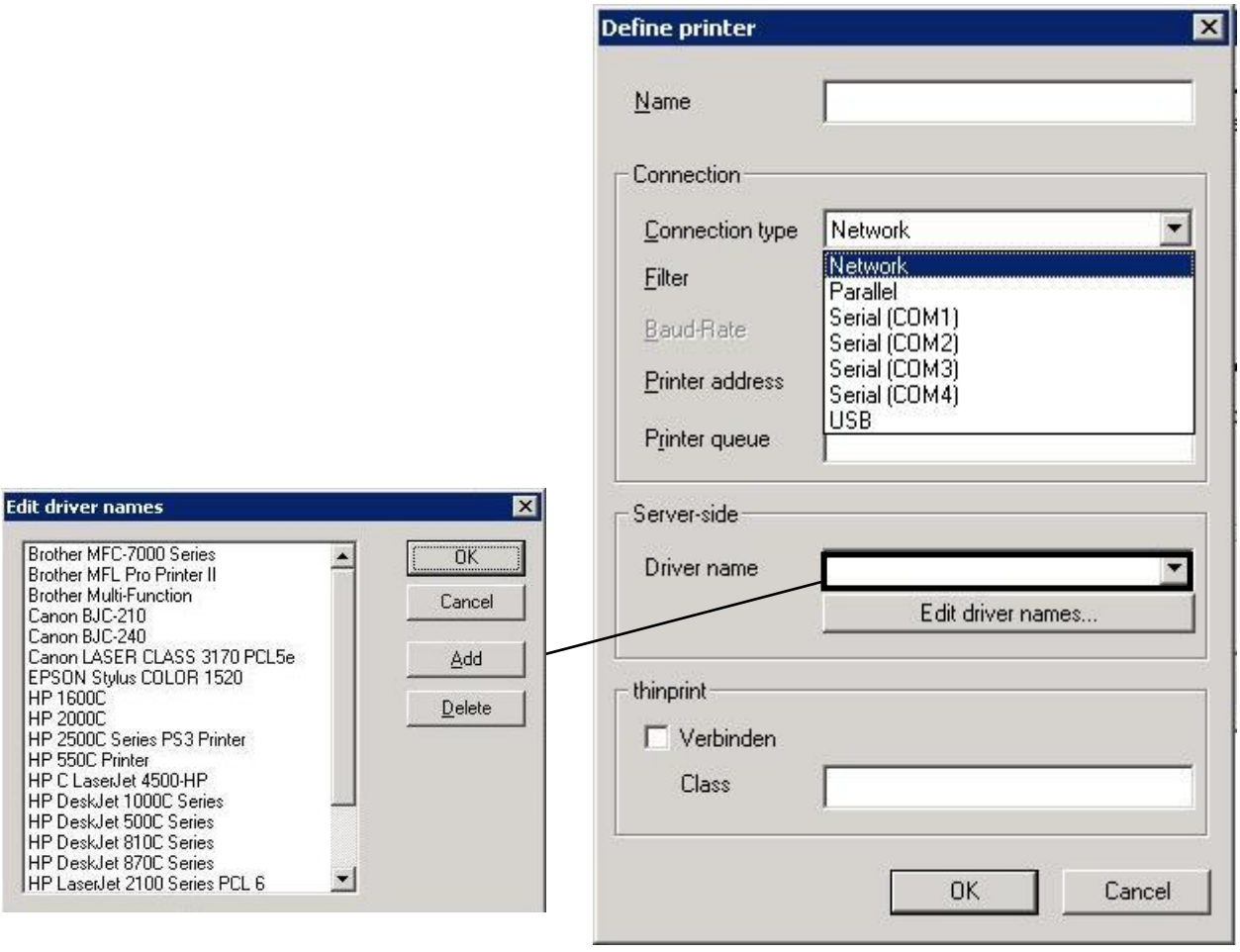


Figure 36: Define a network printer

3.10.3 Default Printer

If desired you can choose a default printer out of the defined printers. Rightclick an **organisation unit** or a **device** to open the **Properties** dialog. Select a printer from the dropdown list in the **Printer** tab.

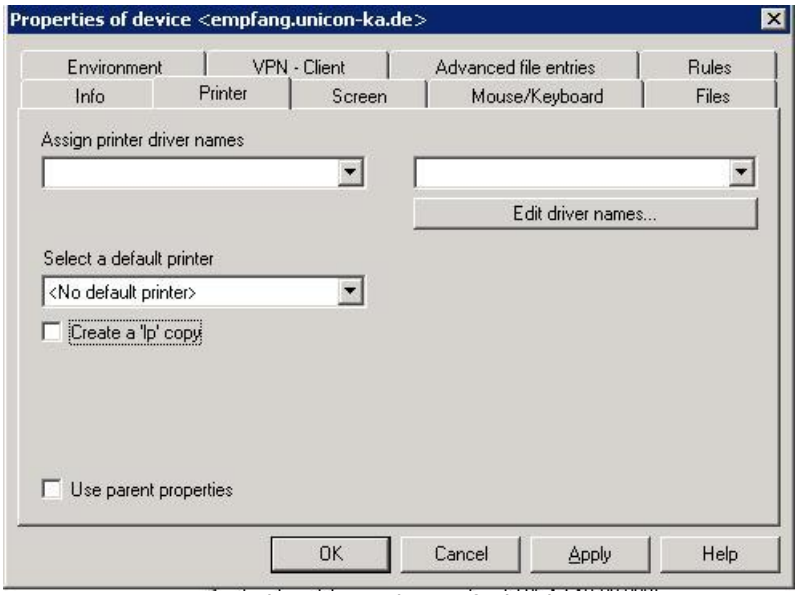


Figure 37: Select Default Printer

Note: All printers defined for the organisation unit or the device are offered in the dropdown list. If against all expectations a printer should not be displayed, please define it in the Printer tab of the base configuration first.

In this properties dialog each printer can be assigned **Driver Names** which is prior to the names defined in the configuration.

3.10.4 Citrix Autocreated Printer

Citrix ICA XenApp servers have a so-called ”autocreated" printerfunction. This means a printer definition is automatically created on the XenApp server when the user logs on via ICA. The printer definition exists only for the duration of the session (it is deleted when the user logs off) and is only available for this user. The driver must be installed on the XenApp server. This section describes the client-side settings required for the autocreated printer function.

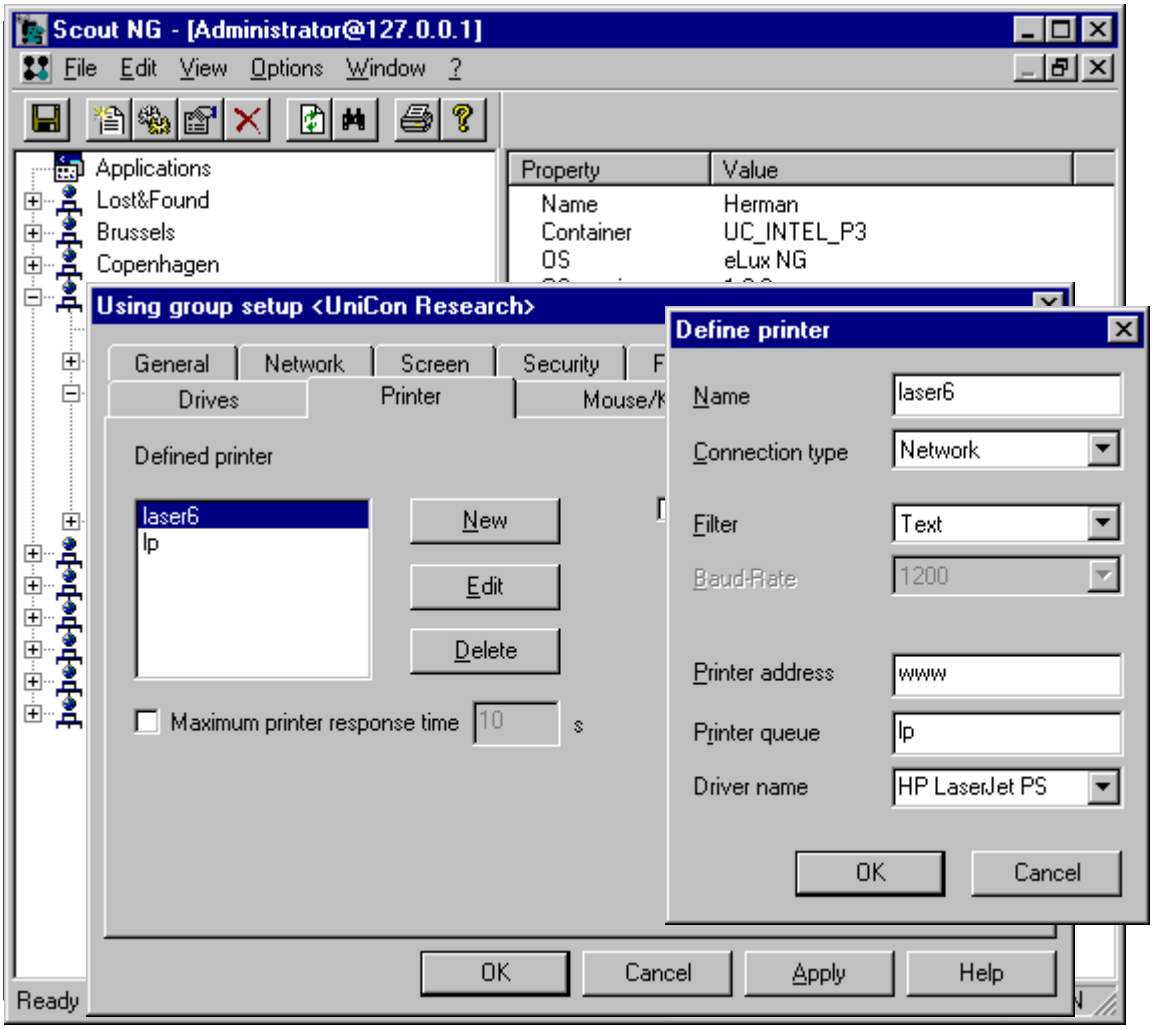
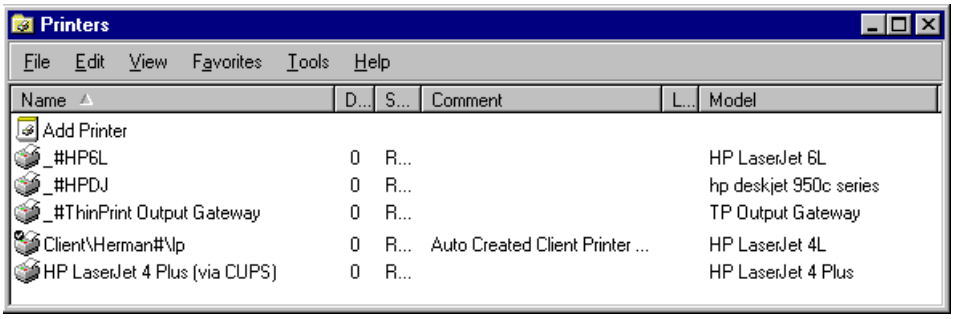


Figure 38: Autocreated printer settings for client

Define one or more printers in Setup > **Printer**. In the **Define Printer** dialog box, enter the Microsoft Windows printer drive name exactly as it appears in the driver list on the server. Capitalization, spelling and spaces matter.

To set a default printer, open the **Edit Properties** dialog box by clicking with the right mouse button on an individual device, Group or Location category and select **Properties**. Choose a printer from the drop-down list. Note: All printers defined in the Setup for that element appear in the list. If the printer you want does not appear, return to Setup > **Printer** and define it.



When the user opens an ICA session to the Citrix XenApp server, in the **Printers** window (**Start** > **Settings** > **Printers**), the user will see icons for the automatically created client printers in the format `Client\`*<hostname>*`#\`*<printer>*, where *<hostname>* is the hostname of the Thin Client and *<printer>* is the name of the printer as defined in Scout (Setup > **Printer**). If the specified driver is not installed on the application server or if the name is not identical, the client printer will not be created.

For more information on server-side printer settings, please see the Citrix documentation for XenApp servers.

In addition, users of XenApp with Feature Release 3 can use a generic printer driver. See the next section.

3.10.5 XenApp Universal Printer Driver 2

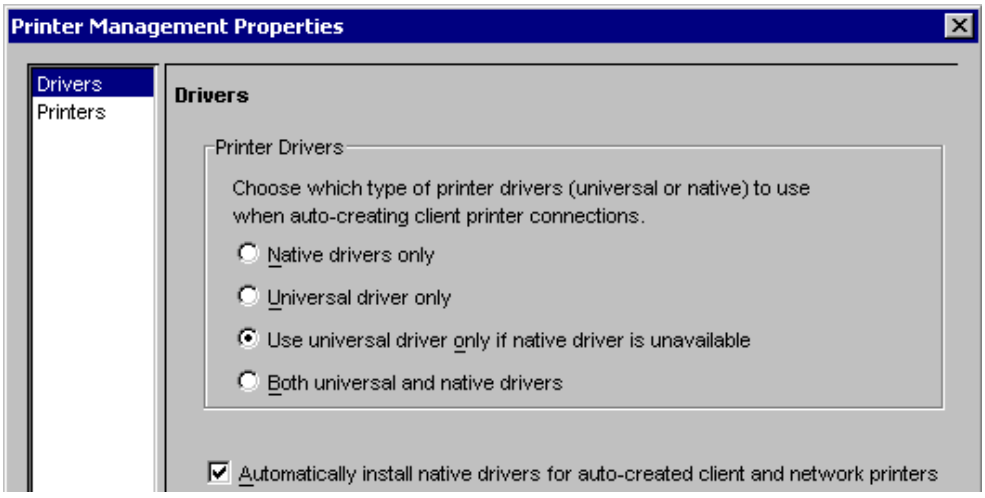
XenApp with Feature Release 3 offers autocreated printers with generic drivers. To use this feature, you must have Citrix ICA Client for Linux V 7.04 or higher installed on your Thin Client.

Client-side settings are described in 3.10.4 Citrix Autocreated Printer

Server-side settings are described in this section.

To configure driver settings, log on to the XenApp server as administrator and open the Management Console for XenApp. From the context menu for **Printer Management**, select **Properties**. The **Printer Management Properties** dialog box opens.

Click **Printers** in the left-hand panel. Here you set autocreated printer settings. See the Citrix documentation for more information.



Click **Drivers** in the left-hand panel. Here you set driver settings.

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

The generic driver used with the Citrix ICA Client for Linux 7.04 and higher is the XenApp PS Universal Driver (HP Color LaserJet PS).

In this example, we activate the autocreated printer function and set driver settings to Universal drivers only if native driver is unavailable."

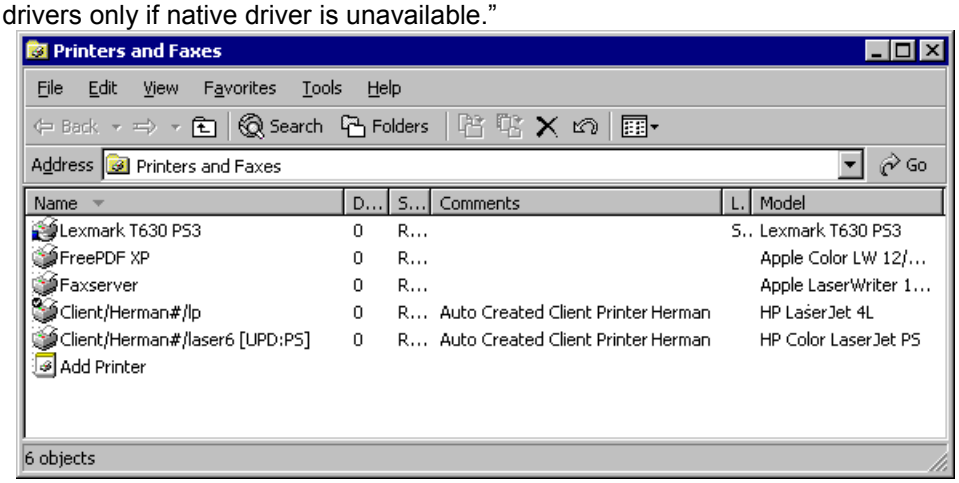


Figure 39: XenApp client printer with generic printer driver

Assume the user opens an ICA session to the Citrix XenApp server. In the **Printers and Faxes** window (**Start** > **Printers and Faxes**), the user will see icons for the automatically created client printers in the format `Client/`<*hostname*>`#/`<*printer*>, where <*hostname*> is the hostname of the Thin Client and <*printer*> is the name of the printer as defined in Setup.

When a universal printer driver is used, the text [UPD:<*generic driver name*>]" is appended to the printer name, where <*generic driver name*> is PS. In the figure above, the client printer Client/Herman#/lpis created using the native driver HP LaserJet 4L" and Client/Herman#/laser6is created using the generic driver for PostScript, as the specified driver HP LaserJet PS" is not installed on the application server.

For more information on server-side settings for Universal Drivers, please see the Citrix documentation for XenApp with Future Release 3.

3.10.6 Printing from Local Applications

Local application (such as Netscape) generally are preconfigured for the printer lp. To print to a printer with a different name, configure the local application's printer settings accordingly.

For local applications that use PostScript as the output format, such as Netscape or Acrobat® Reader®, you must define a PostScript printer.

3.10.7 TCP Direct Print

The printer attached locally to a Thin Client may be used by other machines as a print server if they support TCP direct print. In this case, enter the port number of the local printer's interface (parallel or USB) in the TCP direct print area (most useful for individual device Setup).

3.10.8 ThinPrint

ThinPrint® software from ThinPrint GmbH in Germany allows optimized printing in network across various platforms. Components include the ThinPrint server and ThinPrint client. The server component processes print data for the target printer and sends it in compressed form to the client. The client receives print jobs from the server, decompresses them and sends them to the selected printer. ThinPrint Server and Client are connected via TCP/IP. ThinPrint is a print protocol. Unlike TCP direct, LPR or CUPS, with ThinPrint the bandwidth can be specified, meaning it is a viable option for networks with small bandwidth.

To use this software, on the Thin Client you must install the ThinPrint client software, attach a local printer and define the printer in the eLux NG **Setup > Printer > New**. You need only enable the check box "thinprint", and optionally enter a class name with max 7 characters.

In addition, the ThinPrint-Server must be configured. However, this is not subject of this manual, please consult the ThinPrint Documentation on www.thinprint.com for detailed information.

3.10.9 CUPS

To use this feature, the software CUPS printing front-end (qtcups) must be installed. In addition, the CUPS server must have server options configured.

The Common UNIX Printing System™ (CUPS™) is a software product from Easy Software Products. It provides a common printing interface within a local network and dynamic printer detection and grouping. The advantage of CUPS is that all configuration takes place on the CUPS server. No configuration takes place locally on the client.

The CUPS server contains a list of back-ends, including parallel port, USB connections, serial connections and network (LPD).

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

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

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

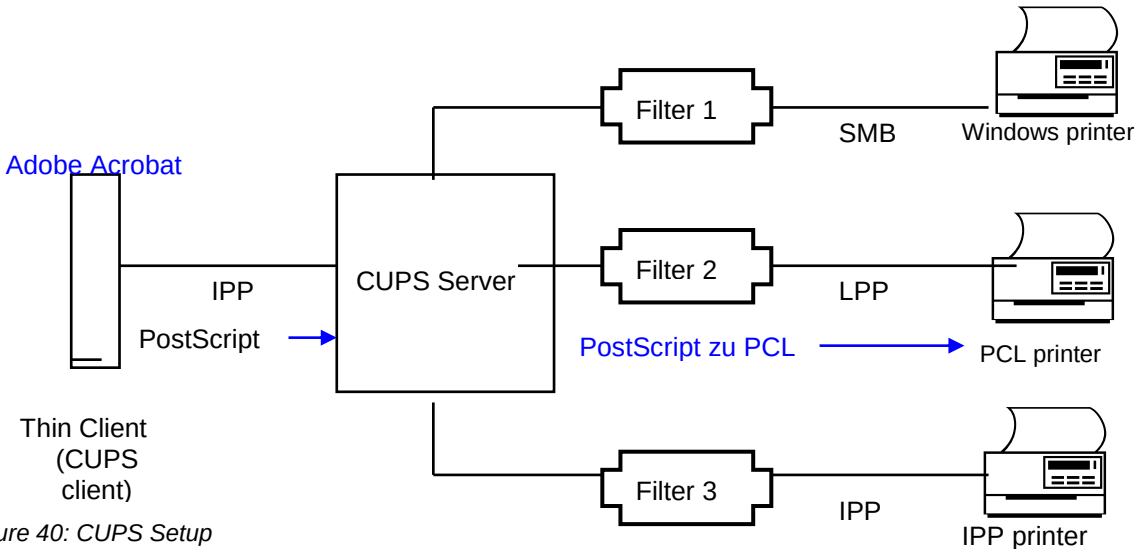


Figure 40: CUPS Setup

CUPS Procedure

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

⇨ To configure the CUPS client

1. Install the CUPS client on the Thin Client.
2. Install the CUPS server on a computer of your choice and configure the CUPS server.
   For information on how to install and configure the CUPS server, see www.cups.org.
3. In Scout Enterprise, set the following environment variables:

   CUPS_SERVER Host name or IP address of the CUPS server.

   CUPS_OPTIONS (optional) Allows you to preset user-dependent print options. These options are defined in the printer's *.ppd file. See your CUPS administrator for this value. For example: `CUPS_OPTIONS=-o OutputBin=Bin2`.

   Tip If you use LDAP or ADS, in place of the environment variable CUPS_OPTIONS set in Scout Enterprise you can use the user variable ELUX_PRINTEROPTIONS set on the LDAP or ADS server. For information on how to set an LDAP user variable, see User Variables.

4. Transfer the environment variables to the Thin Client.

The configuration is complete.

Example 1: Printing from a local browser

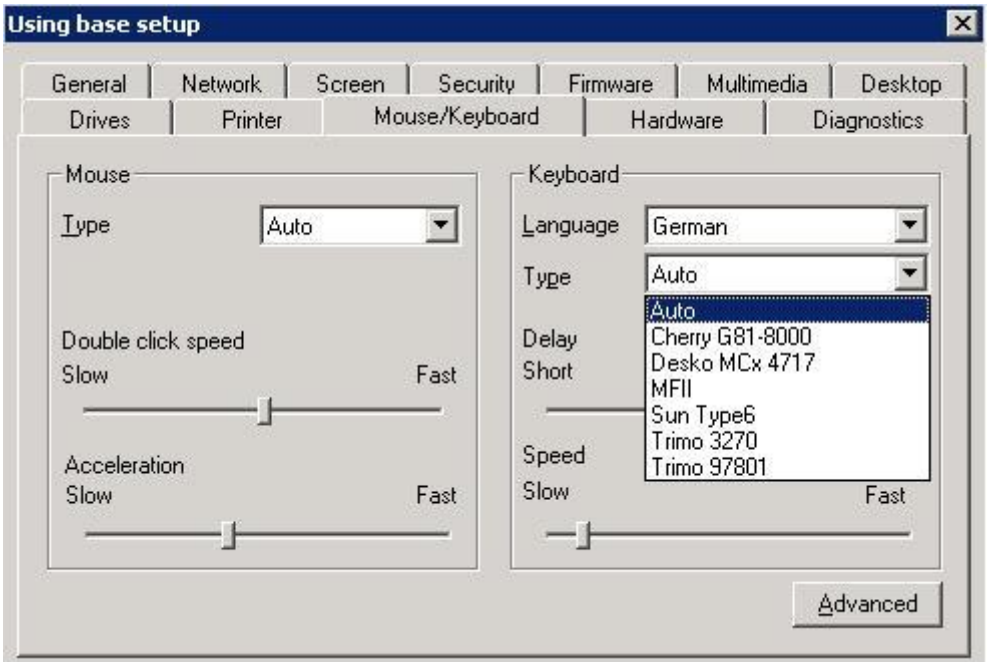
1. On the Thin Client, run Mozilla.
2. Go to the website of your choice.
3. In the **File** menu select **Print**. The **Print** dialog box appears. Do not make any settings in this dialog box. Just click **Print**.
4. The CUPS **Print** dialog box appears.
5. In the **Name** drop-down list, select the name of your printer (whether you can select a printer or not depends on server-side settings). Set other options as desired.
6. Press **OK** to begin printing.
7. After the print job has been sent, click **OK** to close the **Print information** dialog box.

Example 2: Printing from Adobe Acrobat

1. Run Adobe Acrobat.
2. Open the PDF file of your choice.
3. In the **File** menu, select **Print**. The **Print** dialog box appears. Do not make any settings in this dialog box. Just click **OK**.
4. The **Print** dialog box from CUPS appears.
5. In the **Name** drop-down list, select the name of your printer (whether you can select a printer or not depends on server-side settings). Set other options as desired.
6. Click **OK** to begin printing.
7. After the print job has been sent, click **OK** to close the **Print information** dialog box.

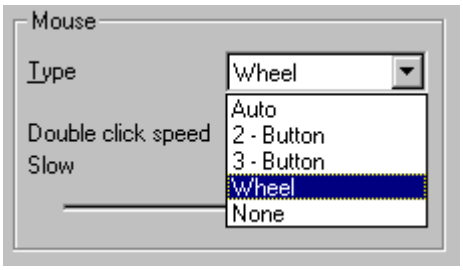
3.11 Mouse / Keyboard

Figure 41: Setup > Mouse /Keyboard



Both eLux NG and eLux *RL* support several types of mouse devices and keyboards.

Mouse



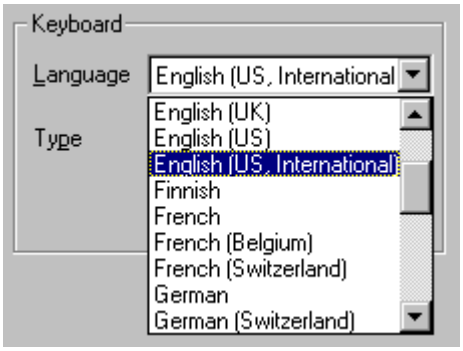
Choose the mouse type.

Auto means the mouse will automatically be detected. **None** is to run the client in terminal mode. The mouse functionality is deactivated and the mouse pointer is fixed in the lower right-hand corner of the user's screen.

Move the slider to the right to decrease the double-click interval.

Move the slider to the right to increase the mouse drag speed.

Keyboard



Choose the keyboard language from the country-specific list. The default is English (US). Keyboard types are automatically recognized when they are plugged in. No further configuration is necessary.

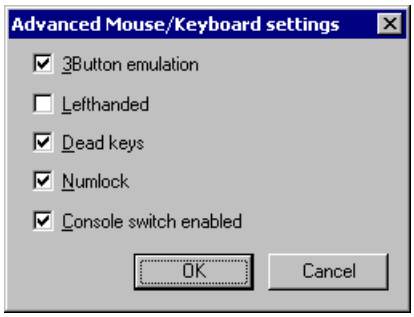
Move the slider to the right to decrease the initial delay before a symbol appears when a key is pressed and held.

Move the slider to the right to increase the key repeat speed.

Attention When configuring a Microsoft application via ICA, if you wish to use the Windows default option which moves the mouse pointer to the default button in a dialog box, set **Mouse connection** to PS/2. Be aware that the wheel function is not supported in this case. This modification is not required for Microsoft Remote Desktop Protocol (RDP).

3.11.1 Advanced Mouse and Keyboard Settings

From the **Setup** > **Mouse / Keyboard** subtab, click **Advanced**. Here you can configure the following advanced settings:



- **3 Button emulation** In general, eLux is used with a three button mouse. However, it is possible to achieve the same functionality with a two button mouse. In this case, the third button is simulated by clicking the left and right mouse buttons at the same time. Select to activate this feature.
- **Left-handed** Select to switch the mouse buttons.
- **Dead keys** Dead keys make it possible to enter accented combination characters. A dead key combination means that you press two keys one after the other (press the first key and release it, then press the second key and release it) in order to form a single character. In general, you press a key for the accent you want (nothing happens), then a key for the letter to apply to accent to (the accented combination character appears).
  By default, dead keys are active. If you use an application that is incompatible with dead keys, click to deselect.

  Note: Some hardware platforms do not offer this option. In this case, it is not possible to deactivate dead keys.
- **Numlock** Select to deactivate the NUM key when the Thin Client boots. By default, the NUM key is active.
- **Console switch enabled** Allows the user to switch between consoles on the Thin Client using the hotkeys. By default, it is active. The following table shows the hotkeys for switching the consoles. These hotkeys can be deactivated, restricting the user to the eLux NG desktop (console 1).

Nr.	Console	Hotkey
1	eLux NG Desktop	CTRL + ALT + F1
2	First XDMCP Session	CTRL + ALT + F2
3	Second XDMCP Session	CTLR + ALT + F3
4	Message Console	CTRL + ALT + F4

Figure 42: Hotkeys for switching consoles

When you are done, click **OK** in Scout Enterprise. Changes take effect the next time the Thin Clients restart.

3.12 Hardware

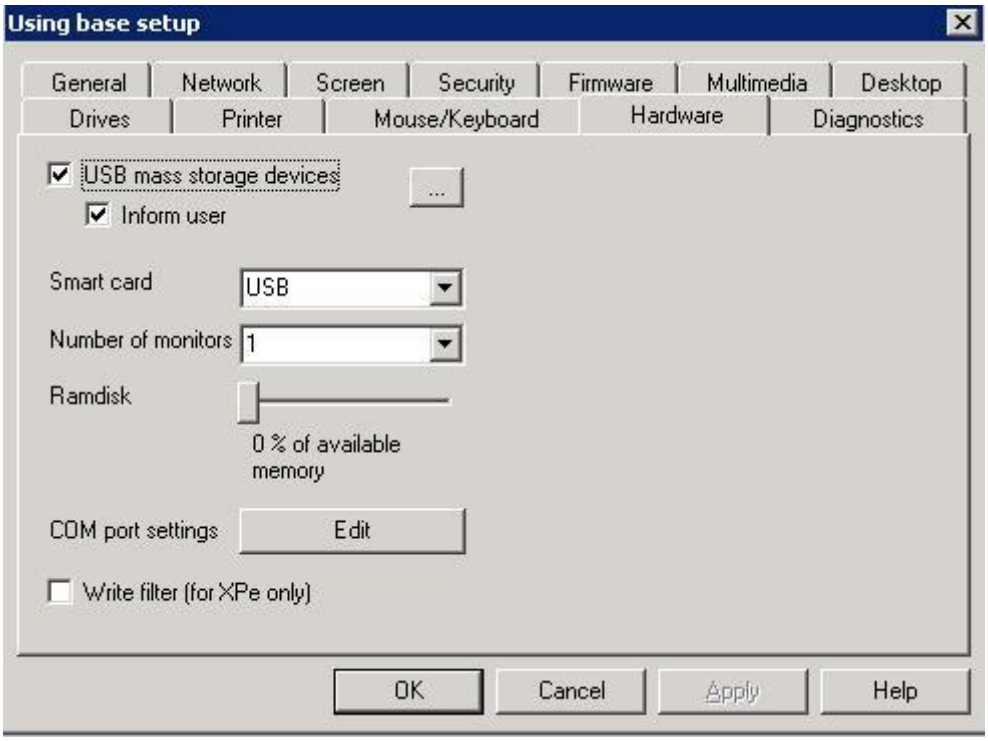


Figure 43: Setup > Hardware

The hardware settings – USB port activation, card reader activation, number of monitors, and RAM disk size – are set in the **Hardware** tab. The COM port settings can be edited from here.

Network hardware settings are described in a separate chapter.

3.12.1 USB Port Activation

In general, eLux supports all USB mass storage devices including, but not limited to, CD-ROM, floppy, USB stick, 2.0 flash card readers, photo mass storage, etc.

However, for security reasons, by default the USB ports for mass storage devices are disabled. To activate the USB ports for mass storage devices, click to select **USB mass storage devices**.

For details to access USB drives please see chapter 3.10.5 "Mountpoints".

3.12.2 Number of Monitors

If Thin Clients have the Matrox G200, Matrox G450 or Matrox G450 MMS graphics card installed, you can set the number of monitors to use in the **Hardware** tab. You can choose between one, two, three or four monitors.

3.12.3 COM Port Settings

You can set COM port settings in the **Hardware** tab.

Click on the **COM port settings** button. The **COM port settings** dialog box appears. Make the desired changes.

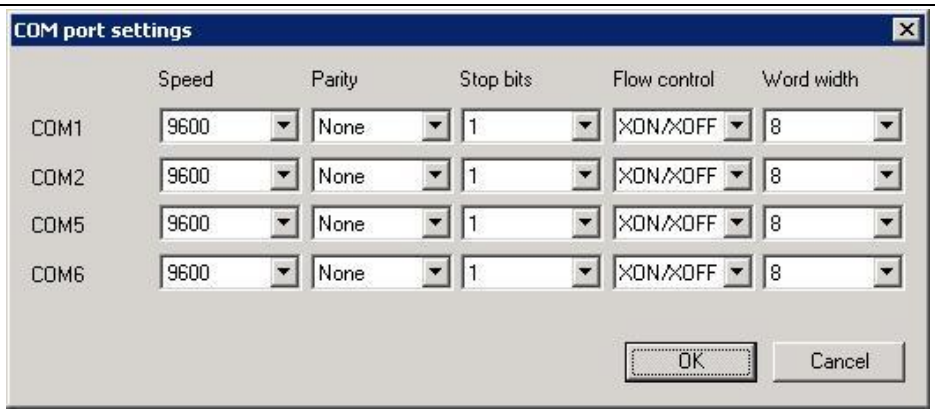


Figure 44: Setup > Hardware > COM-Port Settings

3.13 Smartcard

Smartcards can be used as an eLux security feature, for Citrix logon or for user roaming. The PC/SC lite interface is used.

The following features are supported:

- **Citrix ICA roaming** Allows you to capture a Citrix session that was running on another terminal by removing and inserting a smartcard.
- **PKSC#11** The PKSC#11 smartcard interface can be used by local applications, for example, by Mozilla to sign or encrypt emails.
- **RDP CSP** A Crypto Service Provider is server-side software. CSP can be used for RDP logon or to capture an RDP session that was running on another terminal (roaming).
- **Secure PIN** Allows you to enter a PIN on a card reader instead of via keyboard. The card verifies the PIN itself.

3.13.1 Smartcard Hardware Settings

Required Software

The PC/SC lite software has been removed from the base OS and is now available as a stand-alone upper-level package.

To use smartcards, the PCSC Lite" (pcsc_lite) EPM must be installed. Available driver FPMs:

- Generic CCID reader: Driver for a number of card readers. Supports secure PIN.
- OMNIKEY CCID: Driver for a number of card readers. Supports ICA roaming.
- REINER SCT: Driver for Reiner SCT USB card reader.
- OMNIKEY CT-API: CT-API to readout health insurance cards.

In ELIAS select the FPM to view the card readers supported by this driver. If the list exceeds available space, in the Package Information window click in the description field and drag with the mouse or press the PAGE DOWN key to view remaining entries.

For a description of EPMs and FPMs, see chapter 5.3 ELIAS.

eLux support a number of USB card readers and USB keyboards with integrated card reader. For a table of available drivers and their use, see www.myelux.com (log on > eLux software packages" > select container > click on Details next to PCSC lite").

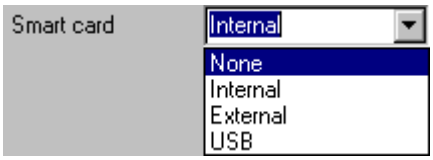
To activate the card reader, in the **Setup** dialog box, click the **Hardware** subtab. From the **Smart Card** list choose **USB** (do not select External").

Note: Internal" and External" are legacy features that are no longer supported by eLux NG. For information on eLux 1.1 smartcard support, see the Legacy" section later in this chapter.

Deactivating the Card Reader

If you do not have a card reader, deactivate the card reader hardware setting. This prevents the user from accidentally being locked out of an application.

1. In the **Setup** dialog box, click the **Hardware** tab.
2. From the **Smartcard** list click **None**.
3. Save your changes.



3.13.2 Local Authentication

You can restrict local access to the Thin Client by requiring a smartcard upon boot.

Local authentication works with the following smartcards:

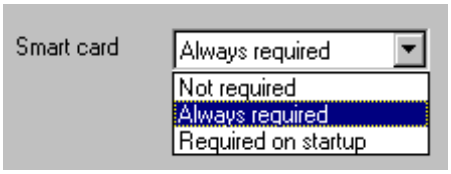
- CardOS® version M2 or M4 Siemens GmbH
- SICRYPT® CryptoCard Fujitsu Siemens Computers

They must be encoded with the users' logon data (name, password, if desired domain) using the SICRYPT SMARTY 2 software.

Local authentication requires a Fujitsu Siemens Computers card reader.

⇨ To configure the client for smartcard authentication

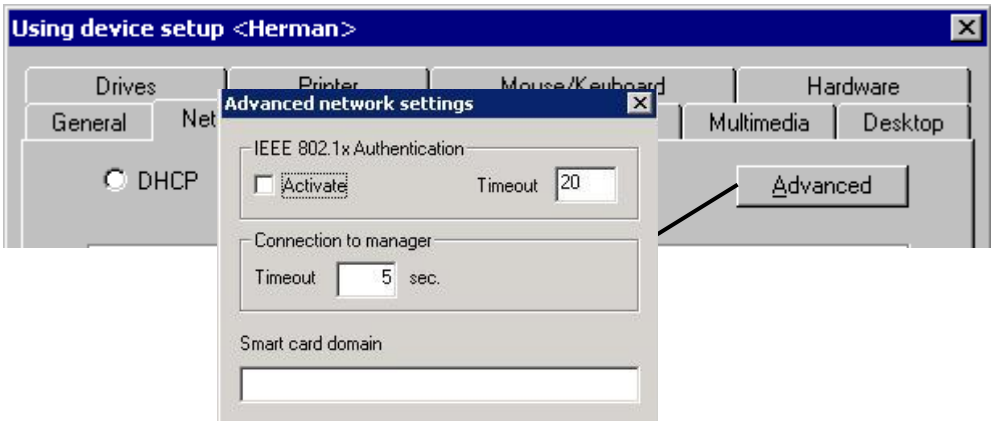
1. Set the smartcard hardware settings as described in 3.13.1 Smartcard.
2. Set the smartcard security settings. In **Setup**, click the **Security** subtab. From the **Smart card** drop-down list, click to select one of the following:



Always required A smartcard is required when the Thin Client boots as well as during the entire eLux session. If the user removes the card, the session will be locked. A smartcard and valid PIN are required to unlock the terminal.

Required on startup A smartcard is required only when the Thin Client starts. The local user can remove the card without interrupting the eLux session.

3. If the information saved on the smartcard includes a domain name, go to the **Network** tab, click **Advanced**, and enter the domain name in the **Smart Card domain** field.



Security settings have now been activated. Depending on the security settings you chose (step 2), the local user must now insert a smartcard into the card reader and enter a PIN at system start and whenever the card is removed and reinserted, or at system start only. The smartcard screen instructs the local user to insert a smartcard into the card reader and enter a PIN. The user is blocked until this is done.

Attention Do not mistype the PIN! If an invalid PIN is entered three times, the card is locked and can no longer be used. It must be reset by the smartcard administrator using the SICRYPT® SMARTY 2 software.

3.13.3 User Roaming

You can combine local authentication with another eLux feature: user roaming.

User roaming is transferring an active Windows terminal server session from one eLux terminal to another. This is useful when you want to move to a terminal with certain hardware – for example, with a special printer – without logging off from your current ICA or RDP session. In user roaming, the terminal disconnects the session when you remove the smartcard (the processes continue to run on the server) and reconnects when you insert the smartcard in a second terminal, using the second device's hardware settings (printer, drive mapping).

All terminals that will be used for user roaming must have user roaming enabled in advance.

User roaming works with the following smartcards:

- CardOS® version M2 or M4 Siemens GmbH
- SICRYPT® CryptoCard Fujitsu Siemens Computers

They must be encoded with the users' Citrix logon data (name, password, domain) using the SICRYPT SMARTY 2 software. A certificate is not permitted.

⇨ To configure eLux for user roaming

1. Set the smartcard hardware settings as described in 3.13.1 Smartcard.
2. Set the smartcard security settings. In the **Setup** dialog box, click the **Security** subtab. From the **Smart card** drop-down list, click to select the following:

3. Click **Apply** and **OK** to close the **Setup** dialog box.
4. Configure one of the following sessions:

   ICA See 4.2.1 Remote desktop.

   RDP See 4.4.1 Configuring a Session.

5. In the application definition, click to select **Roaming**.

   Logon information is read directly from the card. The entries **User**, **Password**, **Domain** in the application definition dialog will be ignored.

   Note: The option **Allow smartcard logon** (see next chapter) cannot be combined with user roaming.

Activating the **Roaming** check box starts the terminal server session automatically. The ID is dynamically read from the smartcard and used to connect to the terminal server. If the local user removes the smartcard, the terminal server session is disconnected. Therefore, certain settings must be defined on the terminal server. For further information, consult the terminal server manual.

Citrix Logon

You can restrict access to a Citrix XenApp server by requiring a smartcard upon logon. This feature is distinct from local authentication and user roaming and cannot be combined.

Citrix smartcard logon works with a number smartcards. Users' logon data (name, password, domain) as well as a certificate are saved to the smartcard. You must have the corresponding smartcard software installed on your XenApp server. See the Citrix documentation for more information.

⇨ To configure eLux for Citrix ICA smartcard logon

1. Set the smartcard hardware settings as described in 3.13.1 Smartcard.
2. Set the smartcard security settings. In the **Setup** dialog box, click the **Security** subtab. From the **Smart card** drop-down list, click to select the following:

   Not required This disables eLux security settings, freeing up the card reader for other applications, in this case, for the Citrix ICA client.

   Click **Apply** and **OK** to close the **Setup** dialog box.
3. Configure an ICA session. Click to select **Allow smartcard logon**. Leave **Roaming** deselected.

3.13.4 RDP Logon

To use this feature, your terminal server must support RDP 5.2 or higher. In addition, on the thin client you must have base OS 1.14.1 or higher and the RDP native client 1.4.0 or higher installed (rdesktop52").

You can restrict access to a terminal server by requiring a smartcard upon logon. This feature is distinct from local authentication and user roaming and cannot be combined.

RDP smartcard logon works with a number of smartcards. Users' logon data (name, password, domain) as well as a certificate are saved to the smartcard. You must have the corresponding smartcard software installed on your server.

The following cryptographic service providers are supported:

- GemSAFE™ from Gemplus®
- SafeSign® from Thales e-Security Ltd.

⇨ To configure eLux for RDP smartcard logon

1. Set the smartcard hardware settings as described in 3.13.1 Smartcard.
2. Set the smartcard security settings. In the **Setup** dialog box, click the **Security** subtab. From the **Smart card** drop-down list, click to select the following:

   Not required This disables eLux security settings, freeing up the card reader for other applications, in this case, for the RDP client.

   Click **Apply** and **OK** to close the **Setup** dialog box.
3. Configure an RDP session as described in 4.4.1 Configuring a Session. Click to select **Allow smartcard logon**. Leave **Roaming** deselected.
4. Click **Advanced**.
5. In the **RDP advanced** dialog box go to the **Advanced** tab and set the protocol to Auto" or RDP V5.
6. Go to the **Local Resources** tab and select the **Enable smartcard** check box.

3.14 Virtual Private Networks

A virtual private network (VPN) is a system that allows two or more private networks to be connected over a publicly accessible network, such as the Internet. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. A VPN can be used to exchange critical information between employees working remotely or to securely deliver information between business partners

The following VPN Clients are supported currently:

- Cisco VPN Client
- VPNC VPN Client
- PPTP VPN Client
- Juniper

3.14.1 Cisco VPN Client and VPNC

The Cisco VPN client is used to connect to a Cisco VPN device to create a secure connection between the Thin Client and a private network. It uses Internet Key Exchange (IKE) and IP Security (IPSec) tunneling protocols to establish and manage the secure connection. You can connect using LAN, DSL or ISDN to one of the following:

- Cisco IOS devices that support Easy VPN server functionality
- VPN 3000 Series Concentrators
- Cisco PIX Firewall Series

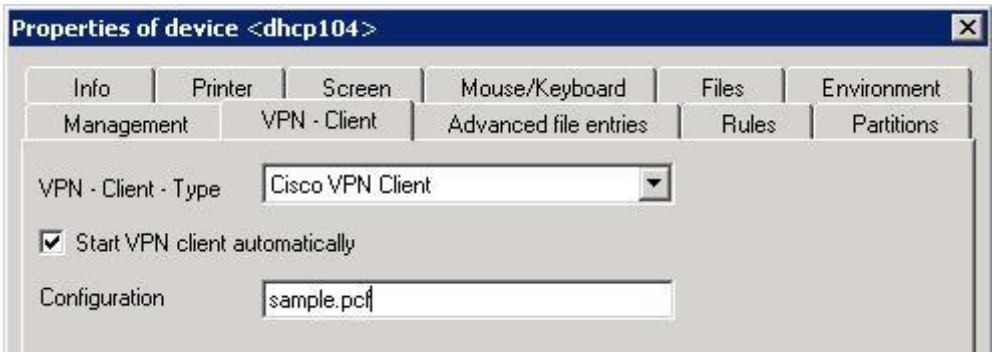


Figure 45 Setup > VPn > Cisco VPN Clilent

First configuration and editing the configuration files must be done on the Thin Client. Depending on the type of VPN Client you use the corresponding configuration file must be available on the client.

Therefore we ask you to consult our manual **"eLux Administrator's Guide"** (chapter 3.17) where we describe the procedure of configuration and editing in detail. You always find the latest version in the download area of www.myelux.com.

4 Management on Application Level

This chapter contains information on how to configure applications..

4.1 Introduction

You can define applications on three levels:

- as default application on the highest level of the hierarchy
- in the default group Lost&Found
- in each organisation unit.

Rightclick the highest level of **Applications** to select from the context menu:

Figure 46: Context menu of applications

Rightclick **Define application icons** to add icon files which then are available for selection in the configuration of the single applications. The files may be of the types xpm, ico or gif.

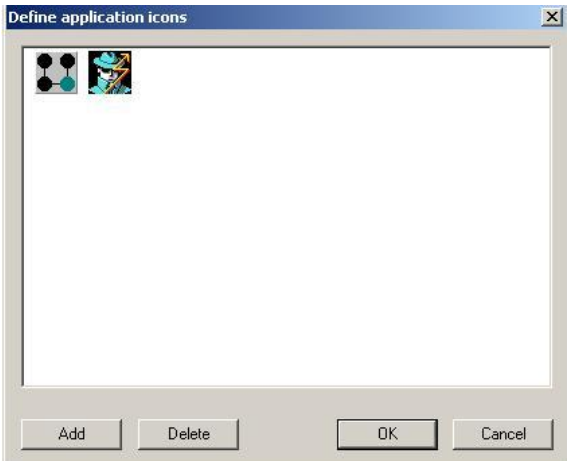


Figure 47 Define application icons

4.1.1 Add

Selecting **Add** from the Application category context menu opens the **Application Properties** dialog box.

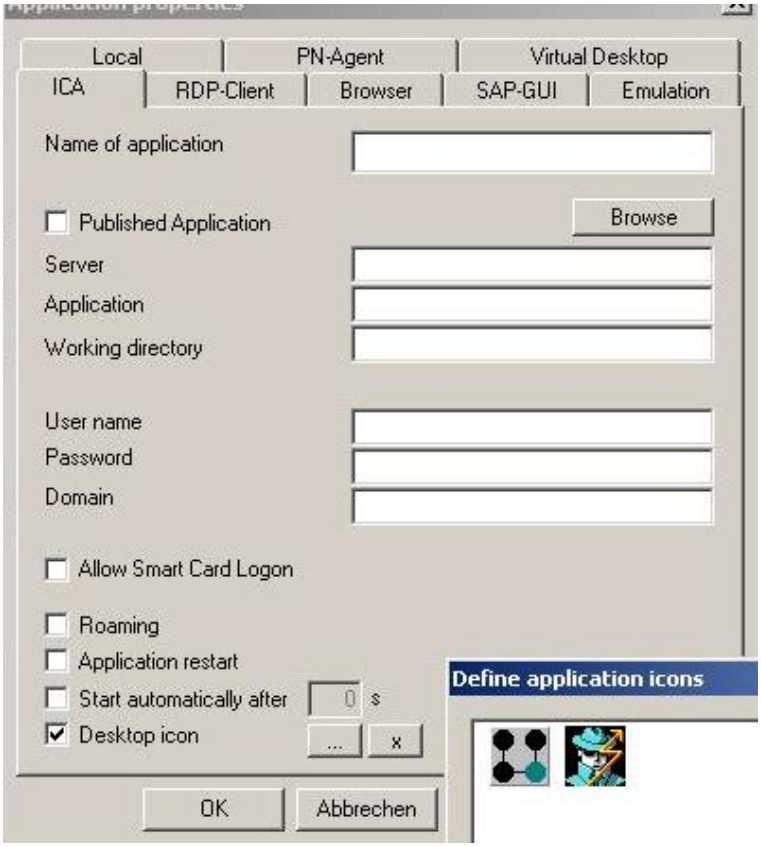


Figure 48: Application Properties

Possible connections include: ICA, RDP, local browser, SAPGUI, emulation, local commands and PN agent.

Every application offers an **Application restart** check box. When this check box is selected, the connection is started when the Thin Client boots and immediately re-established after a user logs off, making it available for the next user.

Every application offers a **Start application automatically** check box. When this check box is selected, the connection is started when the Thin Client boots.

Every application offers a **Desktop icon** check box. When this check box is selected, desktop icons are offered for selection from a list (provided icons have been defined on the highest application level). **Note**: Not available for Program Neighborhood Agent.

If an icon is distorted, on the thin client double-clicking with the middle mouse button on an icon redraws all icons.

The remaining options are application specific. Configuring applications is discussed in detail in the remaining sections of this chapter.

In the **Edit** menu select **Find** or use the shortkey CTRL + F to search for an application name.

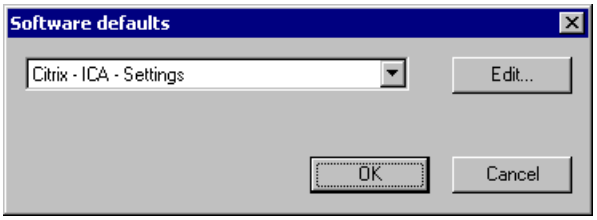
Figure 49: The Find function

4.1.2 Software Defaults

It is possible to set standard parameters for all applications defined for an element.

Rightclick an Applications category to open the context menu. Select **Software defaults**.

In the **Software defaults** dialog box, you can set all standard settings for applications.



At the moment, only ICA is available. Select **ICA** and click **Edit**. In this dialog box you can edit all ICA standard parameters. Settings are valid for the selected organization unit. These settings are described in detail in chapter 4.2.4.

The tabs **General**, **Drive Mapping** and **COM-Ports** are described in chapters 3.10 and 3.13.

4.1.3 Option – Use Parent Applications

In the Applications category context menu (click with the right mouse button on the Applications category), "Use parent applications" is a toggle. If selected, you will assign the applications from the next higher-ranked element to the device in addition to the applications for this element. When the Application category is selected, applications from other elements are displayed in the Properties Window in parentheses.

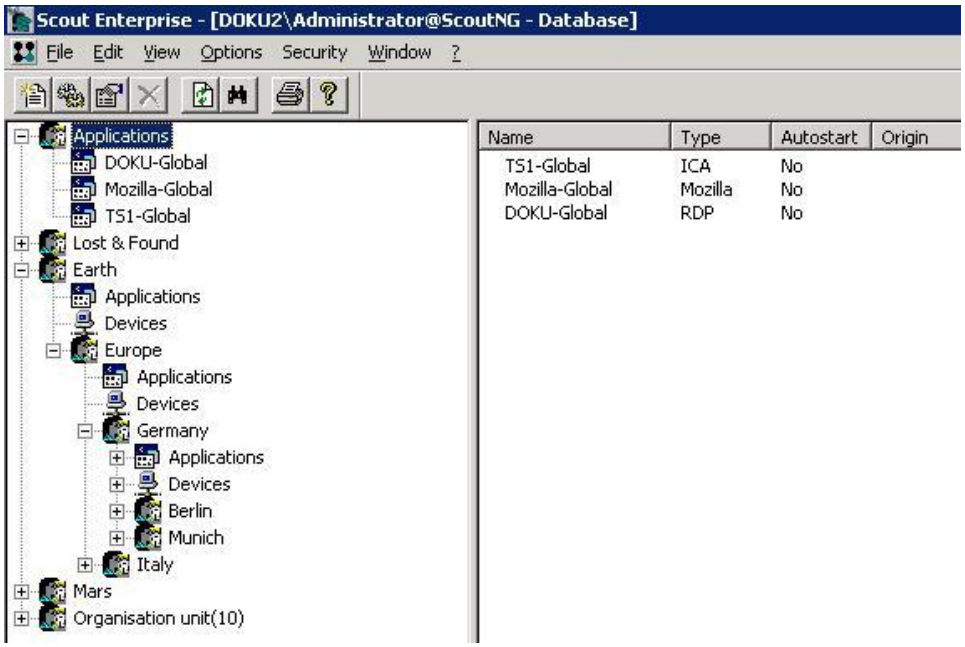


Figure 50: Default Applications

In the figure above, all the organization units Lost&Found", Earth", Europe and Germany have been configured to use parent applications. Devices entered into the different organisation units will receive the applications defined for

1. the selected **ou**,
2. the default set (Applications).

Note: Applications are identified by their name. To avoid conflicts, please use unique names when configuring applications.

4.1.4 Option - Use Parent Defaults

The option "Use parent defaults" applies to the **Software Defaults**, which at the moment are availabe for Citrix ICA settings only, see 4.1.2.

4.1.5 Tree View

Properties Window

Once you have configured applications, click on an Applications category. A list of all applications defined for this element is displayed in the Properties Window. You can customize the information displayed by selecting **Adjust** from the Properties Window context menu (right click in the Properties Window). The following properties are available:

- Name
- Type
- Autostart

If no applications have been defined, the window will be empty.

Commands

In the Properties Window, click to select an application. You can select more than one application by holding down CTRL or SHIFT. Applications can be:

- copied to a new organisation unit
- moved to a new organisation unit
- deleted

using the key combinations CTRL-C, CTRL-X + CTRL-V (copy and paste), or DEL, or the context menu (click with the right mouse button). In addition, you can use the left mouse button to move single application definitions and Application categories to other groups using the drag-and-drop feature. Hold the CTRL key while dragging to copy them to other groups.

4.1.6 User Access to Applications

The applications defined in Scout Enterprise are transferred to the Thin Client when the terminal boots. The local user can then access them in the eLux control panel (**Applications** tab) or from the toolbar menu.

