eLux® *RL* – eLux® Lite
Embedded Linux for Thin
Clients *Reloaded*
Version 3

Administrator's Guide
Build # 11 – August 2011

UniCon Software GmbH

Contents

Table of Figures

1 Before You Begin

This manual is for system administrators responsible for installing, configuring, deploying and maintaining Embedded Linux *Reloaded* (eLux® *RL*), and for experienced users. 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 servers

eLux® *RL* is an embedded operating system based on Linux. However, no significant knowledge of Linux is needed for either the administrator or the end user.

For detailed information please click on "Details" next to the eLux software packages in the Download area on www.myelux.com.

1.1 About this Guide

This guide describes the basic structure of eLux® *RL* and provides the steps to installation and configuration of an eLux® *RL* client. For further information on Scout Enterprise and ELIAS please consult

- the Scout Enterprise Administrator's Guide to manage the eLux® *RL* clients centrally, including the instructions to the eLux Image Administration Service (Elias), a supplementary tool to edit the image definitions files.
- Further information can be found in the ealier Administrator's Guides to eLux NG

1.2 eLux® *RL* in the World Wide Web

UniCon offers online technical support at www.myelux.com.

In the download area > eLux software packages you find

- all available eLux software packages
- the latest updates and hotfixes
- A list of supported client hardware
- A list of supported hardware components and screen resolutions
- > Manuals and Documentation: A current version of this document and other manuals in PDF

2   Installation

eLux® *RL* can be installed on the Compact Flash of a Thin Client or on a hard disk.

The installation (recovery) can be performed in different ways:

- From USB stick ("eLux RL Live Stick" Image on www.myelux.com)
- From CD ("eLux RL Live CD" ISO-Image on www.myelux.com)
- Via PXE Boot

These recovery procedures are described in detail in our Recovery Paper (www.myelux.com) and in our Scout Enterprise Administrator's Guide.

2.1   First Boot Procedure

This is the boot procedure for a Thin Client *with default settings* (upon delivery, after a factory reset, or after a Recovery Installation):

1. Scan BIOS

2. Check if a LAN (Ethernet) connection is available
   If none is found, an error message is displayed, eLux® *RL* is booted, and the First Configuration Wizard appears, allowing the user to set initial user settings. Go to step 6.

3. Make a DHCP server request
   If a DHCP server is not found, an error message is displayed, eLux® *RL* is booted, and the user is asked to enter the network information manually. Go to step 6.

4. Boot eLux® *RL*

5. The device is automatically entered in *Scout Enterprise* and configured. Requirement: The hostname "ScoutSrv" has been set to the *Scout Enterprise* Server IP address on the DNS server.
   If the hostname "ScoutSrv" cannot be resolved, this step is skipped.

6. First Contact: A Wizard appears, helping the user through the initial configuration.

This procedure does not apply to subsequent boots.

2.2 First Configuration Wizard

By default, the first time the Thin Client successfully boots, a Wizard appears to help you through the configuration process.

You have the choice between entering the device in the management software *Scout Enterprise* or configuring it manually.

If a DHCP server was contacted, the IP address is displayed at the top. Otherwise, a default value is displayed.

2.2.1 Management

2.2.1.1 Step 1: Activate Manager

The *Scout Enterprise* server that manages the Thin Clients is referred to as the "manager".

If the device is to be managed and the IP address of the *Scout Enterprise* server is known, select **Yes**.

If the Thin Client will not be managed, you can still configure the device manually. Select **No.**
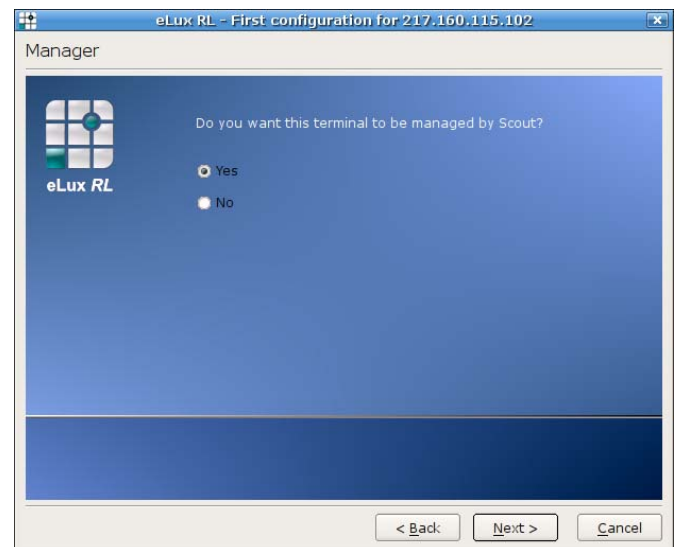
Figure 1 First Configuration Wizard: Activate Manager

2.2.1.2 Step 2: Manager Address

Enter the IP address or name of the Scout Enterprise manager.

Entering information in the Information fields is optional.

Click **Next**.
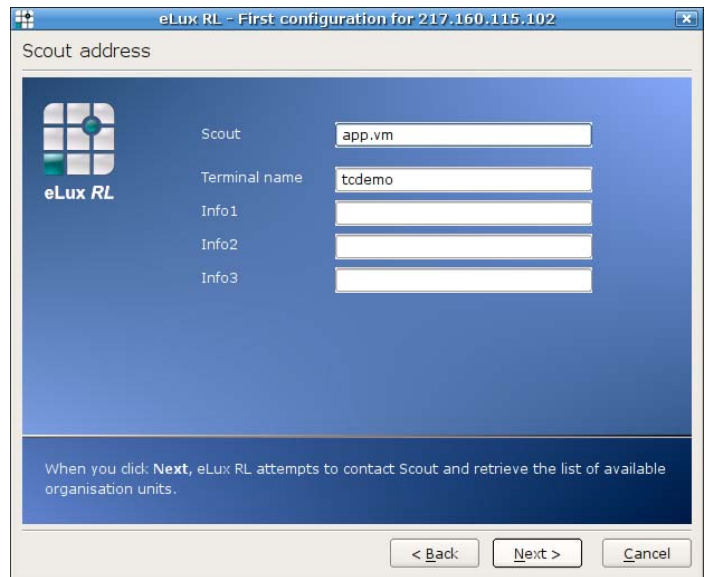
Figure 2 First Configuration Wizard: Manager Address

2.2.1.3 Step 3: Manager Groups

Next, you are asked to select the destination group of the device on the Scout Enterprise server. Default is Lost&Found (ID=0)..
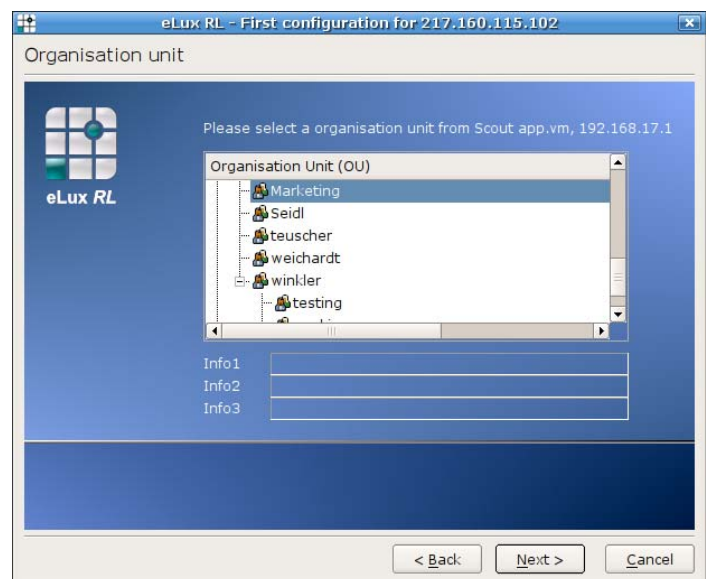
Figure 3 First Configuration Wizard: Manager Groups

2.2.1.4 Step 4: Summary

Finally, you are given a summary of the entered information.

When you click **Next**, the device is registered in the Scout Enterprise Server, entered in the destination organization unit, and restarted. Upon boot, it contacts Scout Enterprise and downloads its configuration and application definitions. In addition, you can configure Scout Enterprise to automatically update the software.

If a profile for this device already exists in Scout Enterprise, the device will not change Groups. Rather, its status in Scout Enterprise will be updated and it will receive the configuration of the existing profile.
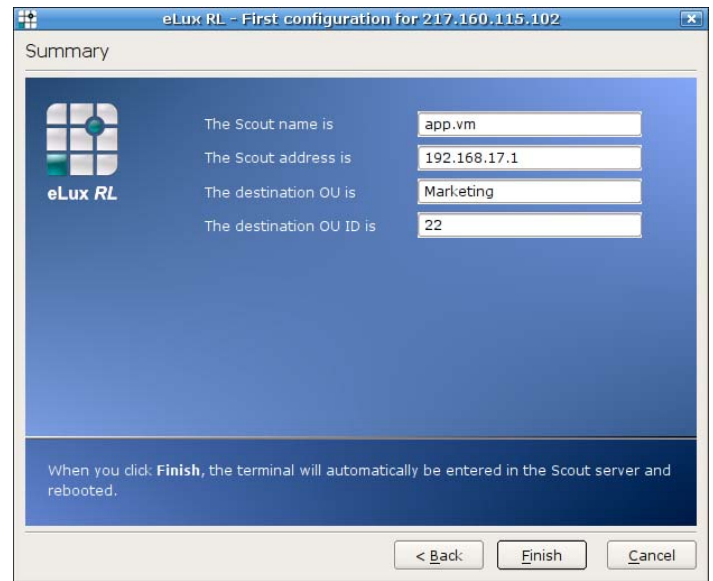
Figure 4 First Configuration Wizard: Summary

For more information on the management software Scout Enterprise, see the *Scout Enterprise Administrator's Guide*.

3 Setup

Setup contains the following tabs:

- General
- Network
- Desktop
- Screen
- Mouse/Keyboard
- Firmware

Click the ► symbol to display the other setup tabs:

- Security
- Multimedia
- Drives (if drive support has been installed)
- Printer (if printer support has been installed)
- Hardware
- VPN (if VPN Client installed)
- Diagnostics.

Setup provides all parameters. For a "quick" start minimum configurations are required in the tabs **Desktop, Mouse/Keyboard, Screen** and **Network, Hardware** as well as in **Configuration.** The **desktop language** and **keyboard** as well as **mouse type** have already been defined by the First Configuration Wizard.

All modifications have to be confirmed or not confirmed by the button **Apply** or **Reset**.

- Click **Reset** to cancel the modifications just entered.
- Click **Apply** for modifications to take effect.

Some modifications will request a restart of the desktop or of the client. In this case a message will appear after having saved the modifications by clicking **Apply: "The changes require a new start of the user interface? Continue?"**

Confirm with **Yes** or **No**.

The following chapters provide a detailed description of the parameter settings in the SETUP tabs in the order displayed.

3.1 General

In the **General** tab you can find the thin client's MAC address, license number, host ID and related hardware information.
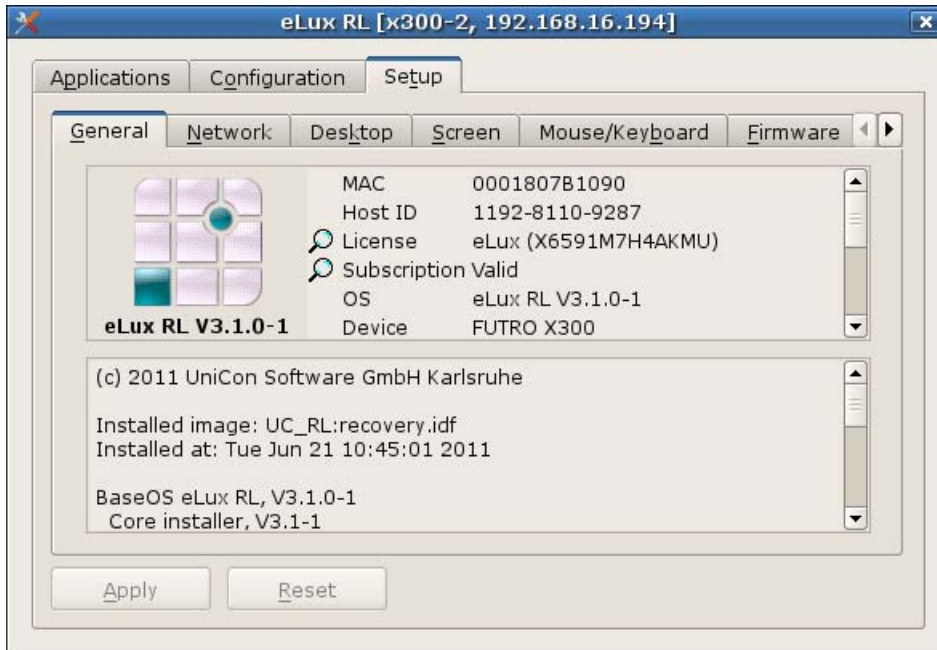
Figure 5 Setup > General

Go to the scroll box to find the name of the installed image, as well as a list of the software packages installed on the Thin Client's flash card (including version numbers). A double-click on "**License**" opens the dialog offering the **manual** entry of a license or to request a license from the server.

By clicking the button "**More**" a license can be entered manually or requested from the server.

Figure 6 eLux® *RL* License Information

3.2   Network

Up to this version of eLux RL only 1 network profile could be configured, now different profiles may be configured simultaneously, e.g. Ethernet, WLAN, UMTS. These are provided at the client and the most convenient way is to select them via the systray icon at the clilent.