If applications do not appear on the Thin Client, check the following:

- **Missing firmware** While the administrator can configure all types of applications, the only applications available on the Thin Client are those whose software is installed in the image file.
- **Hidden option** It is possible to hide applications from the user. This option is only available for local applications that are defined as custom". In this case, you must select the Application restartor Start application automaticallyoption for the application to run.
- **Duplicate names** Applications are identified by their name. To avoid conflicts, please use unique names when configuring applications.

4.1.7 Uploading Applications

You can also upload applications from a Thin Client to Scout Enterprise. Applications can only be uploaded to an organization unit.

Select the device whose applications you want to upload. Use the menu command **File** > **Application upload** or rightclick the device and select **Application upload**. The **Application Upload** dialog box appears.

Check the IP address or host name of the device is correct. Select a Group to upload the applications to.

Click **Start** to begin the upload. All applications defined on the Thin Client are sent to the Scout Enterprise server and entered in the selected organisation unit. Previously defined applications in the organisation unit are deleted.

Note: Please do not upload applications from previous eLux versions to Scout Enterprise, as this has unknown consequences. Only upload applications to Scout Enterprise.from devices running eLux .

Conclusion

The flexible arrangement of applications into organisation units and standard applications opens an array of possibilities for the administrator to define applications – by physical location, type of work, user profiles etc.

4.1.8 Editing Configuration Files

A configuration file is used to store and retrieve settings. Generally, it contains the user's personal parameters for running client software. Configuration files are saved to the Thin Client in the following directory: `/setup/`<*application name*>.

Scout Enterprise offers various ways to edit a configuration file.

Application definition

The application definition is the first step. Often you can set selected parameters directly in the application definition. For example, in the **ICA** dialog you can set the connection parameters by clicking **Connection options**, in the **Emulation** dialog for eterm a number of fields will appear. These parameters will be saved directly to the configuration file.

Software defaults

You can set additional parameters by using the software defaults function (4.1.2 Software). At the time of publishing, this is only available for ICA.

File transfer

You can configure an application locally on a terminal and use Scout Enterprise to transfer the configuration file to other terminals. This is useful for emulations, where configuration takes place inside the application itself. See the respective product documentation for configuration information and for the file transfer function.

INI file editor

Scout Enterprise comes equipped with an editor for initialization (INI) files. This allows you to edit specific keywords in an INI file.

4.2 ICA

To connect to a XenApp® Server by Citrix® Scout Enterprise offers 5 different ways:

- Connect to a dedicated XenApp Server (always desktop) – chapter 4.2.1
- Connect to a published application (could also be a published desktop) – chapter 4.3.1
- Connect via web interface without Browser (PN-Agent) – chapter 4.3.2
- Connect via web interface with Browser – chapter 4.3.3
- Call of the Citrix Receiver (Citrix-own tool to define a connection) – chapter 4.3.4

Independent Computer Architecture (ICA®) is used to connect to a Windows terminal server running Citrix® XenApp® software. You can then access all Windows® applications residing on the terminal server.

All connection parameters and standard parameters for an **ou** can be set in Scout Enterprise (corresponds to the **Citrix ICA Client for Linux** advanced ICA settings on the Thin Client in the eLux control panelusing **Configuration** > **ICA** > **Advanced**).

The ICA Connection Center can be defined as a local application. For details see chapter 4.2.7.

4.2.1 Remote Desktop

A remote desktop session allows users access to the desktop of a XenApp server. Users can run any applications available on the desktop, in any order.

To create or modify a session via ICA, go to **Application Properties** > **ICA**.

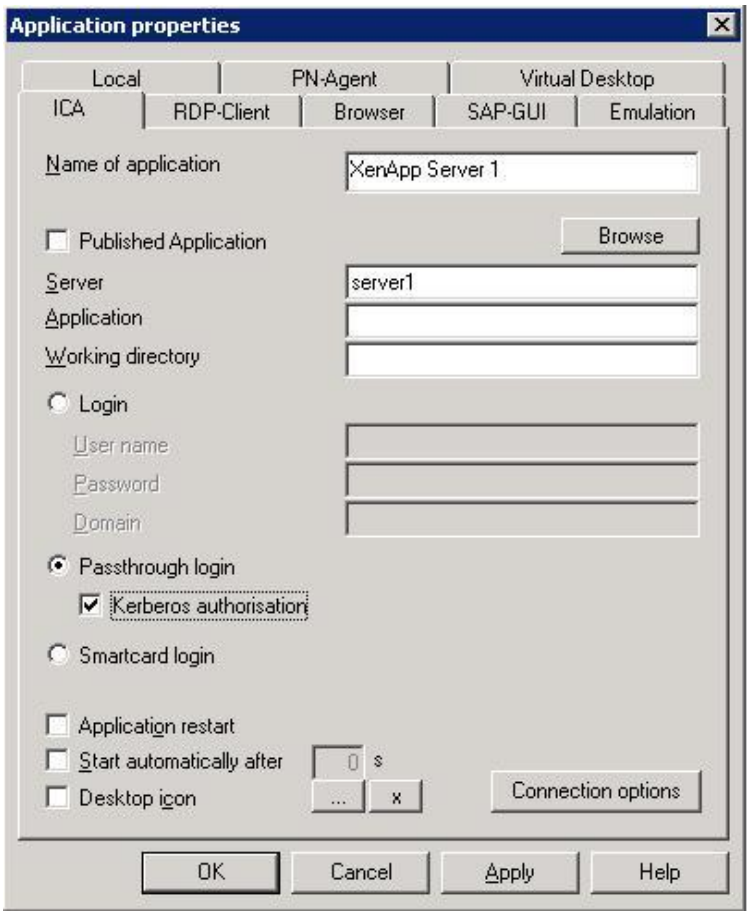


Figure 51: Application Properties for ICA Remote Desktop

Name:	Enter an appropriate name for this application. This is what the local user sees in the eLux NG main screen (**Applications** tab).
Published Application:	Leave deselected.
Server:	Enter the IP address (or name) of a XenApp terminal server.
Application:	Leave blank.
Working Directory:	Leave blank.
Login	Enabling this option the logon data (user name, password, domain) are entered in Scout.
Passthrough Login	Enabling this option the values for $ELUXUSER $ELUXPASSWORD and $ELUXDOMAIN are sent to the client.
Kerberos authorisation	The client uses the user credentials of the Kerberos ticket received from the ADS authentication.
Smartcard Login	The client uses a smartcard to logon.

The flag for **'Roaming'** has disappeared from the ICA dialog. This function is to realized by setting 'Disconnect when removing card' and the 'Autostart' flag fo the application.

4.2.2 Smart Card User Roaming

eLux supports user roaming with USB card readers and CardOS 2.0 and SICRYPT smartcards coded with SMARTY 2 software.

COM card readers are not supported.

4.2.3 Connection Options

From the ICA application definition, click the **Connection Options** button which opens the dialog box **Advanced ICA Settings**.

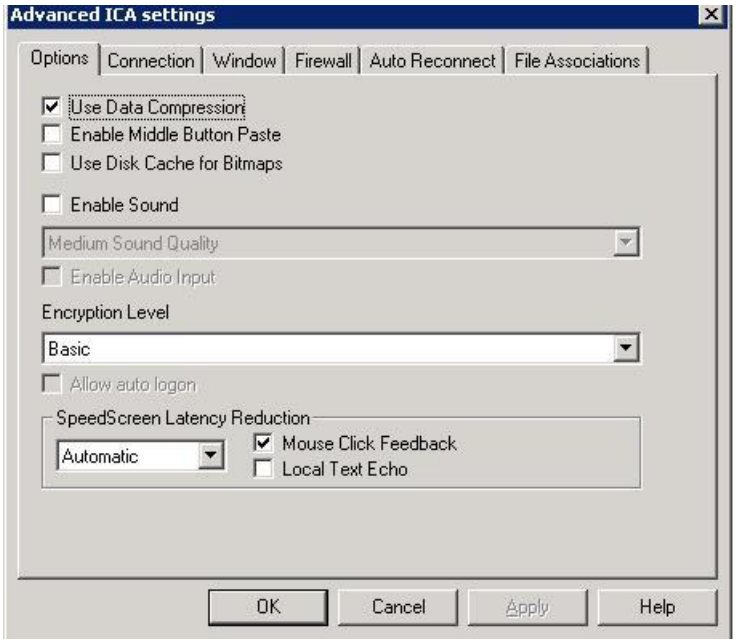


Figure 52: Advanced ICA Settings – Connection Parameters for Citrix ICA

In this dialog box you can set connection parameters such as sound, encryption level, SpeedScreen latency reduction, and Window settings. Connection parameter changes are applied to all devices in this organisation unit.

These parameters correspond to the parameters on the Thin Client in the **Citrix Presentation Server Client for Linux** (eLux NG / RL - ICA definition > **Advanced**) in the **Tools** menu > **Settings**).

It is possible to force an autologin even if the encryption level of ICA settings is not basic. Click to select the **Allow auto logon** check box.

Click to select **Software Defaults** to use the standard settings. These settings are discussed in the following chapter.

For more information on the Citrix ICA connection parameters, see the Citrix documentation.

4.2.4 ICA Software Defaults

The standard parameters are accessed by clicking with the right mouse button on the **Applications** category. Select **Software defaults**. Using the **Software Defaults** dialog box you can access all standard settings for applications.

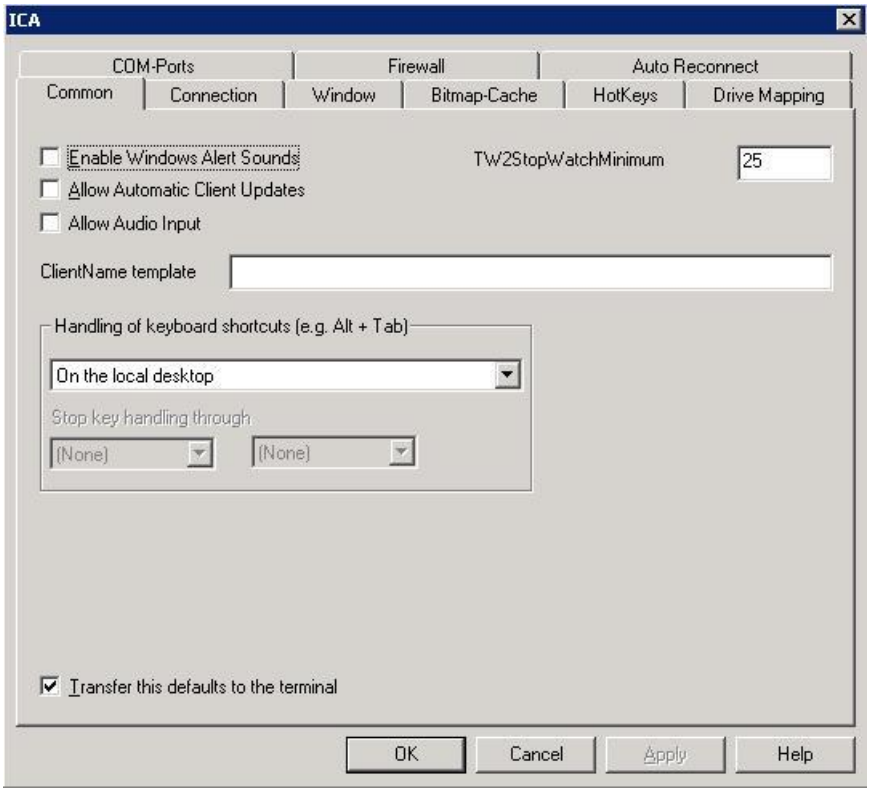


Figure 53: Applications - Software Defaults

Select **ICA** and click **Edit**. In this dialog box you can edit all ICA standard parameters. Changes made to the ICA standard parameters are applied to all devices in this organisation unit.

These parameters correspond to the parameters on the Thin Client in the **Settings** dialog box of the Citrix ICA Client for Linux (eLux ICA definition > **Advanced** > **Tools** menu > **Settings**).

For more information on the Citrix ICA standard parameters, see the Citrix documentation. A few are described below.

Common tab

- **Transfer these defaults to the terminal** When activated, the advanced settings will be transferred to the terminal. Default is activated.
- **TW2StopwatchMinimum** (default = 75) Set the scroll speed for ICA applications (for example, Adobe® Acrobat® Reader, Excel®, etc.). A large value means a slower scroll speed. A low value means a faster scroll speed, however in Excel the delay time will be increased when you drag the cursor outside the lower border when making a selection.
- **ClientName template** Allows you to set the client name in the XenApp session. **Note**: You c an use the Program Neighborhood variables $ICANAME, $ICADOMAIN to set a unique client session name. This is required for Citrix roaming and by some XenApp rame programs.

Drive Mapping

By default, the floppy and CD-ROM drives are automatically mapped to the ICA session at terminal logon.

To view the default drive mapping:

1. Open the standard ICA parameters. Click on **Drive Mapping**.
2. The letters A-Z represent the logical drive names on the terminal server. The field to the right is the mount point on the Thin Client. (The mount point names are standard and listed in section 8.10) The columns are as follows: E = enable,R = read,W = write.”
3. By default, the floppy drive is mapped to A:”, the internal (IDE) CD-ROM to C:”.
4. Confirm that the **Enable drive mapping** check box is selected.
5. Use the drives to access the devices.

To use standard settings, no further configuration is required.

USB drives

USB drives are not automatically mapped.

1. To map a USB drive, open the standard ICA parameters. Click on **Drive Mapping**.

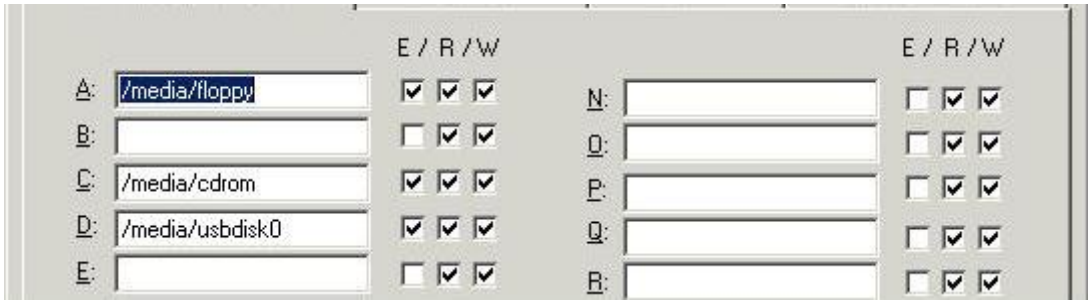


Figure 54: ICA Drive mapping for eLux RL

2. ICA – tab Drive Mapping for eLux RL

The first partition on the first USB stick is assigned /media/usbdisk. Every further partition (on the first stick or a second stick) is mapped to:
/media/usbdisk0, /media/usbdisk1, .../media/usbdisk<N> .

COM Ports

To map a COM port, you must know the device name of the serial port on the client.

The serial port device name always begins with /dev:

- /dev/ttyS0 : external serial port
- /dev/ttyS1 : internal serial port
- /dev/usb/tts/0 : USB v. 24 converter (PL2303 chip only)

Note: Device names are case sensitive. The letters shown here in lower case must be typed in lower case.

Which serial ports are available depends on your hardware platform.

Mapping a COM port in an ICA session involves the following:

1. Configuring the COM port settings in Scout Enterprise
2. Transfer settings to the Thin Clients
3. Configuring the Citrix XenApp ICA server

⇨ To configure the COM port settings in Scout Enterprise

COM port settings are mapped in the Standard Parameters dialog box for ICA.

1. Click the right mouse button on an applications category and select **Software defaults**.
2. Select **Citrix – ICA – Settings** from the drop-down list and click **Edit**.
3. Go to the **COM port settings** tab.
4. Click **Add**. Enter the device name of the serial port.
   Note: Case sensitive.
5. Click **OK**.

A new COM port will appear, numbered automatically in ascending order. If this is the second port you have entered, it will be named COM2.

6. Click **Apply** and **OK** and save your settings in Scout Enterprise.

⇨ To transfer settings to the Thin Clients

Reboot the Thin Clients to transfer settings.

⇨ To configure the Citrix XenApp ICA server

1. Connect to the XenApp server and open a command shell.
2. Map the Thin Client COM port to the COM port on the XenApp server using the following format:
   `net use` <*ICA port*>`: \\Client\`<*Thin Client port*>`: /persistent:yes`
   <*ICA port*> : local port on XenApp server
   <*Thin Client port*> : remote port on Thin Client
   Example:
   `net use com1: \\Client\COM2: /persistent:yes`
3. Following are useful commands:
   net use : To view the mapping (for a drive, printer, COM port, etc.)
   mode com1: : To view the parameters
   mode /? : To change parameters
   net use /help: To view man pages

Normally the port parameters are set within your application.

This procedure should work with all COM port based synchronizing software.

To set COM port hardware settings, see 3.12.3 COM Port Settings.

4.2.5 Keystore for Citrix Server or Access Gateway

The directory `/setup/cacerts` is reserved for Certified Authority (CA) root certificates.

If you have a certificate for logging on to a Citrix Server or Access Gateway, save it here.

4.2.6 Tool xcapture to Create Screenshots

To use this feature, you must have the Utils for ICA Client" package installed. It is located in the ICA client" package.

The Citrix ICA Client for Linux includes a helper application, xcapture, that allows you to exchange graphical data between the XenApp server clipboard and non-ICCCM-compliant X Windows applications on the X desktop. You can use xcapture to grab dialog boxes or screen areas and copy them between the UNIX desktop (including non-ICCCM-compliant applications) and an application running in an ICA Client window.

⇨ To configure xcapture

Click with the right mouse button on an Applications category and select **Add**. Click **Local**.

Name	Enter an appropriate name for this application.
Application	Click **Customized**.
Parameter	Enter `/usr/lib/ICAClient/util/xcapture`
Hidden	Does not display the application in the **Application** tab.
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

How to use xcapture

1. From the **xcapture** dialog box, click **From screen**. The cursor changes to a crosshair.

   Select a window Move the cursor over the window you want to copy and click the middle mouse button.

   Select a region Hold down the left mouse button and drag the cursor to select the area you want to copy.

2. From the **xcapture** dialog box, click **To ICA**.

   The xcapture button changes color to show that it is processing the information.

3. When the transfer is complete, switch to the ICA session. Use the paste command to insert the contents of the clipboard in the application.

4.2.7 Tool ICA Connection Center

By means of the ICA Connection Center the end user can see online all current server connections of published applications, these can be disconnected or logged off without activating the application. The ICA Connection Center can be defined as a local application.

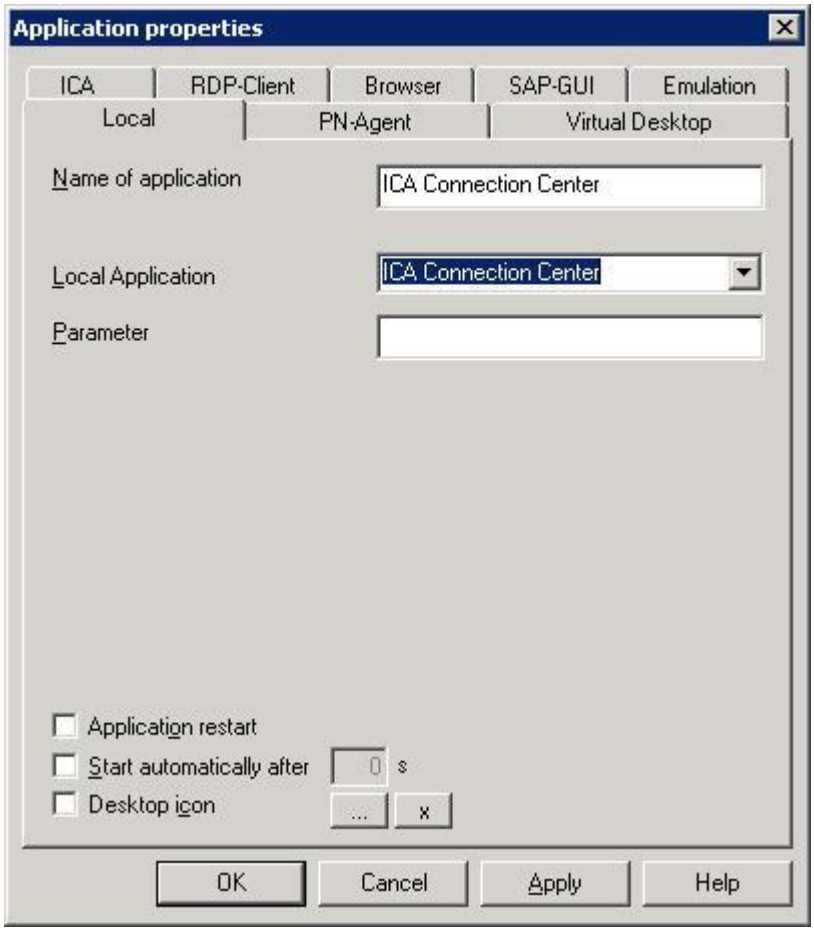


Figure 55: ICA Connection Center

Minimum requirement: At the client the ICA Client version 9.15.-5 or higher and the eLux NG BaseOS 1.36-1 must be installed.

4.3 Connecting to a Published Application

A connection to a published application lets a user access a predefined application and its associated environment.

Published applications can be run in seamless mode, where the applications appear to the Thin Client as if they were running locally, each application running in its own resizable window. If a published application is defined as a seamless window, be sure to activate the eLux NG taskbar in the **Desktop** tab. This allows minimized windows to be enlarged again.

Published applications require server-side and client-side configuration. In this section, we will discuss client-side configuration.

4.3.1 Via ICA Session

This section describes how to configure a session to a published application running on a XenApp server. Note: You must know the application name exactly as it is published on the server.

To create or modify a session via ICA, go to **Application Properties** > **ICA**.

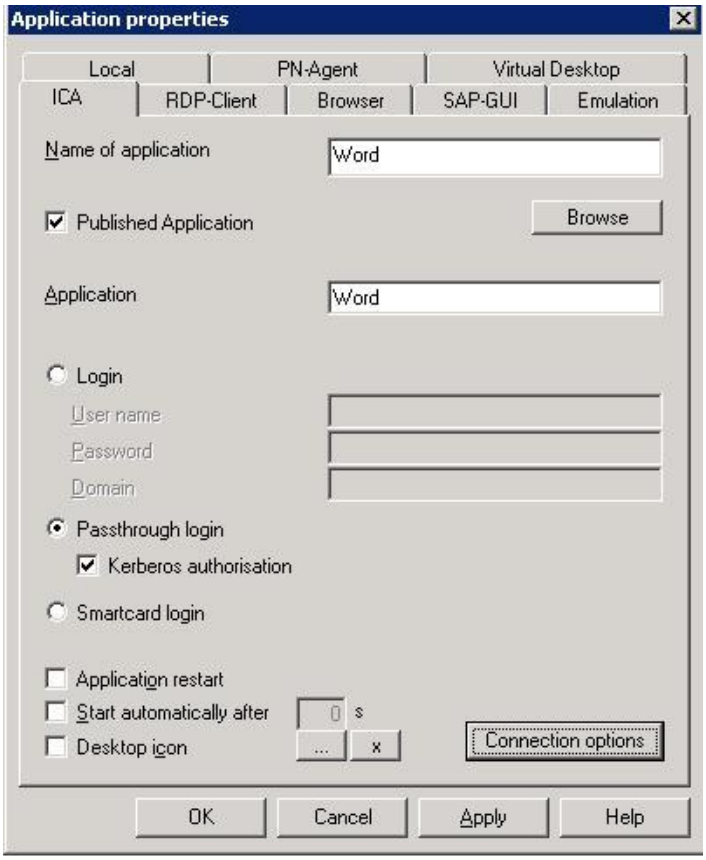


Figure 56: Application properties for ICA – Published Application

Name: Enter an appropriate name for this application. This is what the local user sees in the eLux NG main screen (**Applications** tab).

Published Application: Select.

Application: Enter the name exactly as it is published on the XenApp server.

Login Enabling this option the logon data (user name, password, domain) are entered in Scout.

Passthrough Login	Enabling this option the values for $ELUXUSER $ELUXPASSWORD and $ELUXDOMAIN are sent to the client.
Kerberos authorisation	The client uses the user credentials of the Kerberos ticket received from the ADS authentication.
Smartcard Login	The client uses a smartcard to logon.

4.3.2 Via Program Neighborhood (PN Agent)

PN Agent serves to display all published applications by entering the server name of the XenApp web interface directly into an application definition.

⇨ To configure a session to launch the PNAgent

Click on an **Applications** category of the selected Group with the right mouse button. Select the **Add** context menu. Open the **PC-Agent** tab.

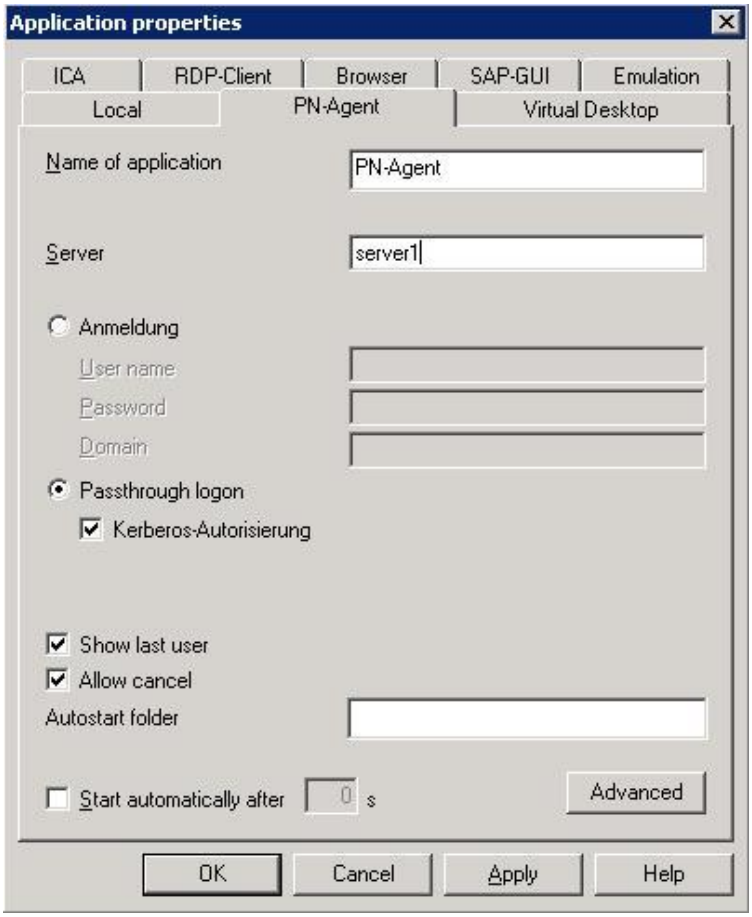


Figure 57: Configuring a PNAgent application

Name	Enter an appropriate name for this application.
Server	IP address or name of the web interface Alternatively, if the Citrix Web interface is not running on port 80 or if the configuration file does not have the standard path /Citrix/PNAgent/config.xml", you can enter an URL to direct the client to

	the configuration file on the server. Format: `http://<server>:<port>` or `http://<server>/<path>` .
	Example:
	`http://server1/Citrix/PNAgent/config.xml`
	`http://server1:81`
	`http://server1/MyNfuse/config.xml`

Passthrough logon	Enabling this option the values $ELUXUSER $ELUXPASSWORD and $ELUXDOMAIN are sent to the client.
Kerberos authorisation	The client uses the user credentials of the Kerberos ticket received during the ADS authorisation .
Show last user	(optional) The user credentials (except for password) of the last logon will automatically be displayed in the XenApp logon dialog box. Note that this option has no effect if you enter user credentials for automatic logon.
Allow cancel	(optional) When activated, allows the user to close the XenApp logon dialog box.

Advanced PN-Agent settings

Click on **Advanced** to display the **Advanced PN-Agent settings** dialog box. Here you can set the **window properties** for this application. If you click **Use default**, the settings as defined on the server will be used.

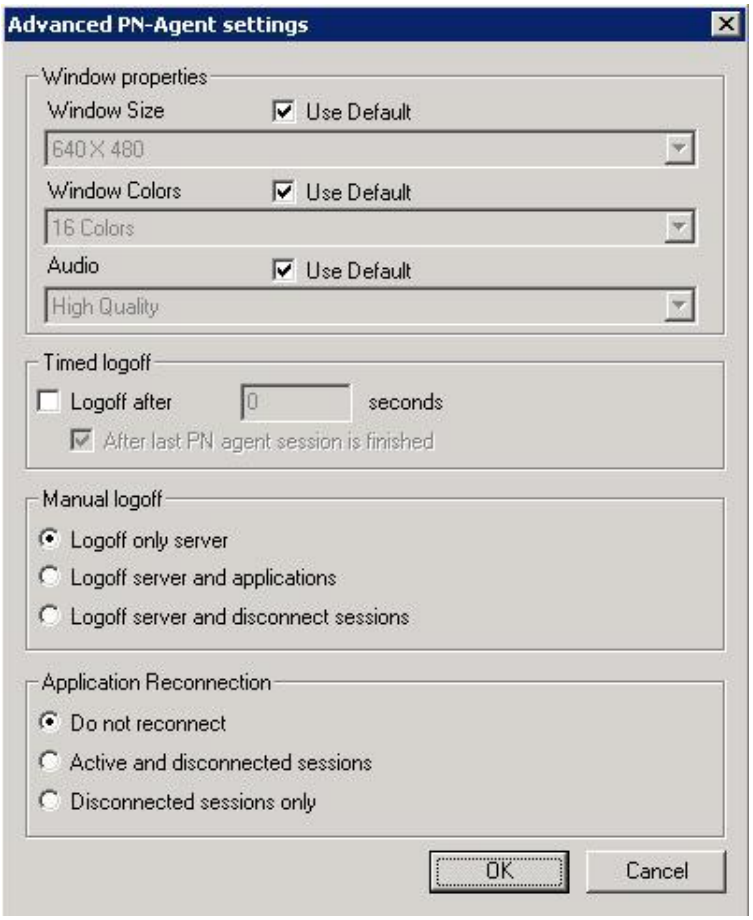


Figure 58: PN-Agent – Advanced Settings

⇨ Time-controlled Logoff of a PN Agent Session

The timed logoff of a PN Agent session can be performed without having to wait for the last o PN Agent session to finish (Forced Logoff).

Additionally it can be defined if in case of timed logoff all active PN Agent applications are to be disconnected as well.

When the session connects, the Thin Client will retrieve all published applications from the defined XenApp server which were published for the given user credentials.

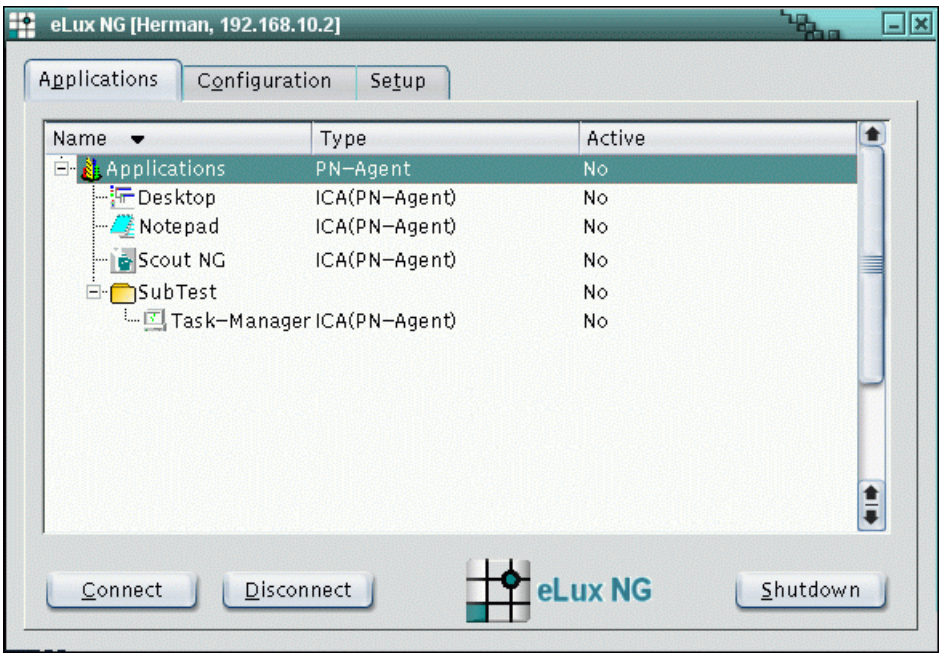


Figure 59: How PN Agent definitions appear to Thin Client user

The published applications will be displayed in the eLux control panel and taskbar menu (in addition to the other defined applications) in a tree-like structure: the top-level name is the PN-Agent application definition name, second level are the published applications or folders from the server (both applications and folders are defined on the XenApp server), etc.

On the Thin Client, the user will see the option **Refresh** in the taskbar menu, which allows the user to periodically refetch the published applications from the XenApp server.

If an autostart folder has been defined, the published applications in this folder will automatically run when the session is connected.

⇨ Manual Logoff

- Logoff only server
- Logoff server and applications
- Logoff server and disconnect sessions

⇨ Application Reconnection

There are 3 options to connect automatically:

- Do not reconnect (default)
- Active and disconnected sessions
- Disconnected sessions only

Program Neighborhood Variables

When you log on to theXenApp server using Program Neighborhood, the following variables are at your disposal (taken from the logon dialog):

$ICAUSER	User name

$ICADOMAIN	Domain for this user
$ICAAPPLICATION	Name of the PN-Agent application definition

For example, you can use the variables to set a unique client name in the Citrix XenApp session. This is required for Citrix roaming and by some XenApp programs.

Domain List

You can set a list of domains for the PN-Agent user to select from.

1. Create the text file icadomains.txt.
2. Enter the desired domains (one domain per line).
3. Save the file to the Scout Enterprise installation directory.
4. Transfer the file to /setup/icadomains(without the .txt" extension) on the Thin Client using the Scout Enterprise file transfer feature.

When the user starts the PN-Agent session, a dialog box to log on to the Citrix XenApp server appears. The domains in this file will appear as a drop-down list next to the **Domain** field (domain1", domain2", domain3"). In addition, you can preset a domain in the PN-Agent application definition (work.myelux.com").

4.3.3 Via Local Browser and Web Interface

The user can launch published applications from a local browser using the Web Interface for XenApp.

Required software: browser software (Netscape, Opera or Mozilla) and Citrix ICA Client version 7.x or higher

To create or modify a Netscape, Mozilla or Opera session, go to **Application Properties** > **Browser**. Enter the following:

Name: Enter an appropriate name for this application. This is what the local user sees in the eLux NG main screen (**Applications** tab).

Start page: Enter the URL used to access your Web Interface (ask your Citrix administrator). Common formats are:
`http://`*<server name>* or `http://`*<server name>*`/Citrix/Nfuse`

Kiosk mode: Leave unchecked.

The remaining parameters are configured as described in chapter 4.5 "Internet".

The local user starts the local browser in the eLux **Applications** tab to access the Web Interface page, enters logon information, is shown a list of available published applications, and clicks on an icon to launch the application.

4.3.4 Connection to Citrix Receiver

The Citrix Receiver is a Citrix tool to configure the connection. It can be defined as a local application.

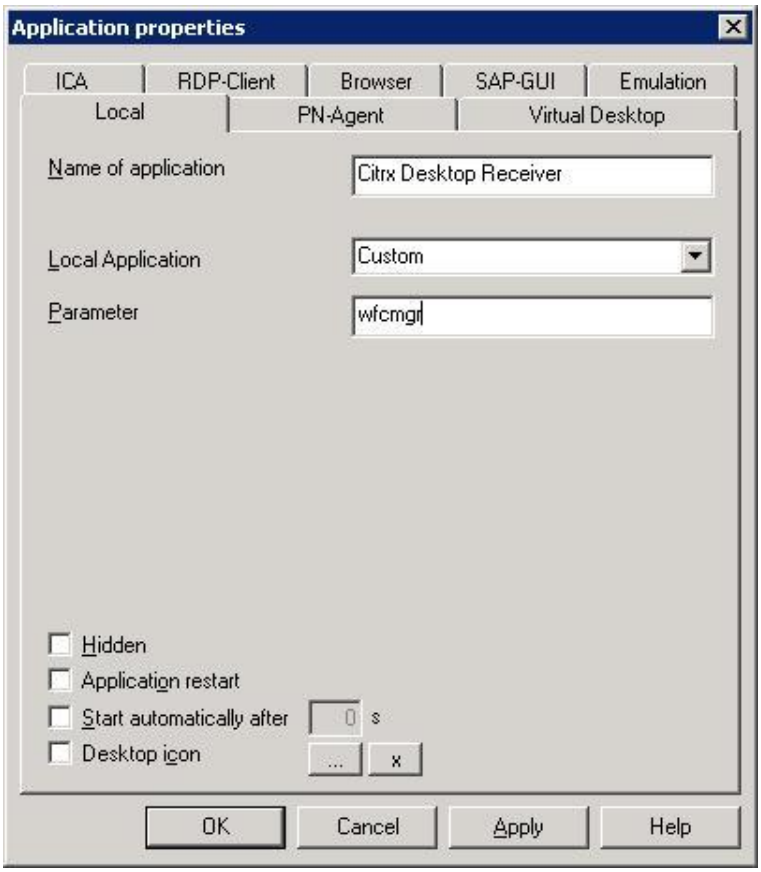


Figure 60: Configuring a local application to launch the PN Agent

Name: Enter an appropriate name for this application.

Local Application: Select **Custom**.

Parameter: Enter `wfcmgr`

The local user starts this application in the eLux **Applications** tab. This launches the **Program Neighborhood Agent.** After a successful logon, the user is shown a list of available published applications, and clicks on an icon to launch the application.

4.4 RDP

This type of session connects to a Microsoft® terminal server using Microsoft Remote Desktop Protocol (RDP). You have the following configuration possibilities: remote desktop or terminal server application.

4.4.1 Configuring a Session

To create or modify an RDP session, go to **Application Properties** > **RDP**. The client is a native implementation of the free software rdesktop. For further information see www.rdesktop.org.

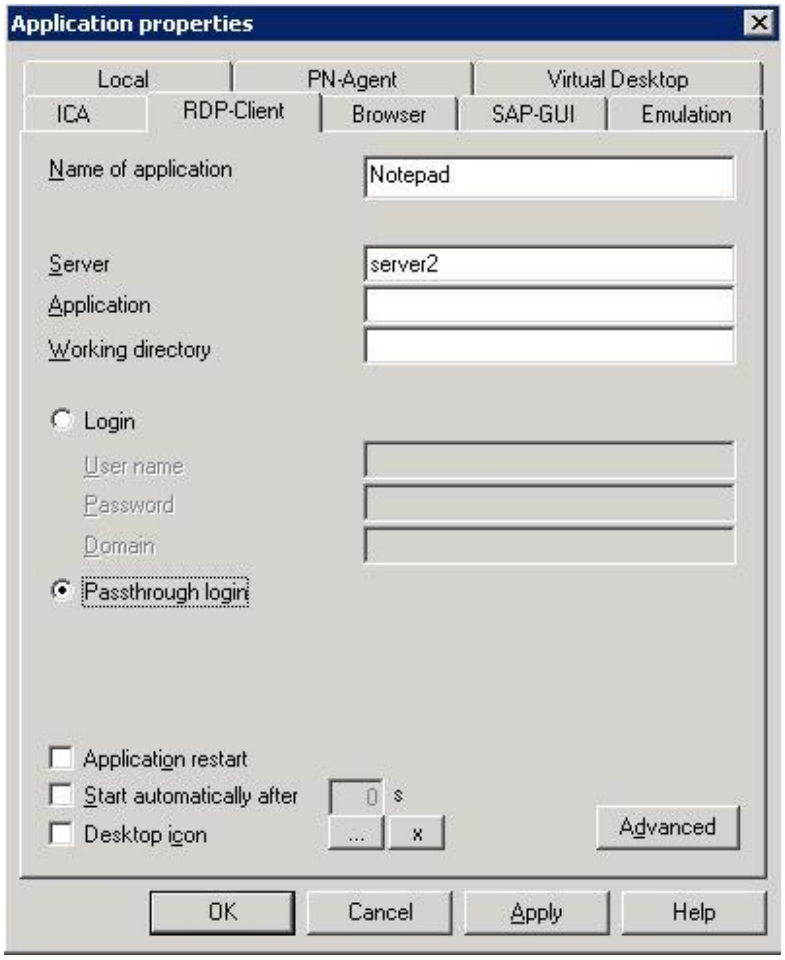


Figure 61: Application Properties dialog box for RDP

Name: Enter an appropriate name for this application, such as RDP." This is what the local user sees in the eLux NG main screen (**Applications** tab).

Server: Enter the IP address (or name) of the terminal server.

Application: For a remote desktop, leave blank. For a Windows application, enter the complete path of the application.

Working Directory: (optional, Windows application only) Enter a working directory for the application.

Login Enabling this option the logon data (user name, password, domain) are entered in Scout.

Passthrough login
Enabling this option the values
$ELUXUSER
$ELUXPASSWORD and
$ELUXDOMAIN are sent to the client.

4.4.2 Automatic Login

This optional feature logs the user on automatically using information in the following fields. Note: When user roaming is active, the information is read directly from the smartcard and overrides the logon information in these fields.

User Name: User name on the server.

Password: User password on server.

Domain: Domain for this user.

4.4.3 Session Parameters

Click on **Advanced** to display the **RDP advanced** dialog box. Here you can set the parameters for this session.

In the **Display** tab, you can set screen settings.

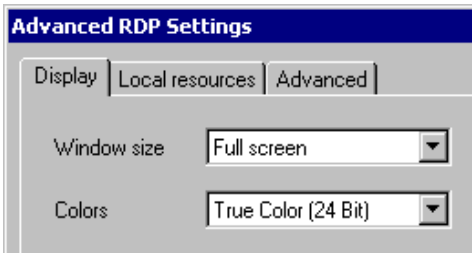


Figure 62: RDP client session settings: screen

In the **Advanced** tab, you can set the following parameters:

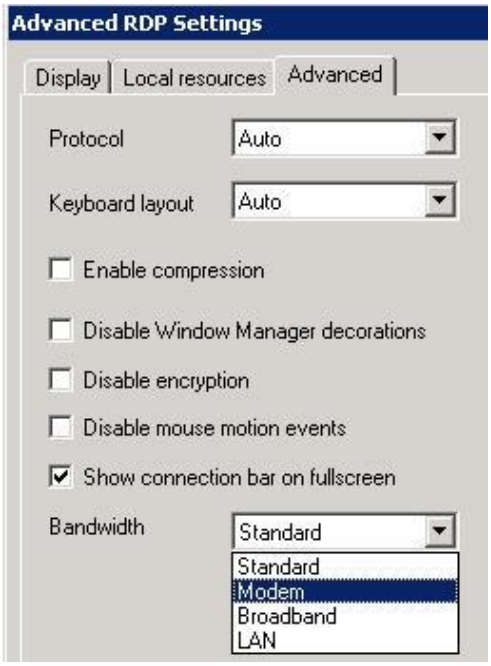


Figure 63: RDP client session settings: advanced

- **Protocol** Allows you to set the protocol to 4 or 5. By default, the server type is automatically detected.
- **Keyboard layout** Allows you to set the keyboard layout within the RDP session. Default setting is **Auto**, which means the setting in the eLux NG starter will be used.
- **Disable window manager decorations** The border that appears on eLux NG windows will be blended out.
- **Disable encryption** Activate if your server does not accept encrypted sessions. Default is deactivated.

- **Disable mouse motion events** Information on mouse position will not be sent to the server continuously, but rather only upon mouse clicks. This improves performance for low-bandwidth connections. Default is deactivated.
- **Show connection bar on fullscreen** This option is available for WindowsCE Clients only. When enabled the connection bar shows on the desktop in fullscreen mode.
- **Bandwidth** Select between Standard – Modem – Broadband – LAN.

The **Local resources** tab offers additional settings for 5.2 servers. Note: The settings in this tab are for the native RDP 5.2 client v1.3.1 or higher (rdesktop52"). If you are using a different RDP client, they will have no effect. In addition, these options will have no effect if you set the protocol to RDP V4" in the **Advanced** tab. To be able to use these settings, you must be using RDP v5.2 server or higher.

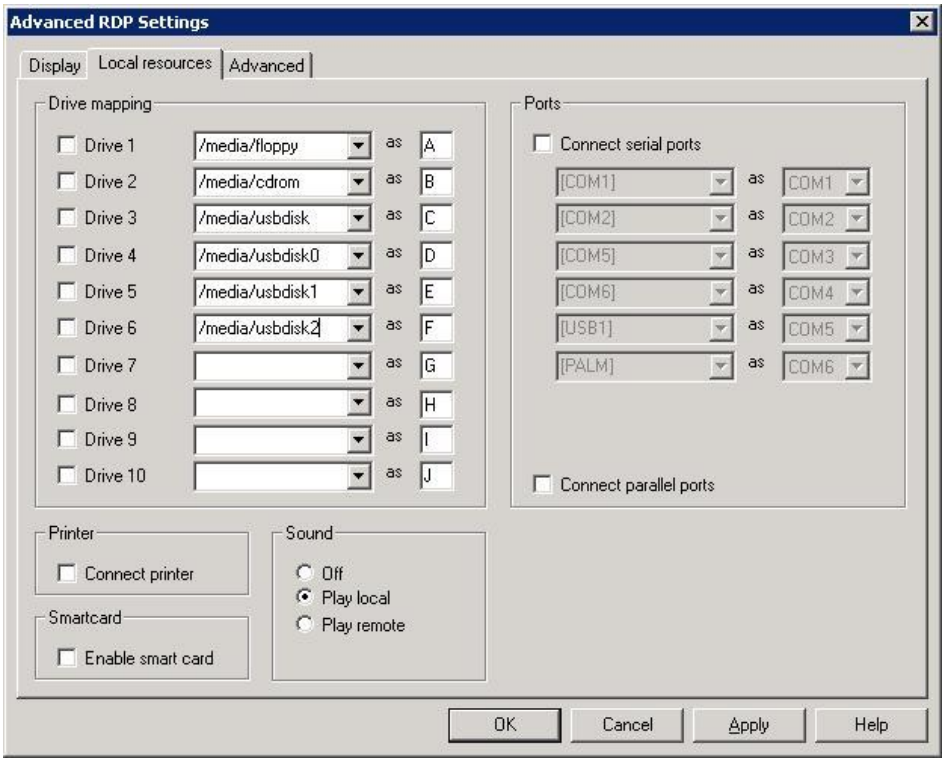


Figure 64: RDP client session settings: local resources

Drive mapping Allows you to map local drives. To map a drive, click to select the drive. Enter the mount point, which is the path to access the drive locally (see 0

- Mountpoints). Enter a letter. This is the drive that will appear in the RDP session. You can map up to 10 local drives.
  To access the drive from the command shell, use `\\tsclient\`<*drive letter*>, for example, `dir \\tsclient\b` would allow you to access the CD-ROM.
- **Printer** Allows you to automatically create up to four printer definitions for this session. The printers must be defined in the eLux control panel > **Printer** tab and have a valid driver name as it appears on the server (capitalization is important). The first four profiles with drivers are used. To set a default printer, click to select the default heck box in the eLux printer profile.
- **Sound** Play localmeans the sound will be played locally on the Thin Client. Play remote" means the sound will be played remotely on the server.
- **Ports** Enabling the check box means the ports will be accessible from within the RDP session.
- **Smart card** This feature is available starting with base OS 1.14.1 and RDP 1.4.0.
  Enabling the check box means smartcards can be used for certificate-based logon..
- **Serial ports** are accessible within the RDP session, too.

4.4.4 Smartcard User Roaming

eLux supports user roaming with USB card readers and CardOS 2.0 and SICRYPT smartcards coded with SMARTY 2 software.

COM card readers are not supported.

4.5 Internet

eLux offers different ways to connect to the Internet as well as various browsers and web tools.

4.5.1 Local Browser

Firefox - Software Requirements

To use this program, the Firefox(firefox) EPM must be installed. Available FPMs:

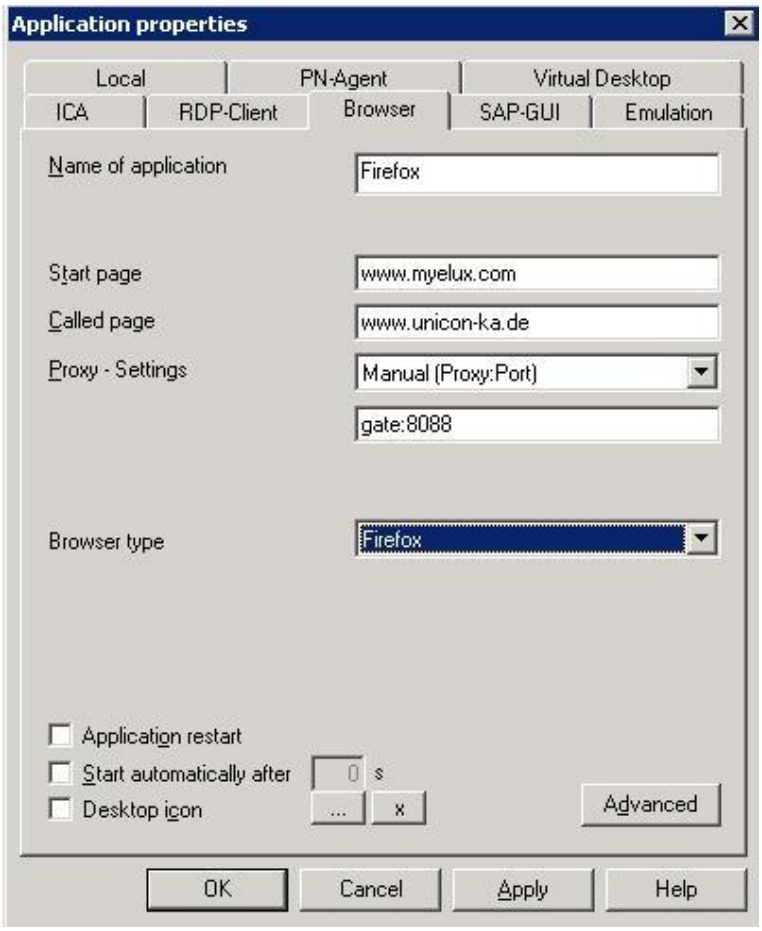
- Kiosk mode" (firefoxkioskmode): Required for kiosk mode.
- Firefox DOM inspector(firefoxinspector): Tool for displaying the structure of HTML and XML pages. For more information, see the Firefox documentation.
- Java support(firefoxjava): Enables Java support in Firefox. Requires SunJava(2)" (j2jre150) EPM 1.5 or higher.
- Various language packs are available for your localization.

Mozilla and Firefox cannot both be installed on the same machine running eLux.

For a description of EPMs and FPMs, see chaper 5.3 "ELIAS"

Firefox is a free, open-source web browser based on the Mozilla codebase. It is just a browser and does not contain a mail client. Firefox offers various security features including control over cookies and pop-up blocking. Firefox is not the stand-alone Mozilla browser. The user interface in Firefox differs from Mozilla in many ways. For example, Firefox has customizable toolbars. For more information, seehttp://www.mozilla-europe.org/de.

4.5.2 Configuring a Browser Application



Local Browser

To create or modify a browser session, go to **Application Properties** > **Browser**.

Figure 65: Browser

Name:	Enter an appropriate name for this application.
Start Page:	Enter an URL for the home page for the browser.
Called Page:	Enter an URL for the first Web page to be called when the system starts.
Proxy:	**No proxy**: If you don't use a proxy server. **Manual (Proxy:Port)**: If you use a proxy server. Use the format *<proxy server IP address or name>:<port number>*. *Example:* ..... *gate:8088* **Auto (URL)**: If you use an automatic proxy configuration file. *Example*: ..... http://www.server.com/autoproxy.pac
Browser type:	eLux supports **Firefox**. The browser types Opera and Mozila are still managed by Scout, however, updates are no longer available.

Click on **Advanced** to set the **kiosk** parameters:

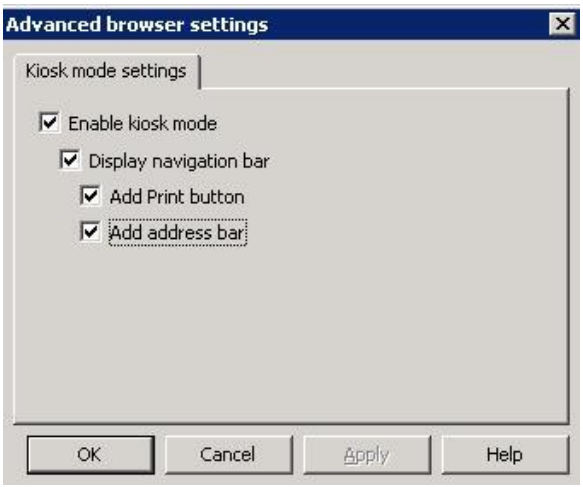


Figure 66: Advanced Browser settings: Kiosk mode

Enable kiosk mode	Kiosk mode is enabled, yet it is not possible to navigate through the browser.
Display navigation bar	Offers a navigation bar, so that you can move back and forward..
Add Print button	A button shows to print the current page.
Add address bar	Display an address bar to enter URLs.

4.5.3 Mail Client

A mail client can be defined in the **Applications** tab > **Local** > select **Thunderbird** in the drop-down list. No parameters need to be entered.

4.6 SAPGUI

To use this feature, you must have the SAP R/3 client PlatinGUI(sapplatingui) and IBMJAVA2" (IBMJAVA2) packages installed.

eLux supports the SAP/R3 client from SAP AG. This feature is not available for all hardware platforms.

System requirements:

- 96 MB flash card or larger
- 128 MB of RAM minimum

4.6.1 Configuring the SAPGUI Tab

This section describes how to launch the SAP client via the **SAPGUI** tab. Configuring the application definition does not configure a session. It simply runs the SAP/R3 interface.

⇨ SAPGUI tab

To create or modify an SAP session, go to **Application Properties** > **SAPGUI**.

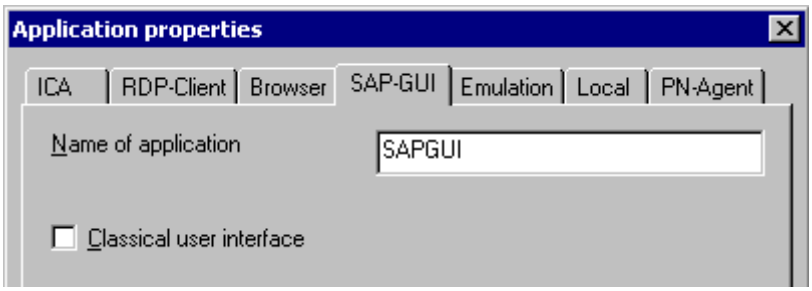


Figure 67: Using the SAPGUI tab to open SAPGUI

Name: Enter an appropriate name for this application.

Classical user interface: By default, the dialog boxes are in the new design. Select this check box for dialog boxes in the former, classical look.

There are two possibilities to configure the SAP client, local user configuration or by transferring a configuration file.

4.6.2 Configuration by Local User

Configuration takes place locally the first time the user starts the SAP client. For more information on configuring the SAP client locally, see the *eLux Administrator's Guide* or the SAP documentation on www.mysap.com or the eLux CD-ROM.

4.6.3 Configuration by Administrator – Transferred File

Alternatively, the administrator can transfer a configuration file or message server list to the Thin Clients.

The SAP client configuration file is: /setup/sapgui/platin.ini.

For information on SAP configuration file options, see the SAP documentation on www.mysap.com or the eLux CD-ROM.

4.7 Emulation

4.7.1 Available Emulations

The following emulations are available (product documentation referred to is available on the eLux CD-ROM):

X32, X52

3270, 5250 is a licensed products from Unicon Software GmbH. 3270 and 5250 come together as the package Terminal emulation for Motif(xemu). It includes a 15-minute trial period. To purchase the product, please contact sales@myelux.com. For configuration information, see the *X32/X52 Administrator's Guide*, available for download at www.myelux.com (log in, go to Manuals> Emulations").

eterm

eterm is a terminal emulation suite that includes the following emulations:
Siemens 97801 (7 & 8 bit), ANSI, AT386, BA-80, VT320
To use this software, you must have the Eterm 97801 terminal emulation(eterm) package installed. eterm is included in licensed eLux NG software free of charge. For configuration information or how to modify the key mapping, see the *eterm Administrator's Guide*, available for download at www.myelux.com (log in, go to Manuals> Emulations").

Tarantella

Tarantella allows users to access their applications over a Web-based interface. To use this software, you must have the Terminal emulation for Motif(xemu) package installed. The server is licensed, the client is free. For more information, see www.tarantella.com.

Virtual Network Computing

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing desktopenvironment 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. The option in the **Emulations** dialog is for configuring the VNC viewer, which is open source and included free with eLux software. To use this software, you must have the VNC client (vnc) package installed.

X Display Manager Control Protocol

The X Display Manager Control Protocol (XDMCP) is used by X terminals (and X servers in general) to set up an X session with a remote system over the network. The XDMCP functionality is included in the base OS. By default, the XDMCP session runs in its own console. To run the XDMCP session as a normal window in the eLux NG desktop, you must have the Xnest(xnest) package installed. For a configuration example, see the *eLux Administrator's Guide*.

To enable sound, go to **Setup** > **Multimedia** and click to select **Enable sound in XDMCP sessions**. **Note**: The application must be e-sound system compatible.

X Window System

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 operating system and hardware independent. An X11 client developed by The XFree86 Project, Inc (http://www.xfree86.org/) and its contributors is included in the base OS.

Note Useful additional software is Accelerated-X™ Display Server, an accelerator for X11 applications. This software is licensed and can be purchased from Unicon Software GmbH (see www.myelux.com) your eLux supplier. Not available for all hardware platforms. Accelerated-X requires a Matrox graphics card.

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. To use this software, you must have the PowerTerm InterConnect" (powerterm) package installed. This is a licensed product. The software includes a 30-minute trial period. To purchase a license, please contact sales@myelux.com.

4.7.2 Configuration Example – PowerTerm InterConnect

To use this software, the package powertermmust be installed on the Thin Client.

PowerTerm® Interconnect from Ericom® Software allows you to connect to IBM Mainframe, IBM AS/400,Unix, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000 and Data General. The following emulations can be simulated:

- **IBM** 3270 (TN3270E), 3179, 3278, 3279, 5250 (TN5250 with device name support), 3477
- **Digital** VT52, VT100, VT220, VT320, VT420, VT520, VT525
- **ANSI** BBS-ANSI, SCO-ANSI, AT386
- **Other** Wyse (50/60), Data General D-412, Siemens 97801, Televideo TVI 925/950, AIXterm

This is a licensed product. The software includes a 30-minute trial period. To purchase a license, please contact sales@myelux.com. The license is distributed using Scout Enterprise.

To run a session using PowerTerm, there must be a PowerTerm setup file (*.pts) on the Thin Client. You can use the default setup file (ptdef.pts), use the PowerTerm configurator to create a new setup file, or transfer a preconfigured setup file to the Thin Client.

⇨ To define a PowerTerm application

This section describes how to configure a PowerTerm application.

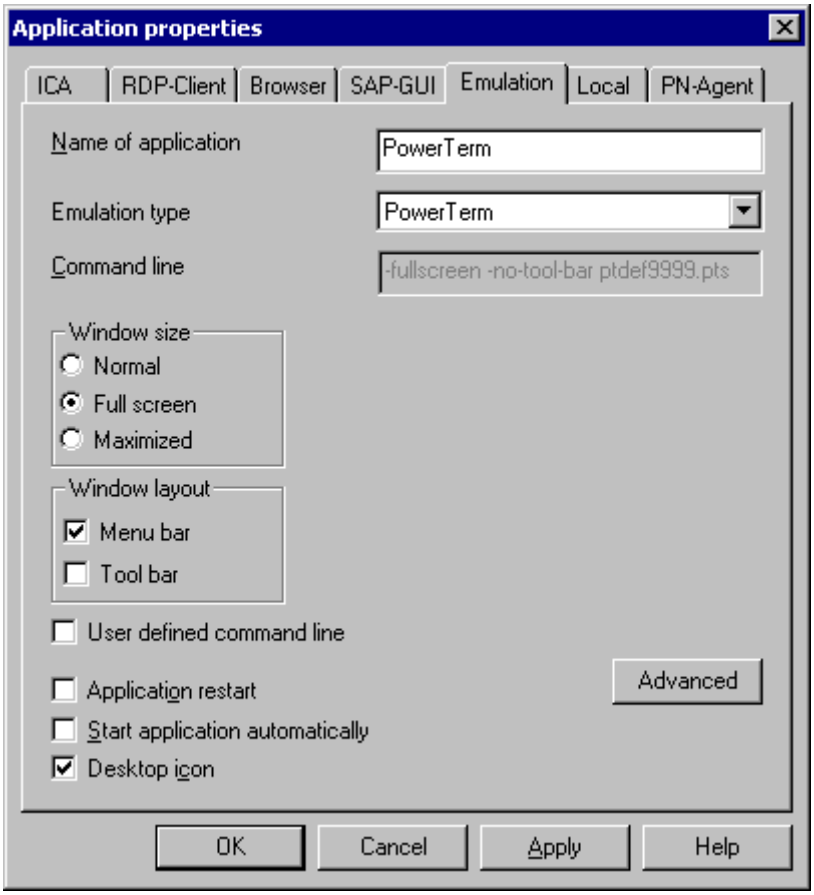


Figure 68: PowerTerm application definition

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Emulation** tab.
   Name: Enter an appropriate name for this application.
   Emulation type: Select **PowerTerm**.

Window size	Click to select the desired window options.
Window layout	Click to select the bars to display.
User defined command line	See User defined command line" below.
Advanced	Click to create a setup file for this application. See PowerTerm configurator" below. Alternatively, you can use the default file ptdef.pts. See User-defined command line."
Application Restart:	Immediately reconnects after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts.
Start Automatically:	Click this check box to open the application when the Thin Client starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

PowerTerm Configurator

This feature is available starting with Scout NG version 5.5.0.

The PowerTerm configurator allows you to configure and test connection settings from the machine running Scout NG. Use the PowerTerm configurator to create a setup file (*.pts) for this application. Alternatively, you can use the default file ptdef.pts. See User-defined command line."

1. In Scout Enterprise, in the PowerTerm applications properties dialog box click **Advanced**. The PowerTerm configurator appears.
2. In the **Connect** dialog box, you can configure the following:

   Host (use FQDN)

   Terminal type

   Security settings

   Scripts

   etc.
3. Make the desired settings. Click **Connect** to verify your entries.
4. When your entries have been verified, in the **Connect** dialog box click **Close** and in the PowerTerm configurator save the setup (**File** > **Save Terminal Setup**).
5. Close the PowerTerm configurator (**File** > **Exit**).
6. In Scout NG, in the applications properties dialog box, the name of the new setup file and selected parameters are displayed in **Command line**.
7. Close the applications properties dialog box and save your settings in Scout Enterprise.
8. Restart the devices.

See the PowerTerm documentation for more information on PowerTerm parameters and scripts.

On the Thin Client, the user starts the application with a double-click on the name in the **Applications** tab or by selecting the name and clicking the **Connect** button.

User-defined command line

This section describes how to use the command line and how to configure a PowerTerm application using the default setup file (ptdef.pts).

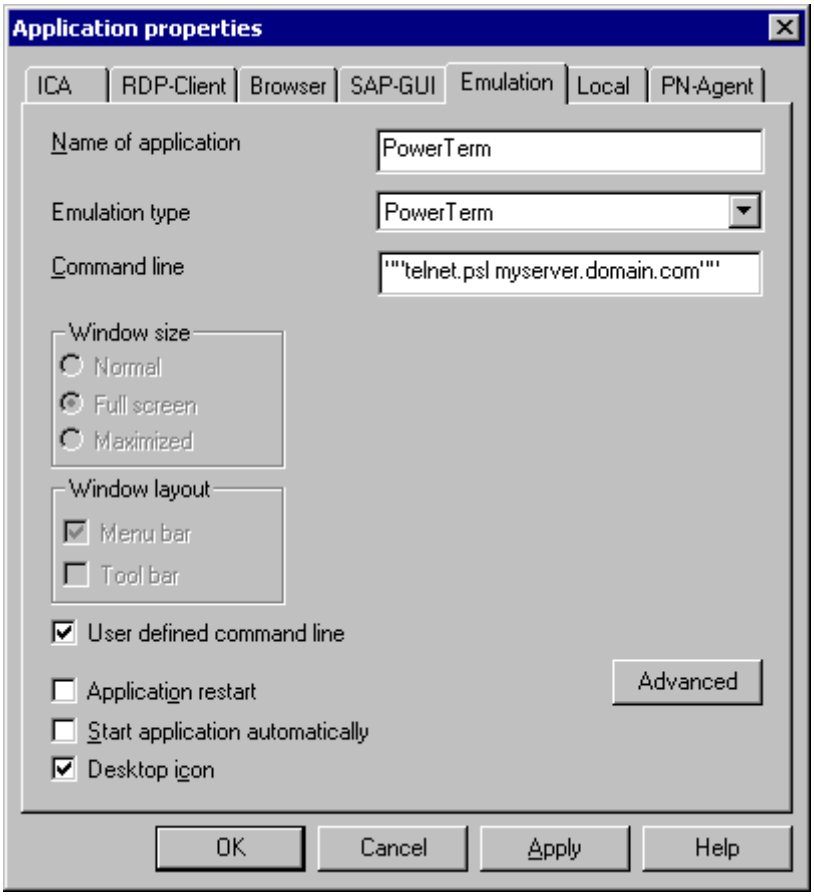


Figure 69: PowerTerm configuration

The **Command line** field displays the parameters you set in the applications properties dialog box and the name of the setup file if you used the PowerTerm configurator.

If desired, you can manually enter the setup file and parameters.

Click to select **User defined command line**. In the **Command line** field, enter one of the following:

- **PowerTerm setup file** A customized setup file. It must have the ending *.pts. Example: `myfile.pts`
- **Parameters + PowerTerm setup file** Enter accepted PowerTerm parameters, followed by the customized setup file. Example: `-no-menu -fullscreen myfile.pts`
- **PowerTerm script** Enter an accepted Power Script Language (*.psl) enclosed in double quotation marks (”). Example: `telnet.psl myserver””`

Note: If you do not enter a specific *.pts file, the default setup file (ptdef.pts) will be used. Transfer any files you enter here to the Thin Client using the File Transfer” feature.

See the PowerTerm documentation for more information on PowerTerm parameters and scripts.

Local PowerTerm configuration

If desired, users can configure the PowerTerm session locally on the Thin Client.

On the device, run the PowerTerm session. In the **Communication** menu select **Connect**. The **Connect** dialog box opens. Set the **Terminal Type** (emulation), the **Terminal ID** (if necessary) and the appropriate **Session Type**. Fill in the appropriate parameter fields and click **Connect**.

The configuration is saved to a file with the extension pts. The configuration files must be located in the directory /setup/PowerTerm/(or /setup/local/PowerTerm") on the Thin Client. The user creates a new configuration file by starting PowerTerm, configuring the settings and saving the file using a different name (**File** menu > **Save terminal setup as**). When opening a connection (**Communication** menu > **Connect**), the user selects the configuration file by clicking on the browse button next to Setup File" in the Upon connection runarea. Initially only the default configuration file (ptdef.pts) is available.

For information on configuring PowerTerm, please see the Ericom documentation available at www.ericom.com or on the eLux CD-ROM.

4.8 Local

The **Local** tab starts a local program. The user is `elux` and has no root authorization. The command can either be predefined (such as XTerm, resource display or SSH) or user defined (so-called customized command).

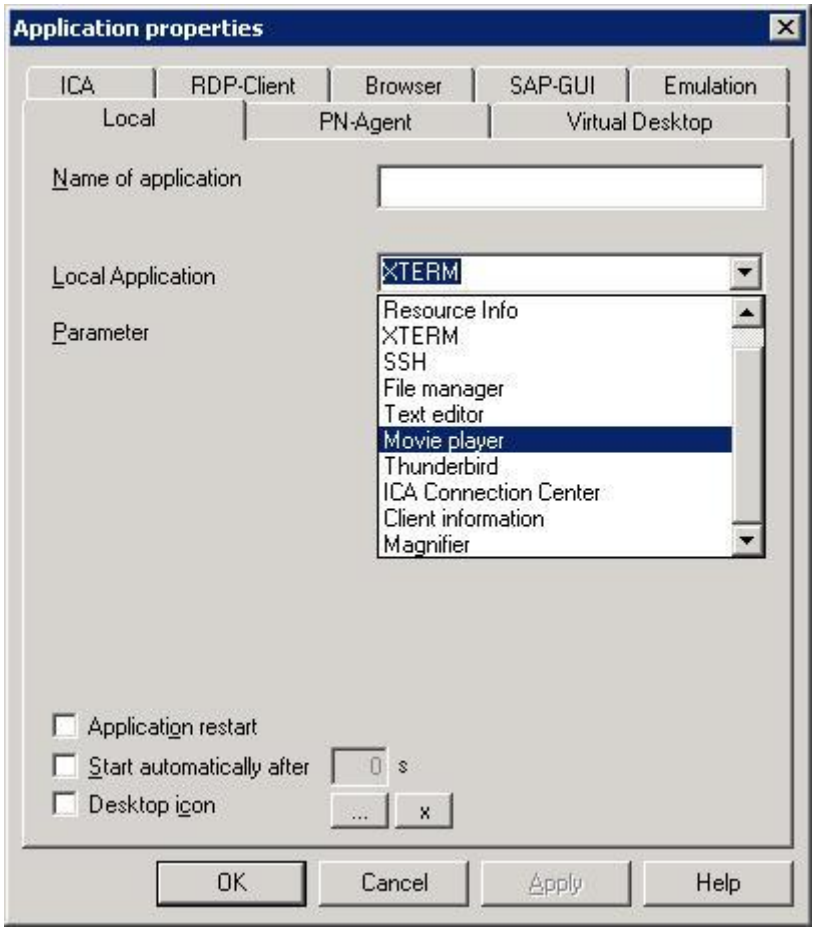
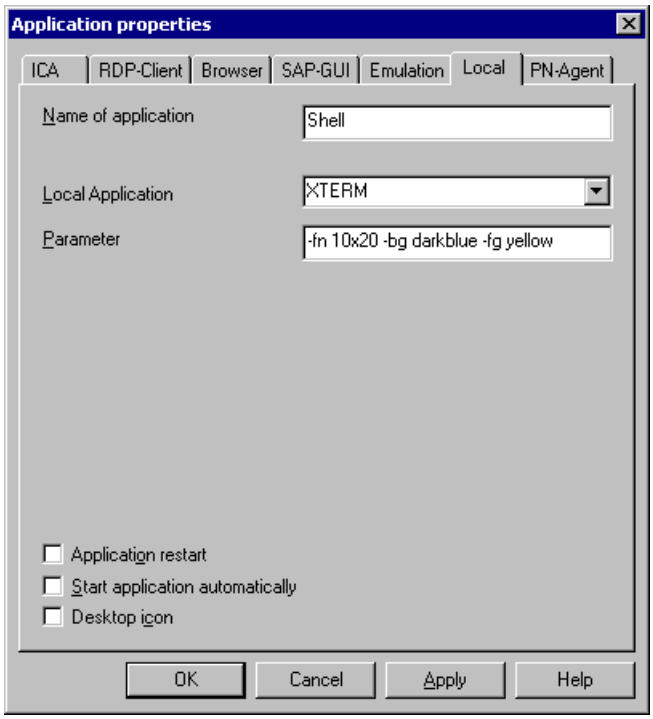


Figure 70: Application Definition - Local

4.8.1 XTerm (Local Shell)

Figure 71: Local shell - XTerm



Click with the right mouse button on an Applications category and select **Add**. Click **Local**.

Name: Enter an appropriate name for this application, such as "shell."

Local Application: Select **XTERM**.

Parameter: (optional) Enter a desired parameter. See the example below.

Application Restart: Immediately reconnects after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts.

Start Automatically: Click this check box to open the application when the Thin Client starts.

Desktop icon Creates a desktop shortcut for this application on the eLux NG desktop.

Example: User specified font size and color

```
-fn 10x20 -bg darkblue -fg yellow
```

fn	font
10x20	font size (big)
bg	background color
fg	foreground color

For more information see the man pages of a Linux system.

4.8.2 Resource Information

This command shows the current resource use (such as memory, CPU) for diagnostics.

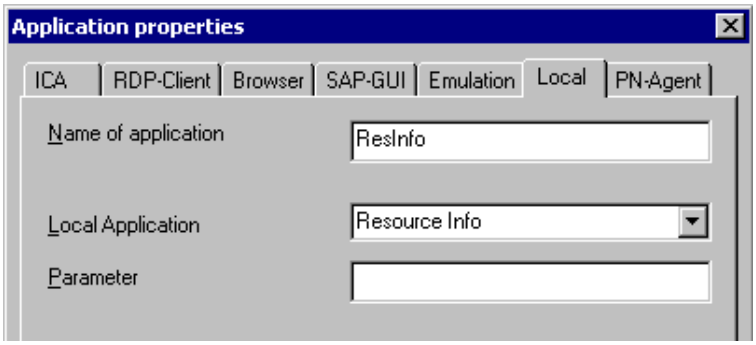


Figure 72: Local Application – resource information

Click with the right mouse button on an Applications category and select **Add**. Click **Local**.

Name: Enter an appropriate name for this application, such as "ResInfo."
Local Application: Select **Resource Info**.
Parameter: Leave blank.

4.8.3 Secure Shell (SSH)

This application allows you to connect to a remote Secure Shell (SSH) server.

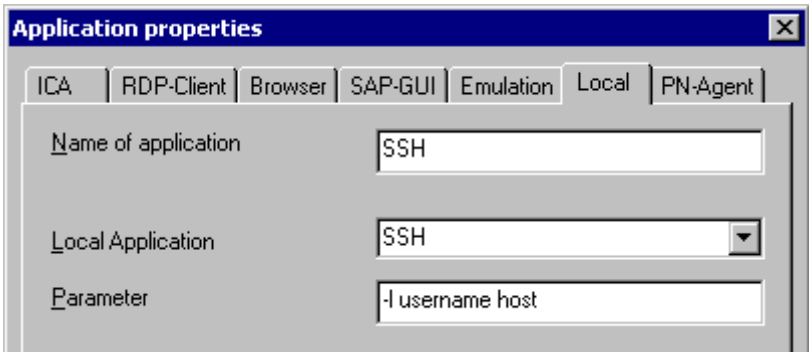


Figure 73: Local Application - Secure Shell

Name: Enter an appropriate name for this application.

Local application: Select **SSH**.

Parameter: Enter the user and the remote host, as shown in the figure above, in the following format: `-l` *<user name> <host>*. See User Authorizationbelow.

User Authorization

SSH server settings determine the authorization needed to connect. To connect using password authorization, the local user can open a session and enter the password (only if permitted by the remote host). For the local user to connect using a public key, do the following:

1. Open a local shell and type `ssh-keygen`.
2. At the Enter file in which to save the keyprompt, press ENTER.

3. At the passphrase prompt, enter a passphrase if you want local users to enter this phrase every time they establish a connection to the server, or Press ENTER to avoid having to enter a passphrase in the future.
4. To create keys, on the SSH server the command `ssh-keygen` creates a private key (located in the file `/setup/ssh/identity`) and a public key (located in the file `/setup/ssh/identity.pub`). Move the file `/setup/ssh/identity.pub` (public key) to `$HOME/.ssh/authorized_keys` on the SSH server. For more information on SSH server configuration, ask the system administrator of the remote host.

4.8.4 Customized Commands

Defining local commands is special – it allows you to define applications which can be called within a shell. The local user must be authorized to start the applications.

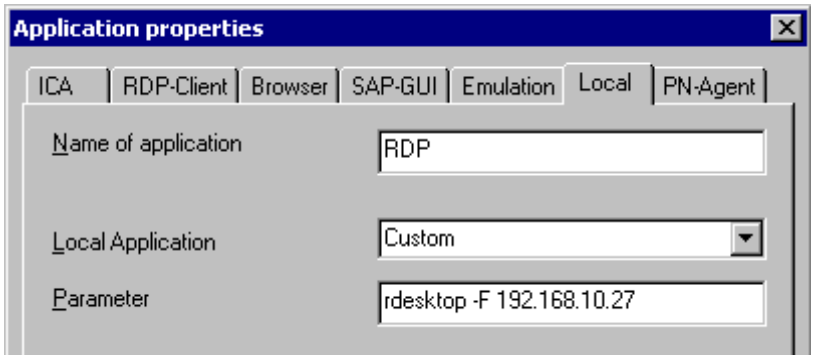


Figure 74: Local Application – rdesktop parameter

Click with the right mouse button on an Applications category and select **Add**. Click **Local**.

Name: Enter an appropriate name for this application.

Local Application: Select **Custom**.

Parameter: Enter the desired command, including all program parameters. For example: `rdesktop -F 192.168.10.27`.

We recommend that you test whether the command works by calling it from within an XTerm session on a Thin Client before entering it in the **Local** tab. This is the only way you will receive feedback via error messages.

For more information and examples see the *eLux Administrator's Guide*, section 4.8.4 User-Defined Commands, or the man pages of a Linux system.

4.8.5 Calculator

To use the desktop calculator, you must have the xcalcpackage installed. It is run using a local command.

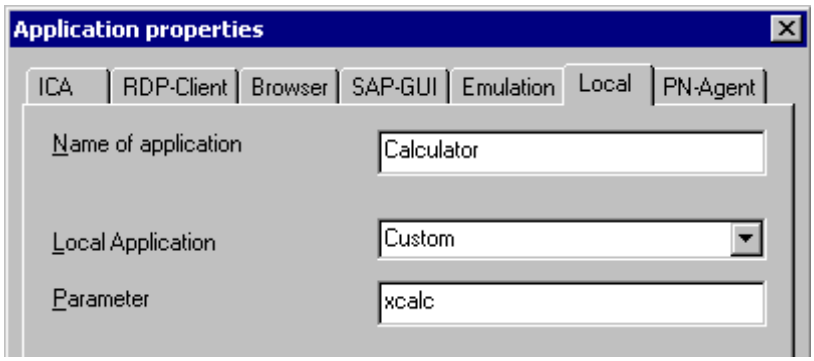


Figure 75: Calculator

Click with the right mouse button on an Applications category and select **Add**. Click **Local**.
Name: Enter an appropriate name for this application.

Local Application: Select **Custom**.

Parameter: Enter `xcalc`.

On the Thin Client, start the calculator with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

4.8.6 Adobe Acrobat Reader

To use Adobe® Acrobat® Reader®, you must have the corresponding eLux package installed. On www.myelux.com the versions 5 and 7 are available.

This section describes how to run Adobe Acrobat Reader as a stand-alone program. To run Adobe Acrobat as a browser plug-in, just install the software. No further configuration is required.

⇨ To run Adobe Acrobat Reader as a stand-alone program

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **Custom**.
Parameter	Enter `acroread` <*parameters*> where <*parameters*> are optional command-line parameters. Note: Capitalization is important!
Hidden	Does not display the application in the **Application** tab. Note: If the application is hidden, you must select either Application restartor Start application automaticallyfor the command to run.
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

You can view a PDF that is saved locally (such as in the directory `/tmp`) or on a network drive (SMB or NFS).

For more information on:

- Available command-line parameters. On the Thin Client, open a local shell and type `acroread -helpall | more`. A list of available parameters is displayed. To scroll, press the spacebar.
- **How to use Acrobat Reader.** See the Acrobat Reader documentation available on the eLux NG CD-ROM. Also describes selected parameters.
- **Online help.** The Adobe Reader Online help is not available.

Also consult chapter “4.5 Internet”.

4.8.7 File Manager

To use this feature, you must have the File Explorer (qfm) package installed. It is in the package Desktop tools (dtt) starting with version 1.4.2. In addition, the base OS starting with version 1.8.4 must be installed.

eLux NG is a Linux-based operating system. While no Linux knowledge is required to install and use eLux NG, to browse local files and directories using a local shell you need to know UNIX commands.

QFm is a QT-based file manager from Nick Battle (http://home.freeuk.com/nick.battle/). It allows you to browse local files and directories on the Thin Client in a graphical interface using the mouse rather than in a local shell using text commands. You can move, copy and rename files.

⇨ To run the file manager

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **File manager**.
Parameter	(optional) Enter <*directory*> where <*directory*> is an optional parameter that enables you define the directory that will be displayed upon start. For example, `tmp` will display the tmp directory. By default, the root directory is displayed. **Note**: Capitalization is important!
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

How to use QFm

Using QFm is similar to other file managers, such as Windows Explorer. You can delete, copy, rename and change files.

Tool tips help you through the basic features (holding the cursor over an object displays a short description).

To understand how files are displayed, the highest-level directory is root. Root contains a number of subdirectories, including setup, tmp, smb, nfs.

- **setup** Contains permanent files needed by applications, such as configuration files. The contents are not deleted upon boot.
- **tmp** Contains temporary files needed by applications for this session. Deleted upon boot. Note: Browser, ICA and SAP cache is stored here. For improved performance, we recommend reducing allocated cache in the respective program or, in the case of the browser, defining a network drive for storing program files (browser home directory"). See 3.9.6 Browser – Home Directory.
- **smb** Displays the currently mapped SMB drives. Note: Only defined SMB drives that are currently mounted are displayed. The user must connect to the SMB drive before it will be displayed.
- **nfs** Displays the currently available NFS drives.

While using QFm is intuitive, we provide the following general guidelines and tips:

- The task bar provides one-click access to the most frequently used commands: Home, Display hidden files, Exit, Refresh, One directory up, Change directory, Shell, New window.
- To expand a directory , click once. To display that directory only in tree view, double-click. To

  return to root, click Home in the task bar or **File** > **Home**.
- To open a file, double-click. By default, applications have been preset for the following files (you must have the respective application installed):

Acrobat Reader	Opens *.pdf files.
Citrix ICA Client	Opens *.ica files.
MP3 Player	Opens *.mp3 files.
Firefox	Opens HTML files.
QT Text Editor	Opens *.cnf, *.conf, *.cpp, *.h, hosts, *.ini, *.java, *.log, printcap, readme, *.txt files. See the following chapter.
Wav Player	Opens *.wav files.

- You can bookmark frequently used files and directories by right-clicking on the file and selecting **Bookmark**. You can then jump directly to the file or directory using the **Bookmarks** menu.
- To open a shell, click Shell in the task bar or **File** > **Shell**.
- The error **Not an executable file** means that the file cannot be displayed. Try installing the appropriate software or clicking with the right mouse button on a file and selecting **Open with** to display a list of available programs.

4.8.8 Text Editor

To use this feature, you must have the Text Editor (qtt) package installed. It is in the package Desktop tools (dtt) starting with version 1.4.2. In addition, base OS version 1.8.4 or higher must be installed.

QT Text Editor is a simple QT-based text editor that offers basic editing features. You can copy, paste, find, undo, redo, select all text, etc. The files must be saved to the Thin Client or available on a network drive.

⇨ To run the text editor

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **Text editor**.
Parameter	(optional) Enter <*file name*> where <*file name*> is an optional parameter that enables you define the file that will be displayed upon start. Enter the complete file name. For example, `tmp/hosts` will display the hosts file located in the tmp directory. Note: Capitalization is important!
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

Tip

To access files on an SMB network drive, you must configure the SMB drive in advance. For information on how to configure SMB drives, see In addition, the user must know the SMB drive name. On the Thin Client, open the QT Text Editor. Click **File** > **Open** > **smb**, enter the network drive and click **Open**. This mounts the drive. It will then appear in the dialog box and can be selected. It remains mounted for the rest of the eLux NG session.

4.8.9 Movie Player

To use this feature, you must have the Movie Player" (mplayer) package installed. In addition, install the individual subcomponents (FPMs) relating to the features you desire. In addition, the base OS version 1.8.4 or higher must be installed.

MPlayer is an open-source movie player from the MPlayer Project (http://www.mplayerhq.hu). It supports all common movie formats including DVD (including encrypted DVD), MPEG, DivX, AVI, ASF, RealVideo, Windows Media Video (.wmv), Quicktime (.mov) and others. The files can reside on the Thin Client, a network drive or the Internet.

This section describes how to run MPlayer as a stand-alone program. To run MPlayer as a browser plug-in (Mozilla only), install the software MPlayer Mozilla support(mplayer_plugger) in the package Movie Player" (mplayer). No further configuration is required.

⇨ To run the movie player as a stand-alone program

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **Movie player**.
Parameter	Leave blank.
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts

Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.
3. (optional) To set a proxy server, you have two options:

Environment variable	Set the following environment variable: `http_proxy=http://`*<proxy server>*`:`*<port>* Capitalization is important!
INI file entry	Set the following INI file entry: File: `/setup/terminal.ini` Section: `Environment` Key: `http_proxy` Value: `http://`*<proxy server>*`:`*<port>* For information on how to use the INI file editor, see

Tip: Environment variables are set for a single device. INI entries can be set for multiple devices.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

How to use MPlayer

Even though using MPlayer is intuitive, we provide the following general guidelines and tips:

- Access commands by clicking the buttons of the remote control. Alternatively, click with the right mouse button in the movie window. This opens the context menu.
- To play a DVD from a local drive, on the Thin Client start MPlayer. Insert the DVD in the drive. Click with the right mouse button in the movie window. In the context menu select **DVD** > **Open disk…** and browse for the DVD. To open a chapter, in the context menu select **DVD** > **Chapters** > <*chapter number*>. Note: MPlayer does not support chapter menus.
- To change the appearance, in the context menu select **Skin browser**. The **Skin Browser** dialog box is displayed. Select your desired theme.
- To configure settings, in the context menu select **Preferences**. The **Preferences** dialog box is displayed.
- You have two drivers available: xv, which provides hardware acceleration with a modern graphics card, and x11, which provides no scaling. If playback does not occur, try setting the driver to x11. This is done in the **Preferences** dialog box. The default driver is xv.

For more information on MPlayer, see the documentation available at http://www.mplayerhq.hu/DOCS/HTML-single/en/MPlayer.html.

4.8.10 NoMachine

To use this feature, you must have the software NxClient (nxclient) installed.

NoMachine from Medialogic S.p.A. enables a UNIX workstation to provide terminal server functionalities. NoMachine software is based on the NX Distributed Computing Architecture, a suite of open source technologies built on SSH and the X-Window System. NX also translates and embeds the RDP (Remote Desktop Protocol) used by Microsoft in its terminal server product family and VNC protocols into X/NX. NX is faster than VNC or X11 and can run on bandwidth as narrow as 10 kBit/sec. It enables users to compress and accelerate remote desktops like Windows, KDE, Gnome and CDE. NX lets you work fluently even across slow links like modems.

NX software consists of the following components:

- **NX server** The NX server is available for Linux and Solaris and is licensed per-server, not per-connection.
- **NX client** The client software is available for eLux NG and other platforms. All NX clients are free of charge.

⇨ To configure the NoMachine NX client

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **Customized**.
Parameter	Enter `nx.sh`.
Hidden	Does not display the application in the **Application** tab.
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

From the **Applications** tab, double-click or use the **Connect** button to run the program.

How to use NX client

- The NoMachine NX server must be installed and running.
- A wizard appears the first time you run the software to help you through the initial configuration.
- For further information, see the NoMachine documentation available at www.nomachine.com.

Tip We recommend setting the cache on disk" (**Configure** > **Advanced**) to zero.

For information on NoMachine, see www.nomachine.com.

4.8.11 Virtual Keyboard

To use this feature, you must have the software Virtual Keyboard (xvkbd) installed. It is in the package Desktop tools (dtt) starting with version 1.4.2.

This is an open-source program to display a virtual keyboard on the screen. You can enter characters into a program using a mouse click. This is useful for kiosk terminals or for a workstation with a mouse but no keyboard.

⇨ To run the virtual keyboard

Click with the right mouse button on an Applications category and select **Add**.

1. The Application Definition dialog box appears. Click the **Local** tab.

Name	Enter an appropriate name for this application.
Application	Click **Customized**.
Parameter	Enter `xvkbd.sh`.
Hidden	Does not display the application in the **Application** tab.
Application Restart	Click to select to immediately reconnect after the user logs off. When this feature is selected, the application automatically starts when the Thin Client starts or restarts.
Start automatically	Click this check box to open the session when the terminal starts.
Desktop icon	Creates a desktop shortcut for this application on the eLux NG desktop.

2. Click **Finish**.

On the Thin Client, start the program with a double-click on the profile in the **Applications** tab or by marking the profile and clicking the **Connect** button.

How to use the virtual keyboard

While using the virtual keyboard is intuitive, we provide the following general guidelines and tips:

- Run a program of your choosing that requires keyboard entry.
- Run the virtual keyboard. The keyboard window always appears on top. Click on a character using the mouse.
- By default, the character appears in the window of the last program used. To set the focus to a specific window, click **Focus** and the window of your choosing.
- By default, the virtual keyboard program uses the keyboard language setting from the eLux NG starter, assuming the language is supported, otherwise English will be used. To manually set the language for this session or to view a list of available languages, click **Main menu** > **Change Keyboard Layout**.

Tip

- To set the size and/or position, enter the following command in the **Parameter** field: `xvkbd.sh -geometry` *<width>*`x`*<height>*`+`*<x position>*`+`*<y position>*

  Examples:

`xvkbd.sh -geometry 600x200`	Set keyboard size to 600x200 pixel
`xvkbd.sh -geometry 600x200+200+0`	Set keyboard size to 600x200 pixel and position it above center
`xvkbd.sh -geometry 600x200+0-40`	Set keyboard size to 600x200 pixel and position it lower left

For further information, see the documentation available at http://homepage3.nifty.com/tsato/xvkbd/.

4.9 Virtual Desktop

The following Virtual Desktop applications can be defined either in the eLux control panel or in Scout Enterprise.

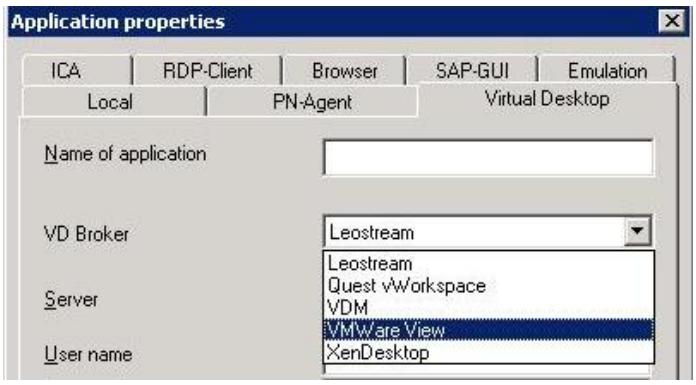


Figure 76: Virtual Desktop – possible configurations

4.9.1 VMware View

The parameters for Vmware View must be correctly entered in compliance with the View Server (Connection Broker). Please ask your View administrator for the correct settings.

The field **USB rules** serves to define which USB devices are to be redirected and which are not.

For further information please consult the "*View Client for Linux*" manual on www.vmware.com.

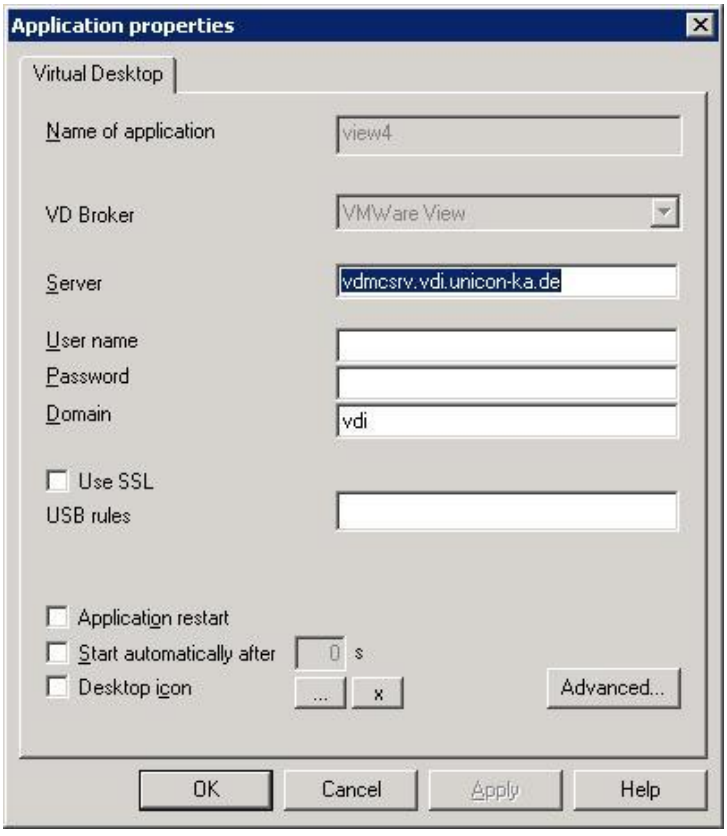


Figure 77: Virtual Desktop –Configuration VMware View4

The protocol which is to be used by the VMware client to display the virtual desktop, can be set now. Valid settings are: **RDP, PcoverIP, RGS, localvm**

4.9.2 XenDesktop

The parameters for the XenDesktop must be correctly entered according to the Citrix XenDesktop Delivery Controller (Connection Broker).

Please ask your Citrix administrator for the correct settings.

For detailed information please consult the "*Citrix Receiver for Linux"* manual on www.citrix.com.

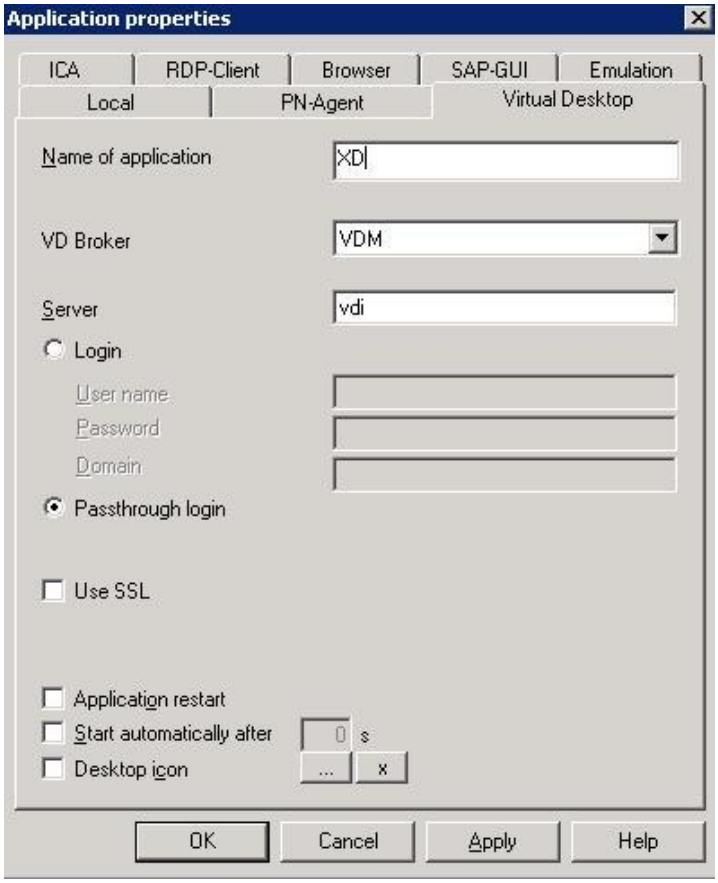


Figure 78: Virtual Desktop – Configuration XenDesktop

Login	Enabling this option the logon data (user name, password, domain) are entered in Scout.
Passthrough Login	Enabling this option the values for $ELUXUSER $ELUXPASSWORD and $ELUXDOMAIN are sent to the client.

4.9.3 Quest vWorkspace

The parameters must be correctly entered according to the Quest (Connection Broker). Please ask your Quest administrator for the correct settings.

4.9.4 Leostream - Unicon LeoConnect Client

The UniCon LeoConnect Client is a client software to use the Hosted Desktop Connection Broker by Leostream Corp., Waltham, MA, USA. For detailed information see http://www.leostream.com.

Requirements:

- eLux NG BaseOS 1.43-3 or higher / eLux RL
- Scout 9.6.0 or higher
- A Virtual Desktop Application must be defined in the eLux control panel or via Scout.

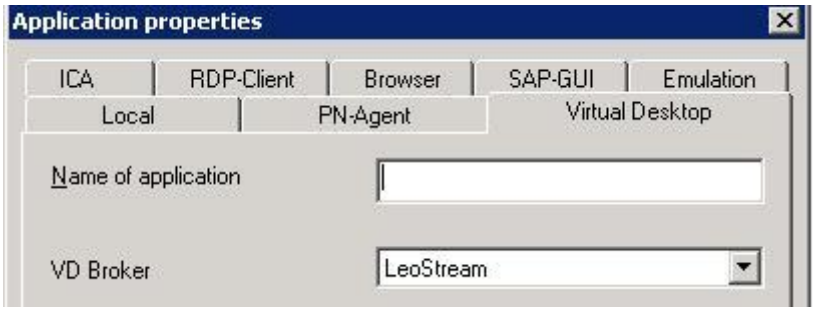


Figure 79: Virtual Desktop – LeoConnect Client

The Application Definition dialog box appears. Click the **Virtual Desktop** tab.

Name	Enter an appropriate name for this application.
VD Broker	Select **LeoStream**

Basics

Having entered the login data and after the successful login at a Leostream Connection Broker LeoConnect shows the user the list of the available Hosted Desktops.
From this list the user can select those Hosted Desktops he wants to build a RDP connection to. Then, LeoConnect requests the RDP connection data from the Leostream Connection Broker and starts the RDP session.

Automatic Login Mode

Having defined the Virtual Desktop application and filled the fields **Server**, **User name**, **Password**, LeoConnect **automatically** logs into the selected Leostream Connection Broker and presents a list of the available Hosted Desktops in the Hosted-Desktop dialog instead of showing the Login dialog.

If you should not want to be logged in automatically, at least one of the above mentioned fields must be left blank when defining the Virtual Desktop application.

LeoConnect Login Dialog

This dialog opens when

- one or more of the fields Server, User name, Password have been left blank when defining the application in the eLux starter or via Scout.
- an error occurs (In addition a dialog shows with an error message.).

Figure 80: LeoConnect Login Dialog

The **Connect** button is only enabled, if the fields **Username**, **Password** and **Connection Broker** have been filled, whereby the field "Connection Broker“ corresponds to the field "Server“ in the eLux Starter rsp. Scout.

Connect	LeoConnect logs into the selected Leostream Connection Broker and requests a list of the available Hosted Desktops.
Exit	closes the LeoConnect Login dialog and also running RDP sessions to Hosted Desktops, if there are any!

LeoConnect Hosted Desktop Dialog

This dialog shows a list of the available virtual machines for this user.

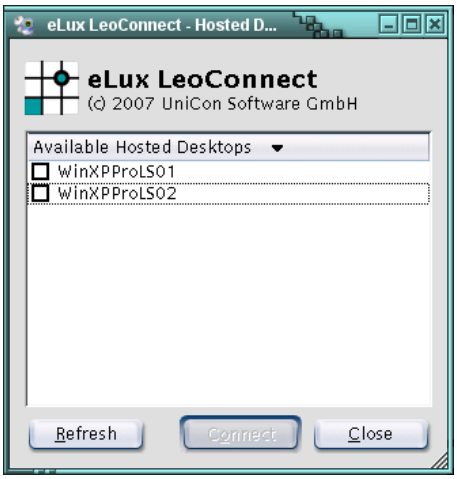


Figure 81: Hosted Desktop Dialog - shows available Hosted Desktops

From this list the user is to select the required machines and click **Connect**.

Then, the single RDP sessions to the selected Hosted Desktops are initiated in the selected order. The selected entries in the list are then displayed lightly grayed.

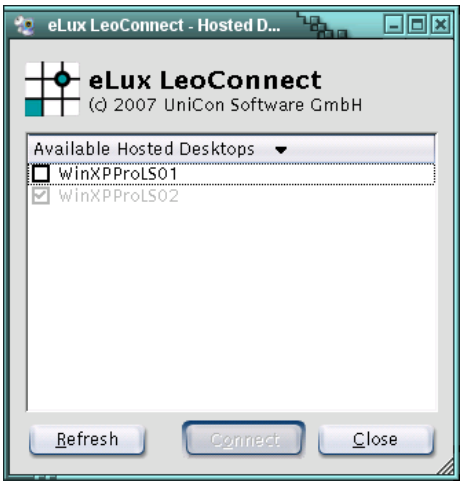


Figure 82: Hosted Desktop Dialog – shows available Hosted Desktops connected to

Refresh an updated list of available Hosted Desktops is requested by the Leostream Connection Broker.

The button **Connect** is only enabled, if at least one Hosted Desktop has been selected.

Close If LeoConnect is in the mode **Automatic Login**, LeoConnect and all running RDP sessions are closed.

If no Automatic Login has been used, only the Hosted Desktop dialog is closed and LeoConnect returns to the Login dialog.
Any running RDP sessions remain active.

5 Management on Firmware Level

This chapter contains information on how to create an image definition file using the program ELIAS (eLux Image Administration Service Next Generation) and how to update the Thin Client's firmware.

5.1 Introduction

When your Thin Client is delivered, it already contains an operating system and basic software: ICA® client, RDP client, browser, emulations, desktop tools, etc. This allows you to begin using your device immediately.

However, as time goes on you will want to change the default software – such as to update to a newer version or to remove unneeded software. This is done using the so-called firmware update. (Firmware is the term used to refer to software saved to the flash card.)

A firmware update takes place in four steps:

1. Installing the update programs and files
2. Modifying the firmware and saving it to an update server
3. Configuring the Thin Client with update parameters
4. Initiating an update

You must modify the firmware in advance and transfer it to the Thin Client. It is not possible to change the firmware online.

These steps are described in the following sections.

5.2 Installing Update Components

If you selected **Typical** during the installation procedure, you already have all required programs and files. No further installation is required.

If you selected **Custom**, please verify that you have installed the container and ELIAS. If necessary, install these components now by running the setup program and clicking **Modify**. Click to select Scout Enterprise Server, Scout Enterprise Console, Container and ELIAS, and follow the directions. Note: An FTP or HTTP server must be available either locally or on a network drive.

5.3 ELIAS

5.3.1 What is ELIAS?

The eLux Image Administration Service, or **ELIAS**, allows you to easily manage the firmware on a Thin Client running eLux NG or eLux *RL*. Each Thin Client comes with a default image (recovery.idf) that contains the operating system, software and applications. If you wish to change the firmware, you need to create a new image definition file. Using ELIAS, in a new image definition file (*.idf) you select exactly those software packages you want installed on the Thin Client. These packages are then saved on the flash memory of the Thin Client. The administrator can use ELIAS to custom-make the image to satisfy end-user requirements.

5.3.2 ELIAS Features

ELIAS offers the following features:

- User-friendly graphical interface that allows you to create software images by a mouseclick
- Easy management of device firmware using the “container method”
- Ability to activate/deactivate software components to optimize your use of available resources
- Image size bar to avoid exceeding flash size
- Automatic proofing of software dependencies
- Easy import feature to add the latest versions of software
- Easy export feature that exports a package along with its software dependency information
- Digital signatures to ensure the installed packages are genuine

5.3.3 ELIAS Terminology

This chapter defines terms that are used in this manual. Please read the following before continuing.

EPMs and FPMs

In server-based computing, client software installed on a device is used to connect to server software. Examples of client software are an ICA client, RDP client, etc. eLux is module-based. In ELIAS, a client program (module) that has been bundled for eLux NG or eLux *RL* use is called a **package**.

All packages saved to the flash card of a device are called **firmware**.

When updating the firmware saved to a device, you add or delete individual packages. This is less time consuming than updating all firmware saved to the device every time you update.

These software packages are divided into **eLux Package Modules** (short “EPM”) and **Feature Package Modules** (short “FPM”). An EPM (upper-level package) contains one or more FPMs (lower-level package).

5.3.4 Starting ELIAS

There are two ways to open ELIAS :

- Scout Enterprise: go to **View** menu > **Elias**.
- Windows: go to Start menu > Programs > Scout Enterprise > ELIAS.

If you have selected the standard installation in Scout, ELIAS will automatically open the container during start. If not, a container needs to be selected.

By default, the container is installed in the FTP or HTTP server root directory under:

…\eluxng\UC_INTEL_P3

…\eluxng\UC_GEODE_P1

…\eluxng\UC_TRANSMETA

...\eluxng\UC_VIA or

...\eluxng\UC_PC

Note: With eLux® *RL* there is only ***one*** container for all hardware platforms.

When it has been located, open the file container.ini. The ELIAS screen displays the name and path of the container that is currently open and the right-hand side of ELIAS should fill with available packages, as shown in the figure below.

5.3.5 What is a Container?

A container contains the firmware packages for a specific hardware. When using eLux NG each Thin Client model has its own container. For example, a Thin Client with an Intel processor has a different container than one from National Semiconductor. Please use the default names.

For eLux RL, however, there exists one container only regardless of the client hardware, as already mentioned above.

The container is a collection of software packages. The administrator chooses a subset of this pool of packages to install on the Thin Client when defining an IDF.

In normal use, it is not necessary to change the container. Packages that are not needed have no effect.

However, at times it is necessary to update the container when:

- new client software is available (ICA®, RDP, emulation, etc.)
- a new base OS is released (eLux NG)
- a software bug is fixed.

Containers are downloaded from the Internet. You must complete a free one-time registration.

⇨ To download a new container from the Internet

1. Go to the Web site www.myelux.com.
2. In the navigation links on the left-hand side, click "Login", enter your user data and click "Submit".
3. The main page is displayed with a Download and Service area. Click "eLux software packages".This opens the page for eLux RL container and eLux NG container.
   Note: for eLux RL there is only container for any client hardware.
4. Locate your hardware platform and click on the link in the column under "Released packages".
5. The container page lists the container, the BaseOS and all available software packages for the hardware you chose.
   Click "container.zip" to begin the download.
6. When the transfer is complete, unzip the file and save the contents to the root directory of your FTP or HTT

5.3.6 Importing Packages to a Container

A container contains ALL software packages available for a given hardware platform.

It is not always necessary to download an entire container. In many instances it suffices to download individual packages

To download an individual package, log on to www.myelux.com as described above. On the container page (step 6), locate the individual package to download (the product name is listed in the right-hand column), and save it to a directory on the machine with the container (note: do not save it directly to the container!).

When transfer is complete, run ELIAS. Select your container (**Container** > **Select**).

In the **Container** menu, select **Import package**. Browse for the *.zip file you just downloaded. When you have located it, click **Open**.

The Import Package function allows you to either import a new software package into a container or overwrite existing packages. The features and software dependencies of every software package remain intact.

Attention To insure error-free functionality, packages should only be imported into a container using the ELIAS Import function! If you copy packages directly into a container directory not using ELIAS, essential software dependencies and components will be lost.

Do **not** unzip the zip file temporarily, ELIAS does this for you.

5.3.7 Creating a New Container

You can construct a new customized container using the Export Package function. This is useful when updating from a USB device with limited memory, such as a memory stick.

- Create a new directory. Copy the file container.ini from your container to this new directory.
- Run ELIAS. Select your container (**Container** > **Select**).
- In the Container area, click to select a package.
- In the **Container** menu, select **Export package**. Browse for the new directory you just created. When you have located it, click **Save**. Do not change the standard file name. The package you selected will be saved to this new directory.
- Repeat until you are finished.
- To differentiate between containers, store them in different directories and label the directories by hardware type.

As with the Import function, all features belonging to a software package are automatically included. To insure all subcomponents are exported, please use the Export Function in ELIAS. Never copy files using Windows Explorer.

Please be aware that you must use standard container names to take advantage of the container macro. For more information on the container macro, see chapter5.10 The Container Macro.

5.3.8 Deleting Packages from a Container

To remove outdated software from your container, you need to delete its package. To delete a package from a container, open the container in ELIAS (**Container** > **Select**). Select the software package you wish to delete and press the DEL key. A confirmation dialog box appears, informing you of the software packages that will be affected. Click **Yes** to delete the package irretrievably.

Attention Package deletion is irreversible! Before deleting a package, check that the package is not used by any image definition file (*.idf). Otherwise it would have to be re-imported.