In particular for mobile clients the multiple configuration of network profiles provides higher flexibility.
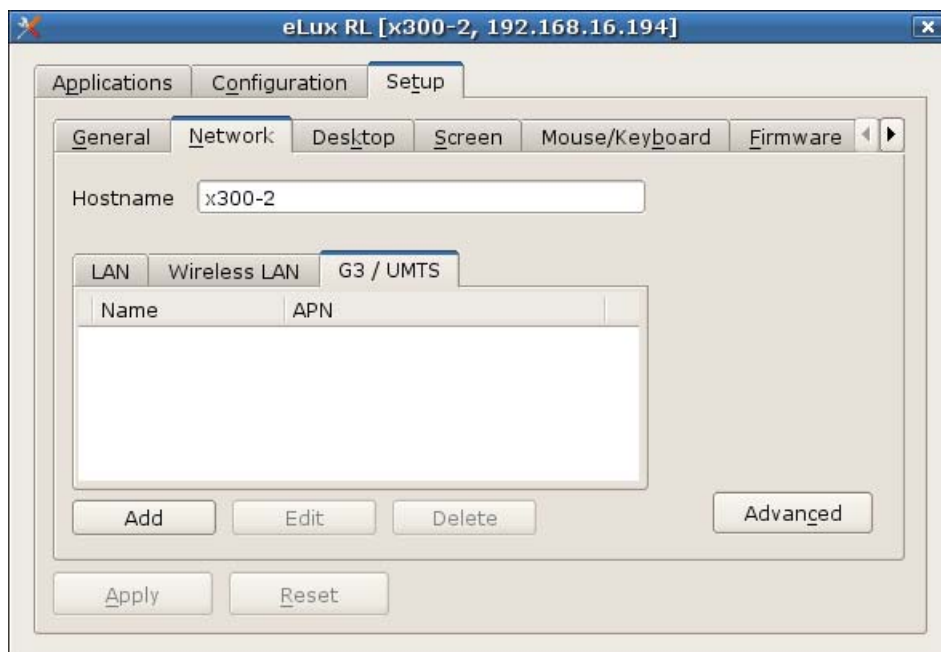
Figure 7 Setup > Network

According to your installed hardware the **network** tab may contain the following subtabs:

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

Click **Add** to define network profiles.

3.2.1 LAN

Depending on your hardware platform you can connect to a local-area network using the onboard Ethernet card, a network interface card, or an adapter card for fiber optic.

Select the **Ethernet** speed from the **Speed** list. If **Auto** does not work, see your network administrator for the correct speed.

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

- **AUI, BNC**: Only available for the 3Com® Combo Network Interface Card.
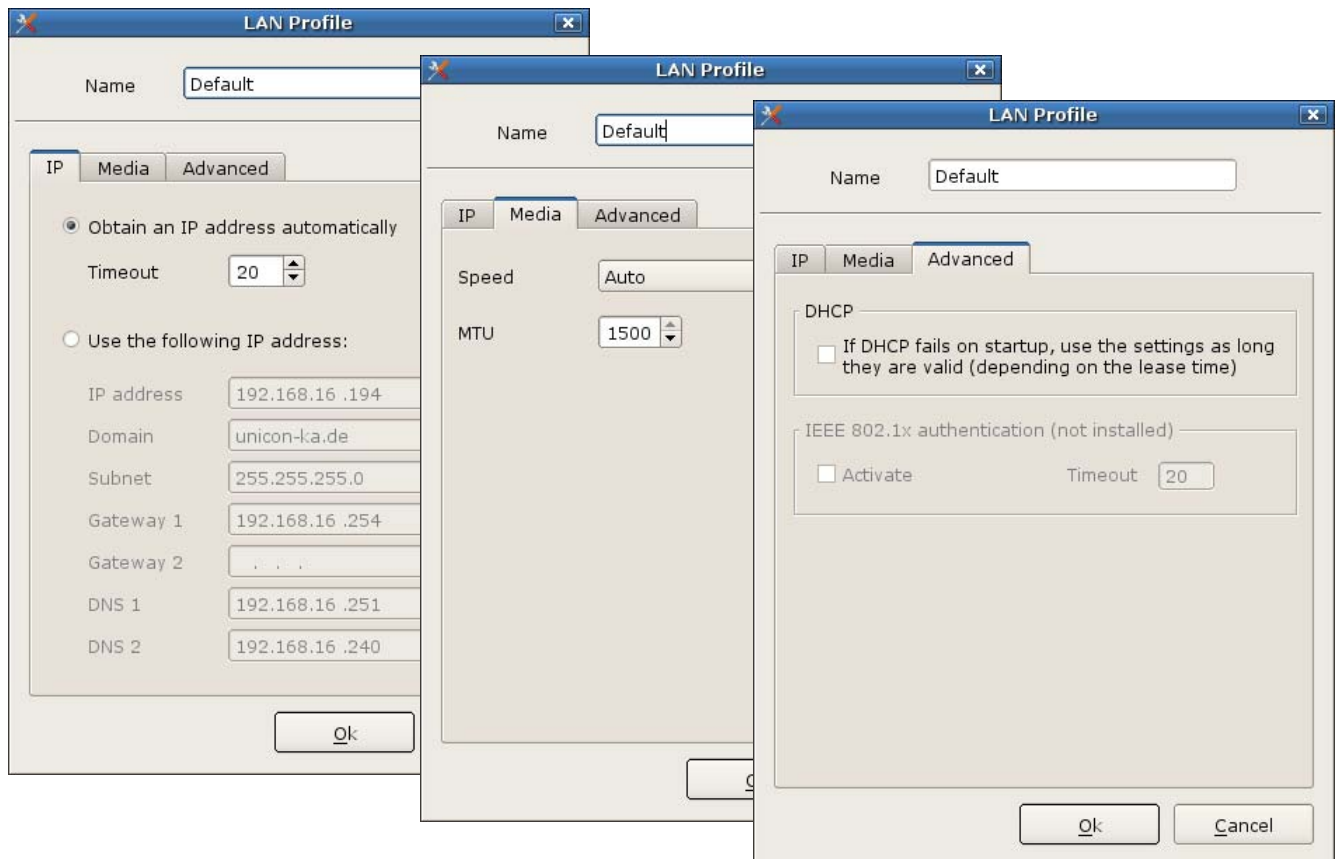
3.2.1.1 IEEE 802.1x Authentication (Xsupplicant)

802.1x is an IEEE standard specifying the port-based network access control (on layer 2 of the ISO/OSI reference model) for IEEE 802 networks. The network access in 802-LANs is done via ports (physical port in a switch). IEEE 802.1x enables the protection of a network from the access by unauthorized devices via controlled ports and the authentication on a RADIUS-Server implementation (RADIUS = Remote Authentication Dial-In User Service).

Both the activation of IEEE 802.1x and the installation of the Xsupplicant firmware is described in detail in our latest *Scout Enterprise Administrator's Guide.*

3.2.2 Dynamic Host Configuration Protocol (DHCP)

A Dynamic Host Configuration Protocol (DHCP) server assigns to the client a dynamic IP address. This means that the IP address assigned to the Thin Client changes periodically (the interval is set on the DHCP server). DHCP also supports a mix of static and dynamic IP addresses. DHCP simplifies network administration because the server and not an administrator assigns IP addresses – when a new Thin Client is added to the network, it automatically receives an IP address and network settings. Due to its flexibility, most networks use DHCP.

1. From the **Setup** tab, click the **Network** sub tab.
2. Select **DCHP**. You can also set a time-out in seconds. The default is 20 seconds.
3. (optional) Enter a local hostname. It will be transferred to the server upon boot if server settings permit (a hostname may not yet be defined on the server).
4. Click **Apply** and **Yes** in the eLux® *RL* dialog box regarding restart.

If a server is not found within the defined time, it uses the settings saved from the previous session.

3.2.3 Bootstrap Protocol

A Bootstrap Protocol (BootP) server assigns to the client a static IP address. This means that the IP address assigned to the Thin Client is fixed. A BootP server is more work for the administrator, because the administrator must configure the server when a new Thin Client is added to the network.

1. From the **Setup** tab, click the **Network** sub tab.
2. Select **BOOTP**. The BootP standard time-out is a fixed 10 seconds.
3. (optional) Enter a local hostname. It will be transferred to the server upon boot if server settings permit (a hostname may not already be defined on the server).
4. Click **Apply** and **Yes** in the eLux *RL* dialog box regarding restart.

If a server is not found within the defined time, it uses the settings saved from the previous session.

3.2.4 Manual Entry

If you do not have one of the above servers, you can enter the IP address and network information directly on the terminal.

1. From the **Setup** tab, click the **Network** sub tab.
2. Click **Manually**.
3. Enter the IP address, subnet mask, host name and domain.
4. To enter a gateway (router) address, click the **Add** button below **Gateway**.
   - Enter the IP address in the dialog box. Click **OK**.
   - Repeat until you have entered all gateway addresses.
   - To delete a gateway entry, select it from the **Gateway** list and click **Delete**. Click **Yes** in the eLux RL dialog box.
   - To change the order, you must delete and re-enter the IP addresses.
5. To enter the IP address of a domain name server, click the **Add** button below **DNS**.
   - Enter the IP address in the dialog box. Click **OK**.
   - Repeat until you have entered all DNS addresses.
   - To delete a DNS entry, select it from the **DNS** list and click **Delete**. Click **Yes.**
   - To change the order, you must delete and re-enter the IP addresses.
6. Click **Apply** and **Yes** in the eLux *RL* dialog box regarding restart.

To avoid network conflicts, verify that the IP address you enter is not in use by another machine or assigned to a DHCP pool.

Those are the three ways to enter the IP address and network information on a Thin Client. The following two sections describe advanced features, such as how to set the client hostname on the DHCP server using the terminal or how to set a local hosts list.

3.2.5 Setting the Host Name via DHCP

With a DHCP request it is possible to transfer the local host name to the DHCP. The host name will then be visible at the DHCP server.

1. Click **Manually**.
2. Enter the host name of the Thin Client in the field **Hostname** and click **Apply**. The remaining fields should stay empty – they are automatically set by the DHCP server.
3. Click **No** in the eLux RL dialog asking for restart.
4. Click **DHPC**.
5. Click **Apply**.
6. Click **Yes** in the eLux *RL* message box asking for restart.

3.2.6 Wireless LAN

Note:

You find a list of the Wireless LAN products supported by eLux on www.myelux.com - **in the Download Area** click on **Hardware Components.**

The following Wireless LAN settings are possible.

(1) WEP
(2) WPA (PSK)
(3) WPA2 (PSK)
(4) WPA2 (EAP)
(5) IEEE 802. 1x (LEAP)
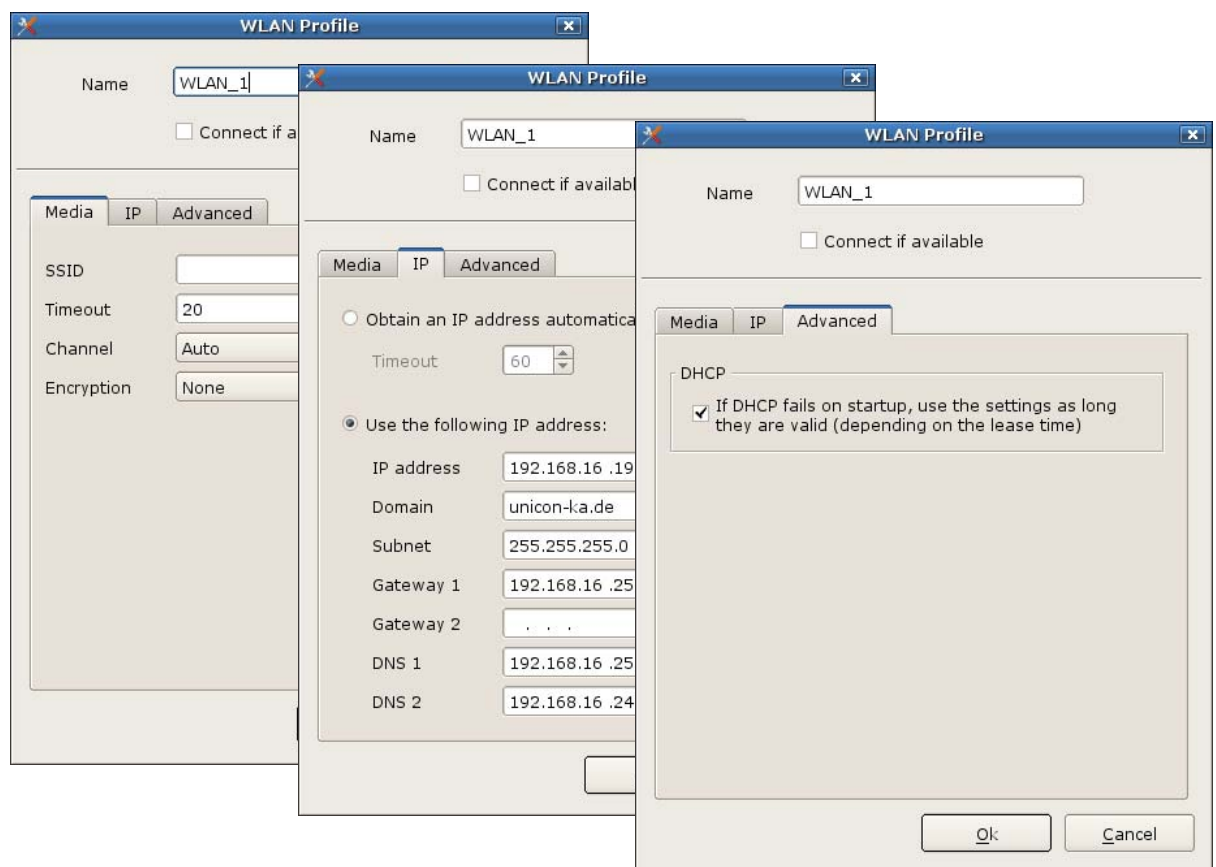
Figure 8: Configuration > Network > WLAN Profiles

eLux *RL* supports different hardware adapters to use WLAN (see www.myelux.com > Download area > eLux software packages > eLux RL > Hardware components). It is not necessary to disable the onboard Ethernet controller in the Thin Client's BIOS Setup. This feature is not available for all hardware platforms, though.

Note: The two status LEDs (Power/Activity) on the card are switched off as soon as the driver is being loaded, because the driver does not support them. However, this has no influence on the functionality.

Enabling wireless LAN on your device involves the following:

1. Installing the required firmware
2. Inserting the card
3. Configuring network hardware settings and entering the WEP key for encrypted transfer

⇨ **To install the wireless LAN firmware**

To use wireless LAN you must install the following firmware:

1. Start ELIAS and add the following packages to the device's IDF:

   - **wlandrives**

2. Save the IDF and exit ELIAS.
3. Install the software on the Thin Client by performing a firmware update over Ethernet.

⇨ **To insert the wireless card**

Insert the card into your device according to the directions that came with the card.

Below you find examples for the 3 configurations.

(1) WEP Configuration:
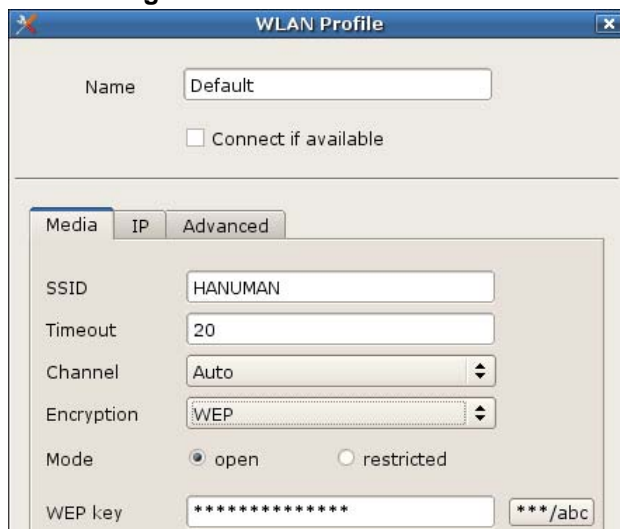
1. Select **WEP** from the **Encryption** list.
2. Enter the WEP key you received from your network administrator.
3. Enter the **SSID** information you got from your network administrator.
   - Service Set Identifier (SSID) defines the network name of a wireless network based on the IEEE 802.11b standard.
4. Configure the **channel** where the Access Point provides its service or set **Auto** for this parameter, in order to make the client scan for the used channel and automatically configure it.
5. Click **Apply** and then **Yes** in the eLux *RL* Control panel.

When the device restarts, it will attempt to contact the access point using wireless LAN.

(2) WPA Configuration:

1. Select **WPA (PSK)** from the **Encryption** list.
2. Enter the **SSID** information you got from your network administrator.
   - Service Set Identifier (SSID) defines the network name of a wireless network based on the IEEE 802.11b standard.
3. Configure the channel where the Access Point provides its service or set Auto for this parameter, in order to make the client scan for the used channel and automatically configure it.
4. Enter the **Preshared Key (PSK)** you received from your network administrator.
5. Click **Apply** and then **Yes** in the eLux *RL* control panel.

(3) IEEE 802.1x/ Leap Configuration:

1. Select **IEEE 802.1X (LEAP)** from the **WPA mode** list.
2. Enter the **SSID** information you got from your network administrator.
    - Service Set Identifier (SSID) defines the network name of a wireless network based on the IEEE 802.11b standard.
3. Configure the **channel** where the Access Point provides its service or set **Auto** for this parameter, in order to make the client scan for the used channel and automatically configure it.
4. Depending on your authentication server enter user name and password as set on your authentication server.
5. The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary method which enables to integrate the authentication of wireless clients into a Radius server.
6. Click **Apply** and then **Yes** in the eLux *RL* control panel.

Display of the signal strength in the taskbar:

When configuring **Wireless LAN** for the network type, the signal strength of your WLAN connection is displayed by an icon on the taskbar..

 Signal strength: none

 Signal strength: low

 Signal strength: medium

 Signal strength: high

 Signal strength: very high

3.2.7 G3 / UMTS

The Network sub tab G3 / UMTS contains the following dialogs:
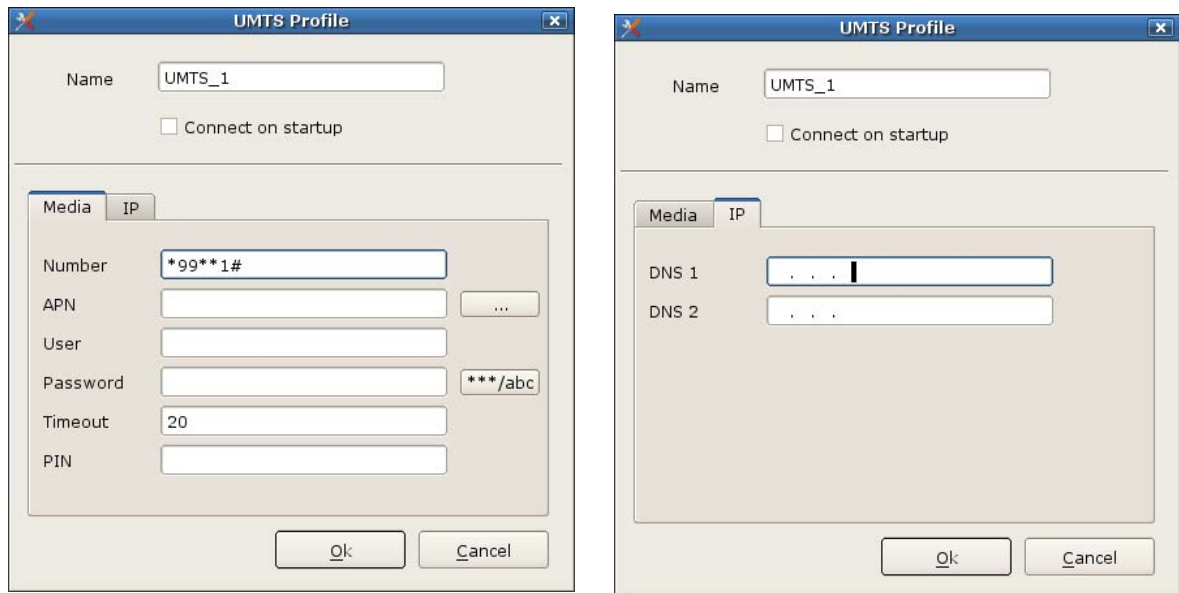
Figure 9: Configuration > Network > G3/ UMTS

Medium:

Number:	Name of the UMTS profile, e.g. the provider's name
APN:	Website of the Provider
User:	The user name assigned by your provider.
Password:	The password assigned by your provider
Timeout:	If you know the period of time for the eLux client to search for the management server (Scout Enterprise) – if management is enabled – enter the time in seconds.
PIN:	The pin of your SIM card assigned by your provider

Dynamic DNS entry:

In the **IP** tab you can define whether the client is to transfer the name to the name server dynamically, in order to allow the entry into the Forward or Reverse Lookup zone.

To close the dialog confirm with **OK**, and repeat the procedure for all further required profiles.

3.2.8 Display of Network Connections via Systray

In the systray

click this icon

to show the defined network profiles, add new ones or modify existing profiles.

Rightclick the systray icon to get information on the current connection, which can be repaired this way.
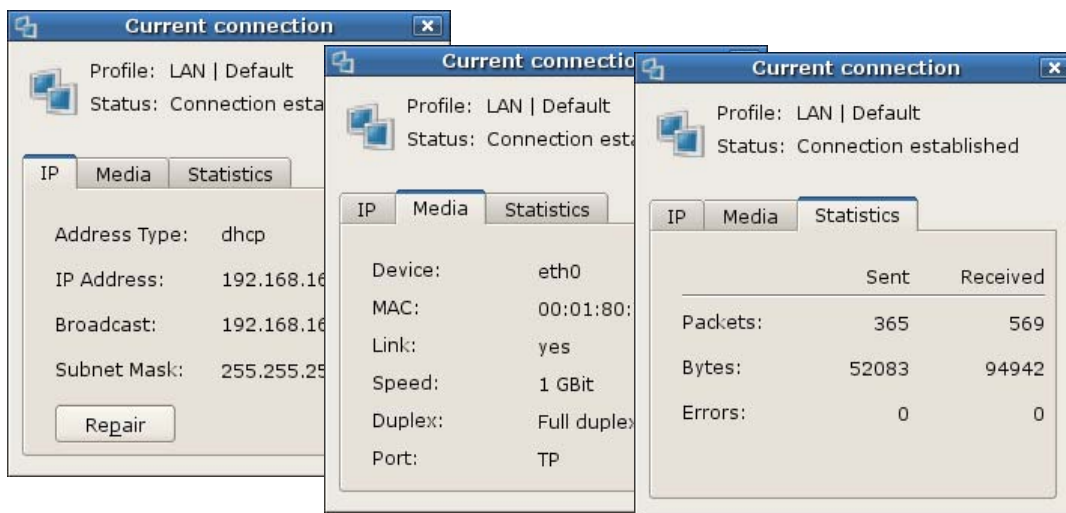
Figure 10 Systray – rightclick the network icon

Requirement: The option "Show network status" in **Setup** > **Desktop** > **Advance** must be activated.

All other systray icons are described in chapter 5.2.5.

3.2.9 Advanced Network Settings
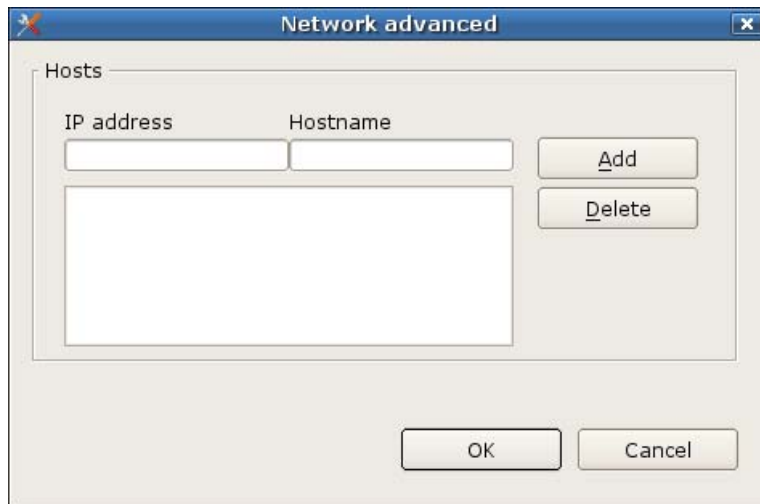
Figure 11 Setup > Network > Advanced

3.2.9.1 Defining a Host Table for Networks without an own DNS Server

If no Domain Name Server (DNS) is available in the network, it is an option to create a local list of hosts, which is stored on the flash.
For this purpose host names and IP addresses must be entered manually.

In the dialog **Advanced Network Settings** you enter host name and IP addresses in the corresponding fields. Click **Add** to add the entries, click **Delete** to remove an entry from the list.

3.2.9.2 Dynamic DNS Entry

This option requires the corresponding eLux software package (**dyndns**) to be installed.

You have 4 options:
1. No entry
2. Entry in the Forward Lookup zone (i.e. the assignment of the host name to IP is entered into DNS)
3. Entry in the Reverse Lookup zone (i.e. the assignment of IP to host name is entered into DNS)
4. Entry in both zones

3.3 Desktop
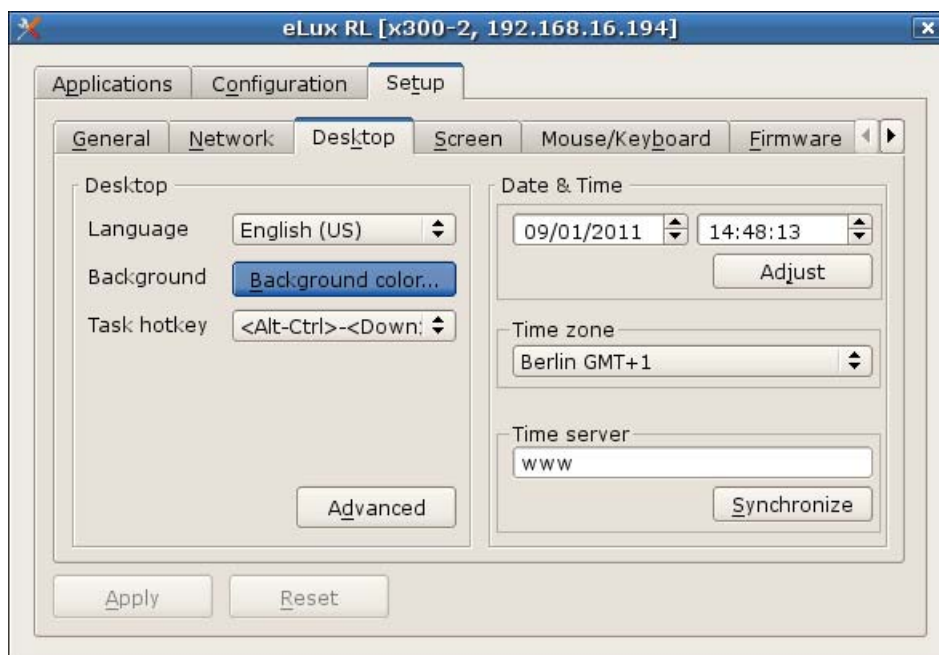
Figure 12 Setup > Desktop

⇨ **Language**

Select your language from the dropdown list. On delivery the language is English. The selected language effects the applications you wish to use, so that the user interface within these applications is presented correctly.

Yet, the eLux® *RL* desktop is available in either English or German, only.

⇨ **Background color**

Click the field **Background color** to select from a great variety of basic or custom colors.

⇨ **Task-Hotkey**
Although eLux® *RL* is mouse-based, several keyboard commands are important. The **Task hotkey** drop-down list allows you to choose the key combination to switch between current open sessions, or "tasks." You can use this not only to switch between applications, such as between an XTerm and an ICA application, but also between eLux® *RL* screens, such as the main eLux® *RL* 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

⇨ **Date & Time**

Select your **time zone**. eLux® *RL* adjusts for daylight savings time automatically..

There are two ways to set the time:

- Manually: Enter the date and time and click **Adjust** to update the settings.

- Automatically: (recommended) Enter a time server and click **Synchronize**. Settings are retrieved when the Thin Client boots. For technical requirements, see the section below.

3.3.1 Time Server

In addition to the time zone, the time must be set on the Thin Client for proper use. This can, of course, be done by filling in the date and time fields as described above. However, due to its better accuracy we recommend using a time server.

Synchronizing the time with the time server can be done **online** by clicking the button "**Synchronize**" in the Desktop tab. In earlier versions the synchronization was done after restart only.

Enter the IP address or the IP name of the time server.

The system detects automatically whether the time server be Windows or UNIX.

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 inter-changeable. 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 Though it is also possible to set the system time directly in the Thin Client's BIOS setup we do not recommend this due to inconvenience.

3.3.2 Advanced Desktop Settings

On the **Desktop** tab click **Advanced**. This leads you to the settings of Taskbar, Control Panel, and Workspaces.