5.3.9 Working with ELIAS

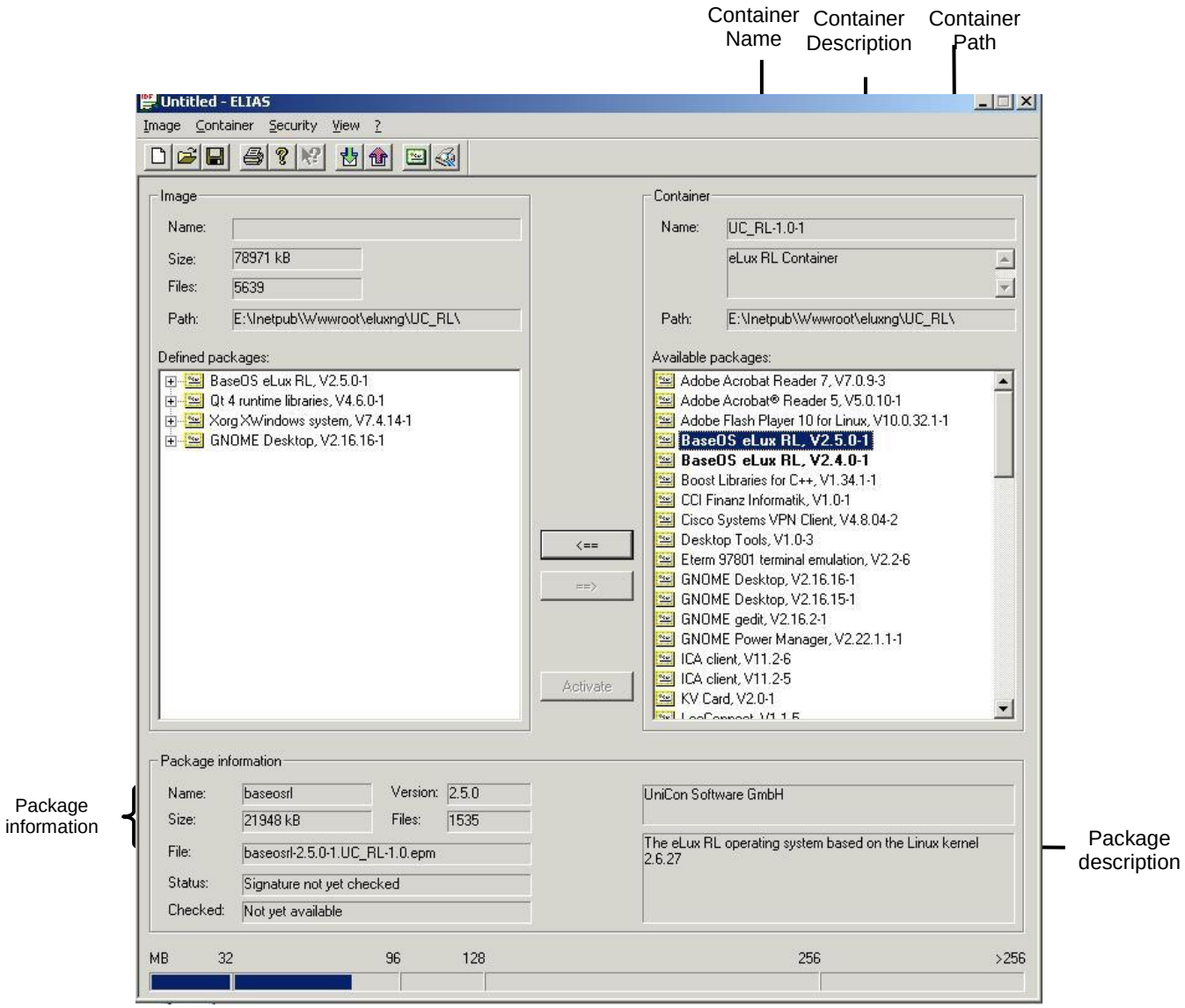


Figure 83: ELIAS – main window

5.3.10 Defining an Image Definition File

In a new image you compose exactly those software packages you want installed on the flash memory of the Thin Client. Before you can start to design your image, there is another requirement: the **container**.

When you select a package in the container area and click the left arrow, the package appears in the IDF area. If you select a package in the IDF area and click the right arrow, the package the package disappears from the IDF area.

A new IDF is created by adding and removing individual packages. In this way, the administrator can select the software suited to his or her needs. Select a package from the right window (the container window) and add it to the left window by clicking the <== button.

- The first package that must be selected is the base OS. This is the core of the IDF. Add requested packages by confirming with OK.
- Next, select software required in your server-based computing network: Citrix ICA®, RDP, browser, emulation, SAP.
- Further software is included to eLux users at no additional charge: desktop tools, VNC server, mirroring software, etc.
- Other software must be licensed: PowerTerm and X97 emulations, third-party software, etc.

Click on the + in front of the icons to expand the software packages and display the single features. The features may have blue, green or red icons.

blue:	Mandatory features which cannot be deactivated
green:	Active features which may be deactivated
red:	Deactivated features which can be activated.

Activate or deactivate a feature by selecting it and pressing the space bar. You can also use the context menu by clicking with the right mouse button.

Information shown during the design procedure

The **Package information** area (below the list of Defined packages) displays the software name, file name, version and size of the selected feature or package.

The **Image** area (above the list of Defined packages") displays the name of the image definition file, the total size of all packages selected so far, and the path of the file. In addition, the size is displayed graphically in the flash usage bar at the bottom of the screen.

One main feature of ELIAS is the built-in conflict test: It carefully tests your selection for incompatibilities and will warn you if two packages conflict. In addition, if a package you select is dependent on another package, you will be prompted with a message and requested to select the other package first. This insures that there are no software incompatibilities in the finished IDF. It cannot, however, check for hardware incompatibilities! This is left up to the administrator.

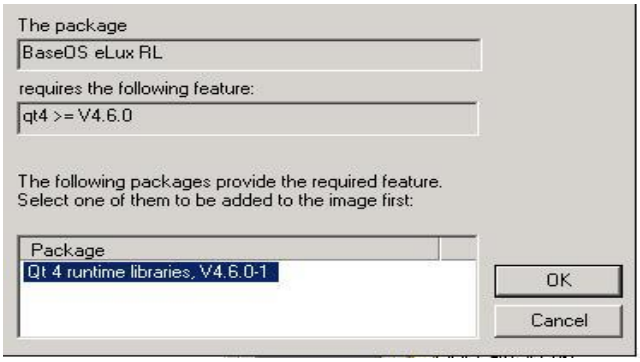


Figure 84: ELIAS – Package requirements

Another new functionality in ELIAS V7: The existing baseOS can be replaced by a new or different version in a fast and secure way. All required packages are also replaced by the corresponding versions, when confirmend by Yes rsp. OK in the following dialogs.

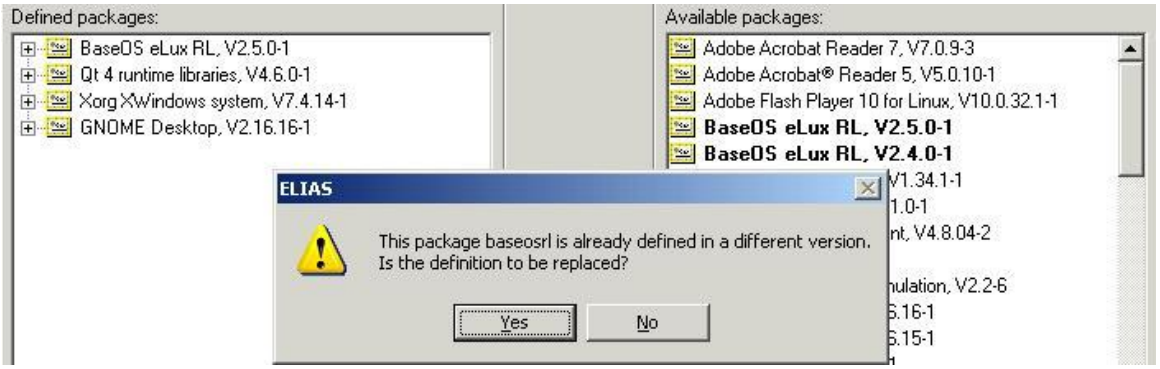


Figure 85: ELIAS – Package replacement

The Web site www.myelux.com contains a list of all currently available packages and is discussed later in this chapter.

5.3.11 The Container Macro

One of the features of eLux is its integrated macros.

The device hardware is automatically detected during the recovery process. The text __CONTAINER__in the Path field of the Recovery settings dialog box represents a macro that will automatically be replaced with the standard container name for that hardware. This greatly eases configuration and is especially useful for networks with more than one hardware platform. You must use containers with standard names.

As administrator, naturally you can replace this text by a different text. In this case, the text in the Path field must be the actual container name.

The container macro is not specific to a recovery and can also be entered in the Firmware tab. For a description of firmware parameters, see section 3.5 Firmware."

5.3.12 The Size Macro

The device hardware is automatically detected during the recovery process. The text __SIZE__" in the **Image file** field of the **Recovery settings** dialog box represents a macro that will automatically be replaced with text corresponding to the size of the Thin Client's flash card as follows:

Text	Flash size (MB)
small"	32
medium"	96
large"	128
xxl"	256 or greater

For example, if a 32-MB flash card is detected, the recovery IDF "recoverysmall.idf" will be installed, if a 96-MB flash card is detected, the recovery IDF "recoverymedium.idf" will be installed, etc. If a harddisk is detected, the recovery IDF "recoveryxxl.idf" will be installed.

This greatly eases configuration and is especially useful for networks with different sizes of flash cards.

As administrator, naturally you can replace this text by the actual name of the recovery IDF. In this case, you lose the dynamic recognition of the macro. The size of the recovery IDF must be equal to or less than the size of the flash card.

The flash size macro is not specific to a recovery and can also be entered in the **Firmware** tab. See section 3.5 Firmware.

5.3.13 Saving

To save your image definition file, from the **Image** menu click **Save**. You must save the image definition file to the container directory! By default, the container is installed in the FTP or HTTP server root directory under the names given in chapter 5.3.

Attention Use a transparent naming scheme for the image definition files! In addition, the name should not contain any blanks.

If you save your files using the pre-set text small(32 MB), medium (96 MB), large(128 MB) or XXL(250 MB or higher), you can take advantage of the built-in macro. See 5.3.12 The Size Macro for more information.

5.3.14 Size Constraint

During the image definition process there is no total size constraint. The total image size can exceed the actual flash memory size, allowing you to experiment with different software combinations, activating or deactivating software components until you have met your requirements. However, the final image cannot exceed the total flash size. Please be aware of this when saving your files.

5.3.15 Printing the Image Definition File Contents

For documentation purposes, ELIAS provides a print feature to let you print a list of the software packages and features in an image definition file. In the **Image** menu, **Print**, **Print Preview** and **Print Options** allow you to configure the print settings.

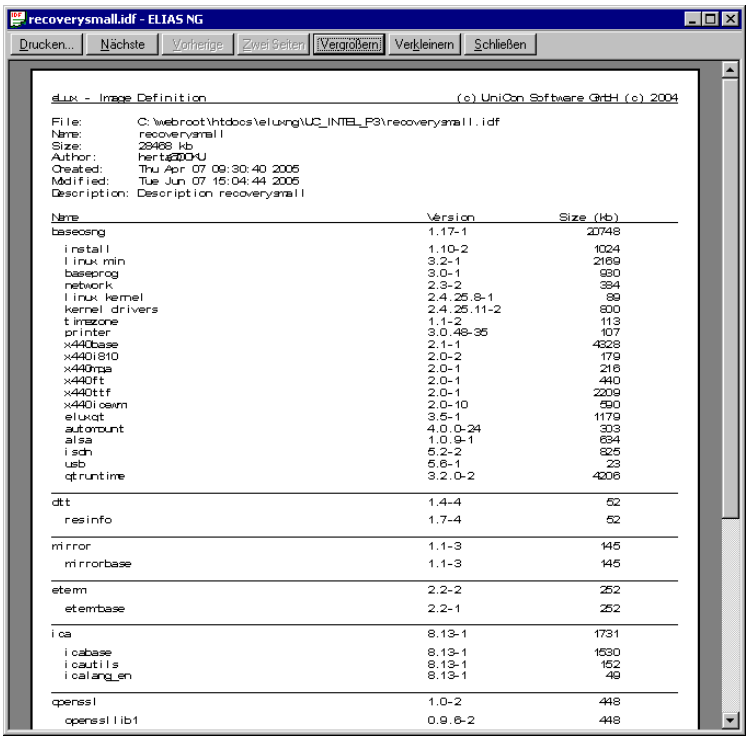


Figure 86: Print Preview of the image definition file

5.3.16 The Image Menu – Export of the IDF

Among others the **Image** menu contains the option **Export.**

Figure 87: Image menu – Export of idf

A dialog opens to **save** the idf. Click on ***Browse*** to change the target directory, if required.

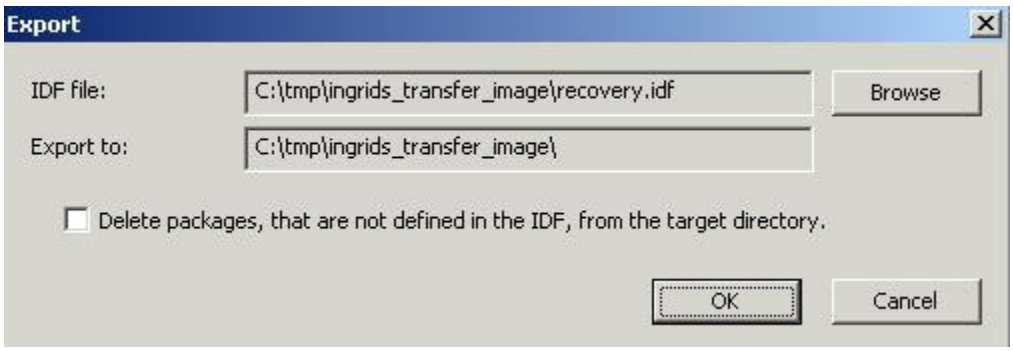


Figure 88: Export > save idf

5.3.17 The Container menu

This offers to select an existing container, to import packages to and export packages from the container.

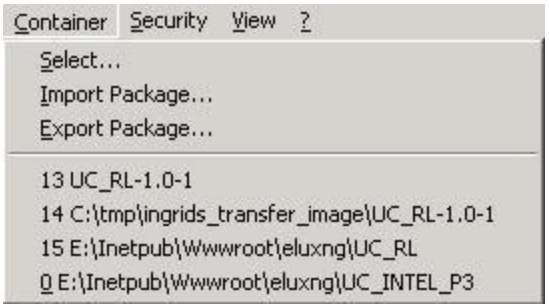


Figure 89: Container menu

5.3.18 The Security menu

This menu contains all options to check for signatures and certification as well as to manage certificates and define the security settings.

- Check signature during import
  If this option is enabled, signatures are automatically checked for during import of packages.
- Check all packages in container
  Checks for the signatures of all packages in the container.
- Check selected packages
  Checks for the signatures of a selected package and its components in the container or image window.
- Signature and certification information
  Displays the security status of a package and its components which had been selected in a container or image window.
- Manage certificates
  Enables the management of certificates in the "Vertrauten Liste" of ELIAS.

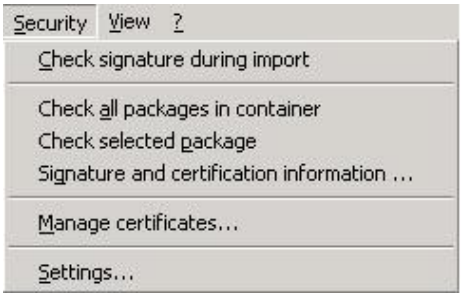


Figure 90: Security menu

- Security > Settings
  An Online Certificate Status Protocol (OCSP) server is used to check the status (valid, revoked, unknown) of a certificate.

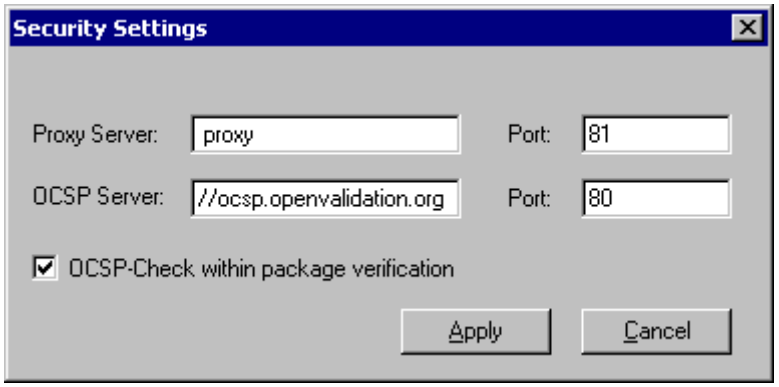


Figure 91: Security settings – OCSP Server

⇨ To set OSCP settings

1. In the **Security settings** dialog box, enter the following:

   Proxy server (optional) If you use a proxy server to connect to the Internet, enter the proxy server IP address (or name) and the port.

   OCSP server In general, the OCSP server is automatically read from the certificate. If this information is not available, you can enter a default OCSP server in URL format and the port by hand. Format: `http://`*<OCSP server URL>*

   Default values are `http://ocsp.openvalidation.org` and `80`.

OCSP check within package verification Every time before checking a signature, the validity of the certificate will automatically be checked.

5.3.19 ELIAS Keyboard Shortcuts

Key Combination	Action
General	
Cursor (arrow) keys: ↑ ↓	Screen navigation
F1	Opens online help.
TAB / SHIFT-TAB	Screen navigation
Container Window	
CTRL + left arrow key: ←	Adds a package to the IDF.
DEL	Deletes the selected package from a container
INSERT	Opens the Import Package dialog box.
Image Window	
Cursor (arrow) keys: ← →	Expands / collapses a defined upper-level eLux Package Module
CTRL + right arrow key: →	Removes a package from the image definition file.
SPACE BAR	1. Expands / collapses a defined upper-level eLux Package Module 2. Activates / deactivates a lower-level Feature Package Module

Further shortcut keys are adjusted to default Windows shortcut keys.

5.4 PUMA

PUMA (Package Update Management Agent) is the service for a fully automated update via Internet of the packages defined with ELIAS.

PUMA consists of three parts:

- service running in the background performing the update
- control program for the settings
- tray icon to start the program and to show the current status

5.4.1 How to Use

After the installation of PUMA you will find a new icon in the Windows taskbar:  .

Right-click the icon to open the following menu on the desktop:

- **Update** –
  starts the update process (see chapter 5: Update)
- **Update in background** –
  starts the update process in the background without user interface
- **Settings** –
  to define the parameters

When the update process is running you will only get the menu item:

- **Stop update**

If the service finds new packages on the web, the icon changes to  , and the update process can be started by a double click on the icon.

After installation, the start menu also contains the item **Puma – Settings**, another option to open the settings menu.

Note:

The main menu now offers the option ***Help*** to open the manual.

When editing the SQL-Server data base connection you can choose between the authentication methods SQL-Server and Windows. In addition, the data base name can be entered.

5.4.2 Settings

- **Database tab**

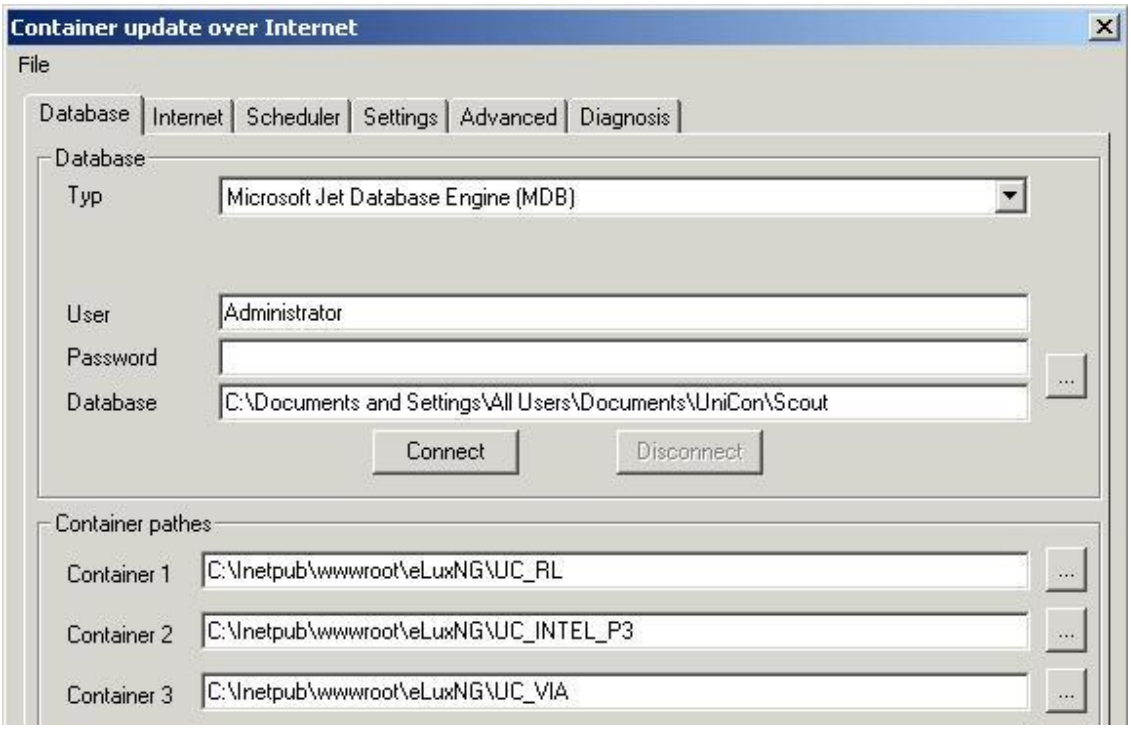


Figure 92: PUMA - Settings - Database

- **Database** – This is to enter the database used by the Scout server.
  As long as there is no connection to the database, the remaining tabs will not be enabled.

- **Container paths** – At least 1 container path must be entered, up to 5 container paths can be entered. The **container.ini** must be included in the path.

- **Internet tab**

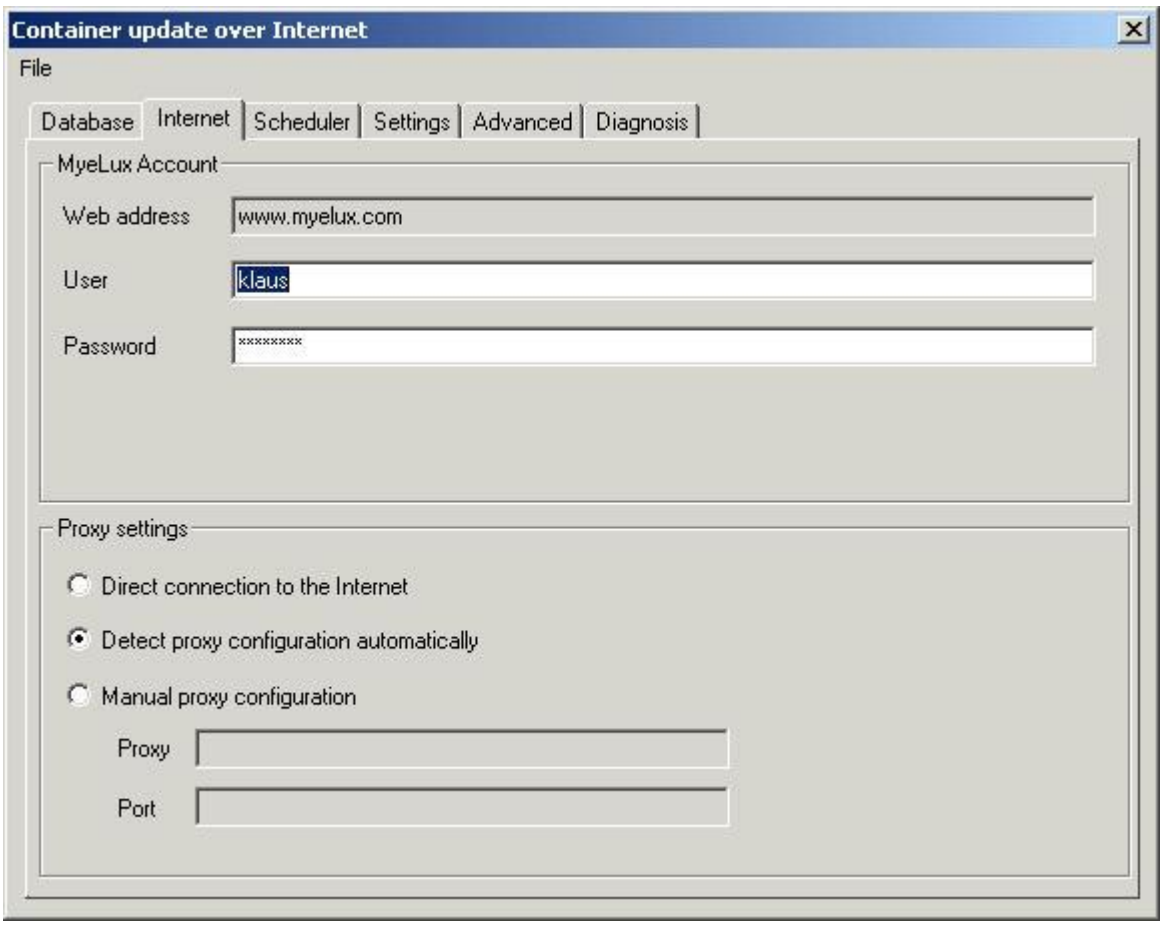


Figure 93: PUMA - Settings - Internat

- Account data for login at www.myelux.com
- Proxy settings

- **Scheduler tab**

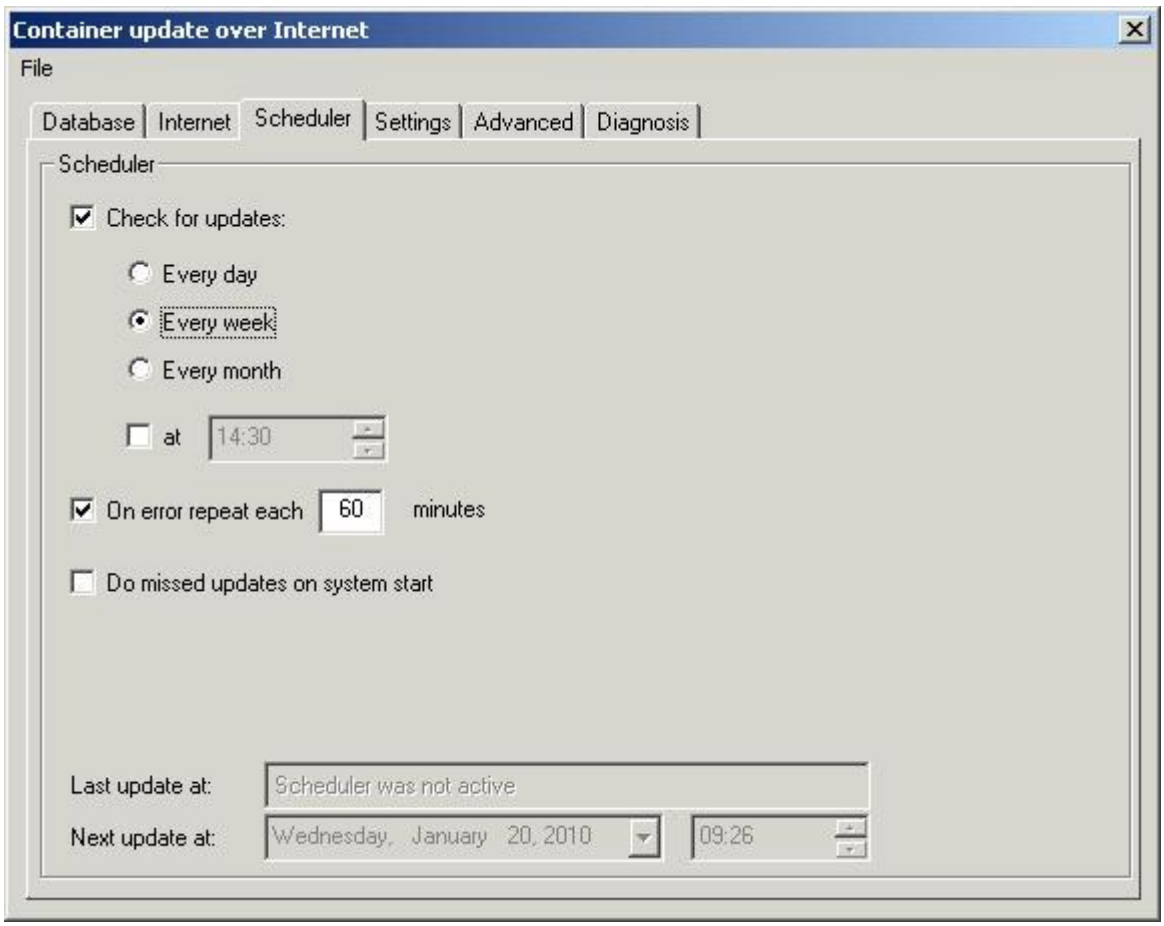


Figure 94: PUMA - Settings - Scheduler

- **Check for update** – enable or disable the scheduler
- **Every day / every week / every month** – time interval for scheduler. Every month means 28 days, thus resulting in the same day of the week.
- **at XX:YY**' – time of day
- **On error repeat each..**– e.g. in case www.myelux.com should not be accessible.
- **Do missed updates on system start** – if the computer had been off at scheduled point of time this option is to initiate the update once the service has been started.

When the scheduler is enabled, it shows the time of the last update and the point of time for the next update.

- **Settings tab** – see Chapter 13.2.1 - Settings tab
- **Advanced tab**

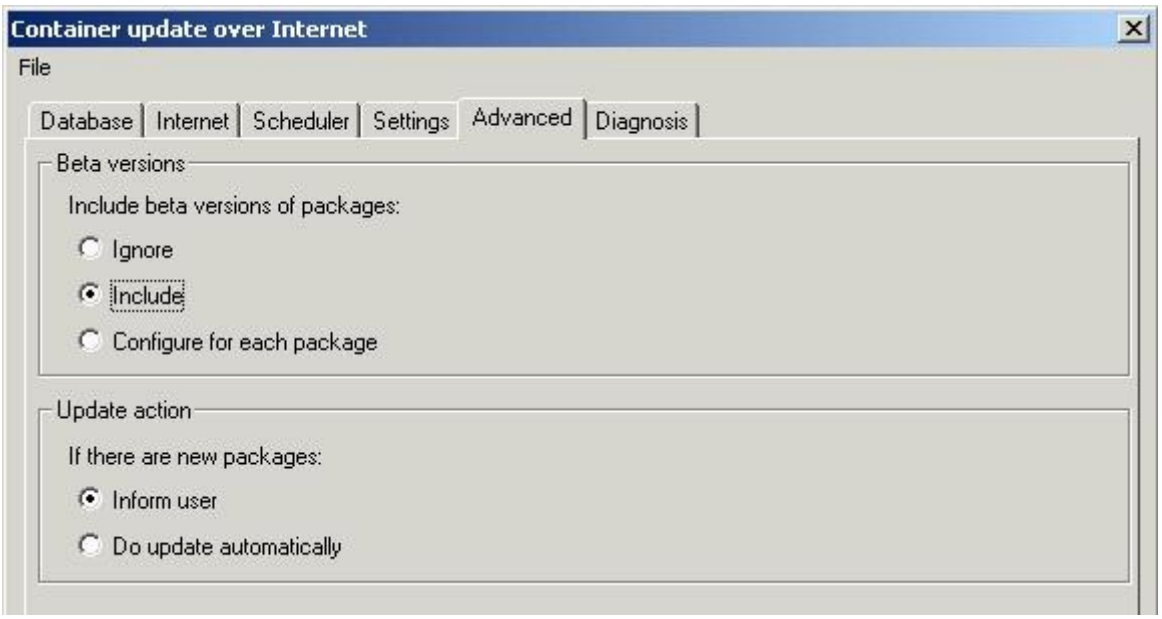


Figure 95: PUMA - Settings - Advanced

- **Beta versions**
  - The options **Ignore beta versions of packages / include / configure for each package** - define, how beta versions are to be handled regarding an update.
- **Update action**
  - **Inform user**– the icon in the Windows taskbar changes to , when new packages are found.
  - **Do update automatically** – the packages are automatically updated in the background.

- **Diagnosis tab**

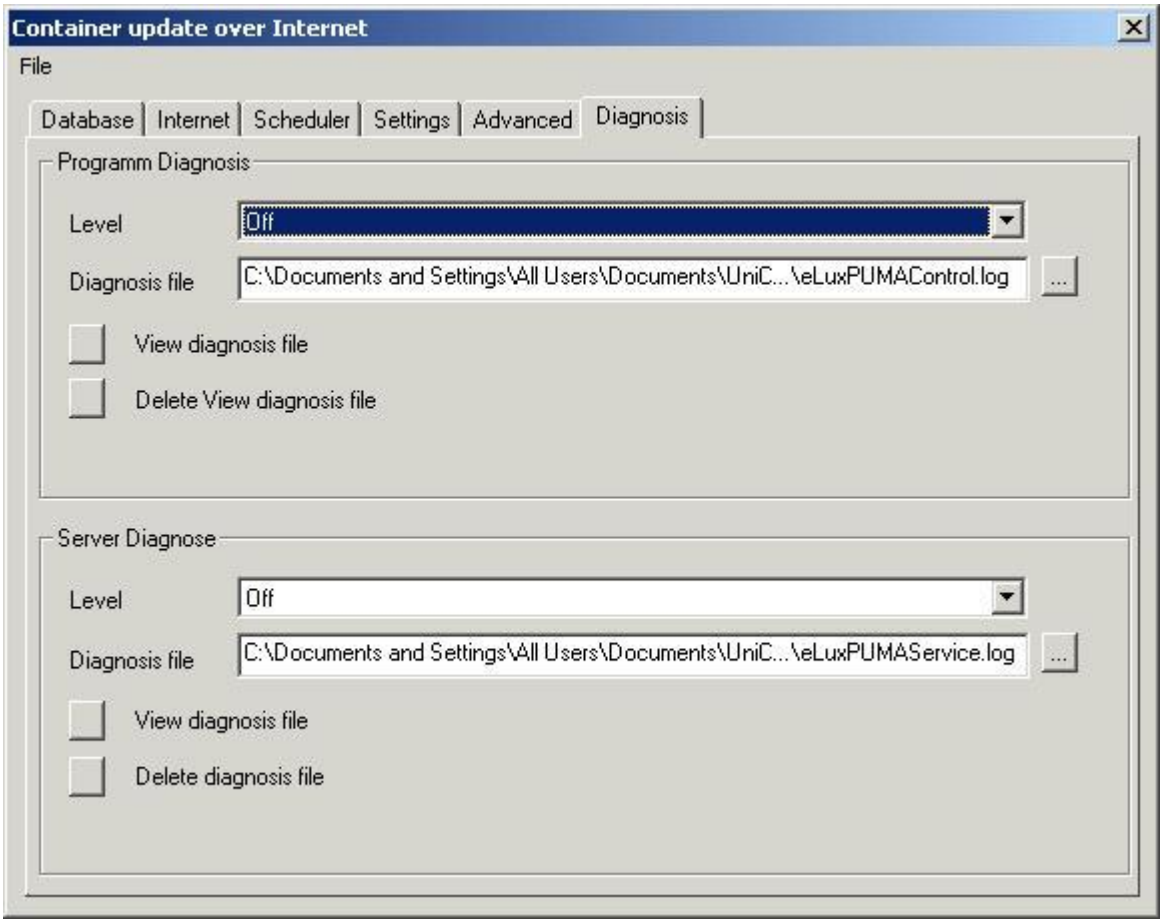


Figure 96: PUMA - Settings - Diagnosis

- **Program Diagnosis** – Diagnosis settings of the control program
- **Server Diagnosis** – Diagnosis settings of the service

5.4.3 Settings tab

This is to configure which software packages are to be downloaded from the Internet.

When the Settings tab is active, the parameters in the tabs **Database** and **Internet** are blocked, since these must be accessible for the settings. You need to close the dialog and reopen it, in order to change parameters in the tabs Database and Internet.

The list on the left – titled Subscription – shows the subscribed packages, the list on the right shows the packages available on the web for the selected container.

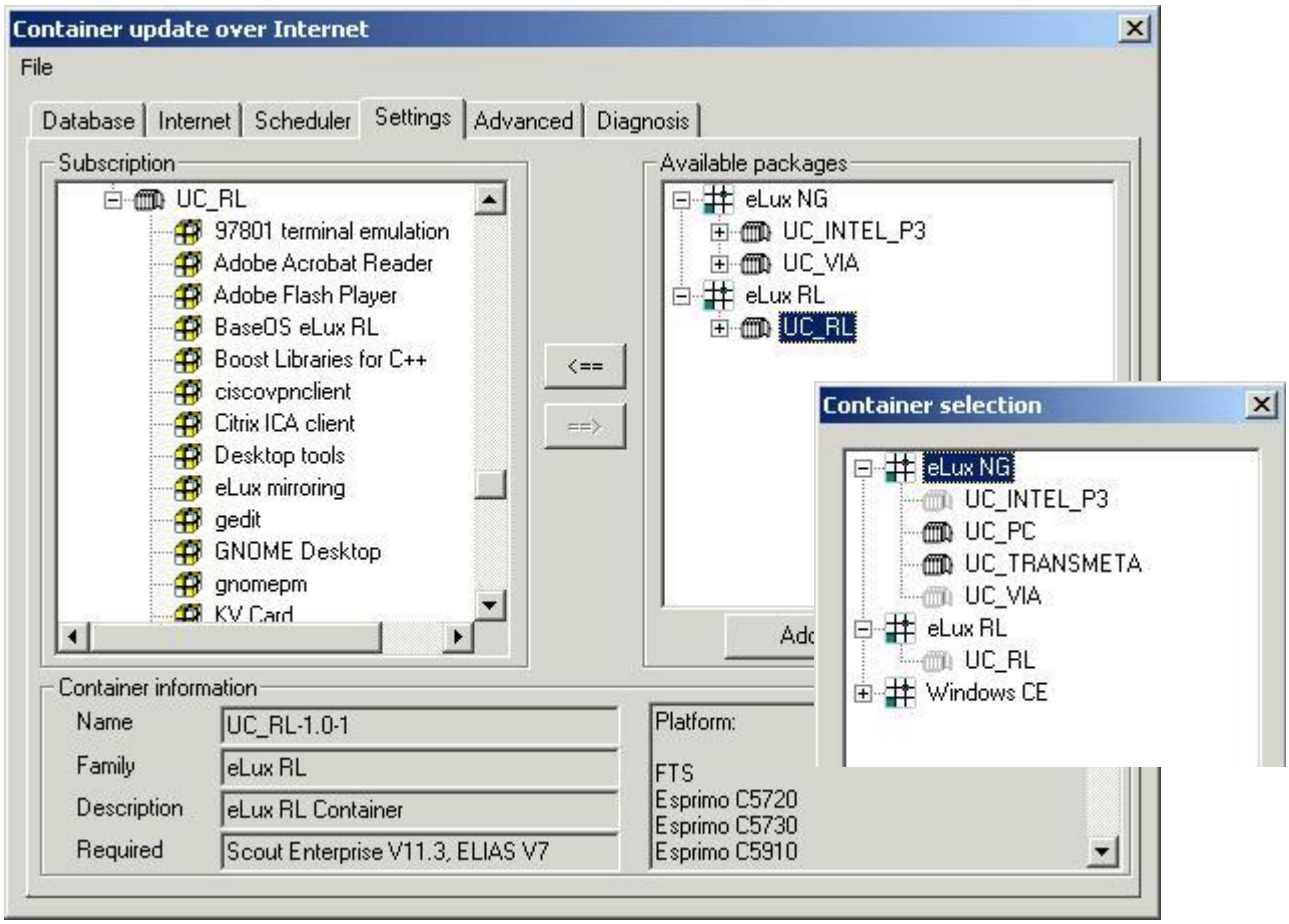


Figure 97: PUMA - Settings

First step is to select at least 1 container in **Available packages** / **Add.** The path for this container must be set in the tab **Database** / **Container paths.**

Then use the buttons ← und → to subscribe or unsubscribe one or all packages. Click on container or package to show detailed information.
If in the **Advanced** tab the option **Configure for each package** is enabled, a right click allows to configure whether the beta versions of a package are to be included in the update process (Use beta).

Instead of → you can press <Del> or <Ctrl>+<Cursor Right> in the window on the left.
Instead of ← you can press <Ctrl>+<Cursor Left> in the window on the right.
Instead of **Remove** you can also press <Del> in the right-hand window.

5.4.4 Update

Starting the update process offers you any new package for download.
Hotfixes are shown in red, beta versions in yellow icons.

To exclude a package from download just disable the checkbox.

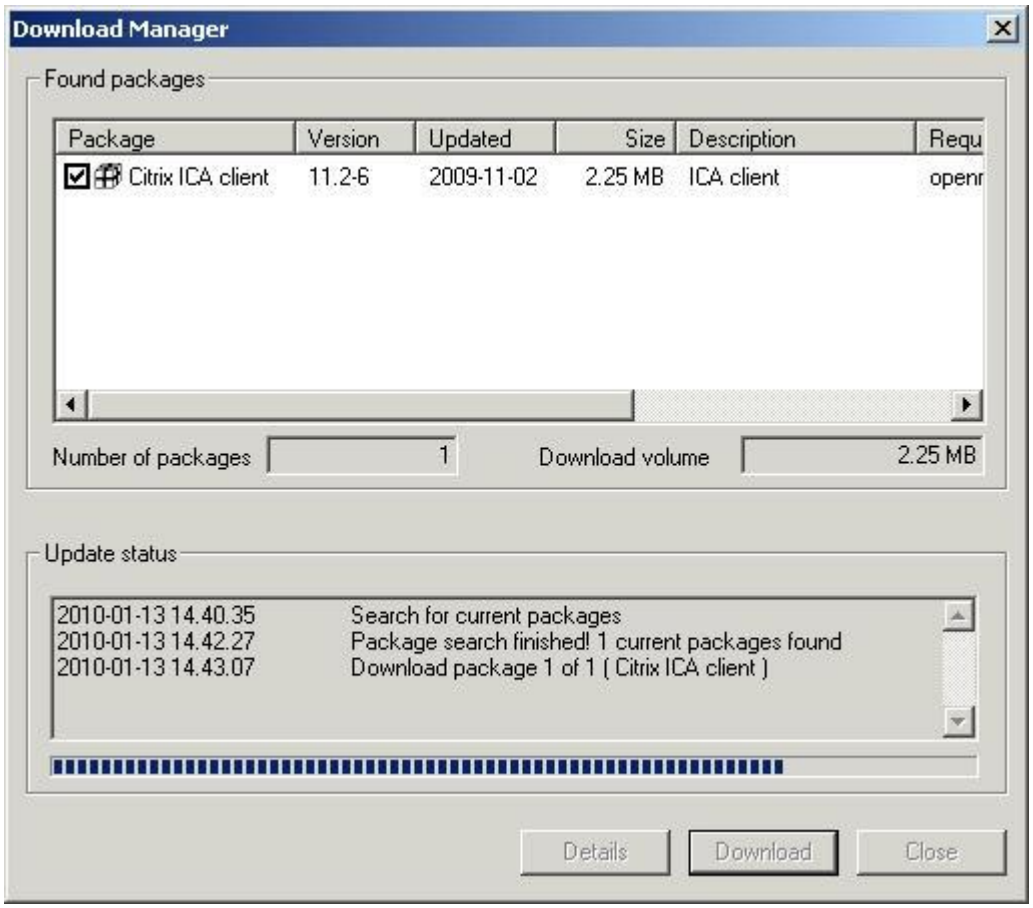


Figure 98: PUMA - Update / Download Manager

A rotating icon in the Windows taskbar shows that the update process is running. You can stop the process by right-clicking the icon.

5.5 Firmware Update

To update firmware, you need the following:

- Image definition file (*.idf)
- FTP or HTTP server
- User name and password on this server
- Container file (container.ini) and software packages (*.epm files)

The image definition file is created using ELIAS, as described previously in this chapter. It must reside in a container directory on an FTP or HTTP server (network update"), along with container.ini and the software packages. Alternatively, the container can be on a CD-ROM or memory stick (file update"). Update via floppy is not supported.

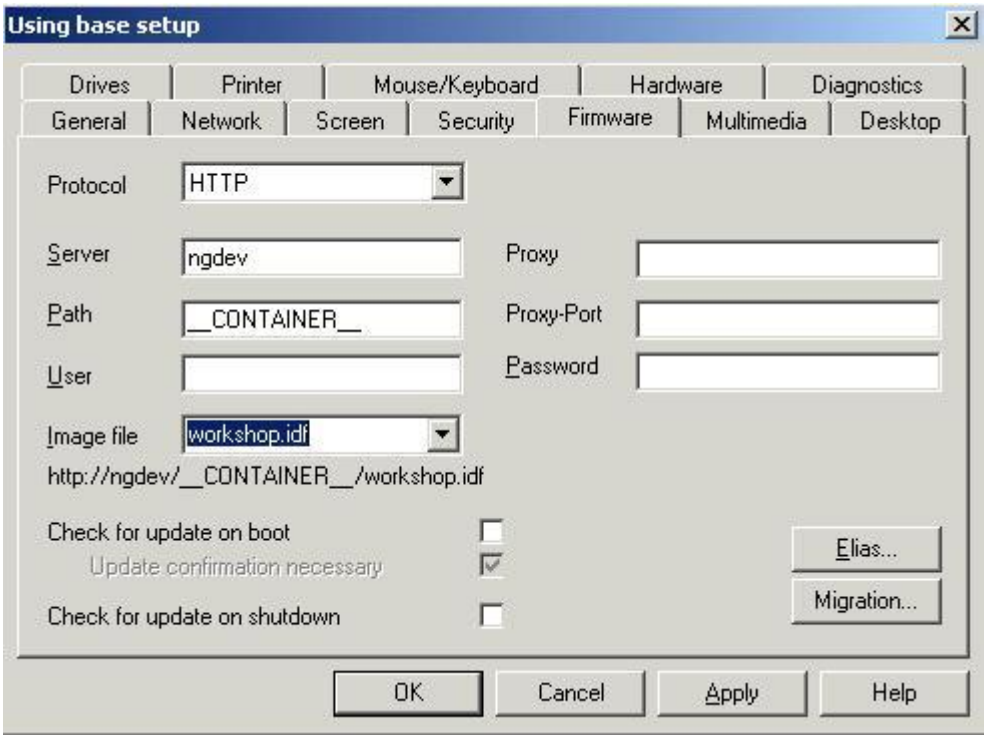
The following sections describe how to configure the firmware settings and use the update command.

5.5.1 Update via Network

To perform an update on a device or organisation unit, you need to configure its Setup, which is either the base configuration or an individualized Setup.

Open the Setup

- for the base configuration: **Options** menu > **Base configuration**
- for an **individualized configuration:** right-click an organisation unit or device, select **Setup** from the context menu and open the **Firmware** tab.



.

Figure 99: Firmware Update via Network

To perform an update over the network using an FTP or HTTP server:

Server:	Enter the IP address or name of the update server.
Path:	Enter the container path. The path name begins without the / character.
User Name:	Enter the user name required to access the update server. If no user name is required, do not leave blank: Enter `elux`.
Password:	Enter the password required to access the container path. If no password is required, do not leave blank: Enter `elux`.
Image File:	Enter the file name of the image definition file without blanks with the extension `.idf`.
Proxy:	(optional) Enter the IP address or name of the proxy server.
Proxy Port:	(optional) Port number of the proxy server.
Protocol:	Select **HTTP** if your software packages are stored on an HTTP server. Select **FTP** if your software packages are stored on an FTP server.

When "Check for update on boot" is selected, an update check is performed when the Thin Client boots. When "Update confirmation necessary" is selected, a confirmation box appears on the Thin Client before an update takes place, allowing the user to cancel.
"Check for update on shutdown" is another option to set a reminder.

Click on the button **ELIAS** to edit the image definition file.

Note: For ELIAS to open the image definition file automatically, you must add the container path to the list in the **ELIAS – Settings** dialog box (**Options** menu > **eLias Settings**).

For information on using ELIAS, the image definition file editor, see the sections earlier in this chapter.

For your convenience, macros have been included in the eLux NG software. They allow the administrator to consolidate firmware settings when updating different hardware platforms and flash sizes.

5.5.2 Performing an Update

Update Command

You can choose to update:

- an organisation unit
- an individual device

The **Update** command (open the context menu of an organisation unit or an individual device) updates the firmware on the device using the firmware information entered in **Setup**.

There are 2 options:

- Inform user for: enter time in seconds to inform user of update.
- The user can cancel the command (from the client)

You can choose to do an update immediately or you can schedule it for a later time.

During an update procedure, the individual device icons are white.

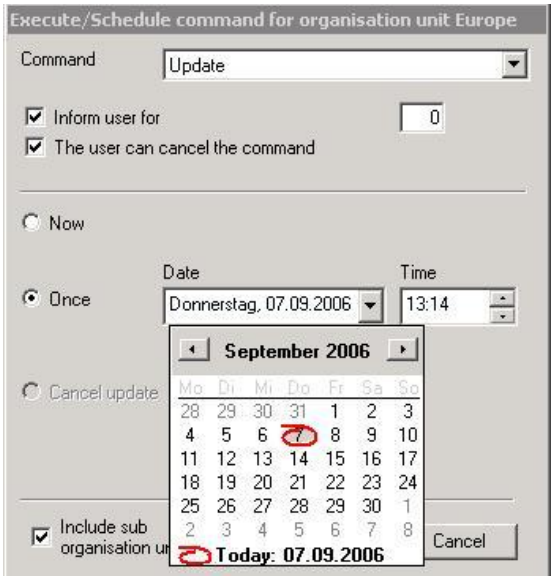


Figure 100: The Update command (Execute/Schedule Command....) from the context menu of an organisation unit

5.5.3 Update Confirmation

Once you have performed an update, you should verify that it was a success. There are several ways to view update information.

1. Properties Window

In the tree view, select an individual device. The time and status of the last update are displayed in the Properties window (right-hand side of the screen. Last Stateshows whether the update is currently taking place, was successful, or if there was an error. See 5.5.4 Troubleshooting .

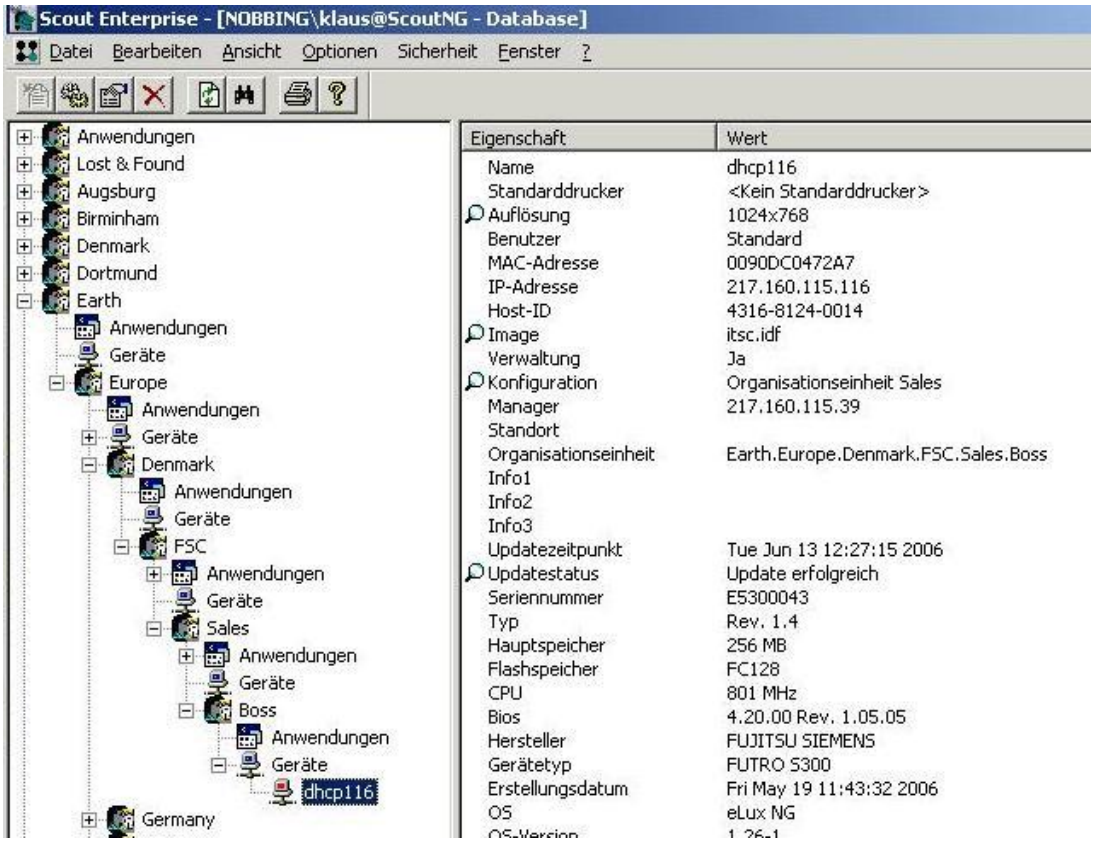


Figure 101: Device properties

2. Update Log – Individual Device

Another option is to view the update log for an individual device.

In the tree view, use the left mouse button to click to select an individual device. Double click on the magnifying glass next to Last State in the Properties Window. Alternatively, you can select **Update Info** from the context menu of the individual device (right mouse button).
This displays the log for the last update performed on the selected device.

The window can be resized.

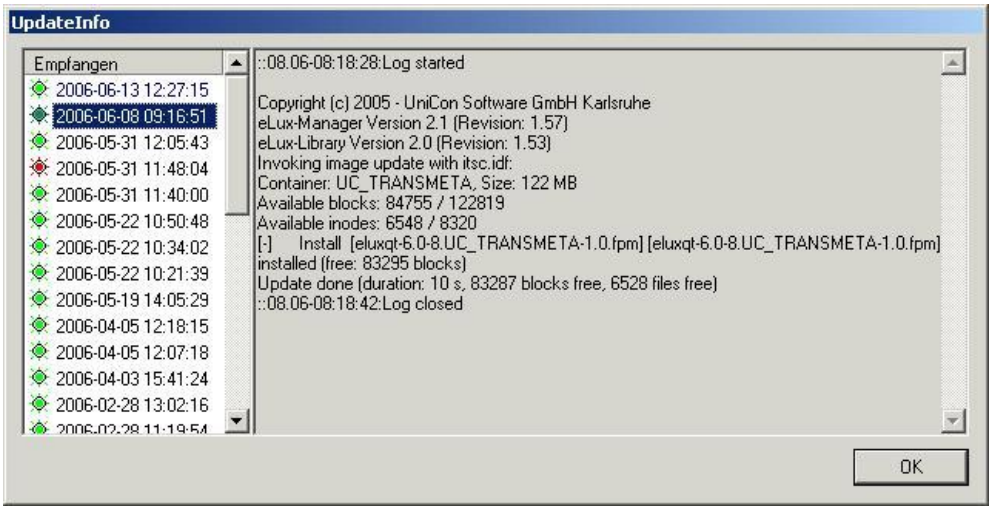


Figure 102: Update log of an individual device

3. Update Log in Scout Enterprise

Scout Enterprise Server includes a log of all performed updates since the installation. You are informed about Status / Time, Type (organisations unit or device) and the name of these. Above all it is useful to check for the status (done or failed).

You can show the Update History in **View** menu > **Update History**.

Figure 103: Update History in Scout Enterprise

5.5.4 Troubleshooting

Error Messages

Last Statein the properties window shows if an update was successful. If an update failed, the reason why will be displayed here. There are several reasons why an update can fail. The most common are:

Bad Container

Container are hardware-specific. Check that your container matches your Thin Client specifications.