Figure 13 Setup > Desktop > Advanced

Interactive Desktop	By enabling these options icons will be displayed on the desktop. Further, you can make the desktop writable. By default the options are not enabled and the desktop is not writable.
Taskbar	By default the taskbar will be visible no matter what program is open. It can be deactivated, set Always on top or Hide automatically, in which case the taskbar disappears, increasing screen space. It reappears when you move the cursor to the lower edge of the screen.
Show clock	A clock appears on the right-hand side of the taskbar. Moving the cursor over the clock to displays the date.
Systray	shows the multimedia icons in the taskbar, when activated. Also see section 5, eLux RL Desktop. Also see chapter 5 for detailed information.
Autostart	Automatically starts the eLux® RL control panel when the system boots. This is the default setting. Deselect this option to deactivate. The control panel can always be accessed by clicking the start menu button in the taskbar.
Workspaces	Sets the number of workspaces. You are allowed up to four. Default is one.
Window manager	By activating the option "Maximize/full screen to a single monitor" in case of dual monitor operation it is possible to configure applications to show full screen on one explicitly defined monitor only.

3.4 Screen

Adjust the settings to your monitor.
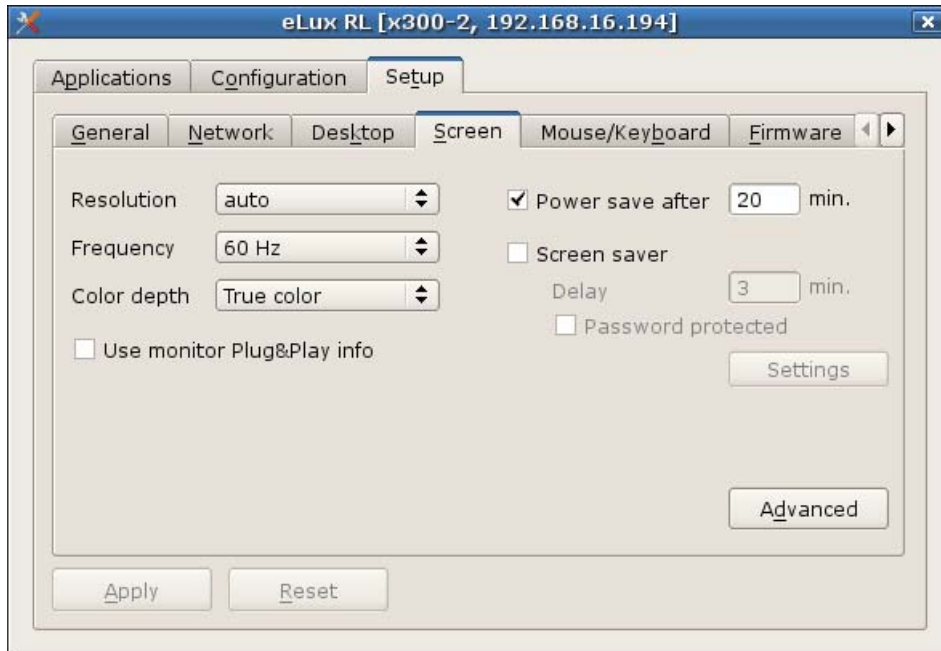
Figure 14 Setup > Screen

Select your monitor **resolution**, **frequency** and **color depth**.

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 disabled which corresponds to **"no ddc=true"** (ddc= Display Data Channel).

This option represents a compromise between a complete Plug & Play function and the individual setting, in case that a requested and set resolution should not be possible.

Background Information

Via DDC present-day monitors can transfer the information to the Thin Client (eLux® RL) as to which resolutions the monitor can cope best with rsp. which it supports. In this case the menu offers the supported resolutions only, otherwise all resolutions will be offered, even those which the monitor cannot cope with (in which case Safe Boot Mode is required). Also, it is quite possible that the DDC information – depending on DVI or VGA – cannot be transferred, though the monitor would be able to. Therefore, please consider this parameter with great caution..

3.4.1 Screen Saver

Password protected

Combined with a server supported user login (e.g. Active Directory Server) the password corresponds to the user password on the server.

If the configuration has been defined without server login the screensaver runs without requesting a password. However, you can protect the screensaver by defining your individual password by Ctrl-Alt-End. This password is valid for one session, i.e. until the client is switched off.
The elux software package "xscreensaver-5.04.3" is required.

In **Setup** > **Screen** click **Settings**. This leads you to the **Screensaver Control Center**. Please consider that this option is only available when the „**xscreensaver**" package has been installed. The figure below shows the settings. Beside the default screen savers you can use your own pictures.
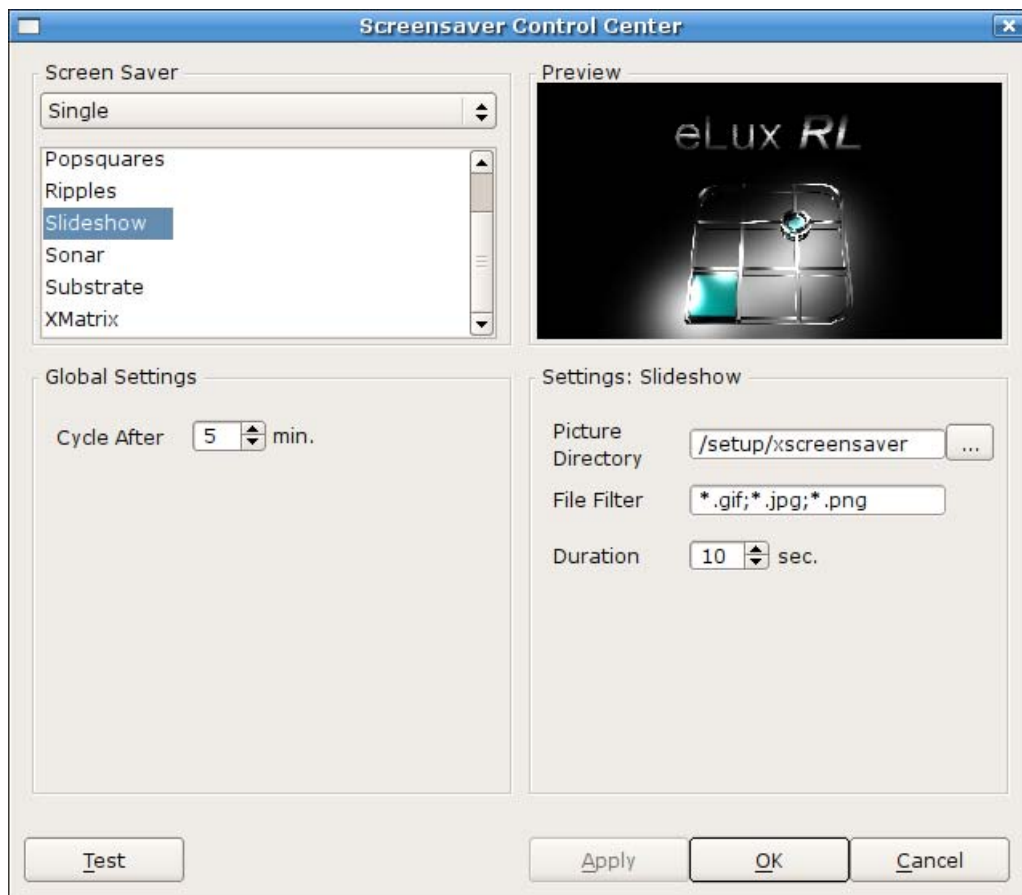
Figure 15 Setup > Screen > Settings

From the **Setup** > **Screen** sub tab click **Advanced** to open the dialog **Screen advanced** for the definition, editing or deletion of font servers. Please note, that this function may not be supported by all hardware platforms.

Backingstore: Saves screen information to the local X11 server on the thin client. When this option is active, a copy of the application window is stored in an off-screen pixel buffer. When hidden sections of overlapping application windows are redrawn, the sections are copied from this buffer rather than fetched from the server. This increases the screen refresh speed when the network connection is slow (especially noticeable by ISDN); however, the main memory requirements are large (128 MB or higher).

Font server: If your network has an X11 font server, you can use it to access fonts. Click **New** in the **Screen advanced** dialog box.
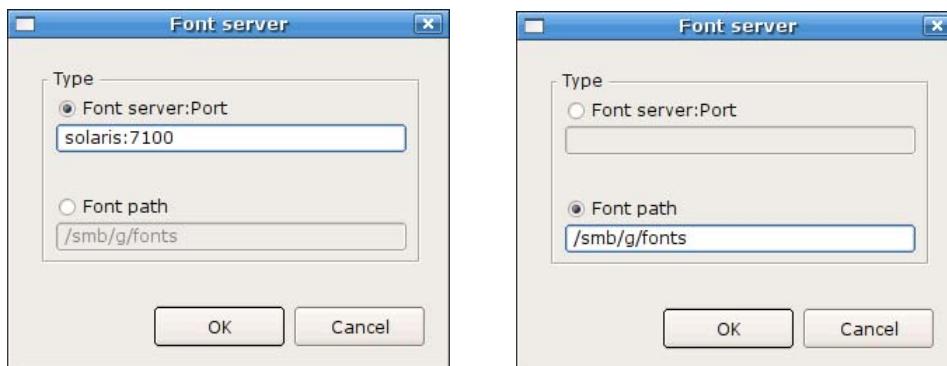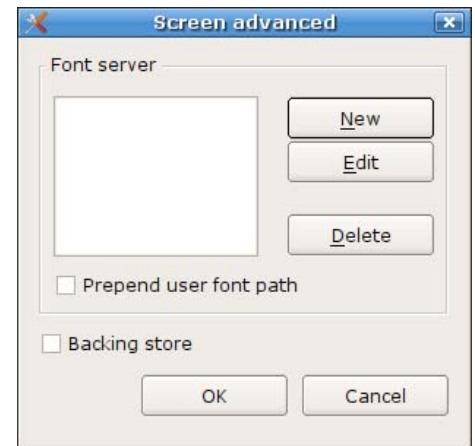
Figure 16 Settings of Font server and Font path

Either click **Font server:Port** and enter the IP address (or name) of the font server and the port number, separated by a colon.

Example: <Fontserver IP address>:<port number>

              `office:7100`

or

Click **Font path** and enter the font path. (Font paths are usually accessed via Samba or Network File System (NFS) drives. Ask your administrator for the correct path.)

Example: `/smb/g/fonts`

Click **OK** in the **Font server** dialog box. If the information you entered is valid, the dialog box closes. If it is invalid, an error message appears. Correct the information and click **OK**.

By default, local fonts have precedence. Select **Prepend user font path** to give the font server/path you just entered precedence.

3.5 Mouse/Keyboard

On delivery eLux® *RL* has a default configuration. For this reason we recommend to use at first boot the mouse coming with the delivery. Use this mouse to enter the setup and adjust the mouse settings.

Figure 17 Setup > Mouse/Keyboard

The **keyboard language** can be set dynamically, i.e. without requesting a restart of the desktop or client. Just click *Apply* to activate the setting.

Keyboard types are automatically recognized when they are plugged in. No further configuration is necessary.

For the time being these keyboard types can be selected:
Auto, Cherry G81-8000, MFII, Sun Type 6, Trimo 3270, Trimo 97801

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, you must set the mouse type to two button or three button (the wheel function will not be supported). This setting is not required for Microsoft Remote Desktop Protocol (RDP).

Click **Advanced** to configure the following advanced settings:

- **3-button mouse emulation**

    In general, eLux *RL* 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. By default it is not active.

- **Left-handed**

    Select to switch the mouse buttons. By default it is not active.

- **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 the accent to (the accented combination character appears).

    For example, pressing "`" on the U.S. international keyboard produces nothing, but subsequently typing "e" produces "è". Other keyboard layouts may produce accented characters in other ways (on the French keyboard there is a key that produces "è" directly).

    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 activate the NUM key when the Thin Client boots. By default, it is active.

- Console switch enabled
    Allows the user to switch between consoles ("virtual screens") on the Thin Client using the hotkeys.
    By default, it is active. The table below shows the defined hotkeys. If disabled, console 1, the eLux desktop, is on top.
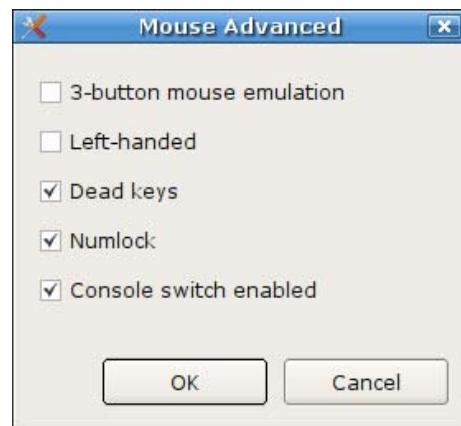
Nr.	Console	Hotkey
1	eLux Desktop	Ctrl + Alt + F1
2 *	First XDMCP session	Ctrl + Alt + F2
3 *	Second XDMCP session	Ctrl + Alt + F3
4	Message console	Ctrl + Alt + F4

Figure 18   Hotkeys to switch between consoles

Note (*) XDMCP sessions are not possible with eLux RL 3 at the time of publishing.

Having set all parameters click **OK** to confirm.

All changes will come to effect during the next restart of the client.

3.6 Firmware

To update terminal firmware, you need a new image definition file (IDF). The new IDF is created using the software tool ELIAS For detailed information on how to create an IDF, see the *ELIAS Administrator's Guide* or the *Scout Enterprise Administrator's Guide.*

This new IDF may reside on an FTP/HTTP server, CD-ROM or USB stick. The image file **must** reside in the same directory as the eLux® *RL* software packages (that is, in the container)! The new IDF file is entered in the Firmware tab.
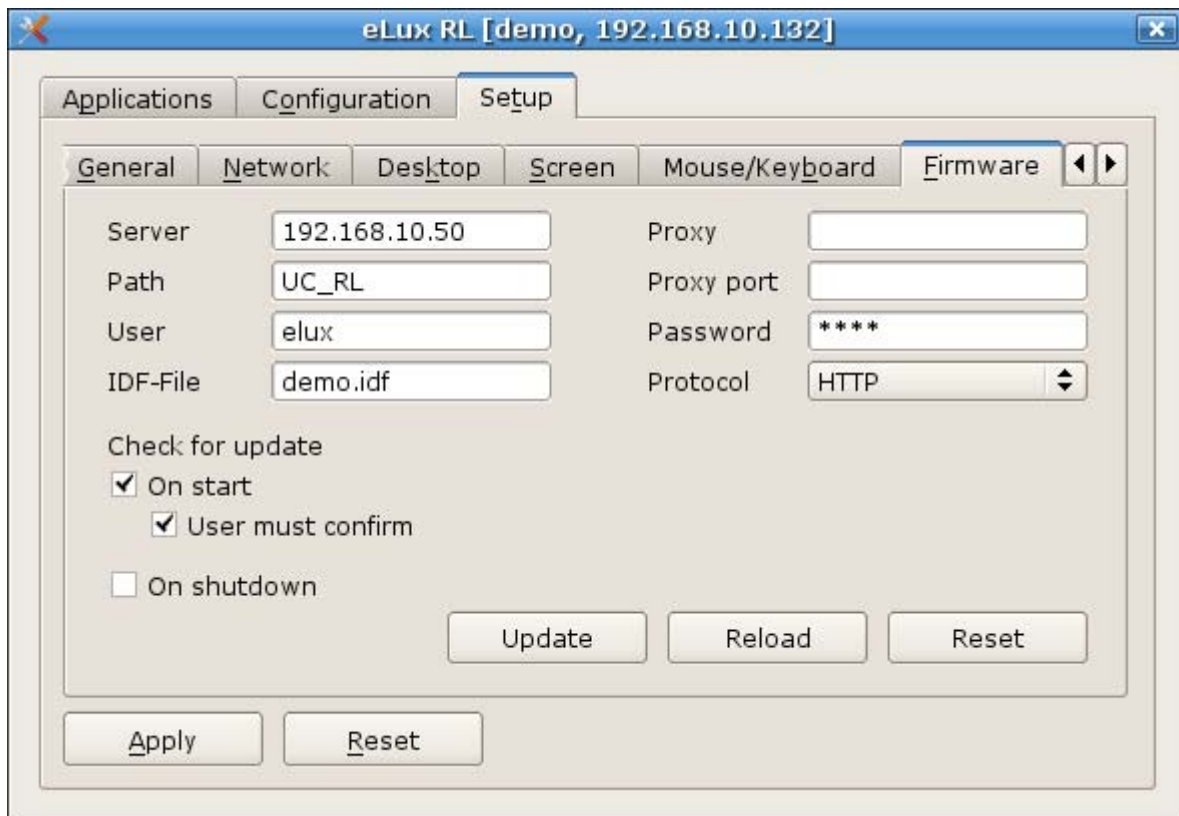
Figure 19 Setup > Firmware

The **Firmware** tab contains 3 more buttons: **Update, Reload, Reset**.

A click on **Update** issues either the eLux® *RL* message asking to confirm the update or the message that no update is required, i.e. the firmware is up-to-date, the IDF has not changed.
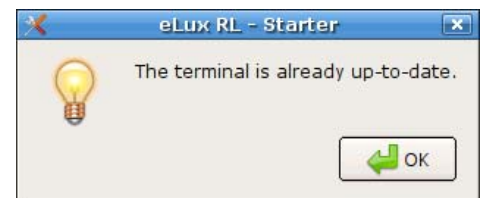
Figure 20 Firmware > Update

If the client is managed by Scout Enterprise, it is principally assigned the settings from the Scout server

- when first registered in Scout Enterprise
- during the initialization of the client

The setup data are loaded during the start of the client only if the configuration had been modified at the Scout Enterprise server by the administrator. If no modification should have occurred by the administrator, the setup configuration will not be reloaded during the start of the client, but the configuration used so far will be set.

In order to enforce the reloading of the settings, click the button **Reload.** The client then loads the configuration from the Scout Enterprise server no matter whether modifications have occurred via the Scout Enterprise Server or not.
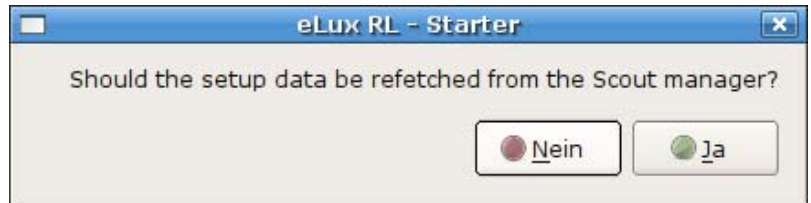
Figure 21 Firmware > Reload

Note: For this functionality the client **must** be managed by Scout Enterprise.

Click on **Reset** if you wish a factory reset.
If you confirm the eLux *RL* message by **Yes and Reboot**, all application data will be deleted and the setup factory settings will be restored.

However, the firmware is not deleted.

Figure 22 Firmware > Reset

The option **Check for Update** enables you to

1. check whether the firmware need to be updated
    - during start and /or
    - during shutdown

2. Activate **User must confirm**, if you want to be prompted before a firmware update.

Always click **Apply** to save the modifications.

3.7 Security

This Setup tab allows defining:
Local security, **User authorization**, **Scout settings** and **Mirror server settings.**
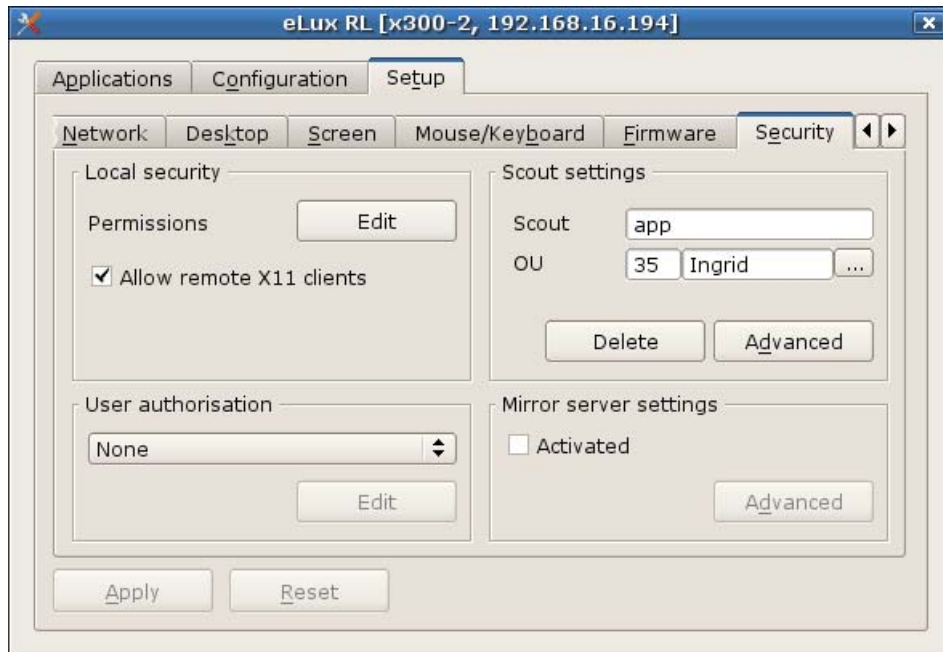
Figure 23 Setup > Security

3.7.1 Local Security

Click on **Edit** to open the dialog **Local Security Settings**.

By default, the user has access to the **Setup** and **Configuration** tabs. In the **Security** sub tab you can set user rights and restrict access. The configuration parameters are displayed in a tree-like structure. Upon restart, the user can only access the functions that you enabled.

All fields modifiable Click to enable local configuration of all fields. The color green indicates that a field is unlocked.

All fields locked Click to disable local configuration of all fields. The color red indicates that a field is locked. In addition, the option "Allow remote X11 clients" allows remote X11 clients to connect to the local Thin Client.
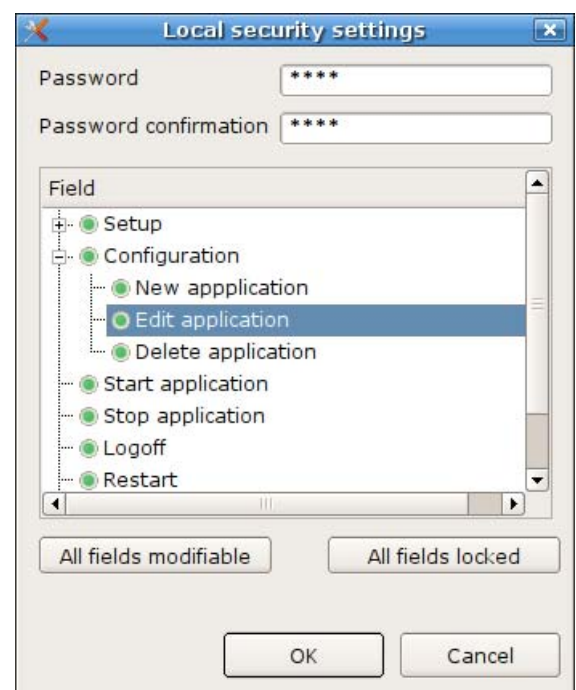
Figure 24 Security > Local security settings

3.7.2 User Authorisation

You can use an authorization server with eLux *RL.* Settings are made in the **Setup** > **Security** tab. Username and password are entered once at eLux *RL* start.

The dropdown field "user authorisation" offers:

None

ADS (Active Directory)

LDAP (LDAP Server)

SmartCard (Smarty)   **with additional authorisation via ADS or LDAP**

ADS+Smartcard

SMB (Windows NT 4.0)

Note In this chapter, there are numerous configuration examples that include unusable IP addresses, passwords, and domain examples. Be sure to use your own IP addresses, passwords, and domains when configuring the authentication server settings.

⇨ **Authorisation**

Settings are made in the **Setup** > **Security** tab.

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

None:	to disable user authorization
LDAP server:	for a Lightweight Directory Access Protocol Server
Active Directory Server:	for an Active Directory® Server (Windows® 2000) if this method is chosen, you can define whether the client data are stored on a server.
SmartCard (Smarty)	with additional authorisation via ADS or LDAP
ADS+Smartcard	Authentication by Smartcard, certificate X509
SMB:	for a Windows NT® 4.0 domain controller

2. Depending on the server being used, different configuration parameters need to be entered. Click   **Edit** to open the dialog **Authorization settings,** and enter the corresponding parameters.

3.7.2.1 PAM - Pluggable Authentication Modules

This functionality contributes considerably to ease the user account and authentication management.

Starting with eLux RL V 2.7.0 the PAM user account expiration is supported.

3.7.2.2 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.

Search 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

Version: the LDAP version to use.
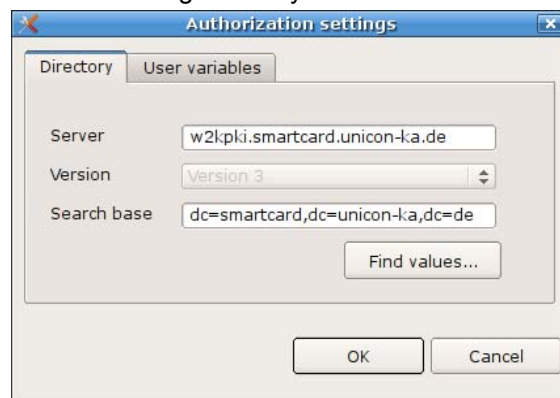
Click **Find values**. The Thin Client will search for the server and automatically fill in the **Search base** field.

Figure 25 Security > Authorization Settings > LDAP

Note: The LDAP password can be changed via Shutdown > Change password.

3.7.2.3 Active Directory Server

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 (FQDN).

Search Base: The search base indicates where in the domain tree (directory tree) 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".

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

When starting the client a user name and password will be requested.

Figure 26 Security > Authorization Settings > ADS

Required Software

User authorization: "User authorization modules" (file name: "userauth") EPM.

To test user variables: "LDAP search module" (file name: "usersearchldap") FPM in "User authorization modules" EPM. By default, it is not activated.

For a description of EPMs and FPMs, see the *ELIAS Administrator's Guide*.

3.7.2.4 Smarty

The Smarty tool allows to store on the Smartcard the user name, password and domain instead of the certificate.
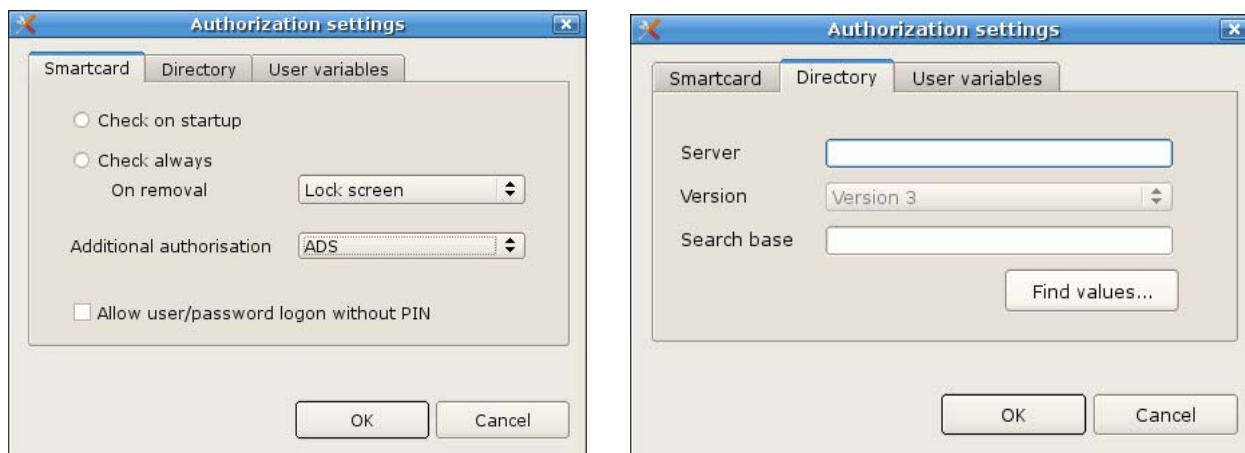
Figure 27: Smarty Access Configuration

Select **additional authorisation** via **ADS** or **LDAP** from the dropdown list to send the user credentials from the Smartcard to ADS respectively LDAP.