Bad Flash Size

Check that the flash size specified in your image definition file matches the flash size of your Thin Client.

Bad Authorization

Wrong Thin Client password. Correct the entry at **Setup** > **Security**.

Client needs recovery installation

When critical FPMs in the base OS are updated, the Thin Client requires a recovery installation before it can be updated.

See the appendix for a complete list of error messages.

Update Options

If update continues to fail, consider adjusting the update settings. Go to the **Options** menu and select **Advanced Options**. The **Advanced Options** dialog box appears.

Here you can set the maximum number of parallel updates (number of Thin Clients simultaneously updated, a block"), the delay time between blocks, and the response time. Optimal values are system-specific. Default settings are shown in Figure 104.

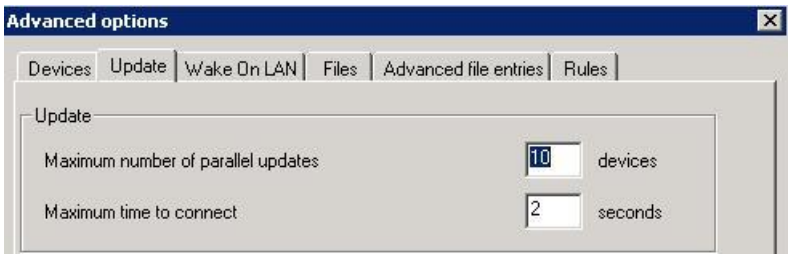


Figure 104: Advanced Options - Update

Microsoft Internet Information Server

To update firmware or perform a recovery using Microsoft Internet Information Server (IIS) or later, there is an additional step: The file extensions requested by eLux are not automatically transferred by IIS, but rather must be explicitly added to the MIME types.

Note: Starting with Scout Version 11 the MIME types may be defined via the Scout Installation Wizard. This chapter descripes themanual entry of the MIME types.

Note Entering the MIME types may not always be necessary. We recommend, however, that you add them when using IIS. For version 6.0 they are required.

1. Open the Internet Services Manager (**Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**).

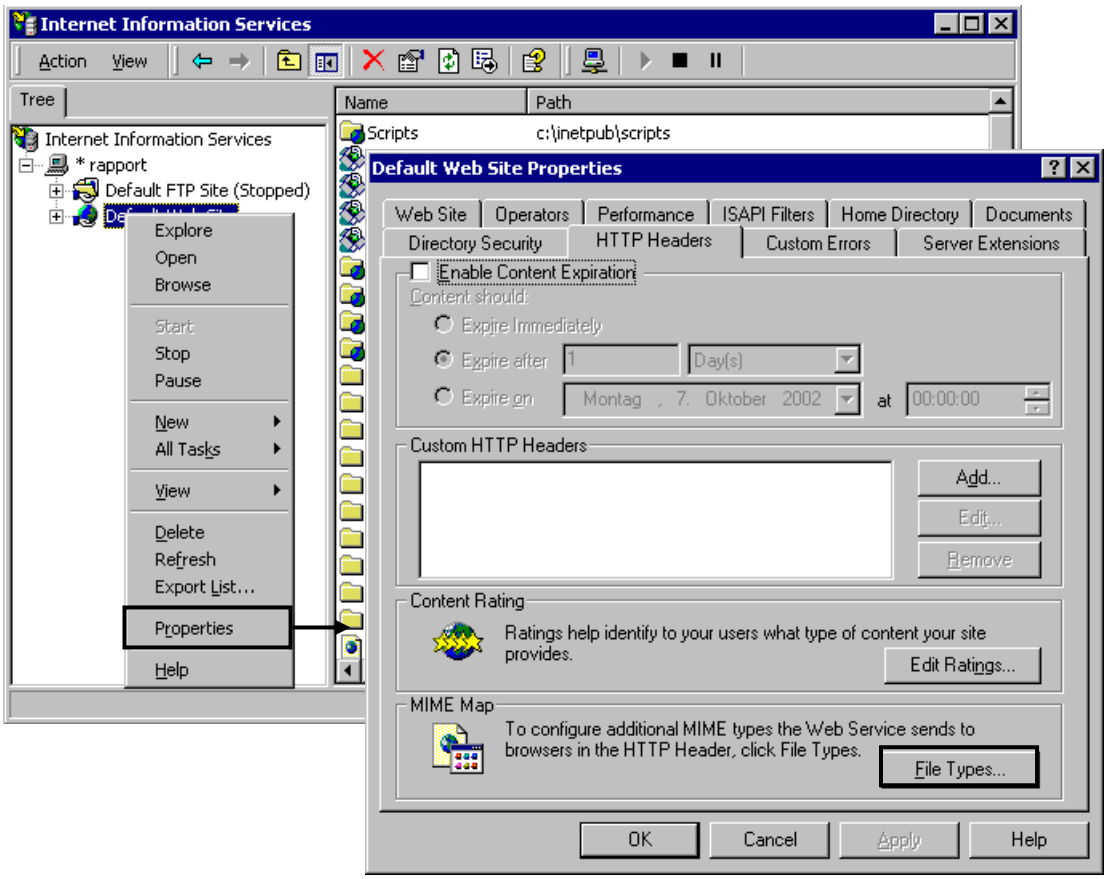
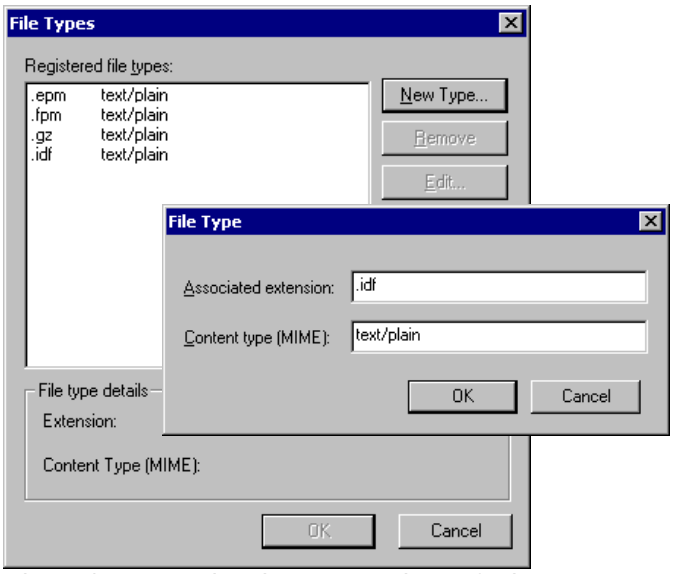


Figure 105: : Microsoft Internet Information Services Manager

2. Expand the branches until the Internet site is visible.
3. Click with the right mouse button on the Internet site and select **Properties**.
4. In the **Web Site Properties** dialog box go to the **HTTP header** tab. Click the button **File Types**.

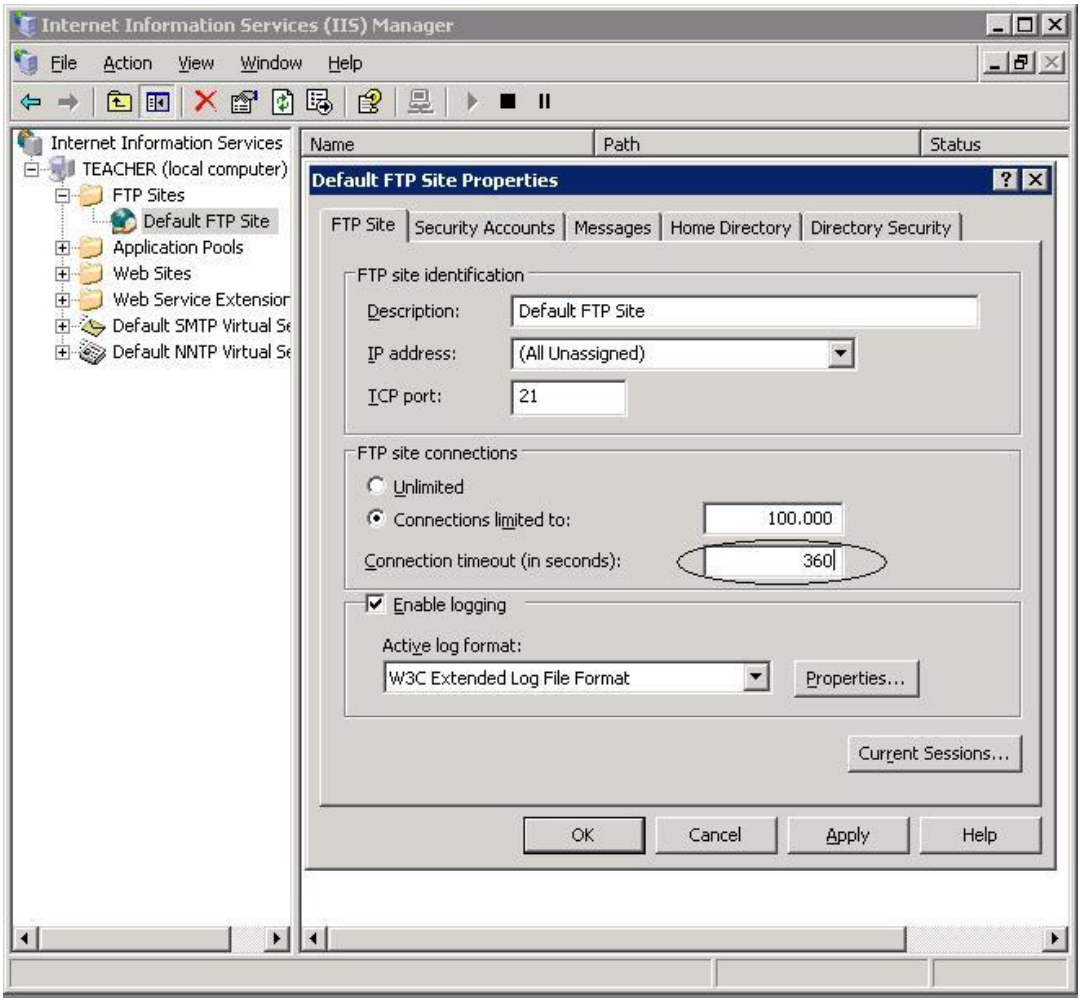
5. In the **File Types** dialog box click **New Type** and enter `.idf`, `.fpm`, `.epm`, `.gz` as `text/plain`.



IIS is configured for an update/recovery.

If FTP is to be used the parameter "FTP site connections" / "Connection timeout" on the Default FTP Site in the Internet Information Services (IIS) Manager is to be changed from the default of 120 to 360 seconds.

106: *Figure IIS*



Manager – StandardFTP Site

Background information: Due to local activities (e.g. removal of software) in some constellations a timeout may occur during a client update after the FTP connection, when using the default of 120 seconds.

5.5.5 Migration from eLux NG to eLux RL via Firmware Update

The procedure described here enables the migration from eLux NG to eLux RL via the comfortable firmware update. Thus the migration is scalable and comprehensible even for a large number of systems, considering the hardware requirements of the individual devices.

5.5.5.1 Requirements

- Thin Client with eLux NG
- Knowledge about the procedure of the firmware update, ELIAS via Scout.
- Thin Client Hardware: at least CPU 500 MHz, RAM 256 MB, Compact Flash 128 MB and an up-to-date CPU
- Scout Enterprise Server Version 11
- eLux NG BaseOS 2.0-1 or higher
- eLux RL BaseOS 2.0.0-1 or higher
- FTP- or HTTP-Server with UC_RL-Container

The stepwise migration procedure described here requires that you are familiar with creating image definition files (IDFs) by means of the tool ELIAS.
If necessary, you find detailed information in our manuals about eLux, Scout and ELIAS on our website http://www.myelux.com/.

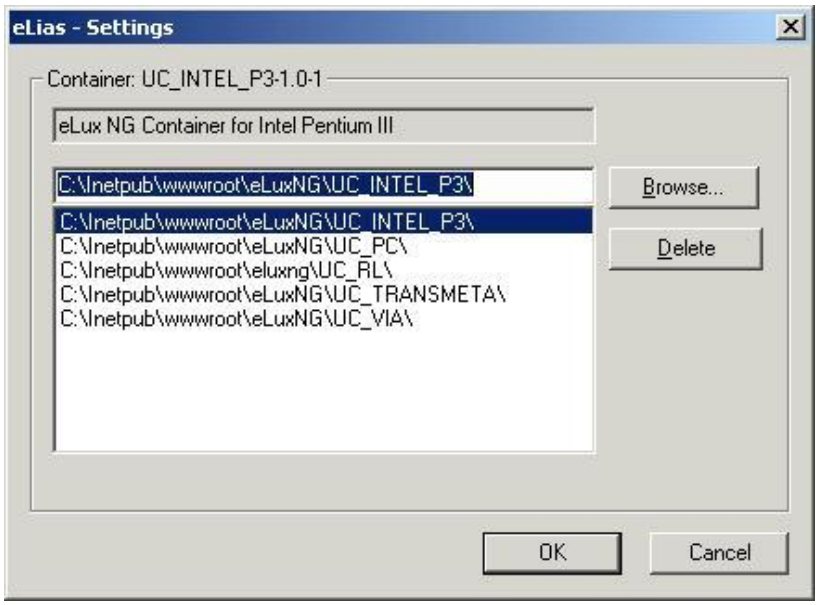
5.5.5.2 Procedure

1.) Download the ***baseosng-2.0-1*** and the RL migration package ***RL_Mig-1.0-1*** from www.myelux.com > eLux software packages > eLux NG Container > Released Packages and import both into your eLux NG container (UC_INTEL_P3, UC_VIA rsp. UC_PC).

2.) Define an eLux NG image with BaseOS 2.0 or higher and include the RL migration package. Save the image definition file.

3.) Download the target container eLux RL from www.myelux.com and save the container in the same subdirectory as your eLux NG container naming it **UC_RL.**

4.) Extend the ELIAS settings in Scout (Options → ELIAS Settings) by the new UC_RL container.



5.) In Setup > Firmware enter the name of the new Image Definition File for the eLux NG Image.

6.) Create new parameters for the eLux RL target image in Configuration > Firmware > Migration. The macro __CONTAINER__ will be resolved to UC_RL for the migration settings.

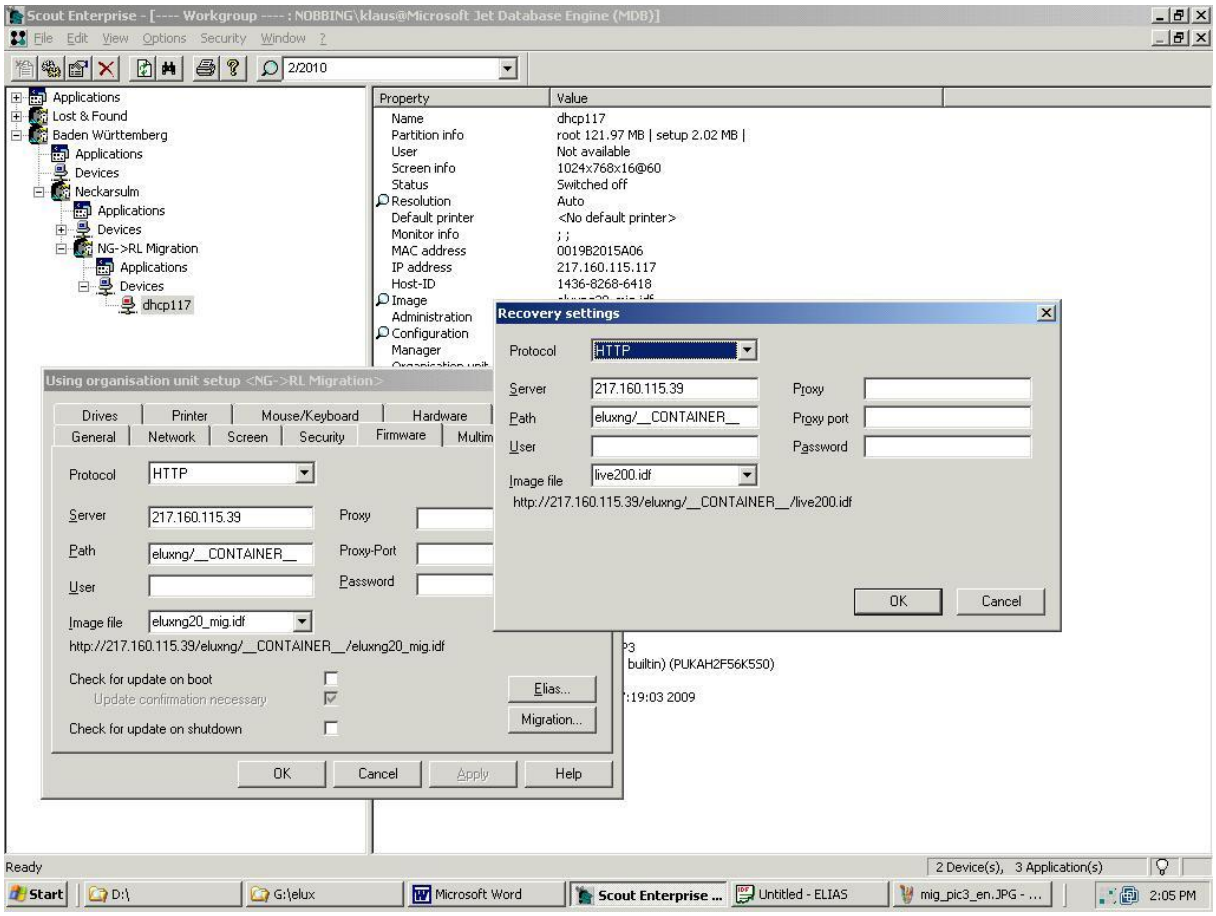


Figure 107: Firmware Migration eLux NG > eLux RL

7.) Initialize a firmware update via Scout.
On success first there will be an update to the new NG image and then, automatically, the update to the target image with eLux RL will be done.

5.5.5.3 Potential Errors

On principle, all error messages are displayed in the update log of the Scout server.

1) The target image definition file for RL has not been found:
http request failed: rc=0, ec=404 (File not found)
http request failed: rc=0, ec=404 (File not found)
URL: http://217.160.115.39/eluxng/UC_RL/eluxRL.idf
Please check your settings in Configuration > Firmware > Migration

2) Insufficient Main Memory
Error: insufficient memory 128MB (expected 256MB)
Your Thin Client requires at least 256 MB RAM

3) CPU too slow
Error: CPU clock speed too slow
At least 500 Mhz are required

4) CPU too old

Error: CPU too old

Transmeta processors, NSC processors, and older VIA processors are no longer supported with eLux RL.

5.) Graphical problems after a successful migration may occur with older PCs and Thin Clients (> 5 years).

In case of a migration from eLux NG for PC to eLux RL for PC we recommend to evaluate eLux RL on your PC in the first step. We cannot be for sure that your PC will run with eLux RL, even if CPU, RAM and clock speed of the processor seem to be adequate. Besides, Scout V11 also provides the complete management of systems with eLux NG.

6.) There is no way to downgrade to eLux NG from eLux RL by firmware update. If nesessary you need to perform a recovery procedure for your system.

For further details see our Recovery Paper on www.myelux.com or the corresponding chapter in this manual.

6 Management Functions Online Commands

The subject of this section are management functionalities. Assuming the administrator works at a PC having the Scout Server installed, whereas the local user works at a Thin Client with eLux at a different remote location ("remote device").

6.1 Status

6.1.1 Device Status

The state of the Thin Client can be easily determined by the icon color.

Green:	Individual device is turned on and ready
Red:	Individual device is turned off or not available
Yellow:	Desktop is being initialized
White:	Update is running
Grey:	Device cannot be managed due to insufficient number of licenses
Blue:	Device has been entered manually and there was no contact between Scout server and client so far.

6.1.2 Update Status

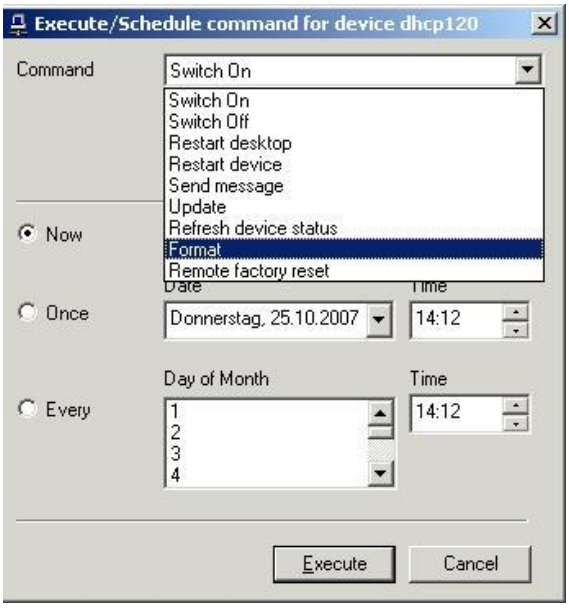
To determine the update status of a Thin Client, select the icon of the individual device. In the properties window, Last State displays the update status, either "Update successful" or "No update necessary".

6.2 Scheduler

Scout Enterprise comes equipped with a command scheduler that allows you to control the state of the device remotely. You can turn the device on and off, restart the device, or restart the desktop. This is useful for desktop configurations that take effect the next time the desktop or device is started.

Click with the right mouse button on an individual device to access the context menu. Select one of the following:

Switch On:	Turns on the Thin Client
Switch Off:	Turns off the Thin Client
Restart Desktop:	Restarts the desktop
Restart Device:	Restarts the device



The **Execute/Schedule command** dialog box appears:

The command "Format" is available starting with **Scout Version 9.6.0** for format partitions at the Client.

Click **Now** to execute the command immediately. Click **Once** to execute the command one time only. Click **Every** to execute the command repeatedly on a given day of the month or weekday. The time is in 24 hours. Note that no warning message is displayed on the Thin Client before the command is executed!

In addition to an individual device, the commands can also be implemented on all devices in an organsiation unit or in Scout Enterprise (global settings).

To open the Command Scheduler, from the **View** menu, select **Schedule**. The Command Scheduler gives you a summary of all upcoming events.

Starting with Scout **Version 9.6.1** selected data in the "Command scheduler" can be copied to the clipboard with the shortcut CTRL+C.

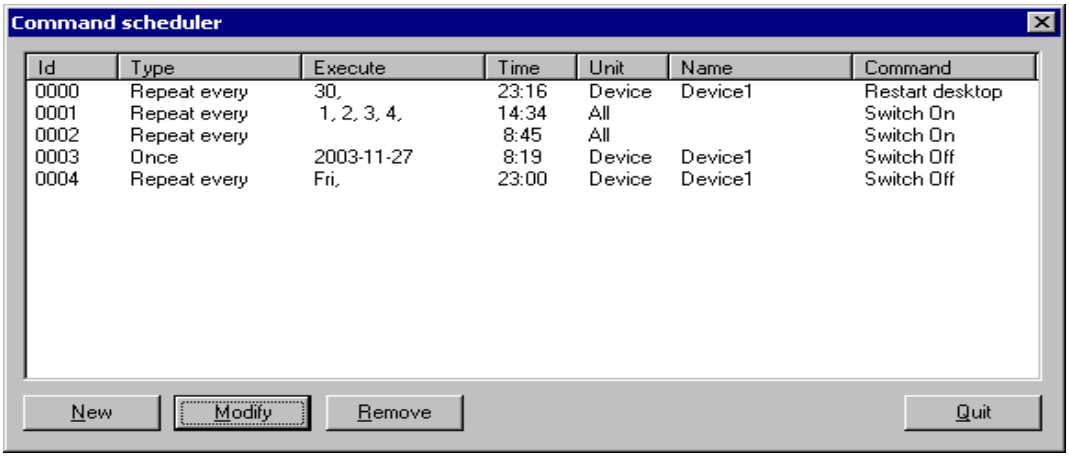


Figure 108: Scheduling

- **ID** Arbitrary number set by Scout Enterprise.
- **Type** Once or repeating.
- **Execute** If the event type was once, the date the event will be executed, otherwise the day of the month or workday, if the event is repeating.
- **Time** The time the event should occur.
- **Unit** The element the event will act upon: device, group, location, or all.
- **Name** The name of the unit as listed in Scout Enterprise.
- **Command** The command to be executed.

Once events occur, they are not automatically deleted. Select the ID and click **Remove** to delete an event.

To change an event's properties, select the ID and click **Modify**.

If you schedule a command from the Command Scheduler, it will affect all devices. Click **New**. The **Execute/Schedule command for all devices** dialog box appears. Select the command to execute and configure as described above.

6.3 Send Message

To have a message appear on the user's screen, click with the right mouse button on an individual device. In the context menu, select **Send Message**. The **Execute/Schedule command** dialog box appears.

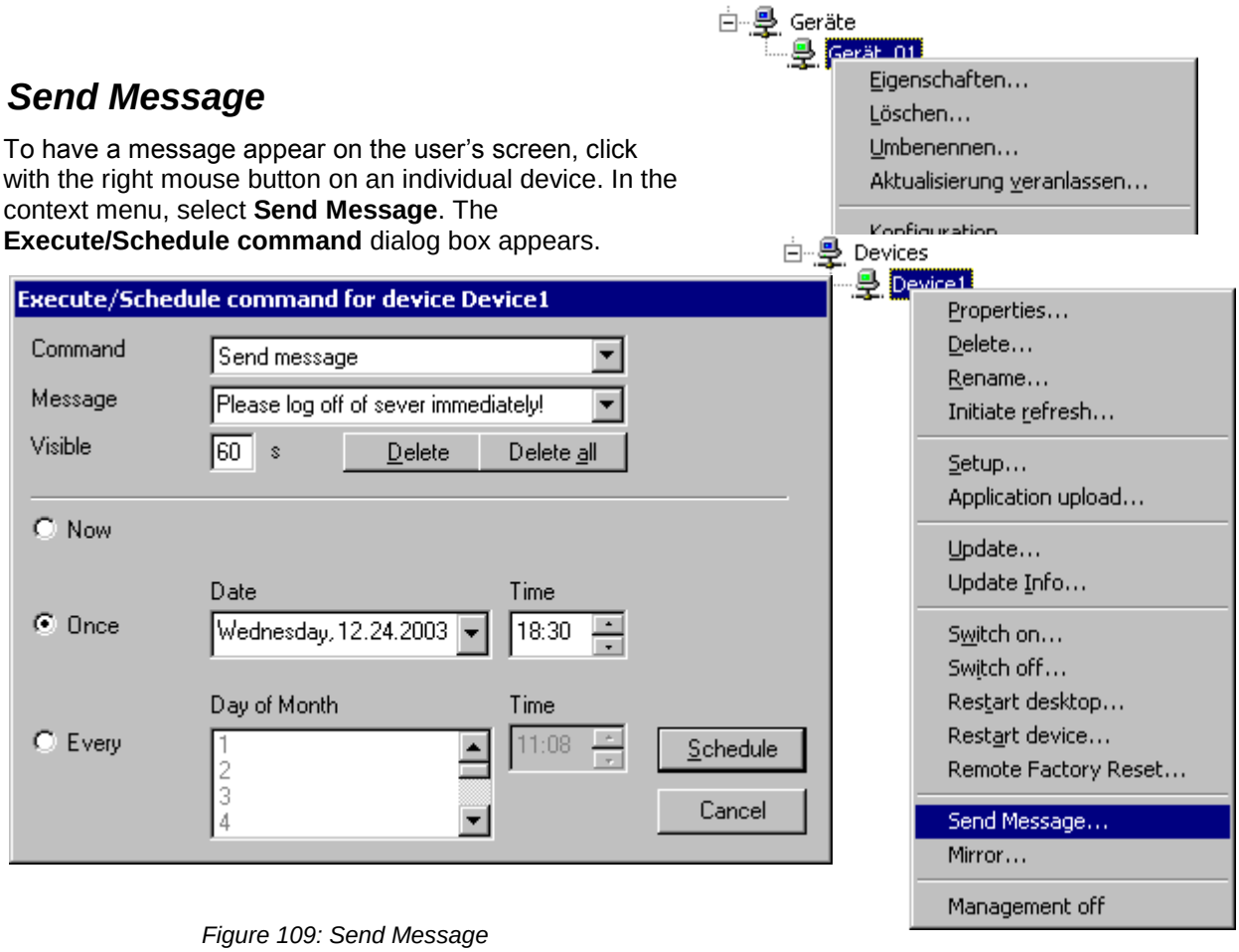


Figure 109: Send Message

Select **Send message** from the **Command** drop-down list. Type your text in the **Message** field. Past messages are automatically saved, allowing you to conveniently select repeat messages from the drop-down list. To remove a message from the list, select it and click **Delete**.
A display time of zero means the message is displayed indefinitely. This is default. For a specific display time, enter the value (in seconds) in the **Visible** field.
Click **Now** to execute the command immediately. Click **Once** to execute the command one time only. Click **Every** to execute the command repeatedly on a given day of the month or weekday. The time is in 24 hours.
In addition to an individual device, the command can also be implemented on all devices in a Group, in a Location, or in Scout NG (global settings)..

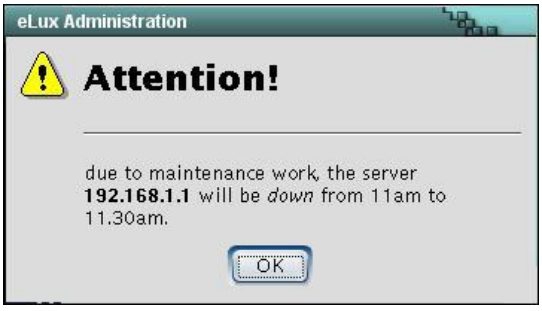
6.3.1 Creating Formatted Messages to the Thin Client

The messages Scout sends to the Thin Client users may be formatted for better understanding and nicer view. We use a subset of HTML.

Example:

The message
"Attention: due to maintenance work, the server 192.168.1.1 will be down from 11am to 11.30am."

will be shown as:



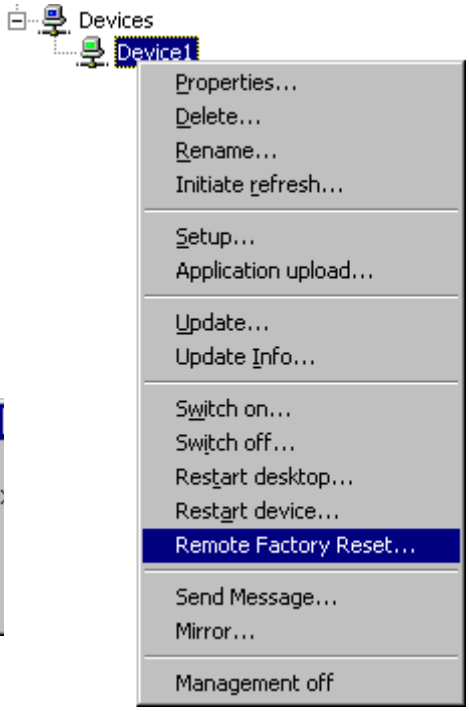
6.4 Remote Factory Reset

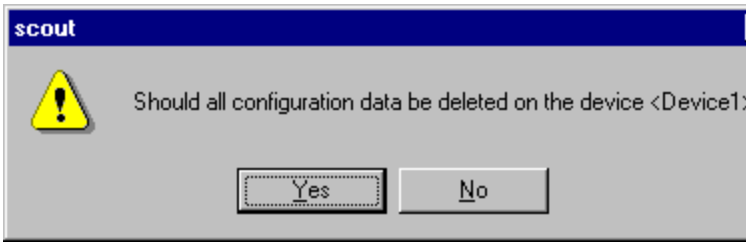
A factory reset is an important troubleshooting feature. It resets the Thin Client to the factory-delivered configured state: the configuration and applications, as well as any locally generated files, are deleted. However, only the configuration is deleted – firmware, licenses and management settings are not deleted.

Afterward the device reboots. Using the saved management settings, it contacts the Scout Enterprise Server and is automatically entered into its previous group and receives the group's configuration/applications.

A factory reset is especially useful when local configuration is allowed, the user has incorrectly configured eLux NG, and the administrator does not know the cause of the problem.

To perform a Factory Reset, click with the right mouse button on an individual device. In the context menu, select **Remote Factory Reset**. Click **Yes** in the message box.





Expert Tip

During a factory reset, all files in the directory /setup/public are deleted.

6.5 Mirroring

Mirroring is an important feature that allows you to see the user's screen without physically going to the Thin Client. It is useful for help desk.

Mirroring involves three steps:

1. Installing the software

2. Setting the Thin Client settings

3. Initiating the session

Step 1: Installing the Mirroring Software

You must have a VNC viewer installed on the administrator's machine, and a mirroring server on the target device.

A VNC viewer is included in the Scout Enterprise server software. No further action is required.

A mirroring server must be installed on the Thin Client (mirrorEPM).

Attention Mirroring is disabled on the Thin Client if the mirror package is not installed in the image definition file.

Step 2: Configuring Thin Client Mirroring Settings

In Scout Enterprise, go to **Base Configuration** > **Security**. Click the **Advanced** button to enable the Mirror settings.

Password: (optional) Enter a password for mirroring consisting of at least 6 characters. This password will be prompted when a mirroring session is initiated.

Read access: Gives the administrator's machine view rights only.

Confirmation necessary: The user must confirm a dialog box that appears on the Thin Client before a mirroring session can start.

Transfer mirror information: The mirroring is audited by logging those taking part as well as the period of time of the mirroring session. The data logged are stored on the Scout server in the \mirror\ folder.

Encrypt mirror session: The mirroring session may be encrypted in order to increase the security level.

Allow Scout only: All the clients which have this option enabled accept mirroring connections for a limited period of time only (default: 20 sec) from IP address of the requesting console.
Scout only sends a mirroring request, if the baseOS version of the client corresponds to the requirements and if the "Allow Scout only" option has been set.
Requirements for Scout : V 11.5.0
Requirements for eLux : BaseOS 2.6.1, Mirror 2.5.1

Otherwise the mirroring function works as before.

XDMCP: Enables an XDMCP session running on the Thin Client to be mirrored.

To disable mirroring completely, deselect the Enable mirroring check box.

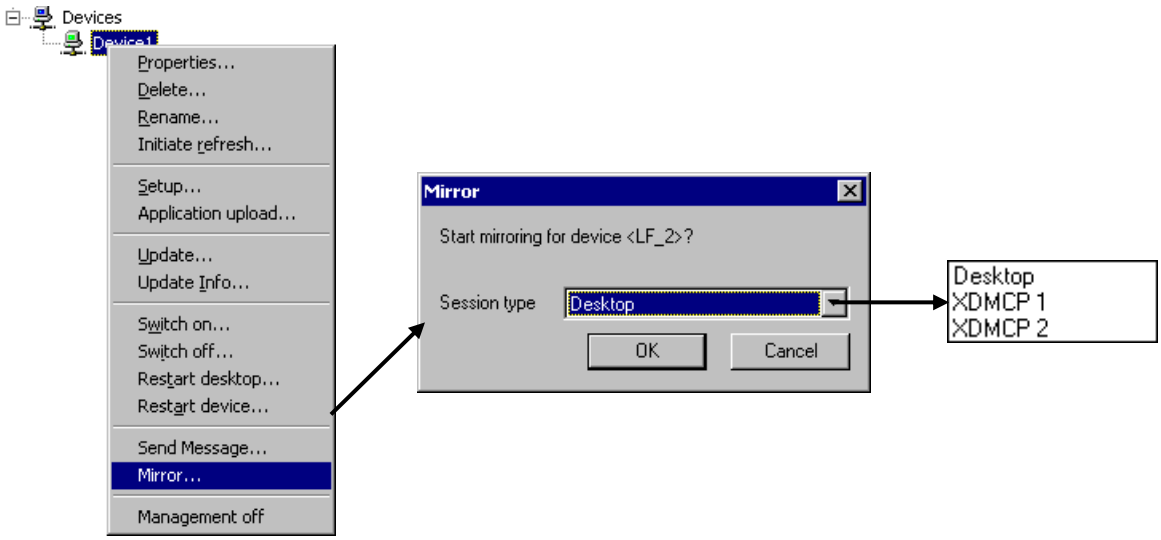
Step 3: Initiating a Mirroring Session

Only an individual device can be mirrored.

Only one Display can be mirrored at a time.

The client's keyboard mapping is not transferred during the mirroring session. Instead, the local keyboard mapping of the PC running Scout NG is used.

1. In Scout Enterprise, rightclick an individual device. In the context menu, select **Mirroring**.



2. In the **Mirror** dialog box, select the desired session type:

- Desktop: To mirror the eLux NG desktop (Display 0)
- XDMCP 1: To mirror the first XDMCP session opened (Display 1)
- XDMCP 2: To mirror the second XDMCP session opened (Display 2)

While more than one display can be open on the Thin Client, only one display can be mirrored by Scout Enterprise at a time. Click **OK**.

- Depending on mirroring settings, you may be requested to enter a password.

3. The mirroring session starts. Depending on mirroring settings, the session may begin only when the user has agreed to the confirmation dialog box.

4. A dialog box appears on the user's screen during the mirroring session. This dialog box cannot be removed.

5. The user/administrator ends the session by clicking the dialog box.

Security concerns

It is impossible to secretly mirror a user without the user's knowledge. During a mirroring session, a dialog box appears on the screen that allows the user/administrator to end the session at any time. In addition, you can set a mirroring password on the Thin Client.

Still, if security is a concern, disable mirroring settings and uninstall the mirroring software on the Thin Client.

6.6 Initiate Refresh

A Thin Client managed using the Scout Enterprise management tool receives its Setup configuration from the Scout Enterprise server:

- the first time it is entered in the Scout Enterprise software
- when the Thin Client starts

However, the Setup configuration is loaded when the Thin Client starts only if a change is registered in the Scout Enterprise server. This takes place when the administrator changes the Setup and then saves.

If the administrator makes no change, the Setup configuration is not loaded when the Thin Client starts. The Thin Client uses the previously saved configuration instead. However, files from the File list feature will be transferred (see section).

To force the Thin Client to reload the Setup configuration from the Scout Enterprise server the next time it boots, use the right mouse button to open the context menu and select **Initiate refresh**. The Thin Client will reload the configuration regardless of whether there has been a change registered with the Scout Enterprise server and files from the File List feature will be transferred

6.7 Environment Variable

Environment variables are device-specific and can only be set for an individual device.

To set one or more environment variables on a Thin Client, rightclick an individual device icon in the tree view. Select **Properties** from the context menu. Enter the environment variable using the format: <*variable name*>=<*value*>.

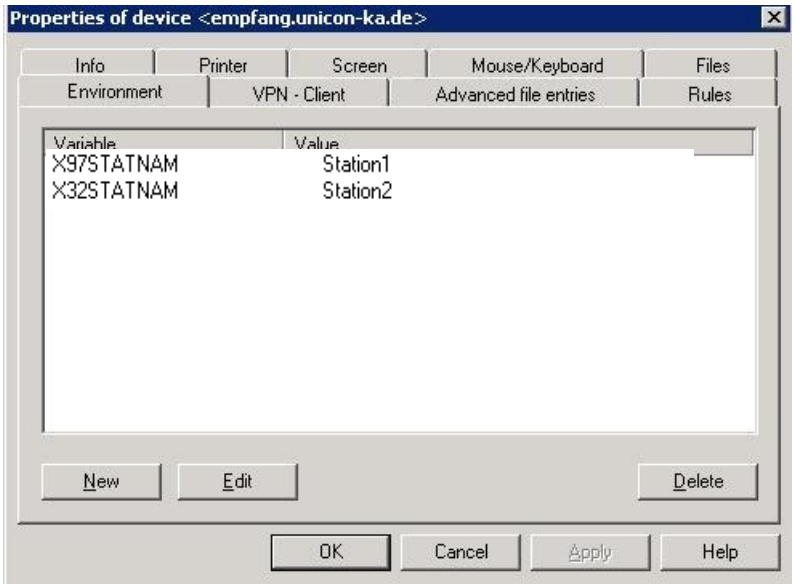


Figure 110: Properties - Environment Variable

On the Thin Client, the variable name is used with a dollar sign: $<*variable name*>.
Environment variables are often used with emulations.
Example: To define the station name for an X97 session, enter the following:
`X97STATNAM=DS104`
In the emulation, access this environment variable using "$X97STATNAM".

6.8 Advanced Options

In the **Options** menu select **Advanced Options** to configure optional parameters.

The dialog "Advanced Options" has the following tabs:

Devices:	gegliedert in die Bereiche Geräte suchen, Feldaktualisierung, Eintragung neuer Geräte, Gerätenamen
Update:	The maximum number of parallel updates as well as the maximum discover time can be set here.
WakeOnLAN:	Server name and protocol settings
Files:	Transfer of ini files
Advanced file entries:	Configuration files and transfer to the clients can be edited here.
Rules:	A selection of actions which are to be performed after the last applications has finished.
Partitions:	It is possible to change the partitions at the client.

The settings are explained in detail in this chapter, unless they are self-explanatory or described in other sections of this manual.

6.8.1 Devices

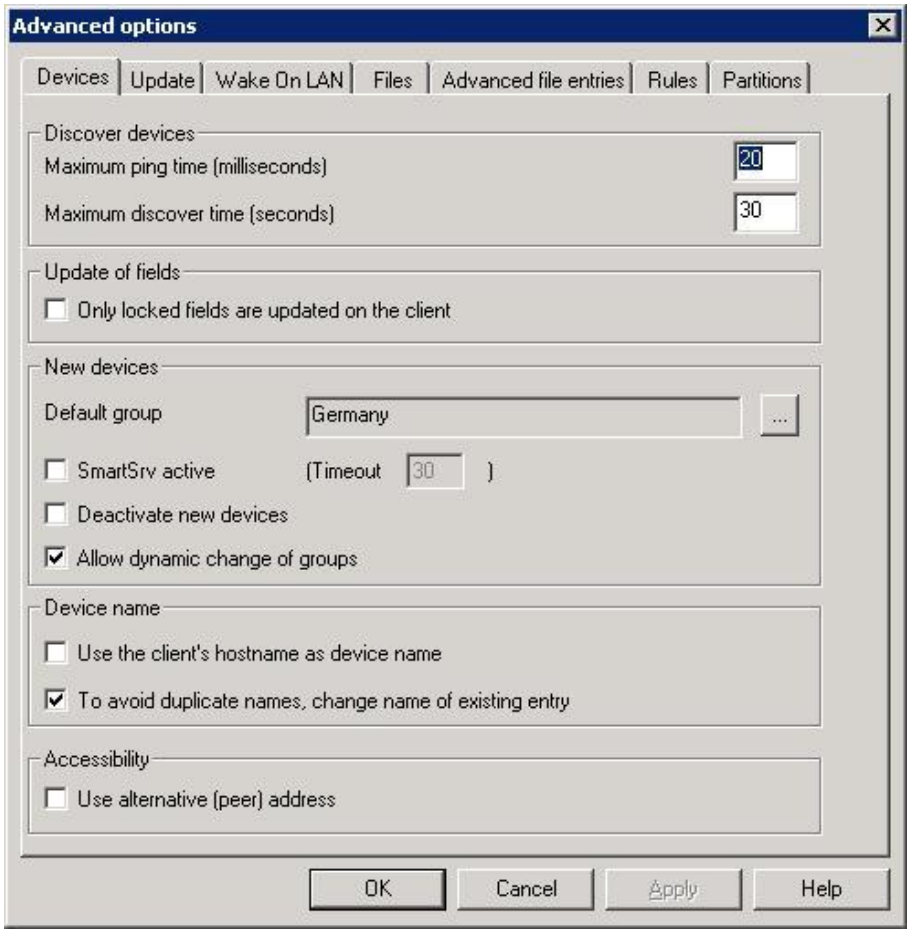


Figure 111: Advanced Options – Devices tab

Update of locked files

In the "Update of fields" area, click to select "Only locked fields are updated on the client."

In other words: Unlocked fields will not be overwritten by Scout. E.g., the end user can configure "his" preferred screen resolution individually, and his settings remain even if Scout changes other parameters.

If the end user should set a parameter not supported by the client (e.g. screen resolution too high), Scout can perform a factory reset of the client resulting in the transfer of all parameters.

New devices

In the "New devices" area, you have the following possibilities:

- **Default group** Devices that contact the Scout Enterprise manager and request to be entered in the default group will be automatically routed to the group that you set. See also .
- **SmartSrv active** Allows you to configure the First Configuration Wizard that appears on the local Thin Client the first time it is started. See 8.1.1 Modifying First Configuration Wizard Settings.
- **Deactivate new devices** When selected, the management for newly entered devices will initially be deactivated. To activate management, select **Management on** from the individual device context menu. The configuration will be transferred to the device the next time it boots. By default deactivated.
- **Allow dynamic change of groups**
  If this option is enabled Scout moves automatically those clients which are assigned a group ID.

Device Name

In the "**Device name**" area, you have the possibility of setting device name parameters.

Decide whether

- the client's host name is to be used as device name
- the existing entry should be changed in case of duplicate names

Accessibility

Enable the field "Use alternative address (peer address)" to use the address of a router to communicates with the Thin Client through NAT.
Example:

The router has an official IP address to the internet and the client's address is 192.168.10.1, which communicates with the internet through Network Address Translation (NAT).

6.8.2 Default Group

Lost&Found is the default group (=organisation unit) which is preset in Scout Enterprise with the ID=0. Lost&Found cannot be deleted or renamed. This insures that there is always a destination group when devices contact the manager. When Scout Enterprise is installed, the default group is set to Lost&Found.However, it can be set to a group of your choosing.
In menu **Options > Advanced Options** click the button next to Default Group in the area New devices". Select an organisation unit in the dialog **Organisation unit selection**.

Devices that contact the Scout Enterprise manager and request to be entered in the default group will be automatically routed to the organisation unit that you set. Examples:

- ScoutSrv No additional configuration necessary.
- DHCP Option Set Group ID to zero.
- Reverse Discovery Enter a Group ID of zero.

Setting a default group only affects devices that should be routed to the default group (generally when the Group ID is zero). Once you have activated this feature, devices will no longer be routed to Lost&Found. To route devices to Lost&Found, open the **Advanced options** dialog box and select Lost&Found as the default group.

This new feature does not affect your ability to route devices to other groups by entering the respective group ID.

6.8.3 Update

In the **Options** menu click **Advanced options**. The **Advanced options** dialog box appears. Click the **Update** tab.

Here you can set the maximum number of parallel updates (number of Thin Clients simultaneously updated, a block"), the delay time between blocks, and the response time. Optimal values are network specific. Default settings are shown in Figure 112.

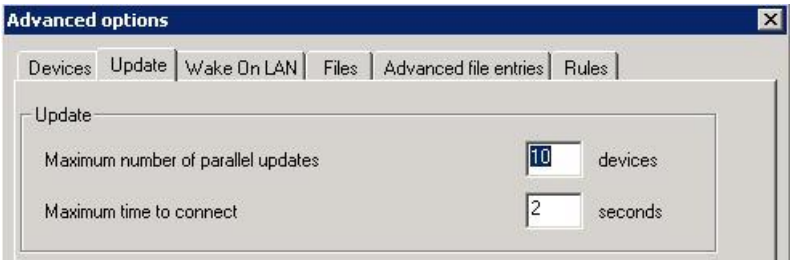


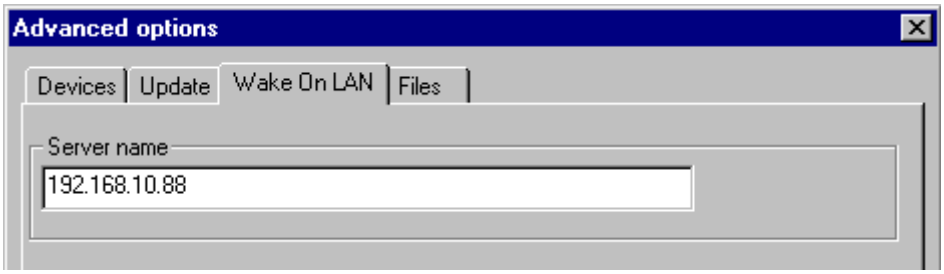
Figure 112: Advanced update settings

6.8.4 Wake-On-LAN

Entering a wake-on-LAN server is optional. Wake-on-LAN remotely controls (turns on) all Thin Clients within its subnet. This is useful for remote subnets, but is not required for the local subnet where Scout Enterprise is located. A wake-on-LAN server is included on the CD-ROM.

A wake-on-LAN server can either be set globally, or for an individual device, Group or Location.

Global Settings



To set a global wake-on-LAN server, from the **Options** menu, select **Advanced Options**. The **Advanced Options** dialog box appears.

In the **Wake On LAN** tab, enter the IP address of the wake-on-LAN server. The wake-on-LAN IP address entered here becomes the default address for all devices.

- To enter an eLux device as a wake-on-LAN server, use the format: `elux:`*<IP address>*

There are two optional protocol settings:

- **Use UDP protocol instead of RAW ethernet for the WOL packet** By default, Scout Enterprise sends an Ethernet RAW MAC broadcast packet to the net. Routers do not route a RAW broadcast packet to other subnets. When this option is activated, the server will send the packet as UDP on port 20000.

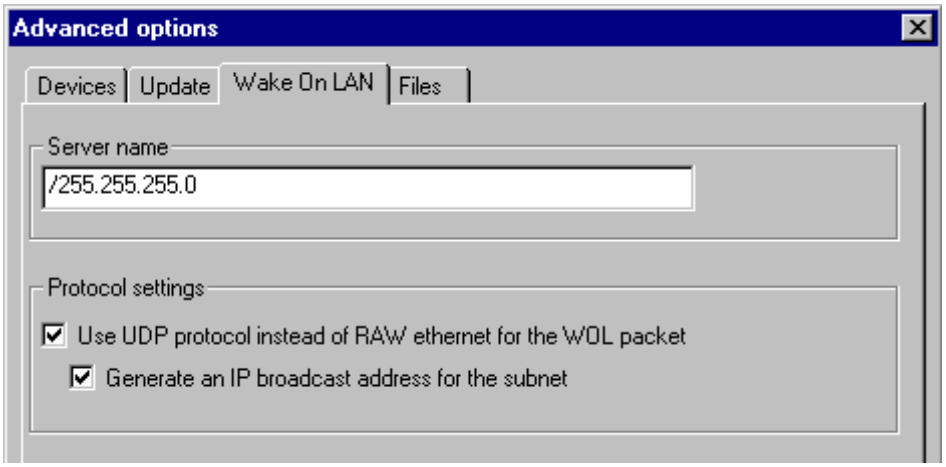


Figure 113: Advanced Options → WakeOnLan

- **Generate an IP broadcast address for the subnet** When activated, sends the packet to the subnet the device belongs to (dedicated subnet). Default is deactivated.
  When this option is activated, you must enter the subnet address in the **Server name** field in the format /255.255.255.0. Do not forget the leading '/'.

  For example, to wake up a device with the IP address 192.168.10.44, enter /255.255.255.0 in the **Server name** field. The broadcast address which is entered in the packet is 192.168.10.255

6.8.4.1 Individual Settings

You can set an individualized Wake-on-LAN address using the **Properties** function of a Location category, Group category or individual device. This wake-on-LAN server IP address will be used only for that specific organisation unit or individual device.

- To enter an eLux device as a wake-on-LAN server, use the format: `elux:`*<IP address>*

In addition, if you selected the option Generate an IP broadcast address for the subnet, you can also enter a subnet for an organisation unit or individual device here.

6.8.5 File Transfer

This function allows you to transfer files from the Scout Enterprise Server to one or more Thin Clients. It eases the workload greatly. For example, you can create a configuration file for the SAPGUI client and transfer it to all terminals to avoid local user configuration. In addition, you can transfer multiple configuration files at the same time.

Transferring files to devices involves the following:

1. Installing the client software on a device
2. Configuring the client software on a device
3. Copying the configuration file to the Scout Enterprise Server installation directory
4. Configuring File Transfer settings
5. Restarting the devices

⇨ Install the client software on a device

The client firmware must be installed on the Thin Client.

1. Start ELIAS and add the required packages to the device's IDF. The required packages are listed in the section describing the software.

2. Save the IDF and exit ELIAS.
3. Install the software on the Thin Client by performing a firmware update.

⇨ Configure the client software on a device

Configure the client software manually and save your settings. Configuration information is listed in the section describing the software or in the product documentation.

⇨ Copy the configuration file to the Scout Enterprise Server installation directory

The path of the configuration file on the Thin Client is listed in the section describing the software.

Transfer the configuration file to the Scout Enterprise Server installation directory or a subdirectory. To do this:

- Save the file to a local drive (portable medium such as a USB stick or floppy) or network drive (SMB or NFS). An SMB drive must be defined in advance. There are several ways to do this:
  1. Many programs have a "Save as" command that allows you to save the configuration file to a local drive or network drive.
  2. In a local shell you can run UNIX commands, for example, the UNIX copy" command. Format: `cp` <*source file*> <*target file*>.

     Example: Saving the SAPGUI configuration file to a USB stick:

     `cp /setup/sapgui/platin.ini /misc/usb0/platin.ini`

     Example: Saving the SAPGUI configuration file to a network drive:

     `cp /setup/sapgui/platin.ini /smb/`<*drive*>`/platin.ini`

     where *drive* is a previously-defined SMB drive.
  3. The File Manager allows you to copy and paste files using an Explorer-like graphical interface. For information on File Manager, see 4.8.7 File Manager.

- Transfer the file using FTP. To do this:
  1. In the **Diagnostics** tab select **User file** and enter the full file name in the field. Select the **Transfer files to** check box. Enter the URL of the destination directory in the format `ftp://`<*FTP server*>`/`<*path*> or `ftp://`<*username*>`:`<*password*>`@`<*FTP server*>`/`<*path*>. Click **Execute**.

     Example: Transferring the ICA configuration file via FTP:

     User file `/setup/ica/wfclient.ini`

     Transfer files to `ftp://elux:elux@192.160.10.71/icafiles`

  2. In a local shell you can run UNIX commands, for example, the FTP command. For information on a local shell, see **Fehler! Verweisquelle konnte nicht gefunden werden.** REF _Ref95628277 \h **Fehler! Verweisquelle konnte nicht gefunden werden.**.

⇨ Configure File Transfer settings

Here you enter the files to transfer and the destination directory. The source file must be in the Scout NG Server installation directory or a subdirectory. You must know the source file name and path relative to the Scout Enterprise installation directory.

The file name on the Thin Client can differ from the source file name, allowing for flexibility.

You can transfer files to all devices (global file list) or to an individual device or organisation unit, Group or Location (individualized file list). An individualized file list supercedes the global file list for that element (individual device, organisation unit).

To set the File Transfer settings:

1. In Scout Enterprise, open the dialog box for setting File Transfer settings.

To transfer files to all devices currently being managed (global file list):

From the **Options** menu select **Advanced options** dialog box is displayed. Click the **Advanced file entries** tab.