The data can either be directly transferred to the corresponding server connection as $ELUX variables or the parameters user name, password and domain can be verified via ADS. If the password should change (group regulation) a dialog will appear at the client with this request. The new password will then be written to the Smartcard automatically.

The option "**Allow user/password logon without PIN**" for the authorization by ADS+Smartcard and SmartCard(Smarty)+ADS/LDAP enables the user – when activated – to switch to login with user/password by pressing the ESC key.

For personalization the **Smarty tool** is available for download on www.myelux.com.

An initial PIN may be set – e.g. 1111 – and the password field may be left blank. The initial PIN can be set in Scout Enterprise (Advanced File Entries), such as:

file: /setup/terminal.ini
section: Security
key: ScInitialPIN
values: 1111

 In this case the user is requested to define an individual PIN and initial password. PIN and password are stored on the Smartcard.

The Smarty tool also allows defining the PIN policy; however, this must not be identical to the initial PIN – as in the example above 1111.

In case of SmartCard/PIN supported user authorizations you can allow or not to shift to authorization with username/password (by ESC key) by defining the following terminal.ini entry:

file: /setup/terminal.ini
section: Security
key: allowScUserAuth
values: true|false

3.7.2.5 ADS+Smartcard

To authenticate by Smartcard (certificate X509) it is required to assign the server address in a known notation and the root certificate to verify the user certificate. Please select the root certificate in order to transfer it to the client. Several certificates may be added and selected.
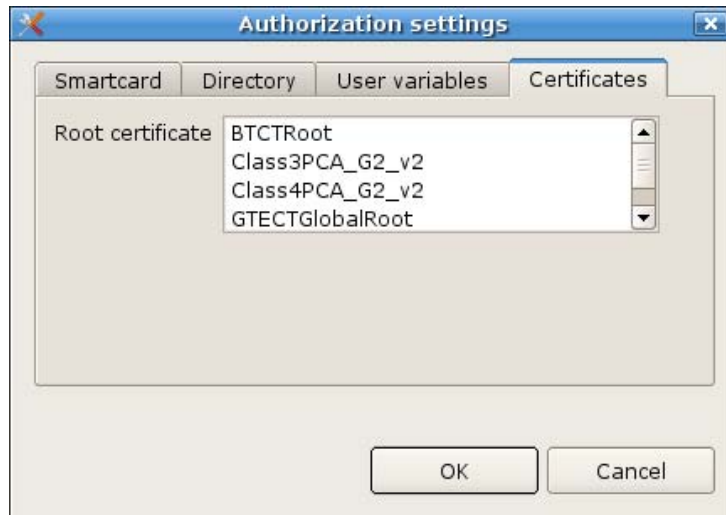
Figure 28: ADS + Smartcard Access Authorization

The tab **Smartcard** serves to define the reaction on removal of the Smartcard. When selecting **Lock screen**, please consider to enable the checkbox **Password protected** in Setup > Screen.

Figure 29: ADS + Smartcard Behavior

3.7.2.6 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.

3.7.3 User Variables

Software Requirements

To test user variables: "LDAP search module" (file name: "usersearchldap") FPM in "User authorization modules" EPM. By default, it is not activated.

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 eLux RL control panel.

Preset variables are $ELUXUSER, $ELUXDOMAIN and $ELUXPASSWORD. They are automatically set when the Thin Client starts. When using LDAP or Active Directory Server as the authorization server, it is also possible to define your own user variables.

⇨ **To set user variables**

1. In the **Authorisation settings** dialog box for ADS or LDAP click on **Add**. The **User variable** dialog box appears.

   - **Local variable**: Enter a name for the variable. The name must begin with the prefix "ELUX" 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. **Test**: The Thin Client attempts to retrieve the value for the attribute you entered from the authorization server.

3. Click **OK** in the **User variable** dialog box and **Apply** in the **Security** tab.

User variables can be entered in the eLux RL Security tab just like normal parameters. Enter each variable with the "$" character as prefix. For example, in an ICA application definition enter $ELUXUSER as the username. This variable will be replaced with the given username when the application is called.

3.7.3.1 Application Possibilities for User Variables

When user authorization is active, user variables can be used in the following fields in the eLux RL control panel.

Applications

Applications Tab

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

Setup Tab

Setup

Sub tab	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

Configuration

Sub tab	Field	User Variable
ICA/RDP	**Server**	Every $ELUX variable
	User	$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

3.7.4 Setting ADS user dependent Parameters

⇨ **LeftHandMouse**

The user variable in eLux must be named "ELUX_USERCONFIG#".
On Windows side we chose a multi-valued attribute, in order to be able to enter multiple values. Please definitely enter "#" at the end of the name.

The only keyword being edited is "LeftHandMouse", valid values are "true" and "false", whereby "false" is the default value. Consider the entry is case sensitive.

Note: If the LDAP attribute is not known, apply the following method:
Enter in Windows:
Logon with "userauth"
ldapseach –LLL samAccountName=<login> - all attributes are listed.

Settings in ActiveDirectory
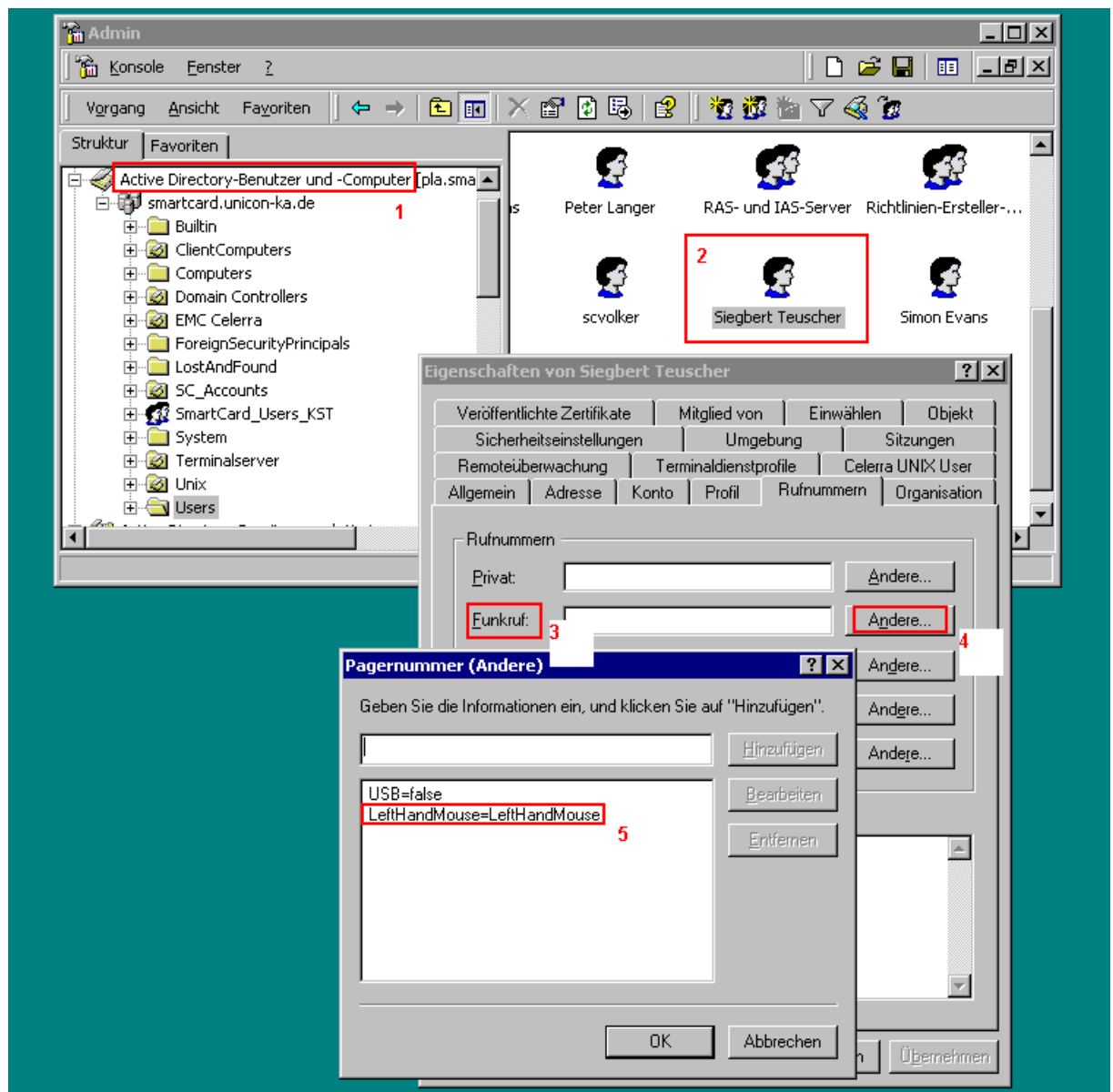
Figure 30: Settings in ActiveDirectory

3.7.5 Scout Enterprise

To manage the clients from a central point we provide the management tool Scout Enterprise. The clients must be registered in Scout which can be done in two ways:

1. The Scout Enterprise „Discovery" function is initiated at the Scout Enterprise Server. With this procedure the clients being integrated in the network are registered in the Scout Enterprise Server, and the IP address or IP name of the management server is automatically set in the **Scout** field at the eLux client.

2. „Reverse Discovery" leads to the same result except that the IP address or the IP name of the Scout management server is being entered manually into the **Scout** field at the client . We describe this procedure here.

First, install and configure the Scout Enterprise Management Software on your administration server. Provide an organization unit for the clients you want to register in Scout. Install the clients and enter the values for the management server.

⇨ **Configuration Wizard**

By default during the first boot of the client a wizard appears to assist you with the first configuration.

At this point you already can choose whether to register the client for the Scout Enterprise management or to configure it manually.

⇨ **Scout Settings**

Having configured the client manually during the first steps, „Reverse Discovery" registers the client in the corresponding organization unit of the Scout manager.

In the area **Scout Settings** of the **Security** tab the following parameters can be set:

*   IP address or IP name of the Scout Enterprise Server in the Scout field.

*   The **OU** (organization unit) can be selected from the provided list of available groups on the server.
*   **Delete**:
    Warning: if the Scout Manager is to be deleted, the device is automatically factory reset , so that all setup parameters must be re-entered.
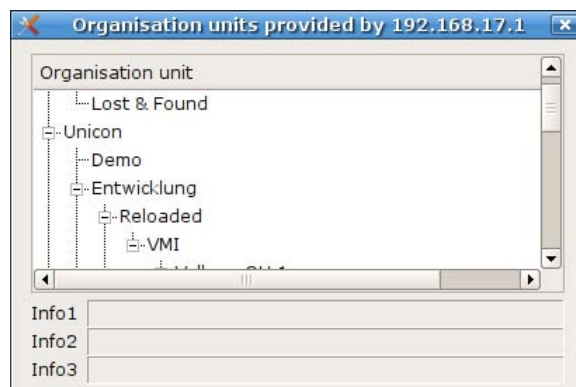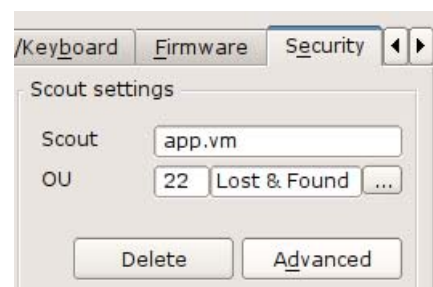
The button **Advanced** opens the dialog with a list of all Scout Enterprise servers, whereby the top entry in the list is the current one. Further, info fields are provided.
The reason for this feature is that eLux can work with so-called Scout Enterprise Farm, i.e. several Scout servers may run simultaneously and the client can use another server in case of a crash. Thus we provide the highest possible availability.
The list of the Scout Enterprise servers is either transferred from one of the Scout servers or may be set by a DHCP-Tag from the DHCP server.

- Fill the **Info1**, **Info2** and **Info3** fields with user-specific information such as name, room number, phone number or similar

- Click **OK** and **Apply** in the **Security** tab.
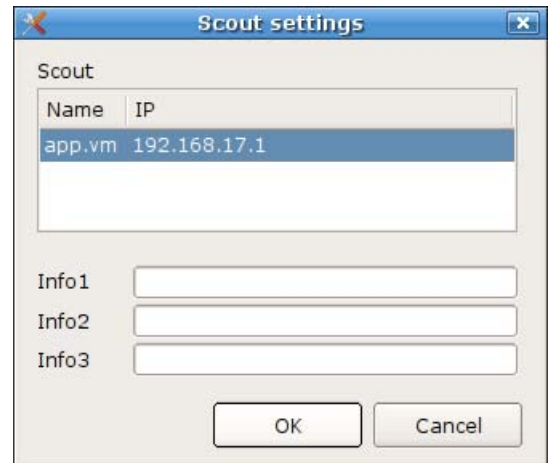
Click on **Delete** if you wish to disconnect from the management, but consider that if so all applications will be deleted and the configuration is reset to the **factory settings**.
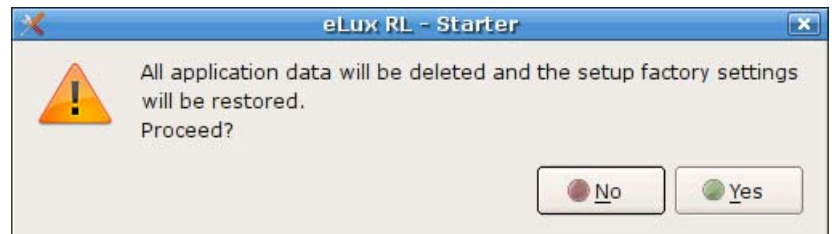
Details on the above functionality and the discovery of Thin Clients by the Scout Enterprise management tool are found in our *Scout Enterprise Administrator's Guide*.

3.7.6 Mirroring

Mirroring is the term used to describe the process of monitoring a user's session remotely and, optionally, participating in the session using your own keyboard and mouse. Mirroring has a variety of uses, including troubleshooting, training and presentations.

Mirroring of a thin client requires a VNC Viewer on server-side to start the mirroring session, and a VNC server on the target client, in this case the eLux *RL* Softwarepaket „mirror". If this software package has not been installed, the mirror settings are disabled.

Scout Enterprise includes a VNC Viewer, so that a client can be mirrored by right mouse click., provided the mirroring function has been activated on the eLux RL client.

⇨ To enable / disable mirroring (client)

From the **Setup** tab, click the **Security** sub tab.

1. Select the **Activated** check box to allow mirroring and click **Advanced**.

2. Options are:

   Read only access: Gives other machines view rights only.

   Confirmation necessary: The user must confirm a mirroring session before it can start.

   Encrypt mirror session

   Allow from Scout only

   Transfer mirror information

   Password: (optional) Set the password that must be entered to start a mirroring session.

3. Click **OK** to confirm.

During the mirroring session, the keyboard mapping of the local system has precedence.
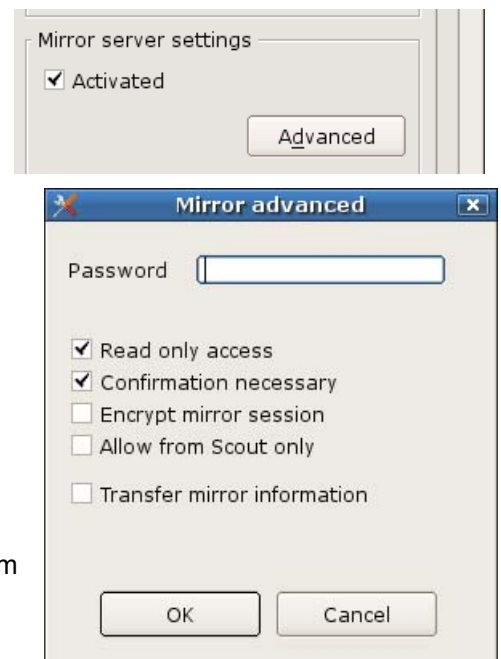
Figure 31: Mirroring Settings

Security concerns

During a mirroring session, a message box appears on the remote machine, making it impossible to "secretly" mirror a user. The user can end a mirroring session at any time. In addition, you can set a mirroring password. Nonetheless, if security is a concern, you can deactivate mirroring entirely by deselecting the **Activated** check box in the **Security** sub tab > "Mirror server settings".

3.8 Multimedia
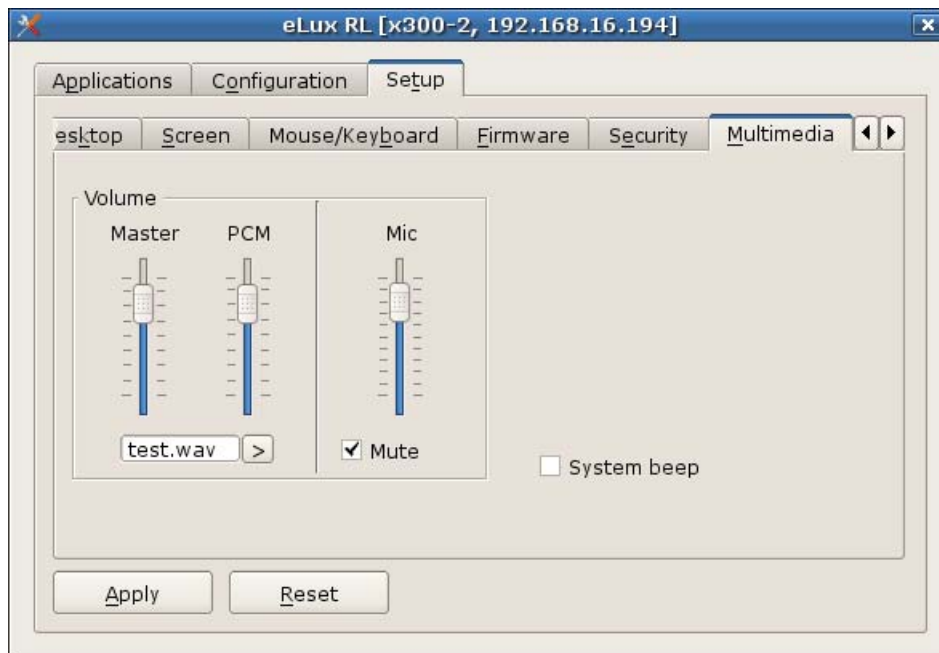
Figure 32 Setup > Multimedia

- To adjust the volume from the **Multimedia** tab move the sliders for **Master**, **PCM** and **Mic** up or down.

- To disable the local microphone click the option **Mute**.

- If **System beep** is enabled the system beeps as a feedback to the user in case of pushing the power-off key at the Thin Client.

3.9 Drives

eLux RL supports the following drives:

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

This section describes how to access the various drives.

> **Note** The **Drives** tab is exclusively for mapping SMB drives! All the other drive types are mapped automatically.
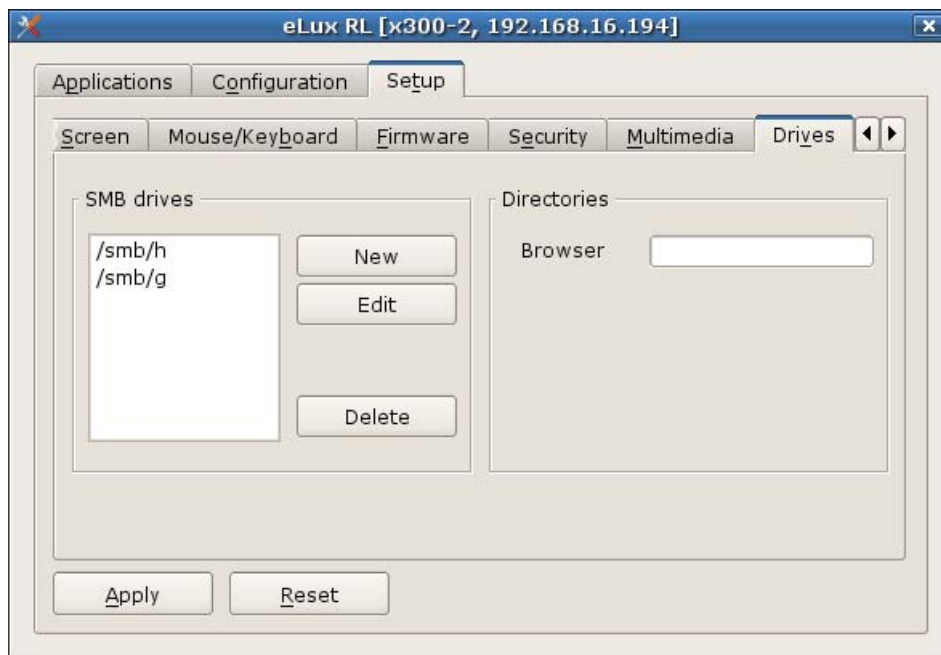
Figure 33 Setup > Drives

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.

⇨ **Defining network drives on NT or Samba**

- From the **Drives** tab, click **New**.
- Fill in the fields in the **Drive settings** dialog:

  Local directory: Enter the directory name.

  eLux *RL* automatically adds "`/smb/`" to the directory name.
  The data can then be accessed locally in the directory `/smb/`*<directory name>*.

  Server: Enter the name of the server.

  Share: Enter the export name of the shared drive as defined on the Windows machine.

  Username, Password: Enter your username and password on the server.

Click **Test**. If the drive can be used, the message "Drive can be used" appears. If the server cannot be located, the message "Server cannot be contacted" appears. If so, check your entries for validity.
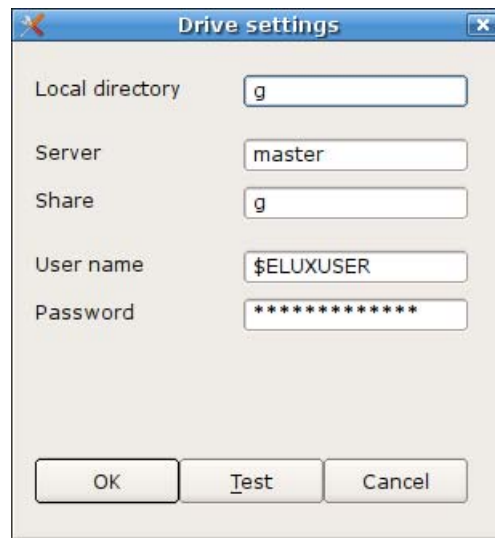
Figure 34   Drive Settings

Note It is particularly important to click **Apply** and **Yes** in the confirmation request dialog box to complete the mapping process.

⇨ **Browser Home Directory**

All browser files are saved to the client's local memory. The local folder /tmp is used for temporary files (cache, etc.) and the local folder /setup/<*browser*> is used for permanent files (history, bookmarks, etc.).

By definition, a Thin Client has very little available memory. For this reason, heavy surfing can use up the available local memory very quickly. When available memory is 5% or less, the user is plagued by recurring warning messages. There are two options: either the user restarts the terminal (the /tmp folder resides on a RAM disk and is deleted when the Thin Client is turned off) or the administrator must go to the terminal and delete the files by hand.

To avoid this inconvenience, you can use a network drive as the home directory for the browser. All browser files (cache, history, configuration, cookies, etc.) are saved to this directory, regardless of whether they are temporary files or not.

In the **Drives** tab enter a net drive path in the "Directories" > **Browser** field.

You can use a network drive or a subdirectory on that drive.
Example: /smb/g/user/paul or /nfs/hal2001/users/paul
In the case of Samba, the drive must have been previously defined.

Click **Apply** to save the modification.
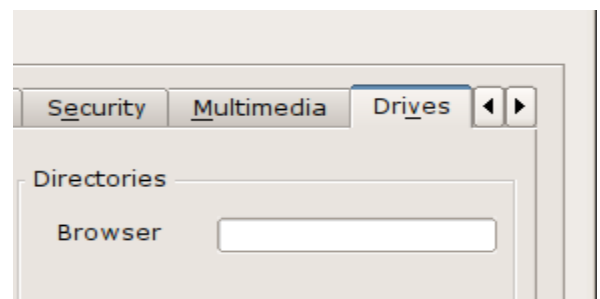
3.10 Printer

The eLux *RL* print service supports both local and network printers. Further, the printers set up at the client can also be addressed by other stations or servers via the network.

New: eLux RL includes a CUPS print server. For further details please have a look at www.cups.org.

If required the WEB Admin front-end can be installed by using the ELIAS tool.

You can use eLux *RL* to configure and assign logical names to local printers, which can be used from within the network. If the printer name for the local or network printer is different from the preset "lp", you must also configure it within the local application, such as a browser.
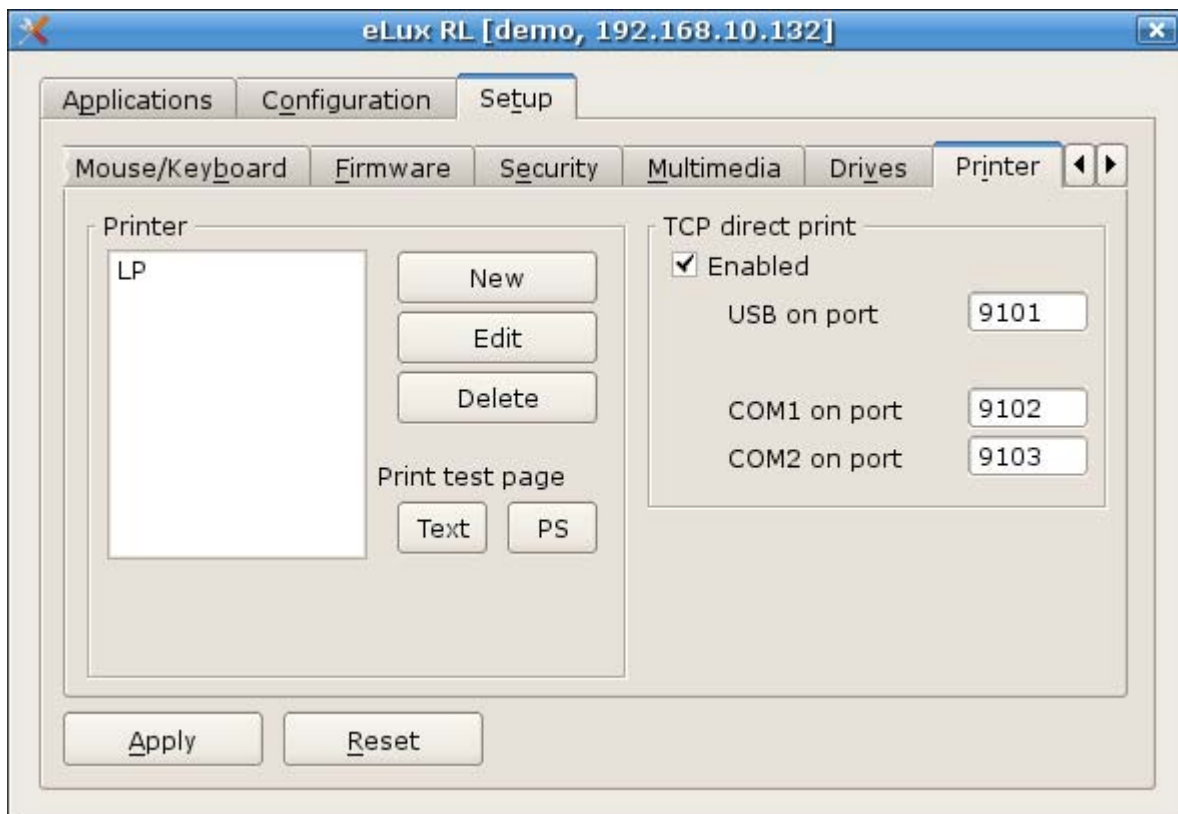
Figure 35   Setup > Printer

The printer locally attached to your Thin Client may be used by other systems provided these support the **TCP direct print** (Windows 2000 and higher). In the "TCP direct print" area enable the check box and enter the port number of the local printer interface (parallel or USB).

For local applications that use PostScript® as the output format, such as Firefox, Acrobat Plug-in, you must define a PostScript printer.

You can print a test page in text format or PostScript format.

3.10.1 TCP Direct Print

In TCP direct print, data are sent directly to the printer. There is no spooling of print jobs on the Thin Client and the data are not modified before printing. The flow is controlled by TCP/IP.

Enable the option **TCP Direct Print** in the **Printer** tab.

At the print server the IP address of the Thin Client, printer name and port number must be entered.