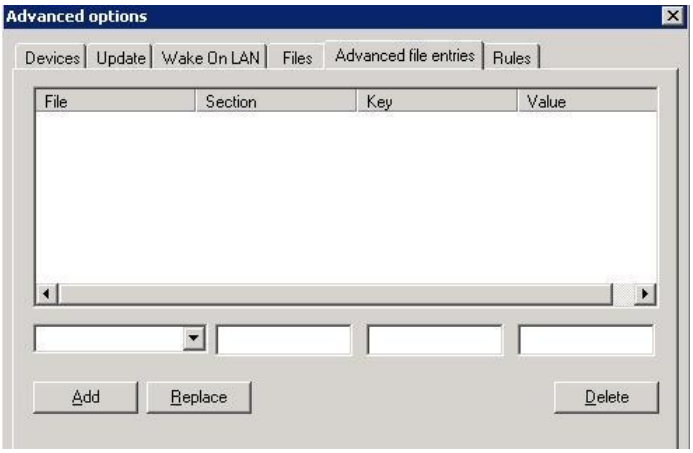


Figure 114:Global file list

To transfer files to an individual device or organisation unit (individualized file list):

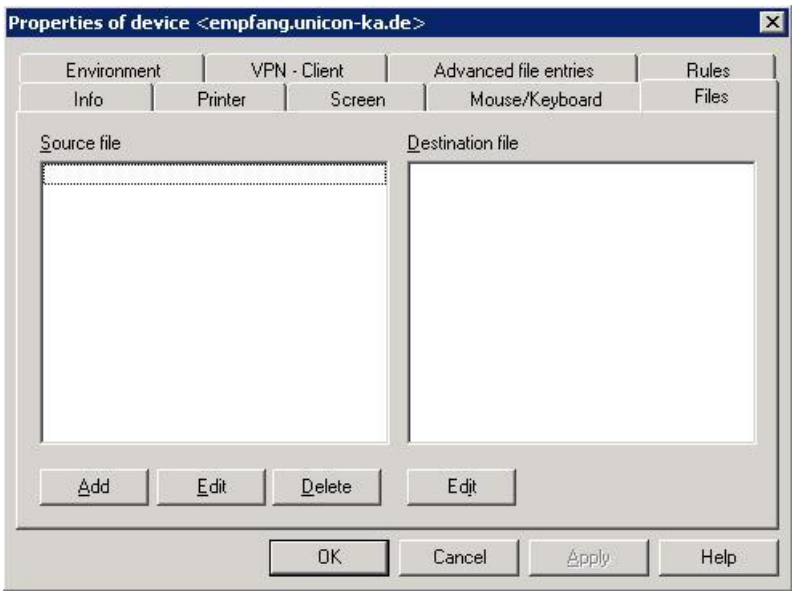


Figure 115: Individualized file list

Rightclick an element (individual device or organisation unit). In the context menu, select **Properties**. The **Properties** dialog box is displayed. Click the **Files** tab.

2. In the Source file" area, click **Add**.

   If the file is in the Scout Enterprise installation directory, enter the file name. If the file is in a subdirectory, enter the subdirectory and the file name.

3. Click **OK**.

   If the file is one of the commonly-used files, the correct path extension will automatically be added. Otherwise in the "Destination file" area, click **Edit**. Enter the path as it should be on the Thin Client. To rename the file, enter a different destination file name. The file will be renamed upon transfer.

⇨ **Restart the devices**

File transfer takes place when the Thin Client boots.

To restart devices and insure files are transferred:

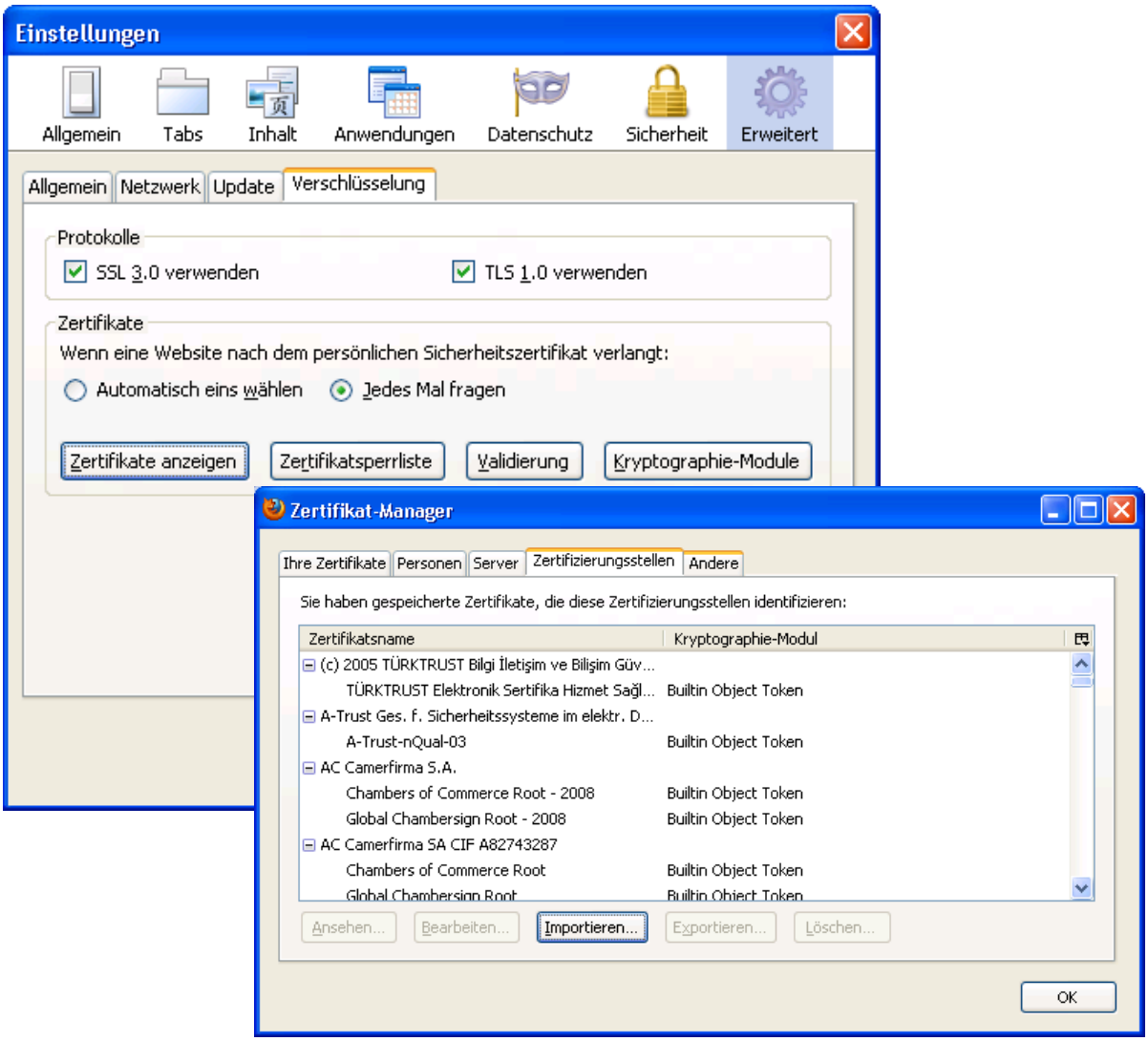
1. Rightclick the target devices. In the context menu select **Initiate refresh**.
2. Restart the devices from the Scheduler. To access the Scheduler:

When transferring files to all devices currently being managed (global file list): In the View menu select **Schedule**. Click **New**.

When transferring files to an individual device or an organisation unit (individualized file list): Rightclick the element and select **Restart device**.

6.8.5.1 Speichern von Zertifikaten in elux RL via Firefox 3

Schritt 1
Aufnahme des Rootzertifikats einer Zertifizierungsstelle im Firefox des eLux RL Clients in die Liste der Zertifizierungsstellen:
a) Bietet die Zertifizierungsstelle eine Website an,- z.B. Microsoft-Zertifizierungsstellen im IIS unter dem Pfad /certsrv - , kann das Zertifikat direkt in den Browser geladen werden.
b) Falls das Zertifikat als Datei vorliegt, kann es via den Zertifikat-Manager im Firefox 3 importiert werden. Wählen Sie dazu im Menüpunkt ***Extras*** > Einstellungen > Erweitert > Tab: Verschlüsselung > Zertifikate anzeigen > Tab: Zertifizierungsstelen > Importieren das gewünschte Zertifikat aus und beenden danach den Firefox.



Schritt 2
Zur Verteilung der importierten Zertifikate auf andere Clients werden die folgenden 3 Dateien auf den Scout übertragen:

/setup/firefox/cert8.db
/setup/firefox/key3.db
/setup/firefox/secmod.db

Dazu gibt es 2 Möglichkeiten:

a) via Scout mit rechtem Mausklick auf das Gerät → **Gerätediagnose** > **Dateien anfordern** öffnet sich der Dialog **Diagnosedateien bearbeiten**. Mit Klick auf ***Neu*** erstellen Sie eine neue Vorlage und tragen in diese die o.g. Dateien ein.
oder
b) Kopieren Sie die o.g. Dateien auf einen USB-Stick und von dort auf einen Ordner im Scout Serververzeichnis.

Schritt 3
Wählen Sie aus dem Menü **Optionen** > **Erweiterte Optionen** > Tab **Dateien** fügen Sie diese Dateien hinzu und benennen Quelle und Ziel.

6.8.5.2 Vom Benutzer bestätigte Zertifikat-Ausnahmen speichern und verteilen

Bestätigen Sie zunächst alle Ausnahmen auf einem Client, schließen Sie den Firefox und übertragen Sie die Datei

/tmp/elux/.mozilla/firefox/elux.default/cert_override.txt

in den Scout wie oben beschrieben oder kopieren Sie sie auf einen USB-Stick.
Verteilen Sie anschließend die Datei **cert_override.txt** via Scout nach

/setup/elux/.firefox/cer_override.txt

auf weitere Clients.

6.8.6 Advanced File Entries

In the **Options** menu click **Advanced options**. The **Advanced options** dialog box appears. Click the **Advanced file entries** tab. Here you can directly edit configuration files.

This feature allows you to set parameters that cannot be set using the graphical user interface (for example, special parameters for the Citrix ICA client configuration files or the Cisco VPN configuration file).

To use this function, the configuration file must be initiation (INI) file format. There are various implementations of the INI format. The INI file editor in Scout NG requires the following:

- An INI file is divided into sections, each containing zero or more keywords. The keyword contains zero or more values.
- A section heading is enclosed in square brackets.
- A keyword and its value are on the same line, separated by an equal sign (=”). A keyword can have more than one value.
- If a section name is used more than once in the same file, or if the a keyword is used more than once in the same section, then the last occurrence prevails.

Example format:

```
[Section]
keyword1=value
;comment
keyword2=value1, value2, value3 ;comment
```

⇨ To set values for individual keywords

- **File**: Enter the complete path of the file you wish to edit or select it from the drop-down list:

  Citrix ICA: /setup/ica/wfclient.ini and /setup/ica/appsrv.ini

  Cisco VPN client: /setup/ciscovpn/sample.pcf
- **Section**: Enter the section heading without brackets.
- **Key**: Enter the keyword.
- **Value**: Enter the value you wish to assign this keyword. You may enter spaces, a separating character and multiple parameters, as shown in the example above. For example, for keyword2" you would enter: `value1, value2, value3 ;comment`

Click **Add**.

⇨ To delete individual keywords

Enter the **File**, **Section** and the **Key** you want to delete. Leave **Value** blank. This keyword will be deleted from the file.

⇨ To delete entire sections

Enter the **File** and the **Section** you want to delete. Leave **Key** and **Value** blank. This section will be deleted from the file.

In the **Advanced options** dialog box you set global settings for all Thin Clients. To set settings for a Location category, Group category or individual device, click with the right mouse button on the icon in tree view, select **Properties** from the context menu and click the **Advanced file entries** tab.

Settings from a lower level overwrite higher-level settings.

Advanced File Entries

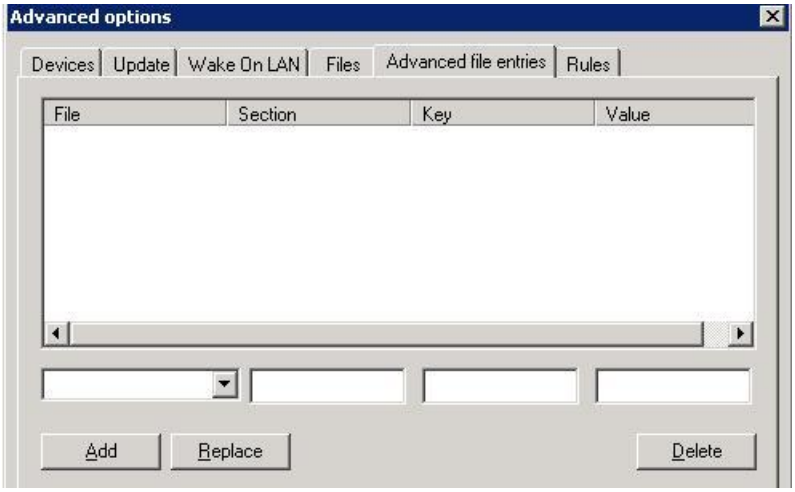


Figure 116: Advanced Options > Advanced file entries

This dialog allows to edit configuration files and transfer them to the clients.

The entries must have the following format:

File : /setup/terminal.ini
Section : Global
Key : ActionIfNoAppRunning
Value : 0|1|2|4|8|16

The values mean:
0 = no action, 1 = restart, 2 = exit, 4 = logoff,
8 = lock, 16 = close VPN tunnel.

File : /setup/terminal.ini
Section : Global
Key : ActionIfNoAppRunningDelay
Value : #sec

If #sec is greater 0, a message will be displayed. The user can cancel the action within the number of #sec seconds or confirm. If the message is neither confirmed nor cancelled, the action will be performed after the set value.

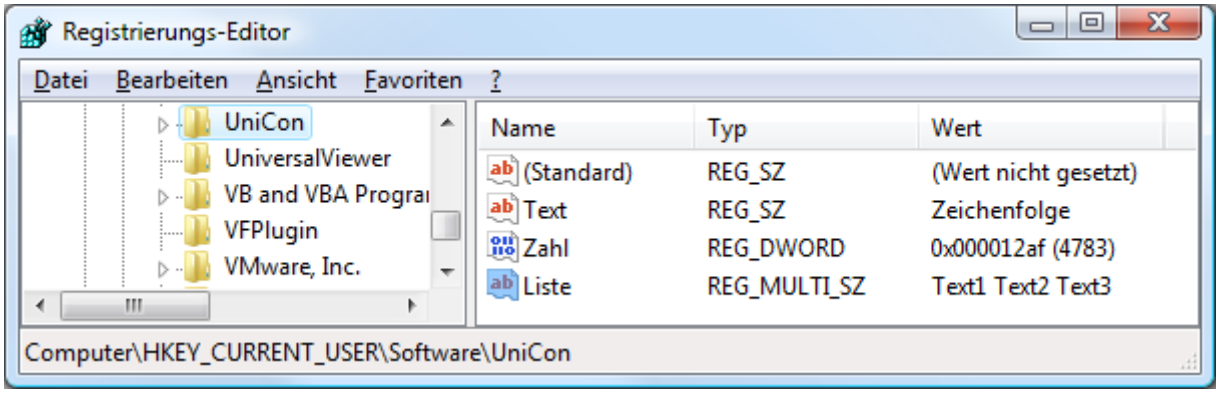
If #sec is 0, the action is performed immediately.

6.8.7 Windows Registry Entries

Even entries into the Registry for Windows-based Thin Clients can be set in the dialog "Advanced Options" > Advanced File Entries.

- For ***File*** enter the text ***#CEREGISTRY*** for Windows CE clients, for Windows XPe/WES7 clients enter ***#XPEREGISTRY***.
- For ***Section*** enter the key name.
- For ***Key*** enter the name of the key.
- For ***Value*** enter the value of the entry. Without futher input the value is entered into the registry as a string of characters. To enter a DWORD value, please enter the text ***DWORD:*** to precede the hexadecimal value. To enter a multi-part character string, please enter the text ***MULTI_SZ:*** to precede the list. The first character of the list will be used as a delimiter.

Example:
In a Windows XPe/WES7 based client the following Registry entries are to be set:



At the console these settings are required:

File	Section	Entry	Value
#XPEREGISTRY	HKEY_CURRENT_USER\Software\Unicon	Text	Zeichenfolge
#XPEREGISTRY	HKEY_CURRENT_USER\Software\Unicon	Zahl	DWORD:000012af
#XPEREGISTRY	HKEY_CURRENT_USER\Software\Unicon	Liste	MULTI_SZ:@Text1@Text2@Text3

6.8.8 Rules

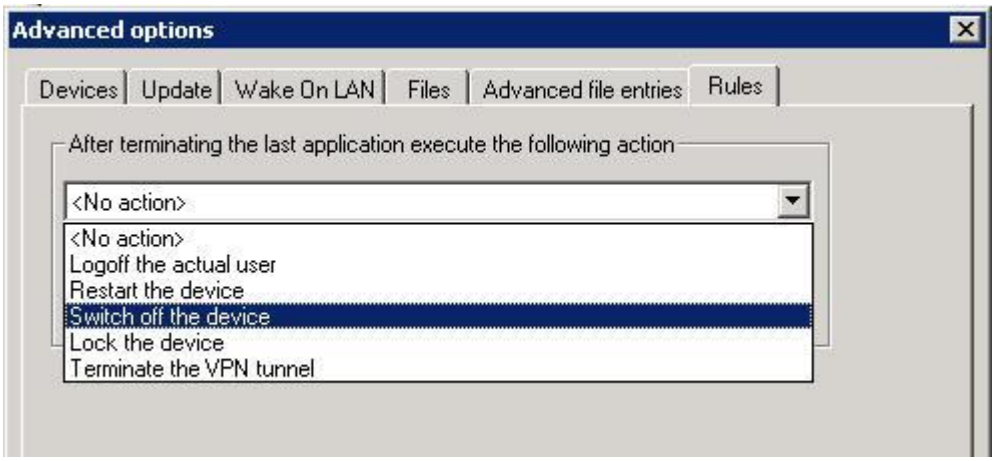


Figure 117: Advanced Options > Rules

This option provides a small selection of actions which are to be performed after the last application has been closed. Default is: No action.

6.8.9 Partitions

It is possible to change the partitioning at the client.

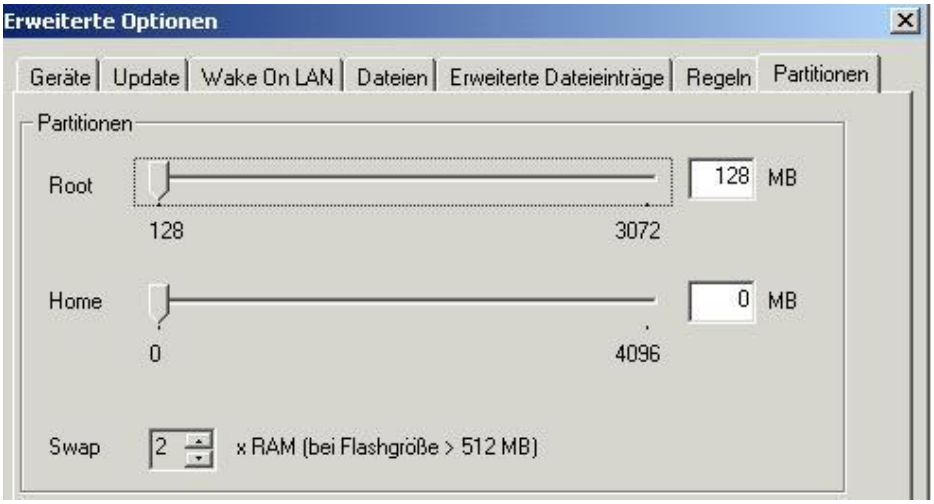


Figure 118: Advanced Options > Partitions

Requirements:

- Thin Client with eLux NG (eLux *RL* is not supported)
- Harddisk (e.g. eLux NG for PC)

This option allows to create a writable partition on the harddisk. For the standard Thin Client operation this functionality is not necessary. Please be aware that it requires expert knowledgle of the local Linux operating system.

Rightclick a device and select **Update** to execute the command **Format**. After formatting the defined image is automatically installed.

7 Organisation Structure, Screen Elements, Main Window, Passwords

By default, the left-hand side of the Scout Enterprise main screen displays a tree view of the managed Thin Clients (devices"). The first time you log on, the only elements visible are the default Applications and the default organization unit Lost&Found.

Click on the plus to expand Lost&Found.The Lost&Found" unit appears. Expanding this unit displays the Application and Organisation Unit.

Applications and organisation units can again be added to each organisation unit. Devices can be assigned to each organisation unit, too. (In former Scout versions devices could be assigned to groups only.) Later on your screen might look like this:

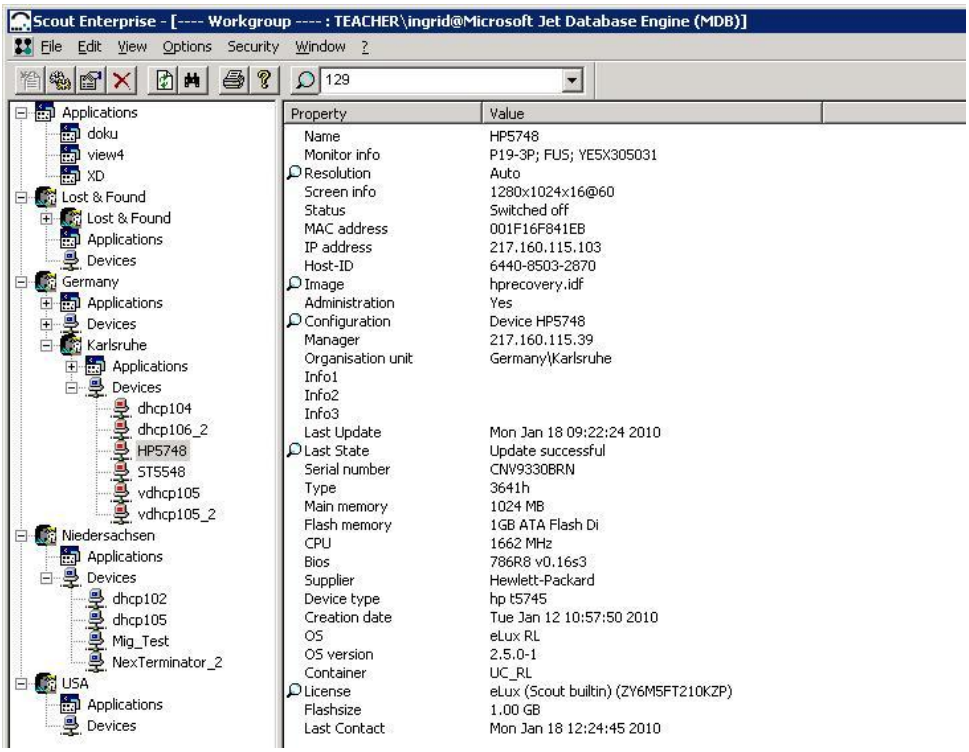


Figure 119: Scout Enterprise Main Window

The left-hand side is the tree view showing the hierarchical structure. If you select an element, its properties are displayed in the right-hand window. Hence, the right-hand window is called the Properties window."

Some essentials about working with the main window (tree view):

- Scout Enterprise organizes the devices hierarchically. Individual devices are grouped into Organisation Units

   Organisation Units, which each contains

   Applications

   Devices

  and as an option further organisation units.

  Devices are represented by icons. The different colors represent the state of the remote device:

   Green: Device is turned on and ready

   Red: Device is turned off or unavailable

   Yellow: Desktop is being initialized

   White: Update is running

   Grey: Device cannot be managed due to insufficient number of licenses

  - The  Applications category lists the individual applications defined for a group.
  - With the drag-and-drop function you can move individual devices and application definitions from one organisation unit to another. Devices are automatically assigned the properties of the new organisation unit.
  - CTRL + drag-and-drop copies applications from one ou to another.
  - Each organisation unit can be configured, that is, properties and applications can be assigned. When you add a new device to an organisation unit (either a new entry or an existing one via drag-and-drop), it automatically receives the configuration of this organisation unit.
  - You can disable the tree view to display the devices in a list. From the **View** menu, choose **Devices**. List view displays the devices without icons. Click the column header to sort. Click on the same column header again to sort in reverse order.
  - Use **Edit** menu > **Find** or CTRL-F to find text in the tree view. Click to select Find in Properties" to find text in the properties window.
  - In tree view, click **View** menu > **Adjust** to select which properties are to be displayed in the Properties Window. In list view, rightclick the Properties window to to select which columns are to be displayed.

7.1 Passwords

We differentiate between two passwords:

- Local device administrator password of the user name LocalLogin
- Scout Enterprise administrator password to log on to the Scout Enterprise management tool.

7.1.1 Local Device Administrator Password (Thin Client Password)

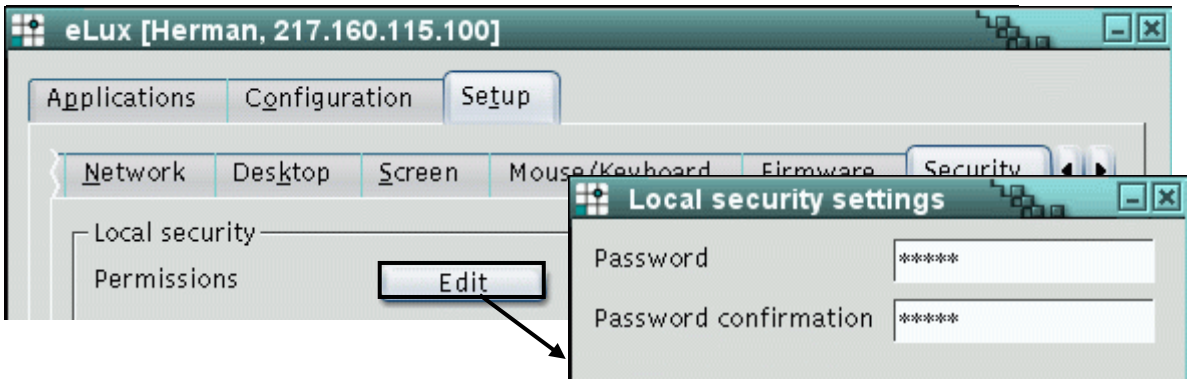


Figure 120: Setting device password on Thin Client running eLux

The Thin Client password is the password on the local device. It can be changed by going to **Setup** > **Security** on the Thin Client, clicking on **Edit** under "Local security settings" and changing the password. By default, the Thin Client password is set to `elux` (all lowercase).

The device password is required to verify access rights. For example, Scout Enterprise requires you to know the Thin Client password when you change the Thin Client's configuration or perform some other management action on a Thin Client (client discovery, update, etc.) to verify that you are allowed to configure this device. Thus, you must know the Thin Client password in advance to enter or update devices.

Figure 121: Setting device password using Scout Enterprise

Once you have entered devices in Scout Enterprise, your access rights have been verified. You can then change the Thin Clients' password using Scout Enterprise.

1. To change the Thin Client password in Scout Enterprise, go to **Options** > **Base Configuration** > Local security settings > **Edit**.
2. Enter the new password in the **Password** box. Repeat in **Password Confirmation**.

When you click **OK**, all active devices (currently turned on) are automatically assigned the new Thin Client password. Devices that are currently turned off are assigned the new password at next system start. **Note**: This affects only devices that have already been entered in the Scout Enterprise software! It does not verify your access rights.

Note: Changing the Thin Client password from the default `elux` prevents unauthorized device configuration by the local user.

7.1.2 Scout Enterprise Console Password

The option **Change server password** in the Options menu is only active if the option **Activate Administrator Policies** in the Security menu is disabled**.** We recommend to enable Administrator Policies (see chapter 10 Multiple Administrator Policy). Then the server password is identical to the password of your Windows account.

The server password is the password for the Scout console. By default it is also `elux` (all lowercase). To prevent unauthorized access it is recommended to change it.

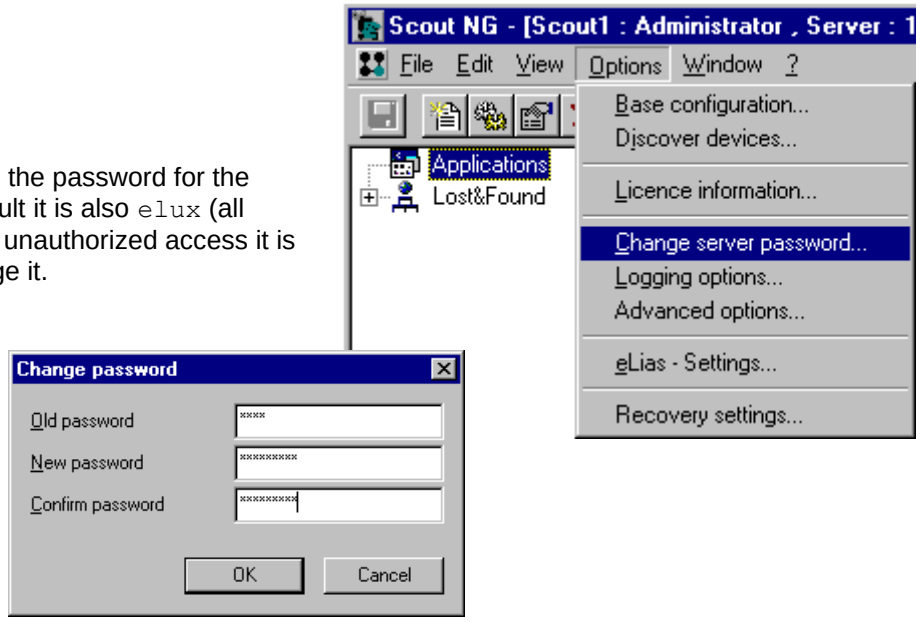


Figure 122: Dialog Change Password

To change the Scout Enterprise password, log on as Administrator and go to **Options** > **Change server password**. Enter the new password in the **Change password** dialog box.

Attention The Scout Enterprise console password can only be changed in **Options** > **Change server password.** Changing the Scout Enterprise console password does not affect the device administrator password described in 7.1.1.

8 Entering Devices

In order to manage Thin Clients, you have to enter their MAC addresses into Scout Enterprise. For ease of management, there are different ways to enter this information. This chapter contains the information you need to enter Thin Clients with eLux® NG, eLux® *RL* or Windows® CE, XPe/WES7 or into the Scout Enterprise software.

8.1 Automatic Entry Using DNS Entry

By default, the first time a Thin Client with factory-delivered settings boots, it automatically searches for the Scout Enterprise server. For this functionality to work, you must configure your domain name server in advance.

1. Place the Thin Client in the default state (either upon delivery or by performing a factory reset). See section
2. On the DNS server, set the host name "ScoutSrv" (capitalization independent) to the IP address of your Scout Enterprise server.
3. Confirm that the Thin Client is connected to the network and that a BootP/DHCP server is running.
4. Turn the Thin Client on.

In the factory delivered default state, the first time a Thin Client boots, it makes a DNS request for the host name ScoutSrv. If this host name has been set to the IP address of your Scout Enterprise server, the Thin Client will automatically contact the Scout Enterprise server and enter itself in the default group (see section 8.6). It will receive this organisations unit's configuration and reboot with the new settings.

To deactivate this functionality, do not configure the host name "ScoutSrv" on your DNS server.

If you enable the hostname ScoutSrv, due to redundancy you should avoid setting Scout Enterprise server settings using a DHCP server (see section 8.2 Automatic Entry Using DHCP or BOOTP Request).

If no DNS server entry for ScoutSrv is found, a First Configuration Wizard automatically runs on the Thin Client to help the user through the initial configuration. See the *eLux Administrator's Guide* for more details.

8.1.1 Modifying First Configuration Wizard Settings

The first time the Thin Client boots, it looks for the hostname ScoutSrv. One of the following two scenarios occurs:

1. If ScoutSrv has been set on the DNS server, the device is automatically entered in the management software. There is no effort on the part of the user.
2. If no manager is located, the device automatically runs the First Configuration Wizard, which helps the user through the initial configuration. The user has the option of configuring the device manually or entering a Scout Enterprise Manager address (or name).

However, it is possible to have both ScoutSrv and the First Configuration Wizard: Start the Scout Enterprise Console. In the **Options** menu click **Advanced options**. The **Advanced options** dialog box appears.

1. In the New devicesarea click to activate the **SmartSrv active** check box. Click **OK**.
2. In addition, set the hostname ScoutSrv on the DNS server.

Now the first time a Thin Client with default settings boots, the First Configuration Wizard runs with the Scout Enterprise Manager information preset to ScoutSrv.

8.2 Automatic Entry Using DHCP or BOOTP Request

Another way to automatically enter the device in the Scout Enterprise Server is per DHCP or BootP server.

8.2.1 DHCP

You can configure the DHCP server to transfer the Scout Enterprise Server IP address (or name) and a group ID to the Thin Client when it boots. This functionality works for Thin Clients in the default state (either upon delivery or by performing a factory reset) the very first time they are booted. It also works for subsequent boots, if you set the Thin Client network settings to DHCP (Setup > **Network**).

The DHCP server must be configured in advance. You can choose between standard options or defining a user-defined vendor class. Warning: Choose one of the methods below – configuring both at the same time can result in errors.

The following examples use the DHCP Manager from Windows 2000. Please note that your user interface may differ depending on your software.

Method 1: Standard Options

Requirements

- DHCP server from Windows NT 4.0 with service pack 6, Windows 2000 or Windows 2003 Server

This method is supported by most DHCP servers, including older versions. It uses the standard options 222 and 223. If options 222 and 223 are unavailable, you must use method two.

1. Open the DHCP Manager (**Start** > **Programs** > **Administration (General)** > **DHCP Manager**).

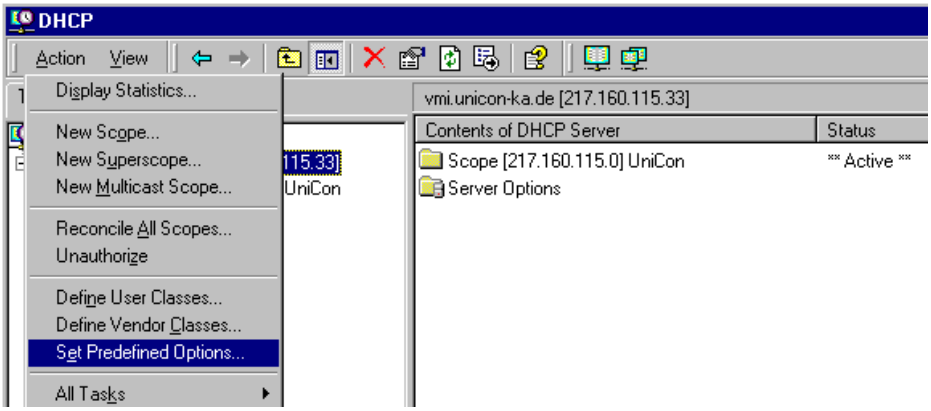


Figure 123: Setting predefined options

2. Click to select your DHCP server. In the **Action** menu select **Set Predefined Options**.

3. Select **DHCP** Standard **options** from the Option classdrop-down menu. Click **Add**. The **Option Type** dialog box appears.

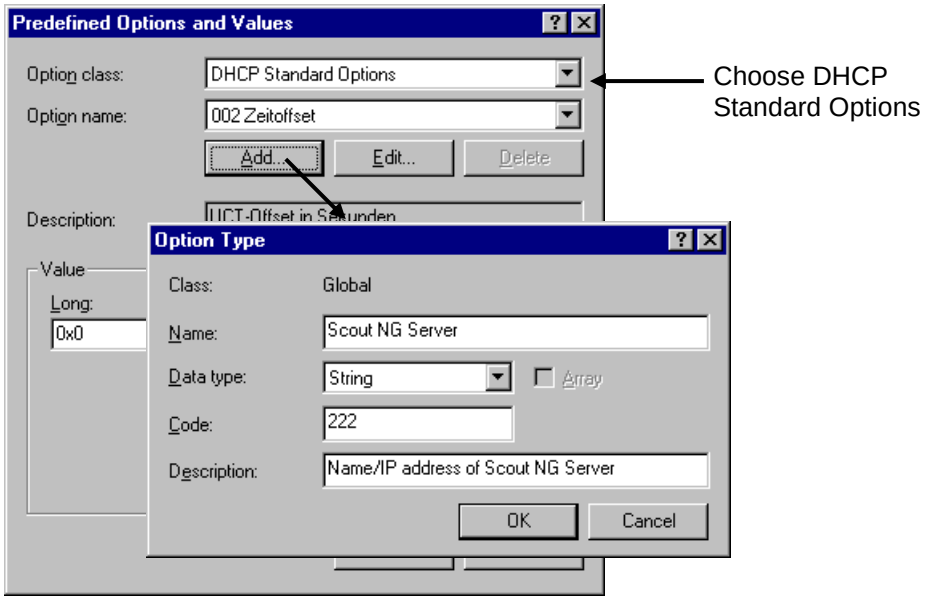


Figure 124: DHCP Default Options

Name	Enter Scout Enterprise Server”
Data type	Select String”
Code	Enter 222
Description	Enter name or IP address of the Scout Enterprise Server.

Confirm with click on **OK**. Click **Add** to enter another one (optional):

Name	Enter: Scout Enterprise Group ID”
Data type	Select Long”
Code	Enter 223
Description	Enter the Device group ID on the Scout Enterprise Server”

Note: **Array** should not be selected.

Click **OK** to confirm.

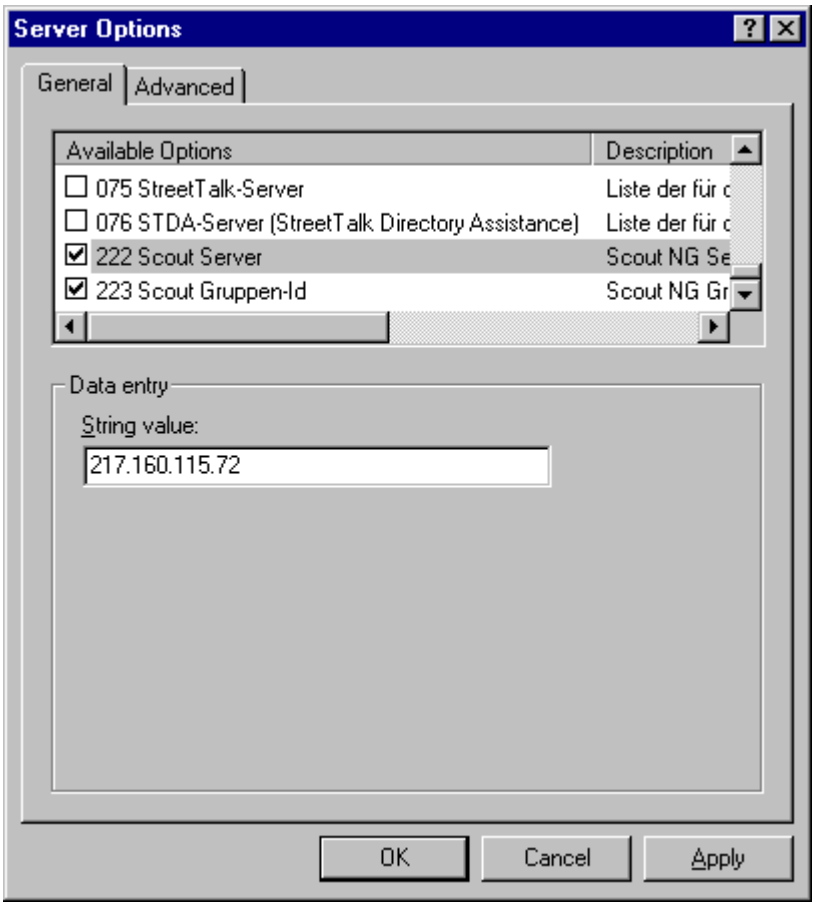


Figure 125: DHCP Manager – Server Options

4. In the DHCP manager, click to select either the server options, scope options or reservations. In the **Action** menu select **Configure**. In the **Options** dialog box go to the **General** tab. (Alternatively: **Advanced** tab > select **DHCP Standard options** from the **Vendor class** drop-down list.) Configure the two options:

222	Enter the IP address/name of the Scout Enterprise server
223	Enter a Scout Enterprise group ID number for the device
224 or 004	Enter a list of Scout servers

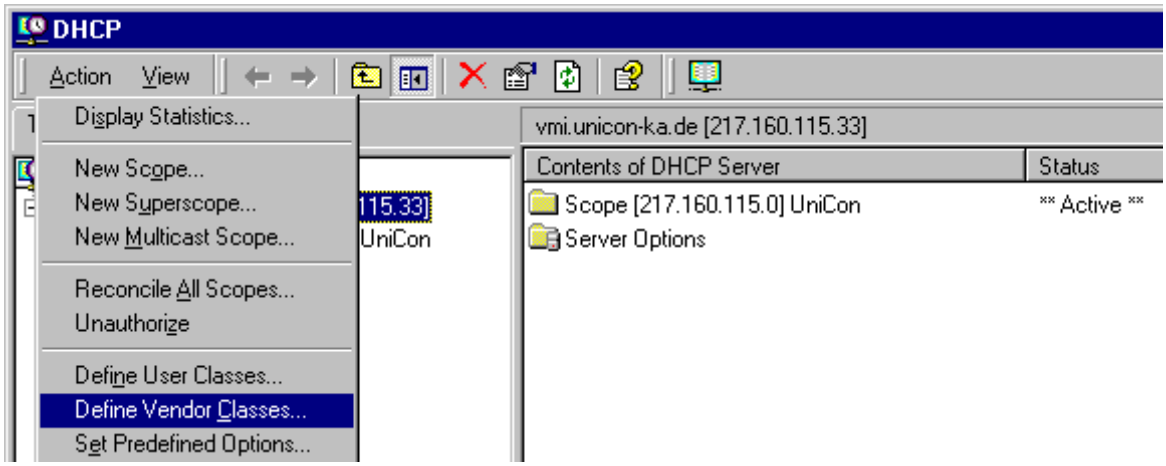
Method 2: User-Defined Vendor Class

Requirements

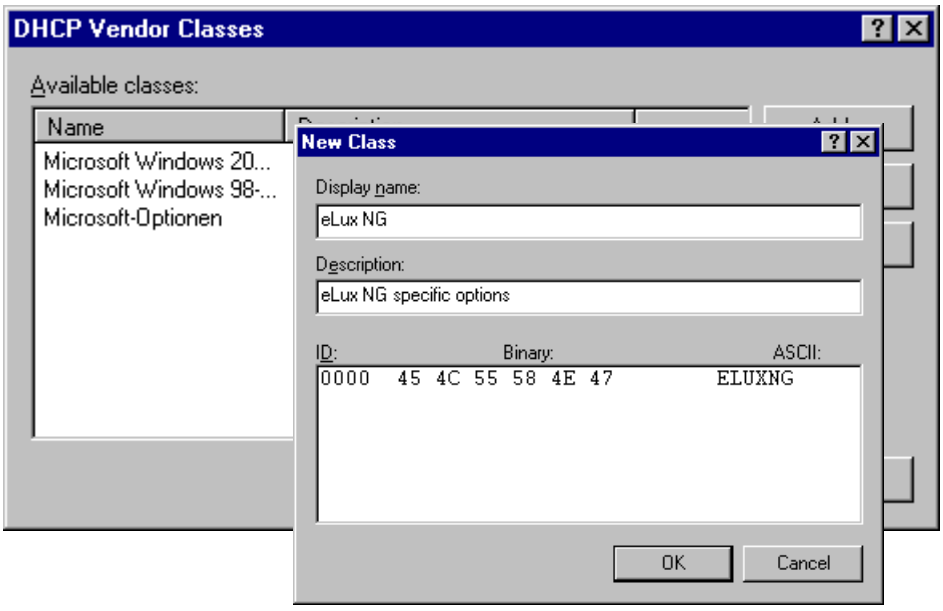
- DHCP Manager from Windows 2000 server or Windows 2003 server
- Alternative: DHCP server from another manufacturer that is compliant with RFC 2132

In this method you define a new vendor class, set two new options, and enter the values for these options.

1. Open the DHCP Manager (**Start** > **Programs** > **Administration (General)** > **DHCP Manager**).



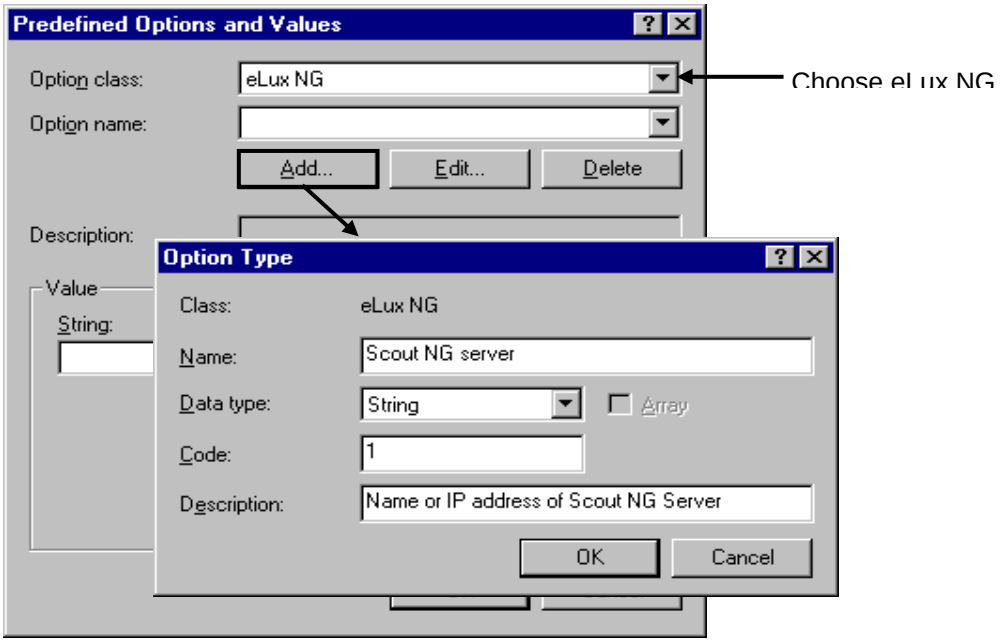
2. Click to select your DHCP server. In the **Action** menu select **Define Vendor Classes**.
3. Click **Add**. The **New Class** dialog box appears.



Display name	"eLux NG"
Description	"eLux NG specific options"
ID	In the ASCIIcolumn type ELUXNG" (all upper case). It will automatically be extended with the binary value (45 4C 55 F8 4E 47).

Click **OK**.

Figure 126: DHCP Default Options



4. In the **Action** menu select **Set Predefined Options** (see Figure 123). Select **eLux NG** from the Option classdrop-down menu. Click **Add**. The **Option Type** dialog box appears.

Name	Enter "Scout Server”
Data type	Select "Character string”
Code	Enter "1”. If 1 is not allowed, enter 222.
Description	Enter "Name/IP address of Scout Enterprise Server”

Click **OK** and **Add** to enter a second option (optional):

Name	Enter "Scout Enterprise group ID”
Data type	Select "Long”
Code	Enter "2”. If 2 is not allowed, enter 223.
Description	Enter the Device group ID on the Scout Enterprise Server”

Note: **Array** should not be selected.

Click **OK**.

5. In the DHCP manager, click to select either the server options, scope options or reservations. In the **Action** menu select **Configure Options**. In the **Options** dialog box go to the **Advanced** tab. Select **eLux NG** from the **Vendor class** drop-down list and enter values for the two options you just created:

   001 (or 222) Enter the IP address/name of the Scout Enterprise server

   002 (or 223) Enter a group ID number for the device

   Click **OK** for confirmation.

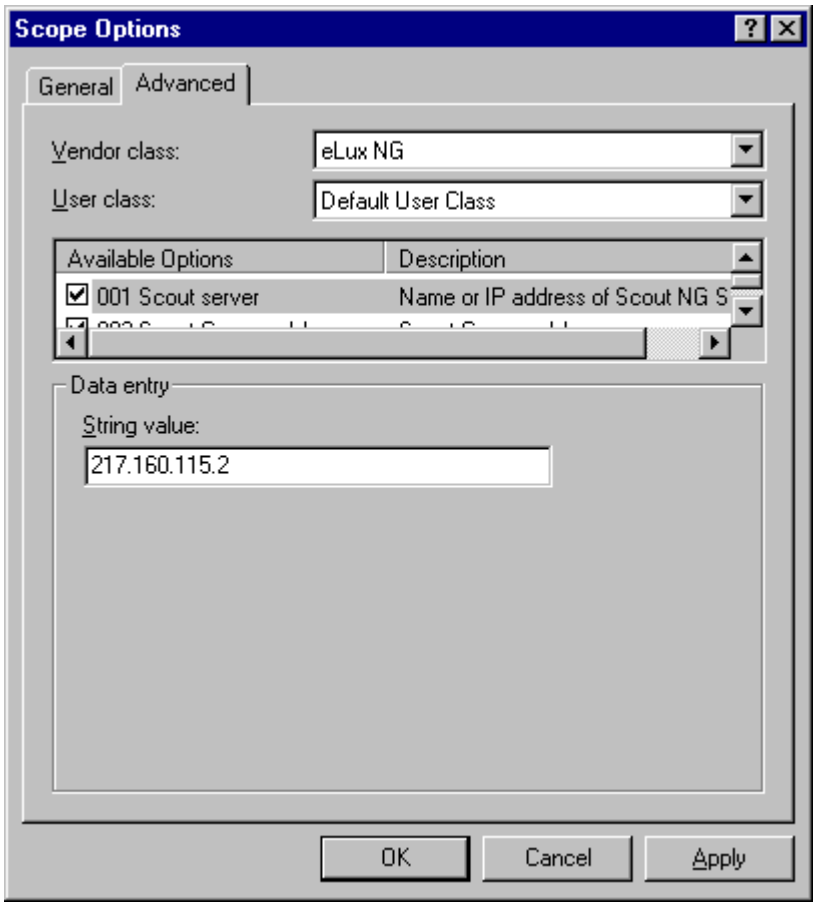


Figure 127: DHCP Manager – Scope Options

Not all DHCP servers support user-defined vendor classes. If this is the case for you, please use method one.

BOOTP

The same functionality is available for a BootP server.

Open the configuration file bootptab" using an editor for UNIX text files. The file is located in the installation directory of the BootP server (default: …/`Unicon/scoutng/bootpd`).

Add the following tags to each profile:

~ ms message size (fixed)

~ T222 IP address of the Scout Enterprise Server

~ T223 group ID of the device as eight-digit hexadecimal number (important!). For the standard group, enter 00000000.

Format:

```
:ms=1024:\
:T222:<Scout NG Server IP address>:\
:T223:<group ID>:\
```

Example: Assume IP address of Scout Enterprise Server=192.160.10.11, group ID=26:

```
:ms=1024:\
:T222=192.160.10.11:\
:T223=0000001A:
```

If the group ID is not in eight-digit hexadecimal format, it will not work

8.3 Client Discovery Function

Client discovery is an important function that highly simplifies the very first entry of devices. Information entry takes place in Scout Enterprise. **Requirements**:

- Devices must be on
- Devices must be running eLux NG
- Devices must have valid IP addresses
- The Thin Client password must be known

The Client Discovery function is based on TCP/IP, so it is possible to discover devices in different subnets.

From the **Options** menu, click **Discover Devices**. The **Discover Devices** dialog box appears.

Please enter the following:

Start address: First IP address in the range

Count: Number of IP addresses in the range

End address: Last IP address in the range

Password: Thin Client device password

Destination group: The desired destination group (=organsiation unit) may either be an already defined **ou** or the default group (ou) Lost&Found.

Click **OK** to begin the search.

The rest of this section provides important information on the discovery process.

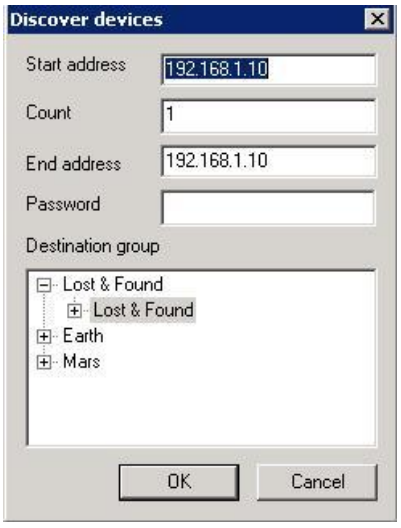


Figure 128: Options > Discover Devices

IP address range

You can search the enter network, a subnet, or for a single device by varying the start and end IP addresses. The search range is restricted to 255.

Destination Group

The destination group is the organisation unit you want to enter the discovered devices in. Devices in an organisation unit are automatically assigned that unit's configuration. Default is Lost&Found" with the base configuration.

Alternatively, you can create a new **organisation unit**. To do this, rightclick anywhere in the tree view window (but not on an element!). Click **Add organisation unit** in the context menu to create an ou on the first hierarchical leve. To create subordinate organisations units, rightclick an existing organisation unit → Add → Organisation unit.

Configuration

When devices are discovered, they automatically receive the configuration of the destination group.

Password

This refers to the device password currently saved locally on the Thin Client. (The default factory setting of the Thin Client password is `elux` [all lowercase]) The Thin Client password you enter in this dialog box must match the LocalLogin password currently saved on the Thin Client, otherwise Scout Enterprise will ignore the Thin Client.

When client discovery is a success, the Thin Client is placed in its destination group and is automatically assigned a new device password by Scout Enterprise (see chapter 0

Security). However, for client discovery to be successful, you must know which password is currently saved locally on the Thin Client.

Management address, local configuration and defined applications

Having succeeded in discovering the clients, the IP address of the Scout Enterprise Server is assigned to the device (on the Thin Client, the IP address of the managing Scout Enterprise Server can be viewed in **Settings** > **Security** > **Management**). From this point in time, the device is managed. Every time the Thin Client starts, it will contact the Scout Enterprise Server and apply any changes to its configuration or defined applications. If the user configures the Thin Client locally, these local configuration changes remain valid until the next system start (when the Thin Client contacts the Scout Enterprise Server). If no Scout Enterprise Server can be reached at system start, the Thin Client uses the previously saved configuration.

When you change the configuration in Scout Enterprise, these settings do not take effect until they are saved and the devices themselves are restarted. To restart a device remotely, in the tree view click the individual device or organisation unit using the right mouse button to access the context menu. Click **Restart Device**.

Previously Registered Devices

When you run a client discovery, previously registered Thin Clients will not change organisation units. Rather, their status will be updated.

Advanced settings

If you are having trouble with the discovery function, you may need to adjust discovery settings.

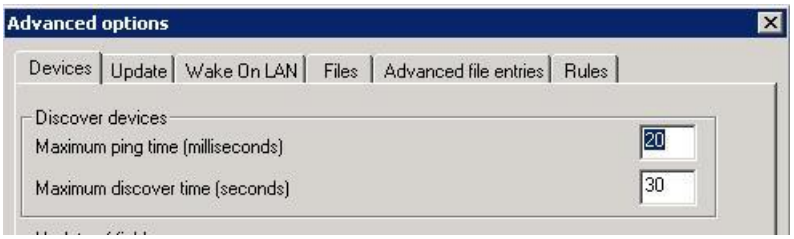


Figure 129: Client Discovery advanced settings

Go to the **Options** menu and select **Advanced Options**. The **Advanced Options** dialog box appears.

Here you can adjust the device reaction time (pingtime) and total time necessary to discover all devices (discover time"). Default settings are shown in the figure.

Troubleshooting Client Discovery

Configured devices cannot lose their applications during a discovery. Rather, once they are entered in Scout Enterprise, all locally defined applications are replaced with the applications defined for their destination group. To avoid downtime, define the destination group's applications in advance. A time-saving feature is **application upload**. For more information, see Application Upload" in chapter

8.4 Reverse Discovery

A reverse discovery is similar to a client discovery, except that management information entry takes place at the Thin Client

On the Thin Client running eLux NG, go to the **Setup** tab. In the **Security** tab enter the IP address of the managing Scout Enterprise Server into the field **Manager** of the manager settings area. Click on the button **Advanced** to fill the fields **Info 1**, **Info 2** and **Info 3** with information (optional), such as room number, phone extension of user name (e.g.: R 232, ext –10, ...).

Group ID refers to the ID of the organisation unit. Default is 0 (zero) (Lost&Found"). Once organisation units have been created, the group IDs are listed here automatically.

Click **Apply** and **Yes** in the confirmation box for restart. When the Thin Client restarts, it automatically contacts the Scout Enterprise Server. If the Group ID is zero (default), the device is entered in Lost&Found" in Scout Enterprise and is assigned the base configuration and base configuration Thin Client password. Otherwise the device is entered in the destination group and is assigned the destination group's settings. See next chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

The device's hostname is used as the device name when it is entered in Scout Enterprise.

Figure 130: Reverse Discovery – eLux NG settings

Discovery and Reverse Discovery are two ways to enter devices in Scout Enterprise. It is also possible to create a profile for the device in Scout Enterprise in advance. In this case, when the Discovery or Reverse Discovery takes place, the devices are automatically directed to the predefined profile. More details in chapter 6.4 Reserving Device Profiles..

8.5 Reserving Device Profiles

This section describes how to reserve profiles in Scout Enterprise. The devices are not entered until a discovery or reverse discovery is done.

You create a profile for a single device using the device's MAC address. Choose the Group in which you want to enter the devices (destination group). Click with the right mouse button on its Devices category. Click **Add** from the context menu. The **Information** dialog box appears.

1. Enter the 12-digit MAC address, without hyphens, and click **OK**.
2. If the MAC address is valid, a Setup dialog box appears. Click **OK**.
3. A profile is created for the device.

Manual entry does not enter a device in Scout Enterprise, it reserves a profile for the device. To enter the device in Scout Enterprise, either perform a Discovery or type the Scout Enterprise IP address in the Thin Client's "Management" field (Reverse discovery). The device will be directly entered in the reserved profile.

8.6 Specifying Destination Groups

If you have not configured your network for automatic entry of new Thin Clients in the Scout Enterprise Server (see sections 8.1 Automatic Entry Using DNS Entry and 8.2 Automatic Entry Using DHCP or BOOTP Request), the First Contact Wizard will appear the first time a Thin Client with default settings boots. The First Contact Wizard is a program that guides the local user through the initial minimum configuration when neither the DNS server nor the DHCP server has been configured for automatic entry. The user has the option of configuring the device manually or entering a Scout Enterprise Manager address (or name).

It is possible for the Scout Enterprise administrator to control the information that will be displayed in the First Contact Wizard if a Scout Enterprise Manager address (or name) is entered.

For example, you can preset the IP address/name of the Scout Enterprise Server by activating SmartSrv and ScoutSrv as described in section 8.1.1 Modifying First Configuration Wizard Settings.

In addition, you can control which Scout Enterprise organisation units are offered as available destinations.

The configuration on the Scout Enterprise Server is as follows: Click with the right mouse button on an organisation unit to open its context menu. Select **Properties** > **Management**. Select **Hidden** to blend out the ou in the First Contact Wizard. Select **Visible** to offer the ou as a destination. If you enter a password, the user must enter this password to select this organisation unit as a destination.

Figure 131: Properties dialog box > Management settings

The configuration on the device running eLux NG is as follows: In the First Configuration Wizard, the user enters the Scout Enterprise Server name/IP address. The Scout Enterprise Server is contacted and a list of available organisation units will be retrieved. In this example, the selected organisation unit is password protected.

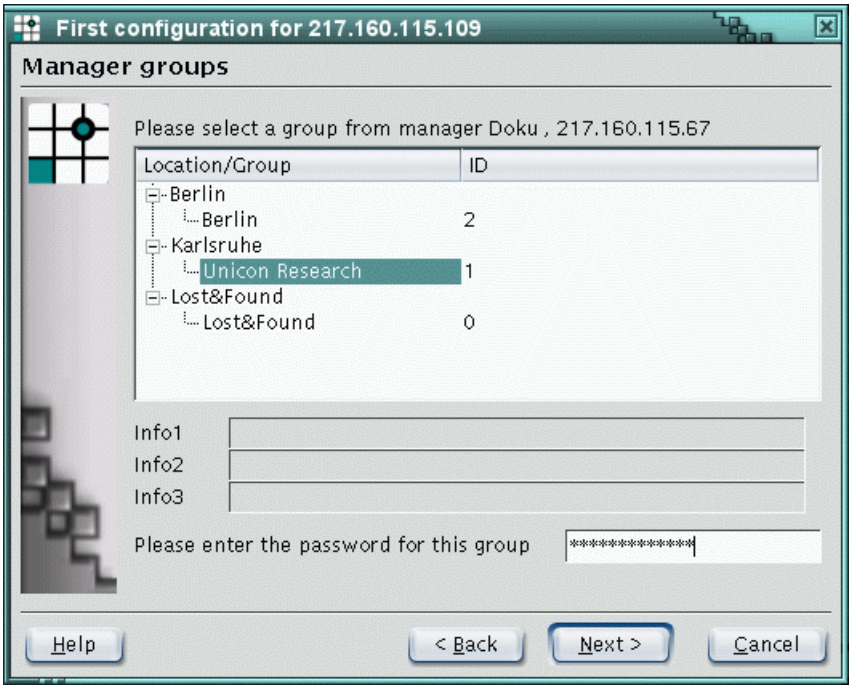


Figure 132: First Configuration Wizard

This organisation unit can only be selected if the password is known.

8.7 How Scout Enterprise Determines MAC Addresses

Scout Enterprise identifies devices by their MAC addresses. When the device is managed by Scout Enterprise, it determines the MAC address as follows:

Network hardware type	How MAC address is determined
ADSL	Read from the LAN card
Ethernet	
ISDN	Host ID (without hyphens) is used as the MAC address of the device
Modem	
WLAN	Read from the WLAN card

Figure 133: How Scout Enterprise determines client MAC address

8.8 Views

There are two possibilities to view devices registered in Scout NG: tree view and list view.

8.8.1 Tree View

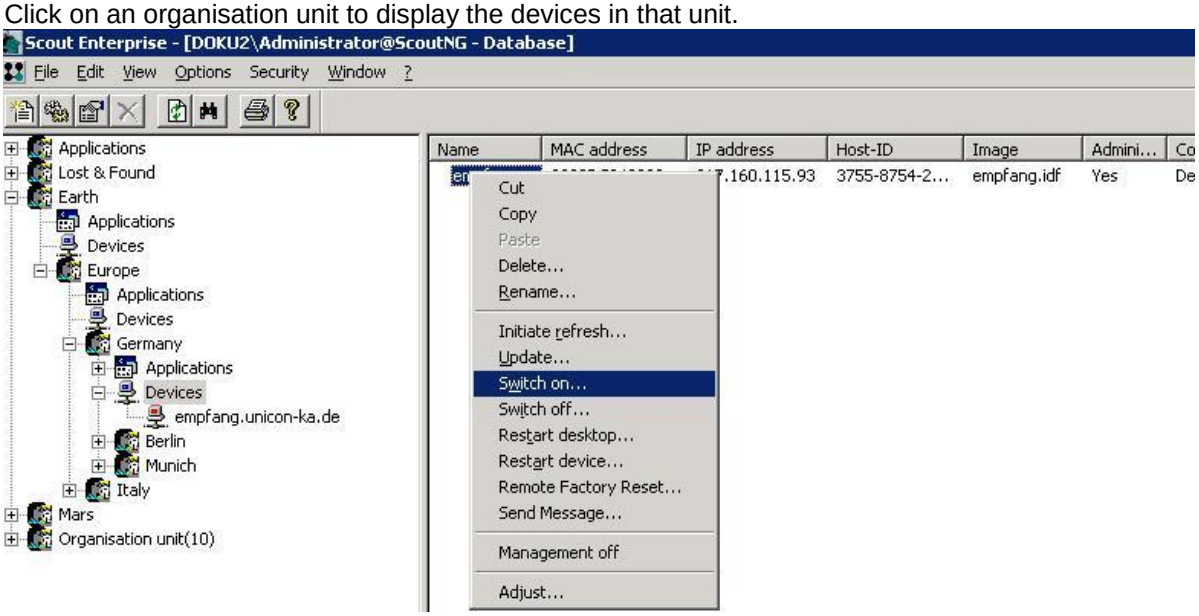
Tree view is the default. Devices are represented by icons and displayed in a branching hierarchy.

Properties Window

The screen is split in two. The right-hand side of the Scout Enterprise screen is called the "Properties window" and contains the properties of the currently marked element on the left-hand side.

Click on an individual device to display important information relating to the Thin Client. See 8.8.3 List of Properties for a description of device properties.

Click on an organisation unit to display the devices in that unit.



.

Figure 134: List of devices

In the Properties window, click with the right mouse button on a device. This opens the Properties window context menu for that device. Here you can cut, copy or remove the device, turn the device or desktop on/off, have a message appear on the user's screen, or update the device's firmware.

Hold CTRL down while clicking with the mouse to select multiple devices.

You can move devices to a different **ou** by selecting and pressing CTRL-X and CTRL-V to cut-and-paste.

After changing the configuration – such as moving a device or adding a new organisation unit – you can reload the configuration by clicking **Refresh** in the **View** menu or pressing F5.

To determine which properties appear in this view, open the context menu and select **Adjust**.

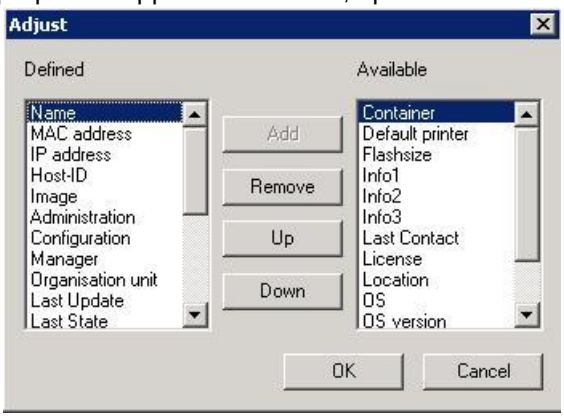


Figure 135: Adjust the list view

Select a property from the **Available** list and click **Add** to add it to the view. Select a property from the **Defined** list and click **Remove** to remove it from the view. **Up** and **Down** allow you to set the order in which the columns will be displayed. Or you can also use drag-and-drop directly in the Properties Window to rearrange the columns. These changes will apply to all device categories.

Magnifying Glass

Select an individual device. In the Properties Window, a double-click on a magnifying glass next to a property displays more information regarding that property.

- Resolution Opens the device setup.
- Image Opens the image definition file installed on this device using the companion program and image definition file editor ELIAS. Requirement: You must have previously entered the location of the container in Menu Options > ELIAS – Settings.
- Configuration Opens the configuration assigned to this device.
- Last State Opens the update info for this device.
- License Opens the information on license type, date of issue and the product id.

8.8.2 List View

You can also choose to display registered devices in a list. From the **View** menu, choose **Devices**. List view displays the devices without icons. Click the column header to sort in ascending order. Click on the same column header again to sort in reverse order. The following figure shows list view when seven devices have been entered in Scout Enterprise.

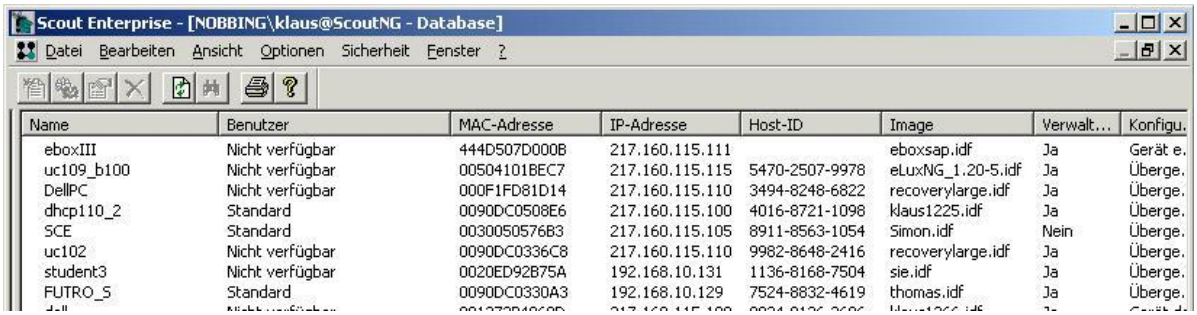


Figure 136: View > Devices

List view displays the same device properties listed in tree view as well as the device's organisation unit. This is especially useful when locating a Thin Client.

For a description of the different columns, see 8.8.3 List of Properties.

To perform a command on a device, click with the right mouse button to open the context menu. Hold CTRL or SHIFT down while clicking with the mouse or CTRL-A to select multiple devices. An alternatiave to the delete command is the key DEL.

If you apply ***Cut*** or ***Copy*** in the list view of applications or devices, a comma-separated list is created and stored in the Windows clipboard.

The fields are arranged in the same order as in the list view, e.g.:
Name,resolution,MAC address,IP address,ou xsDev1,1024x768,0090DC05CED8,192.168.10.1,Sales
xsDev2,1024x768,0090DC05CED2,192.168.10.2,Support

If you want to change the separator for the list, the entry CSVSeparator = <value> in the **Settings** section of the scout.ini file must be performed. <value> must be the numerical value of the character.

z.B.:
CSVSeparator=44 → means a comma ','.
CSVSeparator=59 → means a semicolon ';'.

8.8.3 List of Properties

Hardware information is read directly from the device. Other information is entered automatically by Scout Enterprise.

- **Name** The name as defined for this device. If no name has been defined, Scout Enterprise assigns the device a default name.
- **MAC address** The hardware Media Access Control address of the device.
- **IP address** The IP address currently in use by the device. You have four possibilities to set an IP address: DHCP server, BootP server, Scout Enterprise (using in an individual device configuration) or locally on the Thin Client itself.
- **Host ID** eLux NG host ID assigned to the device. This is required for the eLux NG licensing procedure.
- **Image** This field relates to software and is the name of the image definition file currently installed on the device.
- **Administration** Displays whether device management is currently active or not.
- **Configuration** To provide the most flexibility, Scout Enterprise is hierarchically based. The administrator can choose to assign the device an individual, Group, Location or default configuration. This field displays the configuration currently assigned to the device.
- **Manager** Displays the IP address of the Scout Enterprise Server currently managing the device.
- **Organisation Unit** The organisation unit the Thin Client is assigned to.
- **Info1, Info2, Info3** Fields reserved for the administrator that can be used to enter device-specific information. They are described in the following section.
- **Last Update** Date and time of the most recent firmware update attempt.
- **Last State** Status of the most recent firmware update attempt.
- **Serial number** The worldwide unique serial (or identity") number assigned to the device by the hardware supplier. It can be used for inventory purposes or provided to your hardware supplier, such as when requesting a BIOS update.
- **Type** Product description as set by the hardware supplier (a string).
- **Main memory** Size of the main memory in megabytes.
- **Flash memory** A short description of the flash local storage type and size.
- **CPU** The processor speed.
- **BIOS** The version number of the bootprom image installed on the device.
- **Supplier** The name of the hardware supplier.
- **Device type** The hardware platform.

- **Creation date** The date the Thin Client was entered in the Scout Enterprise management software.
- **Resolution** Shows the monitor resolution set for the client
- **User** User name
- **Default Printer** The printer defined as default.
- **Container** The container this terminal belongs to.
- **Flash size** The flash size of the client
- **License** The device's eLux license key. Double click to display all licenses for this device.
- **OS** The operating system running on the terminal.
- **OS** version The operating system version.
- **Last contact** Time and date stamp of the last time the Thin Client contacted Scout Enterprise. Note: The information displayed is from the time the console was started. To update the display, click F5.
- **Monitor info** shows the current monitor type, serial number etc.
- **Screen info** shows the current monitor setting

To adjust the list view rightclick the list view area and select Adjust from the context menu. You can add or remove fields.

The single columns can be moved easily by Drag&Drop.

8.8.4 Info Fields

The information in the fields Info1, Info2, Info3 is arbitrary and set by the administrator. Choose information that eases your management duties, such as user-specific information. Examples include: user name, room number, telephone extension, etc.

To set information in these fields, click an individual device using the right mouse button to open the context menu. Select **Properties**. In the **Properties** dialog box, enter the desired information (such as name, room number, telephone extension).

This information is the same as described in section 8.4 Reverse Discovery.

9 Recovery

This section describes a Recovery Installation, a useful procedure that resets the eLux *RL* configuration and firmware to the factory-delivered state.

You need to perform a recovery in case:

- eLux *RL* does not boot
- the flash card of the thin client is empty, i.e. does not contain an image
- the password for LocalLogin has been changed and forgotten
- the operating system on the flash is to be replaced by eLux *RL*
- a factory reset on the image on the flash is required
- an update is to be performed from eLux NG to eLux L (wherby this does not necessarily require a recovery)

A recovery overwrites the contents of the flash or the harddisk and installs the eLux *RL* software. It cannot be undone!

A recovery installation can be performed in 2 different ways:

- via USB stick, if the hardware supports the boot from USB mass storage devices.
- via network, if PXE is supported.

9.1 Recovery via USB Stick or CD ROM with eLux RL live

eLux RL Live serves for evaluation as well as installation of eLux RL via USB Stick or CD ROM.
So you can easily use your "old" PC, Notebook or Thin Client to access your virtual desktop.

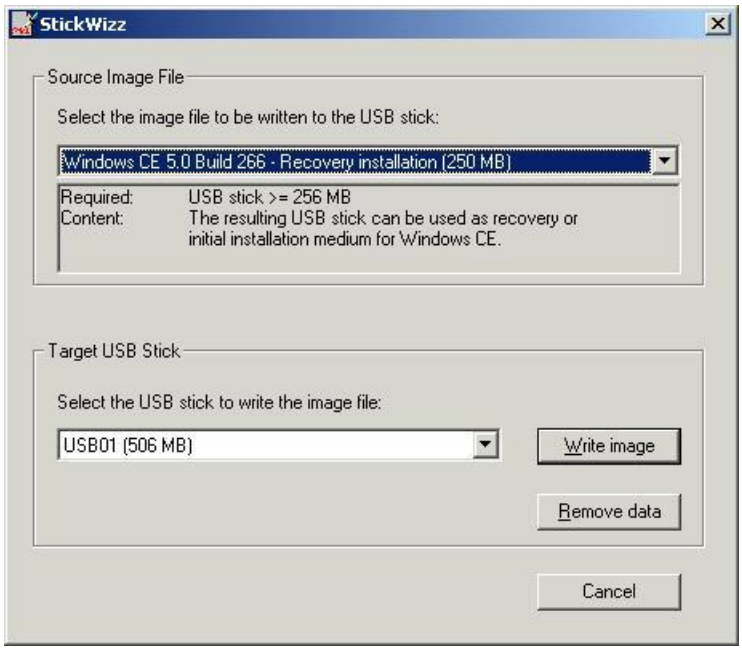
On www.myelux.com registered user find in the area **Download** > **CD/DVD/USB Stick Images > eLux RL Live** the following packages:

- eLux RL V2 Live Stick incl. Citrix Desktop Receiver
- eLux RL V2 Live Stick incl. VMware View
- eLux RL V2 Live CD incl. Citrix Desktop Receiver
- eLux RL V2 Live CD incl. VMware View

9.1.1 Preparing the Recovery via USB Stick

- From the ScoutCD coming with your hardware please select the menu option "Recovery via USB Stick".
- Download the zip file on a Windows PC and unzip it into a /tmp directory.
- Attach the USB Stick to the Windows PC.
- Start the file **stickwizz.exe** to open the following dialog. This StickWizz dialog offers you the image to be written to the USB Stick.

- In the bottom area of the dialog please select the adequate USB Stick and click on **Write Image.**



"StickWizz" for eLux RL Recovery Installation

StickWizz prompts a message of successfull write procedure.

The USB Stick now contains all the files required for a recovery installation at the Thin Client.

9.2 Requirements for Evaluation

- PC / Notebook with the option to boot from USB or CDROM
- Ethernet with DHCP
- Infrastructure for Citrix XenDesktop or VMware View.

9.3 Procedure for Evaluation of eLux RL V2

To evaluate whether eLux RL V.2 will run on your system, you can boot directly from USB stick or CD. This has no effect on the operating system and data on the harddisk.

1. Configure the BIOS of your client to boot from the corresponding medium.
2. Store the required eLux RL V2 Live Image (see above) to an USB Stick or CD and connect it to your client, in order to start the boot procedure.
3. Select the required option from the eLux RL Live boot menu. Choose the first option for evaluation.

```
eLuxRL 2.0 Live                                © 2009 UniCon
Software GmbH

Boot eLuxRL from USB stick *
Install eLuxRL on hard disk from USB *
Install eLuxRL on hard disk using TFTP
```

* - for CDROM the menu is accordingly

4. After the successful boot of the eLux RL Live system the dialog appears for login to:
   a) **Citrix Xen Desktop** or
   b) **VMware View**

Please note: eLux RL may be configured as you like, whereby the configuration will ***not*** be saved due to the eLux RL Live version. The management of the client by Scout Enterprise is ***not*** possible with the Live version of eLux RL.

9.4 Procedure for Installation of eLux RL V2

Proceed as described in chapter 1.2, however, select the second option from the eLux RL Live boot menu for the installation from USB stick or CDROM.
In this case both the operating system and all data are deleted from the hard disk. The procedure corresponds to a recovery installation.
After successful installation eLux RL V2 can be configured, the configuration data being saved. The client can be managed by Scout Enterprise.

Please note: The third option in the eLux RL Live boot menu requires a Scout Enterprise infrastructure with DHCP settings for PXE boot and can be used by devices, which have no PXE boot option. The fourth boot option starts the operating system installed on the hard disk.

9.4.1 Individual adjustment at USB Sticks

The eLux RL V2 live stick comprised the folder "container". At this folder you will find the eLux – Softwarepackages and the Imagefile recovery.idf. With ELIAS you can proceed this container. Do **not** change the Imagefile name recovery.idf. This procedure replace the image factory.

9.5 Recovery via Network (PXE)

A recovery via network requires that the BIOS of the client and the BIOS of the client's network card support PXE (Pre-Execution Boot).

9.5.1 Required Components for the LAN Recovery (PXE)

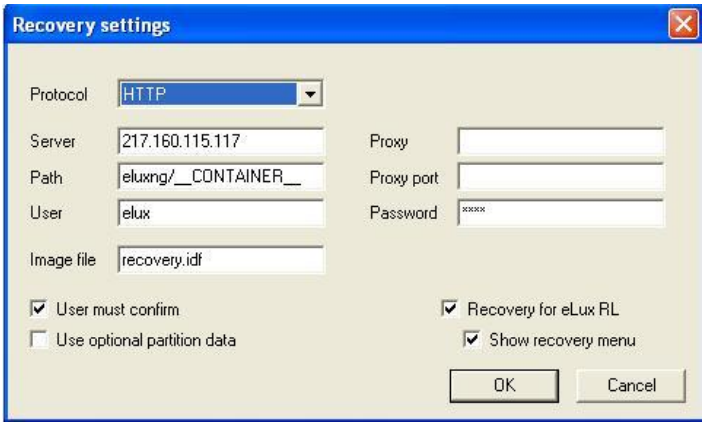
- A Thin Client with BIOS supporting the Pre-Execution Boot Environment (PXE)
- A Local Area Network (LAN) connection
- The ScoutCD coming with the hardware or to be downloaded from www.myelux.com. eLux® *RL* as well as Scout Enterprise Version 10 and all required tools and documentation are provided on the CD and on the website.
- A DHCP Server for Windows 2000 or Windows Server 2003.
- An FTP or HTTP Server.
- The TFTP Server from Unicon Software which is also included on the ScoutCD.

9.5.2 Preparing the LAN Recovery (PXE)

Scout Enterprise provides all the required components to perform a recovery installation via network in an easy and comfortable way.

If you do not already use Scout Enterprise, please follow the installation instructions in chapter 2.5 of our "Scout Enterprise Administrator's Guide". Select the recovery components during the install procedure.
Besides, a TFTP server is being installed (by default the installation directory is: …/Unicon/scoutng/tftpd), which is integrated into your system as a service. Please make sure that no other TFTP server is running on your system at the same time, because the recovery would not work in this case.

1. Edit the recovery settings in Scout via the menu
   Options > **Recovery settings**



Protocol:	FTP or HTTP Use one of the FTP or HTTP servers existing in your network. If your network should not provide any of these, use the Apache HTTP server integrated on the eLux NG CD-ROM (free).
Server:	IP address of the FTP or HTTP servers
Path:	Default: __CONTAINER__ (see our description of the container macro below)
User:	Even if your server does not request a user name or password, these fields must be filled – enter `elux` (uncapitalized). An FTP password allows for symbols – e.g. @ for the anonymous FTP login.
Image file:	Default: __SIZE__ (see our description of the size macro below)
Proxy:	IP address of the proxy server. If there is none, leave it blank.
Proxy port:	Port of the proxy server. If there is none, leave it blank.
Password:	optional

2. Finally, you have to configure your **DHCP Server** to provide the bootfile name and the address of the boot server (TFTP server):
   - Logon to your PC as administrator
   - Open the DHCP Manager.
     Start > **Programs** > **Administrative Tools** > **DHCP**
   - In the DHCP manager, go to the dialog box for configuring options.

Click to select either the server options, scope options or a reservation. In the **Action** menu select **Configure**. In the **Options** dialog box go to the **General** tab. (Alternatively: **Advanced** tab > select **DHCP Standard options** from the **Vendor class** drop-down list.)

- Configure the following options:

003 Router:	Enter one or more router IP addresses
006 DNS Servers:	Enter the DNS server IP address
015 Domain Name:	Enter the DNS domain name
066 Boot Server Host Name:	Enter the IP address of the TFTP server
067 Bootfile Name:	Enter **`pxelinux.0`**

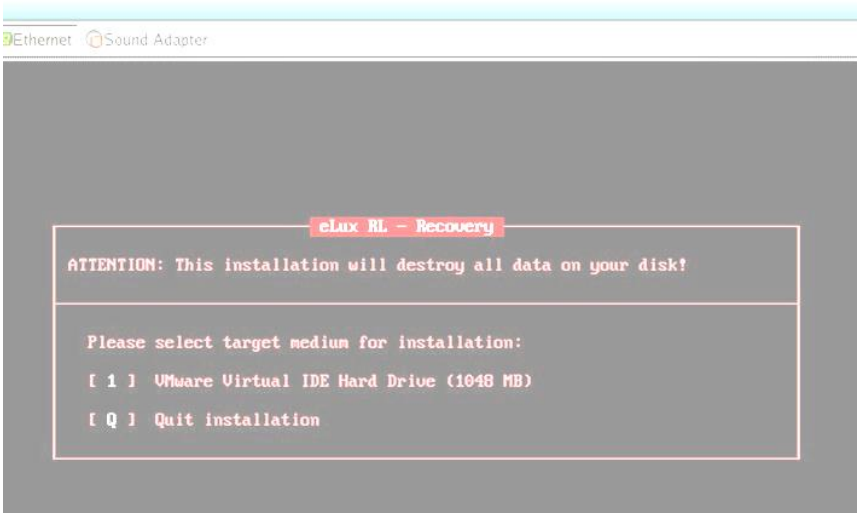
- This completes the DHCP server configuration. These settings can remain on the DHCP server without affecting normal network operation.

9.5.3 Performing the LAN Recovery (PXE)

A recovery is initiated on client-side. Initiate the recovery procedure via PXE by booting the client via LAN. If the client should not boot via network, please check if the First Bootdevice in the BIOS has been set to LAN. Many clients provide a boot menu where you can select the medium to boot from.

See the documentation included with your Thin Client to see what situation applies to you.

- The recovery starts. Do not turn off the Thin Client during a recovery!



- After a successful boot, a “Success” message appears and the Thin Client restarts.

9.6 Troubleshooting

In general we recommend to consult the server log files for troubleshooting during a recovery procedure: `…/Unicon/scoutng/tftpd/tftpd.log` (setting DEBUG=5 for TFTP), rsp. the DHCP server log file.

During a recovery, package installation will be displayed graphically. You can press CTRL – ALT – F4 to leave graphics mode and switch to a text screen. This is useful for troubleshooting, to view any error messages that may be displayed.

Problem: After beginning a PXE recovery, a DHCP time-out occurs and the terminal just boots.

Solution: The DHCP server failed to respond. Check the network connection. Check the DHCP server’s log file for the client to receive an IP address. Adapt DHCP Server settings if necessary.

Problem: The terminal begins a PXE recovery, then boots normally or displays a TFTP time-out error: `TFTP open timeout`

Solution: The TFTP server failed to respond. Check if the TFTP server is available. Check the log file of the TFTPD daemon. Check the router/gateway and boot server settings for DHCP/BootP.

Problem:	After beginning a PXE recovery, the following message is displayed: `TFTP Error – File not found` and the terminal just boots.
Solution:	The TFTP server failed to send the bootfile (pxelinux.0). Check bootfile settings for your DHCP server and TFTP server log. Check access rights for the TFTP server's root directory.

Problem:	Recovery stops. The screen is black and displays:
	`could not find kernel image: eluxrl.krn`
	`boot:`

Solution:	The TFTP server failed to provide eluxrl.krn. Check the TFTP server log. Check access rights for recovery files. If necessary, copy this file from the recovery folder on the ScoutCD to the TFTP server root directory.

Problem:	Recovery stops. The screen is black and displays:
	`could not find ramdisk image: ramfs.rl`
	`boot:`

Solution:	The TFTP server failed to provide ramfs.rl. Check the TFTP server log. Check access rights for recovery files. If necessary, copy this file from the recovery folder on the ScoutCD to the TFTP server root directory.

Problem:	Recovery hangs. The screen displays:
	`ec = 406`
	`...`
	`elux-library....`
	or it displays:
	`failed` http://user:password@webserver
	or
	`failed` ftp://user:password@ftpserver

Solution:	Transfer of the recovery IDF via FTP or HTTP server has failed. Wait for the FTP or HTTP time-out to occur. Check the address shown in: `failed` http://user:passwort@webserver or `failed` ftp://user:passwort@ftpserver If necessary, change the parameters in Scout Enterprise, Options > Recovery settings.

10 Multiple Administrator Policy

Administrator accounts may be set to the Windows accounts which are currently in use on the machine. To allow multiple administrators, Windows accounts are required. By default, this feature is not activated.

10.1 Activate Administrator Policies

⇨ **To activate the multiple administrator policy:**

1. Log on to Windows using the same account you used to install Scout Enterprise.
2. Open an administrator session to Scout Enterprise.:
   Start Scout Enterprise by double clicking the desktop icon or by selecting **Start** menu > **Programs** > **Scout Enterprise**.
3. In the **Login** dialog box enter the following:
   User Select **Administrator**.
   Password Enter the password you set (default: `elux`).
   In the **Security** menu select **Activate administrator policies**. A dialog box appears. Please read the information in the dialog box carefully and click **OK**.

You will automatically be logged off and requested to log on again, this time with the Windows account that was listed in the dialog box. This account is the user with all rights to Scout Enterprise.

If this function is activated, the menu **Options → Change server password** is disabled.

Attention: You can only change the permissions if the 'Multiple administrator policy' is activated.

10.2 Adding Administrators

⇨ **To add administrators**

1. In the Security menu select **Manage administrators**.
2. Click **Add administrators**, the initial administrator profile dialog is displayed.

3. Within this dialog you can decide which initial profile the administrator should have.
   Three options are available.
   - Minimum access
     The added administrator has no permissions to menus and all objects are not visible to him.
   - Maximum access
     The added administrator has full control.
   - Copy of existing administrator
     All permissions of the existing administrator are copied to the added administrator .
4. Select one of the options and click **OK**.
5. Then the standard Windows permission dialogs are displayed to add a new administrator.

Note: At the time being within this dialog only one administrator can be added. If you select more than one only the last one is entered to Scout Enterprise. Repeat the procedure as often as you want.

Once you have added a new administrator this administrator is able to login to Scout Enterprise.

Please be aware that only users of the domain can be added as administrators, and only these users can login to Scout Enterprise.

The new administrator can be assigned **Default object rights** as well as a **Root organisation unit.** If the latter has been assigned only this organisation unit and the subordinate organisation units are displayed when starting Scout Enterprise Console.

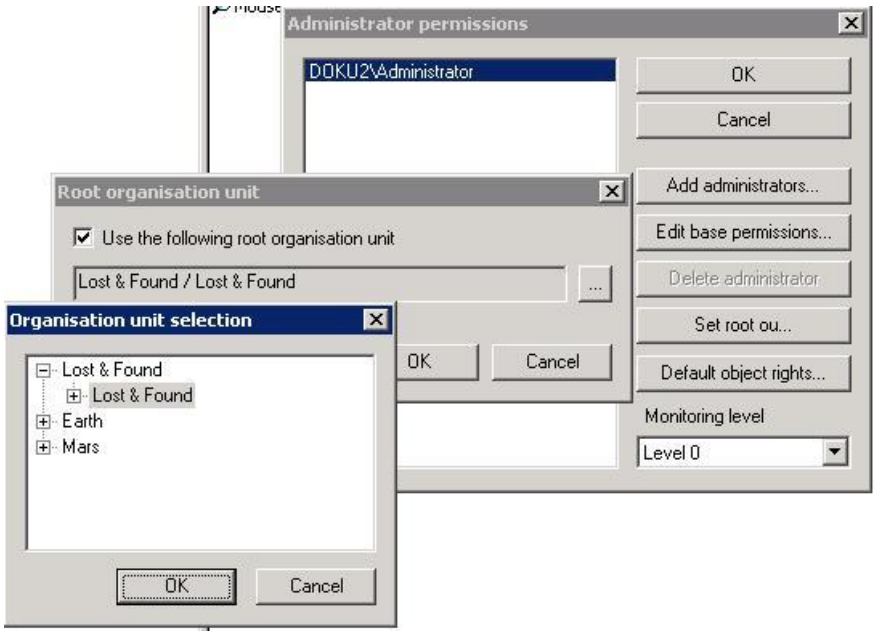


Figure 137: Add administrator > Set root organisation unit

Possible messages:

On Windows 2000 computers the following message may appear. This is because the normal" Windows user does not have the right to logon interactively from a program.

If a message 'Error while connecting database. (unknown) could not be used; file already in use' appears, the user who tries to logon must be a member of the 'Power user' group.

10.3 Setting Administrator Permissions

There are three different kinds of permissions

- **Base permissions**: These permissions control the **main access** for the administrator.
- **Menu permissions**: These permissions control the **menu access** for the administrator.
- **Object permissions**: These rights can be set for each organisation unit.

⇨ To change the basic administrator permissions

1. In the **Security** menu select **Manage administrators.**
2. Select an administrator and click **Edit base permissions**. The **Administrator permissions** dialog box displays the rights which can be set (Full access) or cleared (No access).

⇨ To change the menu permissions

1. In the **Security** menu select **Menu permissions**.
3. Select an administrator and click **Edit menu permissions**. The **Menu permissions** dialog box displays commands available in the main menus and context menus which can be set (Full access) or cleared (No access).

⇨ To change the object permissions

1. Select a Location, Group or individual device.
2. In the **Security** menu, select **Object permissions**.
4. Select an administrator and click **Edit object permissions**. The **Object permissions** dialog box displays the rights which can be set or cleared.
5. If you clear the 'Visible' right the object is not longer visible in the tree view of Enterprise.

If you clear any right for an administrator it is not longer accessible for this administrator.

Restriction: It is not possible to restrict access to the last user with administrator rights. This is to prevent from being locked out of the Console.

11 Command Menus

This section is meant as a reference guide for the various commands. Cross references to more detailed information elsewhere in the manual is provided when appropriate.

11.1 Main Menus

The menu commands are context sensitive, that is, only those commands will be displayed applying to a selected element.

Elements can be:

- Organisation Unit
- Applications
- Device categories
- Individual device
- Individual application in the tree view or in the Propertes window.

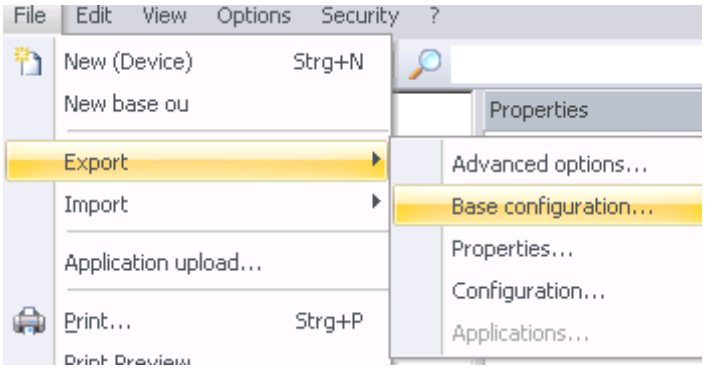
11.1.1 File Menu

File > New

Creates a new screen element based on the screen element that is currently selected.

File > Export / File > Import

Below figures show the areas which can be imported rsp. exported.



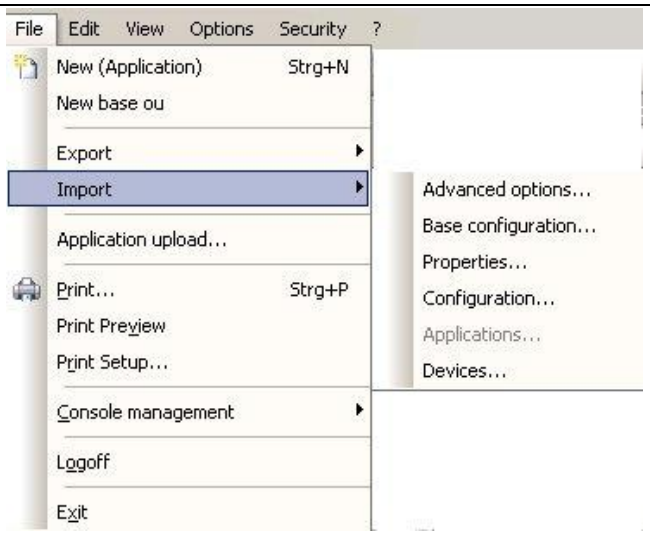
File > Export

Export of devices into a csv file:

Version a) via the list view: Select the 3 columns, then go to Edit > CSV-formatted clipboard.

Version b) via Scout Report Generator: select the 3 colums via "Layout", see the separate Scout Report Generator manual.

File > Import



The csv file for the import of devices consists of 3 colums: MAC address, name, organisation unit.
Example of a csv file:

MAC address	name	organisation unit
00199985F675	S450-1	NameOfOrgUnit
00E0C5422A2E	nexeed-i	NameOfOrgUnit

Note: If the MAC address of a device registered in Scout already exists in the csv file to be imported, then this device will only be moved to the organisation unit stated in the csv file.

All the export and import functions can either be performed via the Scout console or via the scmd interface (see chapter 12.2 and following).

By exporting one of the above mentioned areas files, which contain the data, are created in xml format. Each area is defined by an individual file extension.

Configuration of OU's : .oustp
Configuration of devices : .devstp
Properties of OU's : .oupro
Properties of devices : .devpro
Properties of applications: .apppro

These files can be edited by means of the program "Configuration editor". The installation of Scout creates the link in the Windows start menu "Start > All Programs > Scout Enterprise > Configuration editor".

File > Application Upload

Uploads applications from a Thin Client to an organisation unit. Previously defined applications in the ou are deleted.

Enter the IP address or host name of the source device. The source device can be any Thin Client available over the network and does not have to be a device currently entered in Scout Enterprise. Select the ou to upload the applications to. Click **Start** to begin the upload.

File > Print

Prints a list of all devices registered in Scout Enterprise. This dialog box may vary depending on the printer you select.

File > Print Preview

Previews the device list.

File > Print Setup

Allows you to choose the printer, paper size and orientation, and paper source. This dialog box may differ depending on the printer you select.

File > Console Management

Each console being opened by an administrator, registers to the Scout database. The registered consoles can be displayed by the menu option ***Console management***. The functionality is described in detail in chapter 11.4 Console Communication. The sub menus are:
Close console
Send message
Manage consoles
Manage commands

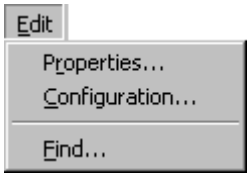
File > Logoff

The currently logged in administrator is being logged off. To logon again a password must be entered.

File > Exit

Logs off from the Scout Enterprise Server and quits Scout Enterprise Console.

11.1.2 Edit Menu



Edit > Properties

Allows you to edit the properties of the selected organisation group or individual device. Allows you to modify the configuration of an individual application definition.

Edit > Configuration

Configures the setup of an organisation unit or device distinct from the base configuration. The element you are configuring it for is displayed in the title bar.

Use Parent

When this check box is selected (**General** tab), the individual device or organisation unit uses the configuration of the element directly above it in the hierarchy. For example, an individual device will use its organisation unit's Setup. When **Use Parent** is selected, the rest of **Setup** on this level is disabled, as configuration information is taken from the next higher level in the hierarchy. Deselecting the check box re-enables Setup on this level.

See chapter 0

Management on the Setup Level, for detailed information on configuration settings.

Edit > Find

Use to find text in the tree view. Click to select **Find** in **Properties** to find text in the properties window. Keyboard shortcut: CTRL-F.

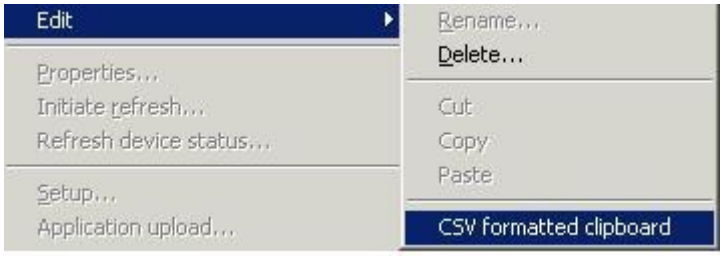
Starting with **V 9.4.0** it is possible to search for switched-on devices and switched-off devices. Enter "on" or "off" in the "Find what" field. Click on "find next" and one after another the "on" or "off" devices will be displayed in the Properties window.

11.1.3 View Menu

View > Devices

Switches between tree view and list view. List view displays the devices without icons.

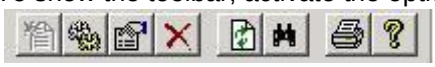
By selecting one or more devices in the device view you can copy the device data to a CSV-formatted clipboard by clicking Edit in the context menu.



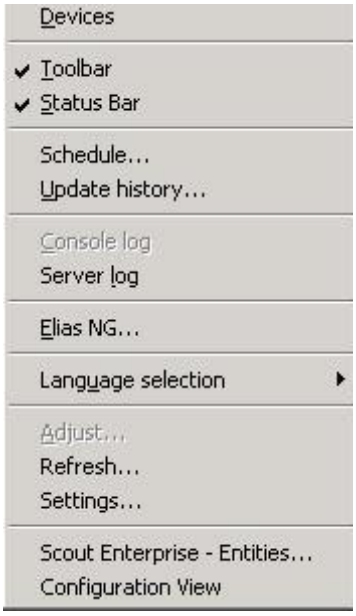
Insert the data into any editor for further processing.

View > Toolbar

To show the toolbar, activate the option.



The toolbar icons allow one-click access to the following commands: New, Configuration, Properties, Delete, Refresh, Discover, Print, Help.



View > Status Bar

When selected, displays the status bar at the lower edge of the Scout Enterprise Console window.

Shows the state of a current process, and the number of devices and applications.

View > Schedule

Overview of the planned tasks. Also allows you to set global tasks that will affect all entered devices.

View > Update history

Displays the date, time, device name and status of updates. It cannot be altered and includes all updates made from the time Scout Enterprise was first installed. It can be used to check update status, that is, whether an update was successful (done") or not (error"). To view the update history, Scout Enterprise Console and Scout Enterprise Server must be installed in the same directory.

View > Console Log

Allows you to view, but not alter, the Scout Enterprise Console log. Viewing the log file may be useful for error tracing or problem solving.

View > Server Log

Allows you to view, but not alter, the Scout Enterprise Server log. Viewing the log file may be useful for error tracing or problem solving.

Attention To view the server log, Scout Enterprise Console and Scout Enterprise Server must be installed in the same directory. See section

View > ELIAS

Opens the ELIAS image builder program. See chapter 5 Management on Firmware Level.

View > Language selection

Changes the language of the Scout Enterprise Console. Available languages: English and German.

View > Adjust

In tree view, allows you to select which properties are displayed in the Properties Window (**note**: Click in the Properties Window to activate this option.) In list view, allows you to select which columns are displayed. For a description of properties, see 8.8.3 List of Properties.

View > Refresh

The configuration is reloaded from the Scout NG Server and displayed. Keyboard equivalent: F5. Alternatively, you can click Refreshin the toolbar (see above).

View > Settings

To set the intervals in which the console is to refresh the device status.

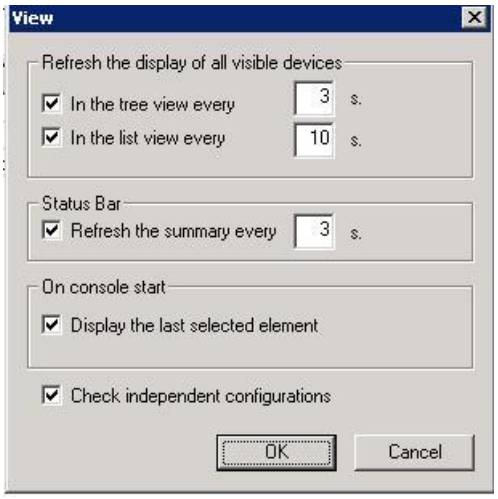


Figure 138: View - Settings

Background: In former versions of Scout the server informed the console about the device status (e.g. changing from green to red). Now the console refreshes the status automatically by a periodic query of the database.

Further this dialog box contains the option **Check independent configurations**. When enabled, all subordinate independent configurations will be checked as soon as a configuration has been modified.

View > Scout Enterprise Entities

This dialog enables to enter for a server a threshold value for the system CPU load. Default is 99%. If the cpu load exceeds this threshold value, the Scout Enterprise Server closes its ports and will not server any more clients. A console which might be open will get an alert message. The alert icon in the status bar changes from white to yellow.

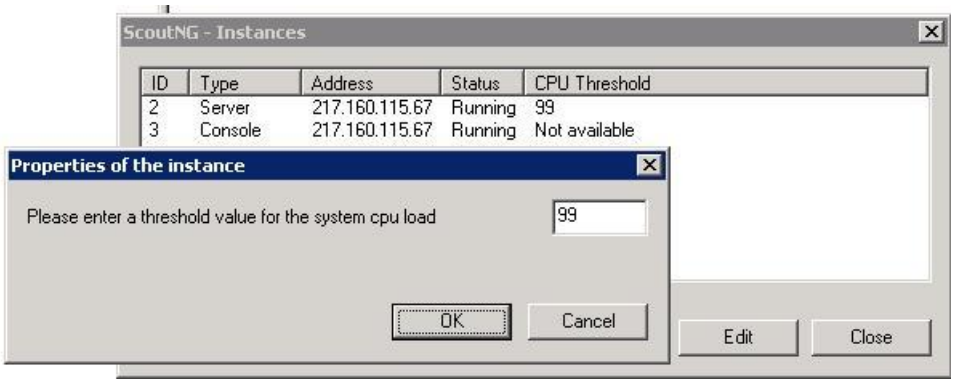
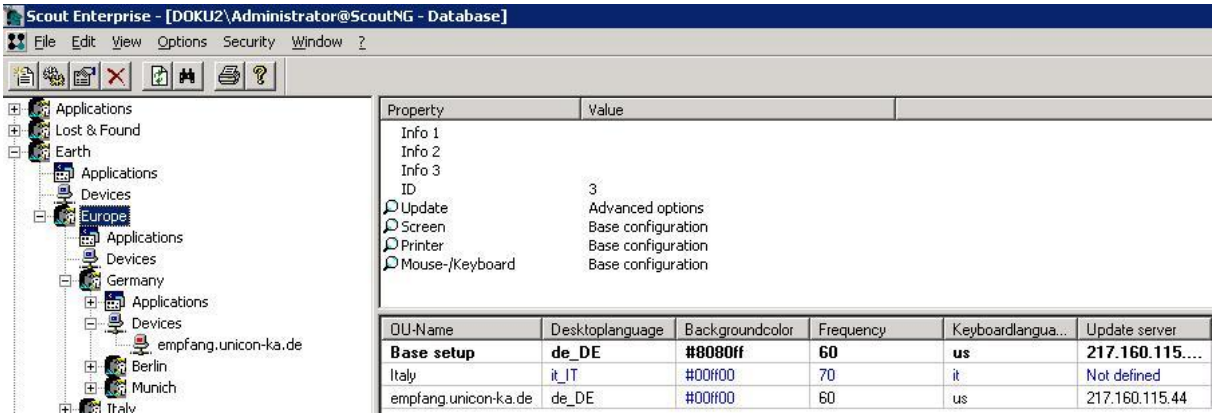


Figure 139: View – Scout Enterprise Entities

View > Configuration View

This option shows a third area below the properties window. The configuration hierarchy for the selected organisation unit or the selected device is displayed in this area.



11.1.4 Options Menu

Options > Base Configuration

Default configuration settings. See chapter 0

Management on the Setup Level, for information on configuration.

Options > Discover Devices

Client discovery procedure is an important tool which enters Thin Clients (devices) in the Scout Enterprise software automatically, greatly saving a large amount of work. See section 8.3 Client Discovery Function,for a detailed description of the discovery procedure.

Options > License Information

Displays all Scout Enterprise licenses. You can enter a new Scout Enterprise license or activate an existing one.

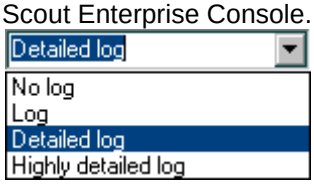
Options > Change Server Password

Allows you to change the Scout Enterprise Administrator password. See section 7.1 Passwords. This option is disabled if the option Activate Administrator Policies has been enabled (Security menu).

Options > Logging Options

Allows you to set log detail information for Scout Enterprise Server and Scout Enterprise Console.

You can choose from the following settings:



- No log
- Log
- Detailed log
- Highly detailed log

Logs are for debugging purposes. Note: Logs are not deleted automatically..

The Scout Enterprise Server log can only be accessed when Scout Enterprise Console has been installed in the same directory as Scout Enterprise Server.

Optionen > Advanced Options

All tabs of the **Adavanced Options** are explained in detail in chapter 6.8.

Options > ELIAS Settings

Enter the container path and the ELIAS directory, if ELIAS should not have been installed in the same directory as Scout Enterprise.

Options > Recovery Settings

This is to set the TFTP server configuration being used for a recovery installation. Detailed information on Recovery can be found in chapter 9.2.

Note: Starting with V 10 there is an option to be enabled for eLux *RL.*

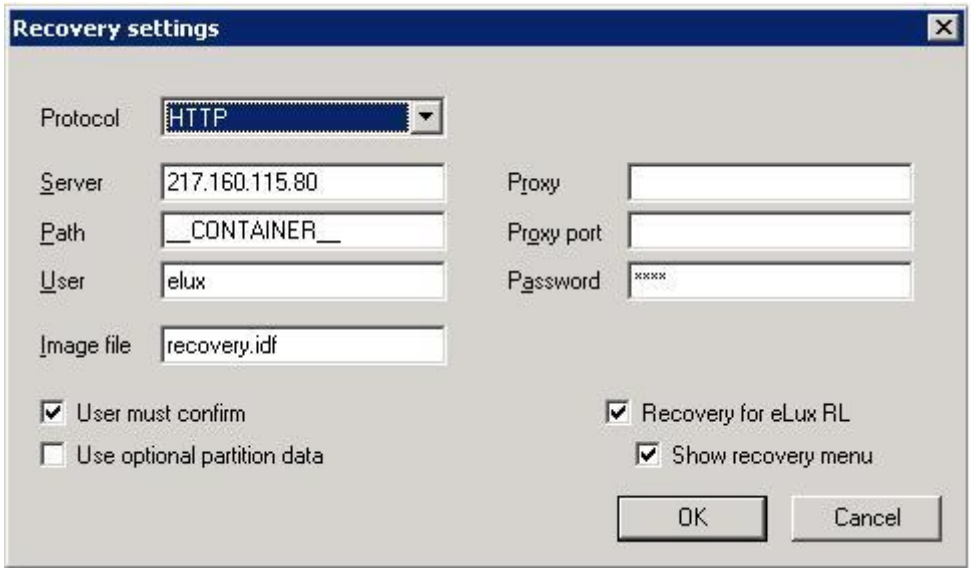
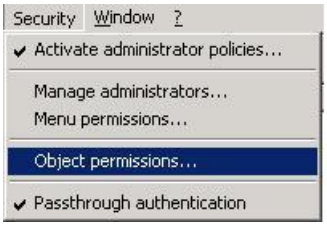


Figure 140: Options > Recovery Settings

11.1.5 Security Menu

With the feature **Multiple Administrator Policy** the menu Security was added.



This menu contains all necessary options and settings for the management of the administrators and their permissions. The subject is described in detail in chapter 10 Multiple Administrator Policy.

Note: If the option Activate administrator policies is enabled, the command **Options > Change server password…** is disabled.

The **Passthrough Authentication** enables the Single-Sign-On. Then your Windows account information is used to automatically log you on the Scout Enterprise. The Scout logon window will not show any more.

11.1.6 Window Menu

Window > Cascade, Tile, Arrange Icons

When multiple server connections are open, multiple windows appear on the Scout Enterprise screen. This allows you to arrange them in cascade, tile or icons (applicable when the windows are minimized). These commands are only useful when multiple server connections are open.

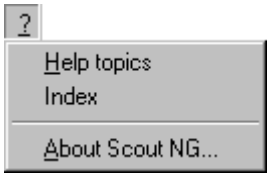
Window > {Session name}

The currently opened server connection(s) are displayed at the bottom of the menu.

11.1.7 Help Menu

Help > Help topics

Opens Scout Enterprise Help Topics. **Note**: If you do not see the Contents,Index" and Search" tabs on the left, move the slider to the right until they are visible.



Help > Index

Opens Scout Enterprise Help Index. **Note**: If you do not see the Contents,Index" and Search" tabs on the left, move the slider to the right until they are visible.

Help > About Scout Enterprise

Displays the name and version number of the software.

11.2 Context Menus

To access the context menus, tree view must be on, i.e. **View > Devices** must be disabled. Screen elementrefers to the icons in the tree view:

Organisation unit

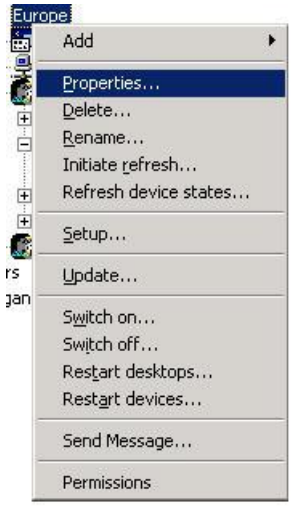
Devices category or individual devices

Application category or individual application

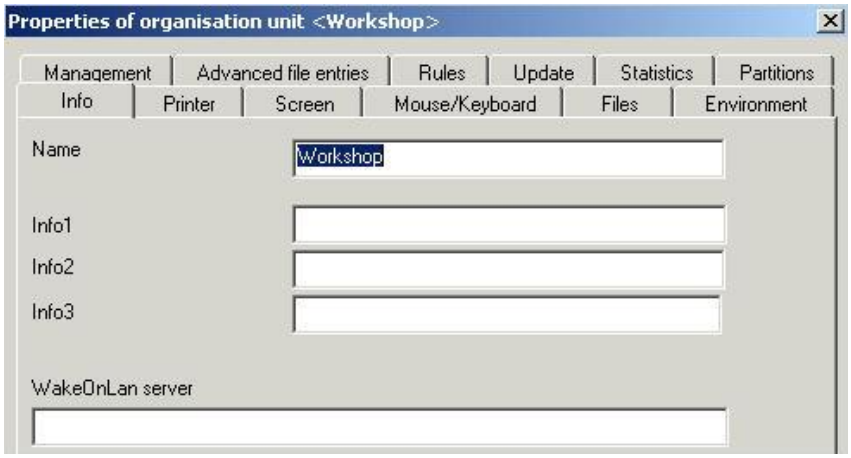
Clicking a screen element with the **left mouse button** selects the element. Its **properties** are displayed on the right-hand side of the screen.

Clicking a screen element with the **right mouse button** opens the **context menu**. When you open a context menu, you can be sure all commands apply to that element. Many context commands are self-explanatory, therefore only some of the options are described in detail here.

Context menu of an **Organisation Unit**:



Properties: Opens the dialog **Properties of.....,** containing the tabs:



Initiate Refresh: Forces the refresh of the Thin Client configuration in this screen element.

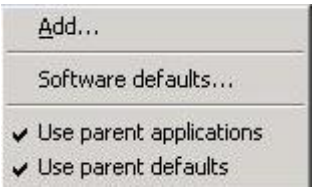
Setup: opens the configuration for the selected screen element.

Update: The update can be scheduled or a defined schedule can be deleted.

Send message: Sends a message to the selected device.

Permissions: Administrator permissions can be set.

Context menu of **Applications**:



Add: This opens the dialog **Application Properties.**

Software defaults: Allows access to standard settings for applications. At the moment, only ICA is available.

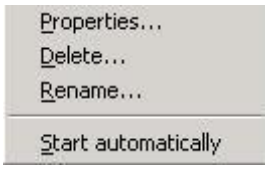
Use parent applications: Assigns the applications of the next higher element in the hierarchy to this element.

Use parent defaults: Assigns the default settings of the applications of the next higher element in the hierarchy to this element.

Context menu für the **Devices** category**:**

Add: Opens the **Informations** dialog box for entering MAC addresses.

Context menu of **individual applications:**



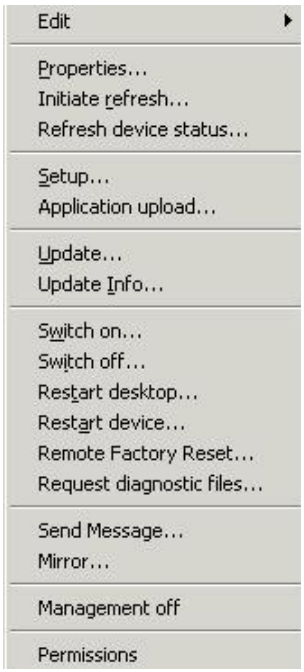
Properties: Opens the window **Application Properties** to set the parameters for the application.

Delete: Deletes the screen element.

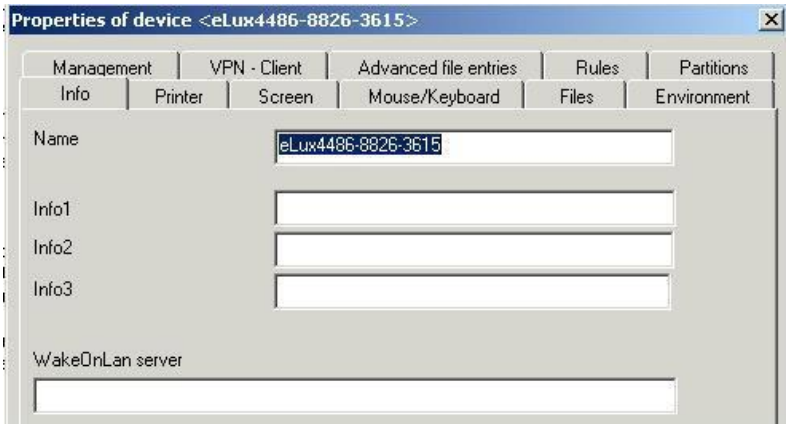
Rename: Renames the screen element.

Start automatically: Starts the application every time the Thin Client starts.

Context menu of an **individual device**:



Properties: Opens the window **Properties of device...**



Initiate refresh: Forces the Thin Client to reload its configuration

Refresh device status: Opens the dialog "Execute / Schedule command for device...".

Setup: Opens the setup dialog for this device.

Application Upload: Applications are loaded from the Thin Client to Scout Enterprise. The applications will be assigned to the corresponding group.

Update: The update can be scheduled or re-scheduled.

Update Info: Opens the update protocol for the individual device.

Remote Factory Reset: Configurations and applications are deleted at the client except for the manager address and the group id. During restart of the device it will automatically be registered in Scout Enterprise and be assigned the corresponding configuration and applications.This function is useful in order to delete files which have been generated by the local user or to fix errors.

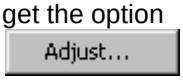
Request diagnostic files: see chapter 8.9 for detailed description.

Send message: Send a message to the device.

Mirror: Mirrors the device.

Management off: Deactivates management. A profile remains reserved for the device, but the configuration will no longer be transferred when the Thin Client boots. Useful for temporarily disconnecting the Thin Client from management services.

In addition, if you click on an empty space in the Properties Window, you always get the option **Adjust**. This lets you determine which properties appear in the Properties Window for the element selected. Settings apply to all instances of that element (for example, all Locations).



11.3 Keyboard Shortcuts

The following keyboard shortcuts are context sensitive. The function they call varies depending on what screen element has been selected.

Shortcut	Selected Element	Description
CTRL-SHIFT-INSERT	Organisation unit	Opens the dialog **Properties of Organisation unit**
	Applications	Opens the dialog **Application Properties**
	Devices	Opens the dialog **Information** to enter a MAC address
CTRL-SHIFT-DELETE	Organisation unit	Deletes the selected screen element
	Individual device	Nothing is deleted until the user has been prompted.
	Individual application	
F2	Organisation unit	Renames the selected organisation unit
	Individual device	Renames the individual device
	Individual application	Renames the individual application
CTRL-F		Finds text in the tree view.
CTRL-X	Individual device	Cuts the device
CTRL-V	Individual device	Pastes a device
CTRL-A	Applications Devices	When the focus is in the Properties window, selects all applications/devices
CTRL-E	Individual device Online Setup Check	This is to check whether a client is configured correctly. The configuration at the client is being compared with the current settings in the database. If there any discrepancies, these are displayed in separate window.

12 eLux/Scout License Model

Starting with Scout Enterprise Version 11 and eLux NG / eLux RL Version 2 there is no differentiation between eLux NG and eLux RL licenses.

12.1 License Types

The operation of a Thin Client infrastructure with eLux/Scout 4 license types are relevant:

- Client operating license ⇨ using eLux at the client
- Scout management license ⇨ management of the eLux clients via Scout Enterprise
- eLux/Scout subscription license ⇨ to update the eLux client with new software packages
- Client application license ⇨ optional – in case of applications which need a separate license

12.1.1 Client Operating License

The operation of client hardware with the eLux operating system needs to be licensed. There are 2 types of operating licenses: eLux NG/eLux RL and eLux Lite [1)] . The client operating licenses are always stored on the client.
Clients with Windows CE and Windows XP embedded [2)] can also be managed by Scout Enterprise. The licensing of the Windows operating system is provided by the hardware manufacturer and is not subject to the licensing procedure of eLux/Scout.

Licensing procedure:

Licensing by….	Description
integrated eLux license ex-factory	By some hardware manufacturers (OEM partners) the clients can be equipped with an eLux license ex factory. In this case no further action is required to license the eLux operating system.
new eLux license locally at the client	A new eLux license is locally entered into the license dialog at the client.
new eLux license via Scout	New eLux licenses are entered into the license dialog of the Scout console. These licenses are automatically distributed to all those unlicensed eLux clients which contact the Scout server.
released / restored eLux license via Scocut	By deleting a client in the Scout console the eLux license of the deleted client is given back to the Scout server, so that this license is free for distribution. It will be deployed automatically to all those unlicensed eLux clients which contact the Scout server. (Example: Replacing Thin Client-Hardware, Migration of a PC to a Thin Client).

[1)] With eLux Lite there is one and only firmware image provided by the hardware manufacturer. It cannot be modified by ELIAS.
[2)] Only in the bundle (Hardware, Windows operating system and Scout-Agent) provided by Fujitsu Technology Solutions.

12.1.2 Scout Management License

This license type is required for the management of Thin Clients with eLux, eLux Lite, WinCE und WinXPe via Scout Enterprise. Each client needs one Scout management license [3)]. The license is stored on the Scout server.

Also, some hardware manufacturers (OEM partners) can deliver the clients equipped with an eLux license and a Scout management license ex factory. We speak of a so-called integrated license "eLux with Scout-builtin".
This type of Scout management license is stored at the client, so that no further server-stored management license is required to manage the client with Scout.

Licensing Procedure:

Licensing by …	Description
integrated Scout management license ex-factory	By some hardware manufacturers (OEM partners) the clients can be equipped with an eLux license and a Scout license ex factory. In this case no further licensing action is required.
new Scout management license via Scout	New Scout management licenses are entered into the license dialog of the Scout console.
released Scout management license via Scout	By removing a client from the Scout console the Scout management license of the removed client is available again.

12.1.3 eLux/Scout Subscription License

The update of eLux Thin Clients with the latest eLux software packages requires a valid so-called subscription license. For more information on Subscription please consult chapter 13.3 in this manual.

A new eLux license includes subscription (i.e. software service) for a 24 months period. By purchasing extra subscription licenses the software service (= validity of subscription) can be extended by 12 months.

The Scout Enterprise server manages the subscription either in device or enterprise mode. If clients are not managed by Scout, the subscription period is calculated locally at the client.

The eLux/Scout Subscription licenses are stored at the Scout Server.

Licensing Procedure:

Licensing by….	Description
Assigning subscription in the subscription pool of the Scout Server	Initial situation: The Thin Clients are managed by Scout Enterprise and the subscription mode is „Enterprise“. New eLux/Scout subscription licenses are entered into the license dialog of the Scout console thus extending the subscription for all clients.
manual assignment for individual clients	Initial situation: The Thin Clients are managed by Scout Enterprise verwaltet and the subscription mode is „devices“. New eLux/Scout subscription licenses are entered into the license dialog of the Scout console. The subscription is distributed manually to individual clients by the administrator via the Scout console.
manual request of subscription from the client	Initial situation: The Thin Clients are not managed by Scout Enterprise. The subscription for a client must be distributed via a Scout server. The Scout server which provides the subscription for the client must be entered in the license dialog of the client. This Scout server may, however, serve just as a license server without managing clients.

12.1.4 Client Application License

This refers to using applications requiring separate licenses, such as the PowerTerm terminal emulation.

These application licenses are stored on the client only.

Licensing procedure:

Licensing by….	Description
new application license locally at the client	The new application license is manually entered into the license dialog of the client.
new application license via Scout	New application licenses are entered into the license dialog at the Scout console.
released / restored application license via Scout	By removing a client from the Scout console the Scout management license of the removed client is restored to the Scout server and thus made available.

12.2 Examples

Description of the Icons

Client Operating License

S eLux/Scout Subscription License

Scout Management License

A Client Application License

Integrated eLux license incl. Scout-builtin ex- factory
During the first contact to the Scout server the Thin Client transmits the license information of its stored eLux and Scout license.

Thin Client		**Scout Enterprise**
	Transfer license information ⇨	✓ ✓

New eLux license locally at the Client and Scout license via Scout
Having entered a new eLux license locally at the Thin Client, the client transfers the license information during first contact to the Scout server.

Thin Client		**Scout Enterprise**
manually	Transfer license information ⇨	✓
	⇦ Distribution Scout license	✓

New eLux and Scout license via Scout
The Thin Client contacts the Scout Server and requests an eLux and a Scout license. The Scout server transfers the eLux license to the client and distributes a Scout license to the client.

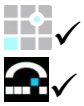
Thin Client		**Scout Enterprise**
unlicenses	License request ⇨	
	⇦ Transfer license information ⇦ Distribution Scout license	✓ ✓

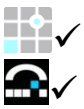
New application license via Scout
A licensed Thin Client (integrated eLux license with Scout-builtin) contacts the Scout Server and requests an application license. The Scout Server transfers the application license to the client.

Thin Client		**Scout Enterprise**
	License request ⇨	A ✓ ✓
A	⇦ Transfer application license	A ✓ ✓ ✓

Released eLux and Scout license via Scout
Removing a Thin Client in the Scout console results in releasing its license/-s and restoring it/them to the Scout server. An unlicensed client can request these licenses.

Thin Client 		**Scout Enterprise** 
	Version 1: an integrated eLux license with Scout builtin is stored at the client	
✖Removal client	Release of licenses⇨	

unlicensed	License request⇨	
	⇦Transfer eLux license ⇦ Distribution Scout license	
Thin Client 		**Scout Enterprise** 
	Version 2: an eLux license stored on the client via Scout	
✖removal client	Release of licenses⇨	

unlicensed	License request⇨	
	⇦Transfer eLux license ⇦ Distribution Scout license	

Entering Subscription to the Subscription-Pool of the Scout Server

Initial situation: The Thin Clients are managed by Scout Enterprise and the subscription mode is "Enterprise".

Entering new eLux/Scout Subscription licenses to the Scout Server extends the subscription pool of the Scout server. Thus the subscription validity is extended for all clients.

Example:
Situation: Enterprise subscription for 1,000 devices, valid until 2/2010
Action: Entry of 2,000 eLux/Scout subscription licences at the Scout Server
Result: Enterprise subscription für 1,000 devices, valid until 2/2012

Manual distribution of Subscription to individual clients

Initial situation: The Thin Clients are managed by Scout Enterprise and the subscription mode is "Devices".

New eLux/Scout subscription licenses are entered into the license dialog of the Scout console. The subscription is assigned to individual clients manually by the administrator of the Scout console.

13 Subscription

Starting with Scout Enterprise V11 and eLux RL/ eLux NG V2.x the subscription information is determined and clearly displayed. For migration from eLux RL 3.10.0 to eLux RP 4.0.0 latest version of Scout Enterprise is needed, Scout Enterprise V.13.1

13.1.1 Definition of Subscription

Over a specific period of time, the subscription ensures that your eLux thin clients and Scout can support latest software technologies, features and hardware.

The subscription provides for

- Software package supply via Internet including free download and installation
- Use of latest hotfixes and beta versions of the eLux operating system
- Use of the latest versions of Scout Enterprise and ELIAS
- Use os the latest released versions of applications
- Free migration from eLux NG V2 to eLux RL V2
- Free migration from eLux RL 3.10.0 to eLux RP 4.0.0

13.1.2 Life-span and Validity of the Subscription

The subscription life-span runs from the first-time use of the eLux license on a thin client. An eLux full license includes a 12 month subscription.

After the period of 12 months the subscription expires no matter how frequently the thin client has been used. Once the subscription has expired, eLux thin clients can still be used with their current image, but cannot longer participate in any of the of the above mentioned benefits, such as software updates. However, the subscription can be renewed any time, so that an eLux thin client can again be updated by purchasing a subscription license. Periods of use without subscription are backdated automatically.

Also, additive subscription can be provided for a client before the expiration of the current subscription. In this case, however, the life-span of the subscription of an eLux full license cannot exceed 12 months.

An additive subscription license provides 12 months of software service.

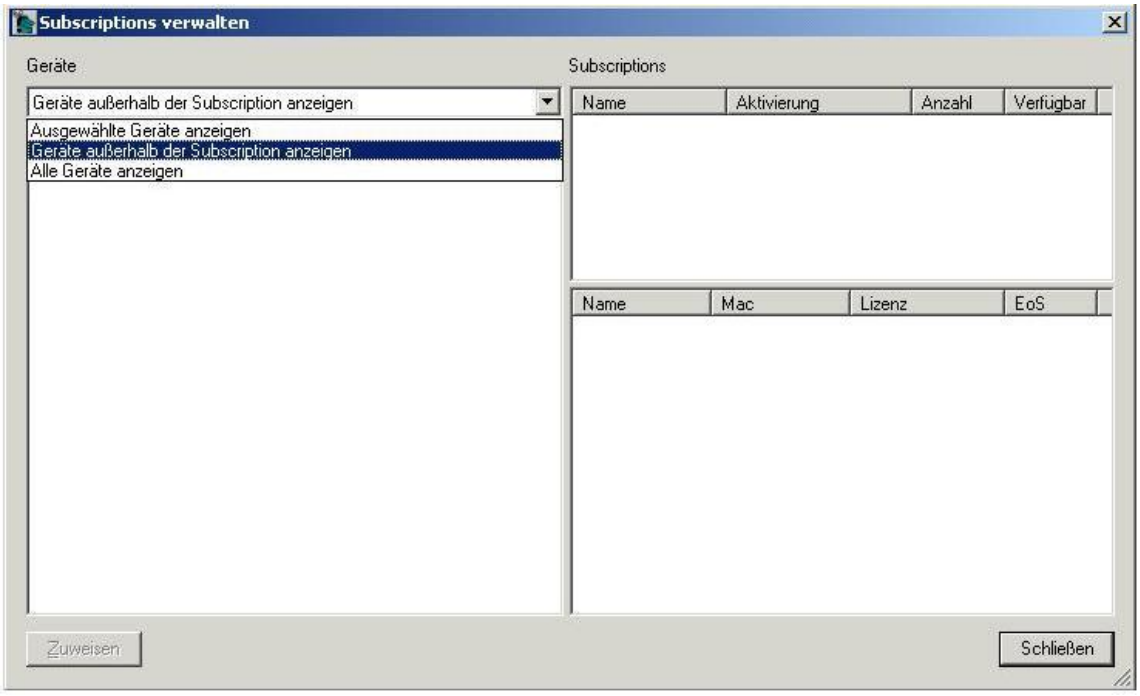
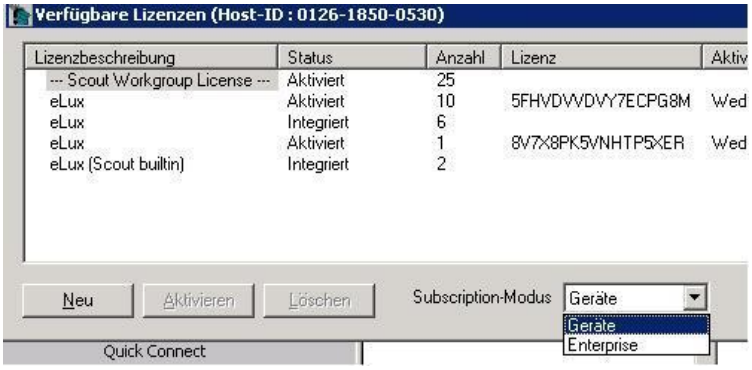


Figure 141: Manage Subscriptions

13.1.3 Managing the Subscription Information

The Scout Enterprise Server takes charge of the management of the subscription information.Which can be done in two different ways:

- **Device mode** (default)
  Scout Enterprise manages and displays the subscription for each thin client individually, i.e. a subscription has to be assigend to each device. Different life-spans are accounted for.
- **Enterprise mode** (to be activated once, no reset to the device mode!)
  The individual subscriptions are consolidated to a subscription pool on the Scout Enterprise Server. From this pool the subscription is evenly distributed to all thin clients. The pool can be restocked by purchasing additive subscriptions.



For thin clients which are not managed by Scout Enterprise, the subscription information is managed locally at the client. However, additive subscription can only be provided by the a Scout Enterprise Server representing the license server. Scout Enterprise itself need not be licensed for this purpose.

OU Mode
This mode corresponds to the Enterprise mode except aht it is limited to the OUs of the highest leve. Each OU has ist own Subscription pool. This constellation is mainly useful when you need to manage Thin Clients of different customers as a service provider.

14 Appendix

14.1 Update Error Messages

Following is a list of status messages after an update, and their meanings. They are displayed in the Properties Window > Last State."

Update in progress

An update is currently taking place.

Update successful

The update was successful.

Update failed

The update was not successful. Details are unknown.

Update not necessary

The Thin Client's firmware is up-to-date.

Update failed: bad firmware parameter

One or more of the firmware parameters is wrong. Go to Setup > **Firmware**. Check that all boxes are filled in and that the server IP address is valid.

Update failed: bad authorisation

The Thin Client password entered in the base configuration (**Security** tab) does not correlate with the Thin Client password saved on the Thin Client.

Update failed: bad flash size

The flash size listed in the container is incompatible with the actual flash size (flash size mismatch).

Update failed: bad container

The container used does not support this hardware (container mismatch).

Update failed: device unreachable

The Thin Client cannot be reached.

Update failed: time-out

The Thin Client did not respond within the allotted response time. The Thin Client may have stopped responding, or hanged,during the boot procedure. There are various causes, such as network problems. If possible, mirror the Thin Client to find out more.

14.2 Thin Client Time Settings

Scout Enterprise and eLux

The easiest and recommended method is to set the time is using the Scout NG or eLux NG GUI.

Select the time zone from the drop-down list in Scout Enterprise in **Setup** > **Desktop**.

To set the time, you have two options:

If your network has a time server, enter it in **Setup** > **Desktop**. The time server must conform to the Internet standard RFC 868 (Time protocol"), RFC 2030 (SNTPv4") or RFC 1305 (NTPv3"). For more information, see section 0

1. Desktop.
2. If your network does not have a time server, or if the time server does not conform to the above Internet standards, you can manually enter the time and date settings in eLux NG on the Thin Client (**Setup** > **Desktop**).

Daylight Saving Time changes will be made automatically.

BIOS Setup

If the GUI is not an option, alternatively you can set date and time directly in the BIOS Setup of the Thin Client. In this case, you must set the system time to Coordinated Universal Time (UTC), the successor to and modern version of Greenwich Mean Time (GMT). To calculate UTC, take local time minus the time zone difference from GMT (found in the **Time Zone** drop-down list in Scout NG **Setup** > **Desktop** tab). In Summer Time, subtract an additional hour to take into account Daylight Saving Time.

UTC in winter months = (local time – time zone difference)

UTC in summer months = (local time – time zone difference) – 1 hour

For example, if you are in Amsterdam, the **Time Zone** drop-down list in Scout Enterprise shows the local time for Amsterdam is GMT plus one hour (GMT + 1). Thus, you should change time setting in BIOS to the local time minus one hour. If local time is 17:45, system time in BIOS should be set to 16:45. If it is Summer Time (Daylight Saving Time), the system time should be set to local time minus two hours, or 15:45. Note that BIOS system time uses the 24-hour system.

You only need to set the system time once. Fall and spring Daylight Saving Time changes are made automatically.

14.3 Directory Services

14.3.1 What is a DN - Distinguished Name?

The LDAP or ADS directory is hierarchical. It has the concept of fully-qualified names called distinguished names (DN). A DN is a series of name-value pairs that uniquely identify an entity.

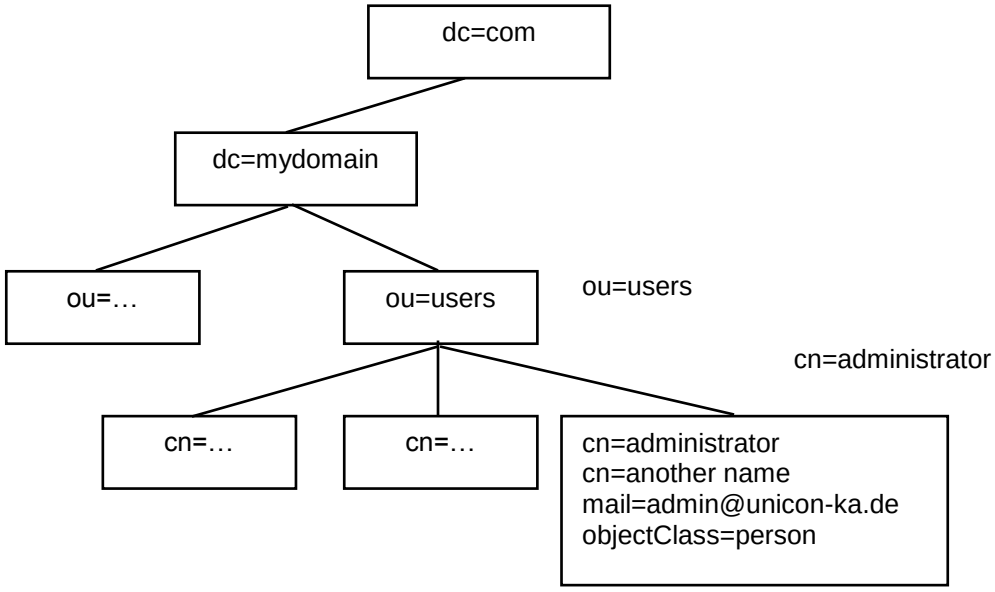


Figure 142: LDAP-based name space

For example, the DN for administrator is:

cn=administrator,ou=users,dc=mydomain,dc=de

The DN for users is:

ou=users,dc=mydomain,dc=de

The abbreviations before each equal sign in these examples mean:

`cn`	Abbreviation for “common name”. The value of this attribute is a string which is the name of an object. If the object corresponds to a person, it is typically the person's full name.
`dc`	Abbreviation for “domain component”. The value of this attribute is a string holding one component of a domain name. Case insensitive.
`ou`	Abbreviation for “organizational unit”. The value of this attribute is a string holding the name of a part of the organization.

The rules governing the construction of DNs can be quite complex and are beyond the scope of this document. For more information about DNs, see your server documentation and RFC 2253.

14.3.2 Search base

Accessing an LDAP- or ADS-based directory is accomplished by using a combination of DN, filter, and scope.

base DN:	Indicates where in the hierarchy to begin the search.
filter:	Specifies attribute types, assertion values, and matching criteria.
scope:	Indicates what to search: - the base DN itself - one level below the base DN - the entire subtree rooted at the base DN

You only need to enter the base DN (filter and scope are set automatically). For example, in Figure 142 setting the base DN to: `ou=users,dc=mydomain,dc=de` will search all levels below the entity "users".

Note: For advanced users, the filter and scope used are:

- Scope: the entire subtree rooted at the base DN ("sub").
- Filter: depends on the server:
  ADS: sAMAccountName=%s
  LDAP: uid=%s

where %s is replaced with the user name entered at login.

14.3.3 Determining values for search base, user-DN, version number

For the search base, DN and version of your authentication server, we recommend asking your LDAP or Active Directory administrator.

If your administrator is unavailable, it is still possible to determine the values using the following Thin Client-based method. Note: Knowledge of the LDAP/Active Directory server is required.

Overview:

1. Install the FPM "LDAP search module" ("usersearchldap") on the Thin Client. It is part of the "user authorization modules" EPM.
2. On the Thin Client, open a shell. Enter the following command (one line):

   ```
   ldapsearch -xLLL -b "" -s base -h <server> 'ObjectClass=*'
   defaultNamingContext supportedLDAPVersion namingContexts
   ```

   Where <*server*> is the IP address/name of your ADS/LDAP server.
3. The values returned are:

`defaultNamingContext`	search base (ADS)
`supportedLDAPVersion`	version number (LDAP version 3)
`namingContexts`	search base (LDAP version 3)
4. Further steps are required depending on whether you are using an LDAP server or ADS. These are described in detail below.

This Thin Client-based method works for ADS and LDAP version 3. This method does not work for LDAP version 2. For an alternative method that works with version 2, see "LDAP – Determining Server Version Number" in this section.

Active Directory – Determining Search Base

You must know the IP name/address of your ADS.

On the Thin Client, open a shell. Enter the following command (one line):

```
ldapsearch -xLLL -b "" -s base -h <server> 'ObjectClass=*'
defaultNamingContext supportedLDAPVersion namingContexts
```

The value that is returned for “defaultNamingContext” can be used for the **search base**. Example (server=”server1”):

```
bash$ ldapsearch -xLLL -b "" -s base -h server1 'ObjectClass=*'
defaultNamingContext supportedLDAPVersion namingContexts
dn:
defaultNamingContext: DC=server1,DC=unicon-ka,DC=de
bash$
```

In this example, you would enter “`DC=server1,DC=unicon-ka,DC=de`” in the **Base** field for ADS.

Active Directory – Determining User-DN

Once you have the search base, you can use it to find the value of the User-DN. In the shell on the Thin Client, enter the following command. The value of “defaultNamingContext” can be used for the search base. Format:

```
ldapsearch -xLLL -b "<search base>" -s base -h <server> 'ObjectClass=*'
managedBy
```

Continuing the example above, we use “`DC=server1,DC=unicon-ka,DC=de`” as our search base and server1 as our server:

```
bash$ ldapsearch -xLLL -b "DC=server1,DC=unicon-ka,DC=de" -s base -h
server1 'ObjectClass=*' managedBy
dn: DC=w2k,DC=unicon-ka,DC=de
managedBy: CN=Administrator,CN=Users,DC=w2k,DC=unicon-ka,DC=de
```

The value that is returned for “managedBy” is the **User-DN**. Enter the value for `managedBy` in the **User-DN** field for ADS. Alternatively, you can use any other member of the group ”Schema-Admins”.

LDAP – Determining Server Version Number

For an open LDAP server, on the Thin Client open a shell. Enter the following command (one line):

```
ldapsearch -xLLL -b "" -s base -h <server> 'ObjectClass=*'
defaultNamingContext supportedLDAPVersion namingContexts
```

The value of “supportedLDAPVersion” that is returned is the **version number**. Example (server=”server2”):

```
bash$ ldapsearch -xLLL -b "" -s base -h server2 'ObjectClass=*'
supportedLDAPVersion namingContexts
namingContexts: dc=unicon-ka,dc=de
namingContexts: o=Unicon Software GmbH,l=Karlsruhe,c=DE
supportedLDAPVersion: 2
supportedLDAPVersion: 3

bash$
```

If the command works, you have version 3 server. In this example, you could select either **Version 2** or **Version 3** from the **Version** field for LDAP. Both are supported by our server. If your server supports more than one version, we recommend you choose the latest version.

If the command does not work, you have version 2 server. The text returned is

```
LDAP V2
ldap_bind: Protocol error (2)
additional info: version not supported
--
ldapsearch -xLLL -b "" -s base -P 2 -h server2 'ObjectClass=*'
namingContexts supportedLDAPVersion
No such object (32)
```

LDAP – Determining Search Base

Version 3 Server

If you have version 3, the value for "namingContexts" that is returned can be used for the **search base**. All namespaces are returned, meaning there can be multiple entries, as in the example above:

```
namingContexts: dc=unicon-ka,dc=de
namingContexts: o=Unicon Software GmbH,l=Karlsruhe,c=DE
```

In this example, two search bases were returned. However, only one of these values is correct.

To determine which value is correct, in the shell enter the following command. Use the value of "namingContexts" for the search base to test. Format:

`ldapsearch -xLLL -b "`*<search base to test>*`" -a search -s sub -h` *<server>* `'uid=`*<a valid user ID>*`' uid`

<a valid user ID> is a user account on this server. Continuing the example above, we use "`o=Unicon Software GmbH,l=Karlsruhe,c=DE`" as our test search base, "server2" as our server and "smith" as our user-ID. If the search base is incorrect, you will receive a referral, as in the following:

```
bash$ ldapsearch -xLLL -b "o=UniCon Software GmbH,l=Karlsruhe,c=DE" -a
search -s sub -h server2 'uid=smith' uid
Referral (10)
Matched DN: O=UniCon Software GmbH,L=Karlsruhe,C=DE
Referral: ldap://server2.unicon-ka.de/dc=unicon-ka,dc=de
```

The value of "Referral" lists the correct value of the search base and server in the format: `ldap://`*<server>*`/`*<search base>*.

In this example, you would enter "`dc=unicon-ka,dc=de`" in the **Base** field for LDAP.

Version 2 Server

The ldapsearch command does not work with LDAP version 2, as we saw above. In this case, it is not possible to determine the search base using the Thin Client-based method.

However, it is still possible to determine the search base if you have access to the LDAP server configuration. Open the configuration file slapd.conf (the directory it resides in varies). The value of the parameter "suffix" can be used for the **search base**. Example:

```
suffix "dc=greenworm,dc=de"
```

In this example, you would enter "`dc=greenworm,dc=de`" in the **Base** field for LDAP.

Verify Your Values

ADS

To verify your values for ADS, use your values in the “ldapsearch” command. Use the following command (one line):

```
ldapsearch -xLLL -b '<search base>' -s sub -P <version> -h <server> -D '<user-DN>' -w '<password>' 'sAMAccountName='<a valid user-ID>' sAMAccountName
```

Example. Values to test:

user-DN	CN=Administrator,CN=Users,DC=w2k,DC=unicon-ka,DC=de
search base	DC=server1,DC=unicon-ka,DC=de
server	server1
user name	smith
password	12345
version	3

```
bash$ ldapsearch -xLLL -b 'DC=server1,DC=unicon-ka,DC=de' -s sub -P 3 -h server1 -D 'CN=Administrator,CN=Users,DC=w2k,DC=unicon-ka,DC=de' -w '12345' 'sAMAccountName='smith' sAMAccountName

dn: CN=John Smith,CN=Users,DC=server1,DC=unicon-ka,DC=de

sAMAccountName: smith


#refldap://w2k.unicon-ka.de/CN=Configuration,DC=s2k,DC=unicon-ka,DC=de

bash$
```

If the parameters are correct, the request will return the user-DN for smith (“dn”) and the user name that we entered (“sAMAccountName”).

LDAP

To verify your values for LDAP, you must know the name of a user on this server. Use the following command (one line):

```
ldapsearch -xLLL -b '<search base>' -s sub -P <version number> -h <server> 'uid=<a valid user-ID>' uid
```

Example. Values to test:

user-DN	dc=unicon-ka,dc=de
server	server2
user name	smith
version	3

```
bash$ ldapsearch -xLLL -b 'dc=unicon-ka,dc=de' -s sub -P 3 -h server2 'uid=smith' uid

dn: uid=smith,ou=employees,dc=unicon-ka,dc=de

uid: smith

bash$
```

If the parameters are correct, the request will return the user-DN for smith (“dn”) and the user name that we entered (“uid”).

14.4 X Application Resource File

The properties of X applications are set in their resource file. This file is located on the Thin Client in the directory:

`/usr/X11R6/lib/X11/app-defaults/`<*X application name*>

For example:

- XTerm /usr/X11R6/lib/X11/app-defaults/XTerm

You can set properties for all X applications by creating a system resource file.

You can use an application resource file from one of the X applications on the Thin Client as a template (located in /usr/X11R6/lib/X11/app-defaults/"). However, copy only the parameters you need and not the entire file!

⇨ To create a system resource file for all devices

This transfers a resource file to all devices currently managed by Scout Enterprise.

1. Create the resource file Xdefaults(without period) using a UNIX editor.
2. Enter only the parameters you wish to configure.
3. Save the file to the Scout Enterprise installation directory (default: "…\Unicon\scoutng\Xdefaults").
4. The file will automatically be transferred to all devices and saved to `/setup/.Xdefaults`.

The file must be located in the Scout Enterprise installation directory with the name Xdefaults.

⇨ To create a system resource file for selected devices

This transfers a resource file to all devices in an element (organisation unit, individual device).

1. Create a resource file using an a UNIX editor. The name is arbitrary, for example, "resource".
2. Enter only the parameters you wish to configure.
3. Save the file to the Scout Enterprise installation directory (default: "…\Unicon\scoutng").
4. Transfer the resource file to the Thin Clients using the File List function in Scout Enterprise to the Thin Client with the destination name ".Xdefaults" (with period) and destination directory /setup. Example:
   Source: `resource`
   Destination: `/setup/.Xdefaults` (with period)

To use the File List feature, the source file in the Scout Enterprise installation directory may not be named Xdefaults.

14.5 Port Assignments

The following is a list of TCP/IP ports for eLux and Scout Enterprise. The port numbers are fixed. Exceptions are indicated with a footnote.

eLux NG

Port	Type	Description	How to Deactivate	Port Type
	ESP	VPN (Cisco)	Uninstall the package Cisco Systems VPN client" (cisco_vpnclient)	Incoming
	ESP	VPN (Cisco)	Uninstall the package Cisco Systems VPN client" (cisco_vpnclient)	Outgoing
21	TCP	Updating via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	3270, 5250, 97801 emulations and telnet sessions		Outgoing
37	TCP	Time server – RFC 868	Do not configure a time server (**Setup** > **Desktop**)	Outgoing
37	UDP	Time server – RFC 868	Do not configure a time server (**Setup** > **Desktop**)	Outgoing
53	TCP	DNS server (Windows)		Outgoing
53	UDP	DNS server		Outgoing
67	UDP	DHCP server		Outgoing
68	UDP	DHCP client (or BootP client)	Configure a local IP address (**Setup** > **Network**)	Incoming
69	UDP	TFTP server (only used during a Recovery Installation)		Outgoing
69	UDP	TFTP server (only used during a Recovery Installation)		Incoming
80	TCP	Updating using HTTP (and proxy port, if used)		Outgoing
102	TCP	Emulations to BS2000 mainframes		Outgoing
111	UDP	Port mapper – drive access on NFS servers. Works with NFSD drive access (port 2049) and mountd (random)	Uninstall the FPM Drive Support(automount) in baseOS	Outgoing
111	TCP	Port mapper – RPC internal use only. Works with nlockd (random)	Uninstall the FPM Drive Support(automount) in baseOS	Incoming
139	TCP	SMB drive mapping (NetBIOS) and SMB user authentication	Uninstall the FPM Drive Support(automount) in baseOS and the package User authorisation modules(userauth)	Outgoing
139	UDP	SMB drive mapping (NetBIOS) and SMB user authentication	Uninstall the FPM Drive Support(automount) in baseOS and the package User authorisation modules(userauth)	Outgoing

Port	Type	Description	How to Deactivate	Port Type
161	UDP	SNMP	Uninstall the package net-snmp" (snmp)	Incoming
161	UDP	SNMP	Uninstall the package net-snmp" (snmp)	Outgoing
162	UDP	SNMPTRAP		Outgoing
177	UDP	XCMCP protocol		Outgoing
389	TCP	LDAP user authentication		Outgoing
500	UDP	VPN (Cisco)	Uninstall the package Cisco Systems VPN client" (cisco_vpnclient)	Incoming
500	UDP	VPN (Cisco)	Uninstall the package Cisco Systems VPN client" (cisco_vpnclient)	Outgoing
514	TCP	Shell, RSH applications		Outgoing
515	TCP	Printing over LPD		Outgoing
515	TCP	Printing over LPD	Cannot be deactivated, in the future can be deactivated by uninstalling the package Printer support"	Incoming
631	TCP	CUPS (IPP) print client	Uninstall the package CUPS Druckclient(qtcups)	Outgoing
631	UDP	CUPS (IPP) print client	Uninstall the package CUPS Druckclient(qtcups)	Outgoing
2049	UDP	NFSD drive access NFS	Uninstall the FPM Drive Support(automount) in baseOS	Outgoing
5681	TCP	Scout NG management port	Cannot be deactivated	Incoming
5900	TCP	Mirroring eLux NG desktop	Disable mirroring (**Setup** > **Security**) or uninstall the EPM eLux mirroring(mirror)	Incoming
5901	TCP	Mirroring first XDMCP session	Disable mirroring (**Setup** > **Security**) or uninstall the EPM eLux mirroring(mirror)	Incoming
5902	TCP	Mirroring second XDMCP session	Disable mirroring (**Setup** > **Security**) or uninstall the EPM eLux mirroring(mirror)	Incoming
6000	TCP	Remote X11 applications	Click to deselect the check box Allow remote X11 clients (**Setup** > **Security**)	Incoming
6001	TCP	First XDMCP session		Incoming
6002	TCP	Second XDMCP session		Incoming
7100	TCP	Font server[1]		Outgoing
22123	TCP	Scout Enterprise Manager (secure)		Incoming
22123	TCP	Scout Enterprise Manager (secure)		Outgoing
7777	TCP	Scout manager		Incoming
7777	TCP	Scout manager		Outgoing
9100	TCP	Direct Print to parallel port[2]	Deactivate the check box TCP direct print(**Setup** > **Printer**).	Incoming
9101	TCP	Direct Print to USB port[2]	Deactivate the check box TCP direct print(**Setup** > **Printer**).	Incoming

[1] Port number can be assigned by the administrator in eLux NG starter (**Setup** > **Screen** > **Advanced**)

[2] Port number can be assigned by the administrator in eLux NG starter (**Setup** > **Printer**).

Scout Enterprise Server

Port	Type	Description	How to Deactivate	Port Type
7778	TCP	Scout Enterprise Console		Incoming
7779	TCP	Wake-on-LAN gateway		Outgoing

15 Functionality for Clients with WindowsCE, XPe/WES7, eLux NG / eLux® *RL*

The following pages show the majo differences of the Scout features between the 3 operating systems. Mostly affected are the configuration and properties of devices as well as the application definition.
Features which have not been mentioned are available for all the 3 operating systems without restriction.

Feature	CE	XPe/ WES7	eLux	Remarks
Boot Procedure				
Manager via DHCP Options 222/223	X	X	X	
Manager via Vendor-DHCP Options 1/2	X		X	XPe/WES7: Vendor Options do not work
Manager via Vendor-DHCP Options 222/223	X		X	XPe/WES7: Vendor Options do not work
Manager via DNS	X	X	X	
Host name via DHCP	X	X	X	
Host name via reverse DNS	X	X	X	
First Contact dialog	X	X	X	
Boot in VGA mode	X	X	X	CE: Shift key must be held during boot. XPe/WES7: Works via XP boot (F8-key)
Device Hotkeys				
Ctrl-Alt-Home (Device password)	X	X	X	
Ctrl-Alt-End (Connection manager)	X	X		
Ctrl-Alt-Up (Previous active session)	X	X		
Ctrl-Alt-Down (Next active session)	X	X		
Device Control				
Application Upload			X	
Update	X	X	X	
Switch ON	X	X	X	
Switch OFF	X	X	X	

Feature	CE	XPe/ WES7	eLux	Remarks
Restart of desktop	X	X	X	CE: implemented as 'Restart of device' XPe/WES7: implemented as 'Logoff'
Restart of device	X	X	X	
Factory reset	X	(X)	X	XPe/WES7: delicate. It is easier to re-flash the device.
Send message	X	X	X	
Mirroring	X	(X)	X	XPe/WES7: RealVNC must be installed on the device as service, and winvnc4.exe must be replaced by a special version.
Device Configuration - Network				
DHCP	X	X	X	
DHCP Timeout			X	
BOOTP	X	X	X	CE/XPe/WES7: implemented as DHCP
IP-Address - IP-Address	X	X	X	
IP-Address - Subnet Mask	X	X	X	
IP-Address - Gateway	X	X	X	
IP-Address – Host name	X	X	X	
IP-Address - Domain	X	X	X	
IP-Address – DNS Server	X	X	X	
Advanced Settings			X	
Device Configuration - Screen				
640 x 480	X	X	X	XPe/WES7: not 56Hz, not 66Hz
800 x 600	X	X	X	XPe/WES7: not 66Hz
1024 x 768	X	X	X	XPe/WES7: only 56Hz, not 66Hz
1152 x 864	X	X	X	XPe/WES7: only 60Hz and 75Hz
1280 x 1024	X	X	X	XPe/WES7: only 60Hz, 75Hz and 85Hz
1440 x 900			X	
1600 x 1200	X	X	X	XPe/WES7: not 56Hz
1680 x 1050			X	
1920 x 1200	X	X	X	CE: not 90Hz, not 100Hz XPe/WES7: only 60Hz
56 Hz		X	X	
60 Hz	X	X	X	
66 Hz		X	X	
70 Hz	X	X	X	
75 Hz	X	X	X	
80 Hz			X	
85 Hz	X	X	X	
90 Hz	X		X	
100 Hz	X	X	X	
8 Bit color depth	X	X	X	
16 Bit color depth	X	X	X	
24 Bit color depth	X	X	X	CE/XPe/WES7: 32Bit
Powersave function	X	X	X	
Screensaver	X	X	X	XPe/WES7: The image of Fujitsu Siemens does not contain a screensaver
Screensaver – Password protection		X	X	

Feature	CE	XPe/ WES7	eLux	Remarks
Screensaver - Settings			X	
Advanced Screen settings			X	
Device Configuration - Security				
Setup	X	X	X	CE/XPe/WES7: Call of Control Panel is blocked.
Configuration	X	(X)	X	XPe/WES7: The configuration of a local session is not implemented. Therefore this feature has no effect.
All other features			X	
Device Configuration - Firmware				
Protocol: HTTP	X	X	X	
Protocol: FTP	X	X	X	
Protocol: file			X	
Server	X	X	X	
Proxy	X	X	X	
Proxy-Port	X	X	X	
Path	X	X	X	
User	X	X	X	
Password	X	X	X	
Image file	X	X	X	CE: Files of the format "Flash*.bin" are transferred as complete flash image, all other files are transferred as 'Ship.bin' (CE image file). XPe/WES7: Only complete flash images can be transferred.
Check for Update during start	X	X	X	
Confirmation of Update required	X	X	X	
Device Configuration - Multimedia				
Volume – Over-all	X	X	X	
Volume - PCM		X	X	
Volume - microphone		X	X	
Microphone – Sound off		X	X	
Use audio in XDMCP sessions			X	
Device Configuration - Desktop				
Language	(X)		X	CE: switches the format of numbers, currency, date and time to the selected language. The description always is in English.
Background	X	X	X	
Task Hotkey			X	
Time zone	X	X	X	
Time server	X	X	X	
Time server Windows/Unix switching			X	
Theme	(X)		X	CE: The theme 'XP' switches from the thin client shell to standard shell.
Background image	X	X	X	CE/XPe/WES7: always as complete picture
Taskbar - Show			X	

Feature	CE	XPe/ WES7	eLux	Remarks
Taskbar – Always on top	X	X	X	
Taskbar – Hide automatically	X	X	X	
Taskbar – Show clock	X	X	X	
Autostart Starter			X	
Workspaces			X	
Device Configuration - Drives				
Defined drives	X	X	X	XPe/WES7: "Directory" corresponds to drive letter.
Browser home directory	X	X	X	CE/XPe/WES7: If at least one start page is defined in a browser session, this setting is ignored.
Device Configuration - Printer				
Network printer	X	X	X	CE/XPe/WES7: no filter
Parallel port printer	X	X	X	CE/XPe/WES7: no filter
Serial port printer	X	X	X	CE/XPe/WES7: no filter
USB port printer	X	X	X	CE/XPe/WES7: no filter
Maximum printer response time			X	
Print service activated	X		X	
TCP Direkt print			X	
CUPS			X	
Thin Print Mode	X		X	
Device Configuration - Mouse/Keyboard				
Mouse: Type			X	
Mouse: Double click speed	X	X	X	
Mouse: Acceleration	X	X	X	
Keyboard: Language	X	X	X	
Keyboard: Delay	X	X	X	
Keyboard: Speed	X	X	X	
Advanced: 3-button emulation			X	
Advanced: Left hand	X	X	X	
Advanced: Deadkeys			X	
Advanced: Numlock	X	X	X	
Advanced: Console switching activated			X	
Device Configuration - Hardware				
USB mass storage devices	X	X	X	
Network type			X	
Speed	X	X	X	CE/XPe/WES7: Nicht BNC / AUI
Card reader			X	
Multiple monitors			X	
Ramdisk			X	
COM Port settings			X	
Device Configuration - Info				
Name	X	X	X	
Info1-3	X	X	X	
WakeOnLan - Server			X	

Feature	CE	XPe/ WES7	eLux	Remarks
Device Configuration - Drucker				
Printer driver name	X	X	X	
Default printer	X	X	X	
A copy as 'lp'			X	
Device Configuration - VPN-Client				
VPN Client type: F-Secure			X	
VPN Client type: FreeS/WAN			X	
VPN Client type: Cisco VPN Client			X	
VPN Client type: PPTP VPN Client	X	X	X	
Server	X	X	X	
User	X	X	X	
Password	X	X	X	
Domain	X	X	X	
Deactivate local network	X	X	X	XPe/WES7: Default Gateway Router is not deleted, but set to Metric 21.
Device Configuration - Rules				
Logoff the current user			X	
Restart of device			X	
Switch off device	X	X	X	
Lock device			X	
Terminate VPN tunnel			X	
Application ICA				
Published application	X	X	X	
Server	X	X	X	
Application	X	X	X	
Work directory	X	X	X	
User name	X	X	X	
Password	X	X	X	
Domain	X	X	X	
Allow smartcard Logon		X	X	
Roaming			X	
Application restart	X	X	X	
Start automatically	X	X	X	
Desktop icon	X	X	X	
Options: Use data compression	X	X	X	
Options: Insert with mouse wheel click			X	
Options: Store bitmaps to harddisk	X	X	X	
Options: Enable sound	X	X	X	
Options: Sound quality	X	X	X	
Options: Enable audio port			X	
Options: Encryption grade	X	X	X	
Options: Allow automatic Logon	X	X	X	
Options: SpeedScreen	X	X	X	
Options: SpeedScreen-Mouseclick Feedback	X	X	X	

Feature	CE	XPe/ WES7	eLux	Remarks
Options: SpeedScreen – Local text echo	X	X	X	
Connection: Network Protocol			X	
Connection: Server Group			X	
Window: window colors	X	X	X	
Window: window size	X	X	X	
Firewall: none			X	
Firewall: Browser settings	X	X	X	
Firewall: HTTPS			X	
Firewall: SOCKS			X	
Proxy address			X	
Auto-Reconnect: enable Auto-Reconnect			X	
Auto-Reconnect: max. number of attempts			X	
Auto-Reconnect: elapse time			X	
File types: File types			X	
Application RDP				
Server	X	X	X	
Application	X	X	X	
Work directory	X	X	X	
User name	X	X	X	
Password	X	X	X	
Domain	X	X	X	
Roaming			X	
Application restart	X	X	X	
Start automatically	X	X	X	
Desktop icon	X	X	X	
Display: window size	X	X	X	
Display: colors	X	X	X	
Local resources: Drives	X	X	X	CE/XPe/WES7: If the minimum of one drive is enables, all the local drives will be available.
Local resources: Printer	X	X	X	
Local resources: smartcard	X	X	X	
Local resources: sound	X	X	X	
Local resources: Serial Ports	X	X	X	CE/XPe/WES7: Mapping is ignored.
Local resources: Parallel Ports			X	
Advanced: Protocol			X	
Advanced: Keyboard language			X	
Advanced: Switch on compression			X	
Advanced: Disable Windows decorations	X	X	X	
Advanced: Disable encryption			X	
Advanced: Disable mouse movements			X	
Advanced: Show connection bar when full screen	X	X	X	
Application Browser				
Start page	X	X	X	CE/XPe/WES7: If a start page is set in several sessions, the last session makes use of it.
Page to be called	X	X	X	

Feature	CE	XPe/ WES7	eLux	Remarks
Proxy settings	X	X	X	CE/XPe/WES7: If a proxy is set in several sessions, the last session makes use of it. No automatic configuration.
Browser type			X	
Kiosk mode	X	X	X	
Application restart	X	X	X	
Start automatically	X	X	X	
Desktop icon	X	X	X	
Local Application				
Local Application: User-defined	X	X	X	
Local Application: Resource Info			X	
Local Application: XTERM		X	X	XPe/WES7: Starts "cmd.exe".
Local Application: SSH			X	
Local Application: File manager		X	X	XPe/WES7: Starts "explorer.exe".
Local Application: Text editor		X	X	XPe/WES7: Starts "notepad.exe"
Local Application: Movie Player	X	X	X	CE/XPe/WES7: Starts Windows Media Player.
Local Application: Thunderbird			X	
Hidden		X	X	
Application restart	X	X	X	
Start automatiacally	X	X	X	
Desktop icon	X	X	X	
CE/XPe/WES7 GUI Advanced Functions				
Information page (diagnosis)	X	X		CE: Go to 'Setup Device' rsp. <F2> XPe/WES7: As a tab in the Connection Manager
Diagnosis page	X	X		CE: Go to 'Setup Device' rsp. <F2> XPe/WES7: As a tab in the Connection Manager
All sessions available in the start menu	X	X		CE: Go to "Programs→ Connections" XPe/WES7: Go to "Start→ All Programs → Connections"
Connection Manager Icon on the desktop	X	X		