The Thin Client can resolve the host name of the machine initiating the print job. If you don't have a domain name service (DNS), enter the host name and the IP address in the local file "hosts" (**Setup** > **Network** > **Advanced**).

3.10.2 Network Printer

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

⇨ **To set up a network printer**

On the **Printer** tab

1. Click **New**.
2. Enter the name of the printer in the **Printer settings** dialog box.
3. From the **Connection type** drop-down list, select **Network**.
4. From the **Filter** drop-down list, select **None** to disable filtering. Select **Text** to print from a local shell (print shell command: `lpr –P<printer name>`). Select **PCL2** for the PCL2 protocol (not supported by all hardware platforms).
5. Enter the IP address or name of the remote system or printer box in the **Printer address** field.

   If your network does not have a DNS server, alternatively you can use the name of the printer if it has been defined in the local hosts file on the Thin Client (**Setup** > **Network** > **Advanced**)
   Enter the name of the printer queue of the remote system or printer box in the **Printer queue** field.
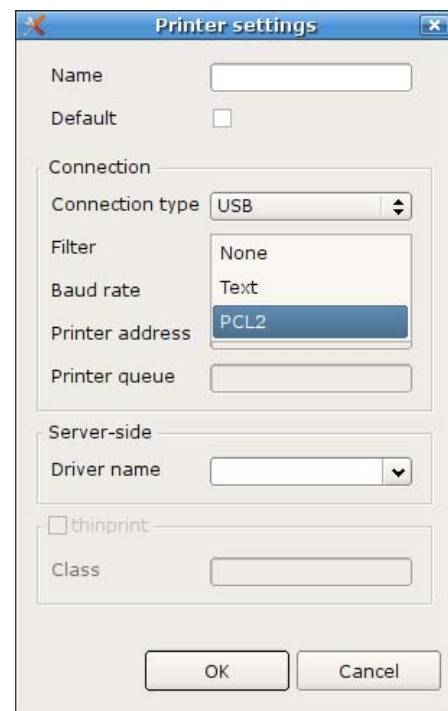
Figure 36 Printer Settings

6. Terminal servers can automatically create a printer definition ("autocreated printer") using parameters you entered on the Thin Client. These parameters are transferred to the server when you connect via ICA. Enter the following:
   Driver name: Enter the driver for your printer. **Note**: The printer driver name must be exactly the same as the driver installed on the server. See the installed printer driver list on the server if you are unsure. The server will not autocreate a printer if the printer driver you entered here is not installed on the server (check capitalization and blanks!).
   Default: Sets the printer to your default printer on the server.
7. Click **OK** in the **Printer definition** dialog box and **Apply** in the **Printer** tab.

3.10.3 Local Printer

The default printer definition "lp" is preset to a local printer. This means you can attach a printer to the Thin Client parallel port and print without additional configuration (depending on your printer, you may need to activate the filter).

The main memory is used to buffer print data. The following describes how to configure a local printer.

⇨ **To configure a local printer**

1. Connect a printer to the parallel, serial or USB port of the Thin Client.
2. From the **Setup** tab, click the **Printer** sub tab.
3. Click **New**.
4. Enter the name of the printer in the **Printer settings** dialog box.
5. Click the interface type in the **Connection type** list.

   - **Parallel**: If the printer is attached to a parallel port.
   - **Serial (COM1)**: If the printer is attached to the external serial port. Click the baud rate from the **Baud rate** list.
   - **USB**: If the printer is attached to a USB port.

6. Printer From the **Filter** drop-down list, select **Text** to print from a local shell (print shell command: `lpr –P <printer name>`). Select **PCL2** for the PCL 2 protocol. Select **None** to disable filtering. In this case, the print data will be sent to the printer in the output format of the application. See also "Filtering" below.

8. Terminal servers can automatically create a printer definition ("autocreated printer") using parameters you entered on the Thin Client. These parameters are transferred to the server when you connect via ICA. Enter the following:
Driver name: Enter the driver for your printer. **Note**: The printer driver name must be exactly the same as the driver installed on the server. See the installed printer driver list on the server if you are unsure. The server will not autocreate a printer if the printer driver you entered here is not installed on the server (check capitalization and blanks!).
Default: Sets the printer to your default printer on the server.

Click **OK** in the **Printer definition** dialog box and **Apply** in the **Printer** tab.

3.10.4 Filtering

To configure the filter, you must determine which page description language is being used by the application and by the printer. The two most common are PostScript® from Adobe and Printer Control Language (PCL®) from Hewlett Packard.

If the output format of the application differs from the local printer format, you will have to activate the filter.

File format		Convert to	Filter Setting
UNIX text	⇨	DOS text	"Text"
PostScript	⇨	PCL2	"PCL2"

If the application output format is the same as the printer format, disable the filter ("None").

Troubleshooting

Printing is a complex topic beyond the scope of this manual. For help with a specific printer, please contact the printer manufacturer. As a guide, below is help for some common questions.

1. PostScript file – PostScript printer (Filter = "None")
Most local applications – such as the local browser or Acrobat Reader – generate PostScript output. To print PostScript files to a PostScript printer, the filter should be set to "None."
If your printer prints a large amount of ASCII text, your file could be PCL. To check the file format, in the print dialog select "Print to file" and save to a network drive or to the local directory "tmp". Open the resulting *.prn file using Notepad or vi. If the first line starts with `%!` the file is PostScript.

2. PostScript file – PCL printer (filter should be set to "PCL2")
For this filter option to be displayed, the PCL package must be installed on the Thin Client ("PCL printer support" located in the base OS). By default, it is not installed.

3. Is the printing problem affecting multiple devices or just one device? If one device, make sure the Thin Client is working properly – try printing to other printers, accessing network drives, contacting other devices, etc. If it cannot, it is not a printer problem. If it can, see if the print job reaches the printer (most printers have a status line). If it does, the problem is most likely the file format. See 1 and 2 above.

4. Attempt to communicate with the printer on a protocol level. If the printer has an IP address, ping it from a local shell. If you are unsuccessful, or if the problem is affecting multiple Thin Clients, it may be a network problem.

5. If the application stops responding, or "hangs," you may have a performance problem. For example, the Thin Client buffers print data in main memory. How large is the main memory compared to the file you are trying to print? The more complex the file, the larger it will be. Graphics and color increase file size. PostScript files are often much larger than the original file. If your main memory is small, printing large files could cause a delay if the printer is not ready at the time a print task is running (see 6). Avoid this by checking the printer status in advance and by setting a "Maximum printer response" time-out.

6. Hardware problem: Verify that the printer is on and ready, that the paper tray is full, and that there are no error messages in the display.

3.10.5 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 RL **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.

3.11 Hardware

The First Configuration Wizard automatically detects an Ethernet LAN connection and configures it. If you wish to use ADS or other network connection you must enter this manually for the startup.

In the **Hardware** tab you can set various parameters:

- USB port activation
- Smart card
- COM port settings
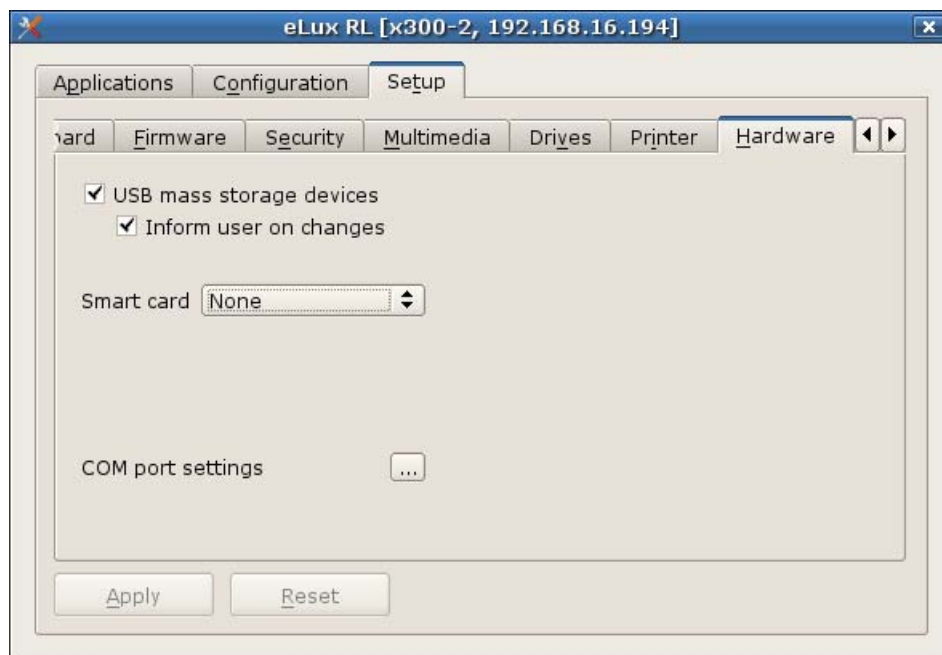
Figure 37 Setup - Hardware

3.11.1 USB Devices

The following USB devices are supported:

- Card readers
- USB ISDN adapter
- Mass storage devices
- Mouse / keyboard

USB Card Readers

Card readers are used with smart cards. For information on smart cards and a list of supported card readers, see http://www.myelux.com, in the Download area > eLux software packages > eLux RL > Released version > components.

USB Mass Storage Devices
In general, all USB mass storage devices are supported including, but not limited to, CD-ROM, floppy, USB stick, 2.0 flash card readers, photo mass storage, etc. A maximum of eight mass storage devices can be used at one time.

For security reasons, by default the port is disabled. To enable the USB ports for mass storage devices, select the check box **USB mass storage devices** in the **Hardware** tab.

Attached USB storage devices can be displayed by an icon in the systray. Click on the icon to show the available devices.

Accessing USB storage devices is described in the chapter **Drives**.

USB Mouse / Keyboard
A USB keyboard / mouse can be used without further configuration (plug-and-play). For a list of supported keyboards, see http://www.myelux.com, , in the Download area > eLux software packages > eLux RL > Released version > components.

3.11.2 COM Port Settings

In the **Hardware** tab you can define the COM port settings.

Click the button **COM Port settings** to open the dialog, and make the desired changes.
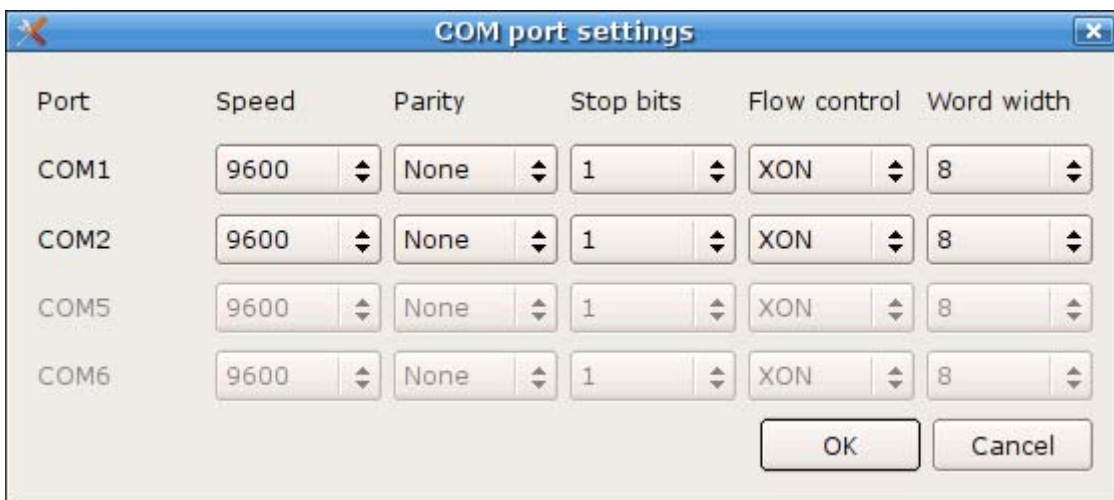
Figure 38 Setup – Hardware – Com Port Settings

3.11.3 Multiple monitors

The number of monitors – if switched on – is now recognized automatically.

See the currently valid information on www.myelux.com for a list of supported monitors

The **Setup** tab **General** shows the attached monitors.

Figure 39 Setup – General – installed screens

3.12 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

3.12.1 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

Depending on the type of VPN Client you use the corresponding configuration file must be available on the client.

Figure 40: Setup > VPN > sample.pcf

Click on **Edit** to open the file *sample.pcf* for configuration.

Auto connect: Enable this option if you want to connect and disconnect automatically.

In case of manual connection click on the network icon in the systray to display the corresponding information in the opening tabs General, Network Support and Device.

Requirement: Enable the check box "Show network status" in the **Desktop** tab > **Advanced**.

3.12.2 VPNC Client

To select the VPNC Client click **Edit**. The file *vpnc.conf* opens for configuration.
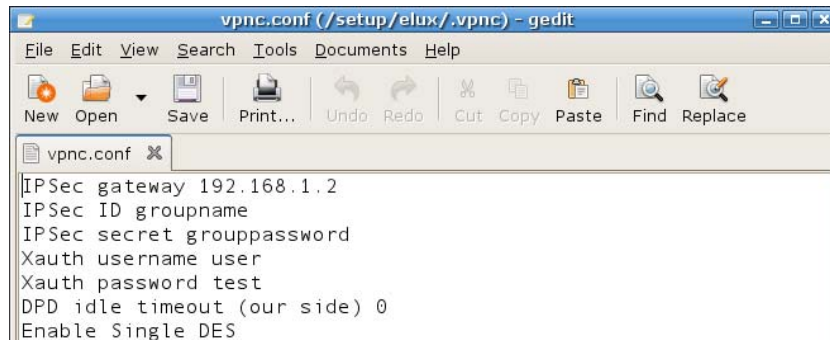
Figure 41: Setup > VPN > VPNC Client > vpnc.conf

3.12.3 PPTP VPN Client

To confiture the PPTP VPN Client please fill in the fields in the Setup tab.

Figure 42: Setup > VPN > PPTP VPN Client

3.12.4 Juniper

Having selected the Juniper Client click **Edit** to open the file *sample.conf* for configuration.

Figure 43: Setup > VPN > Juniper

3.13 Diagnostics

This tab is for diagnostic purposes, such as:

- define a debug level
- create files, system information, screenshots for debug transfer
- send the files to the FTP or Scout server or save them on a disk.
- make a Ping test
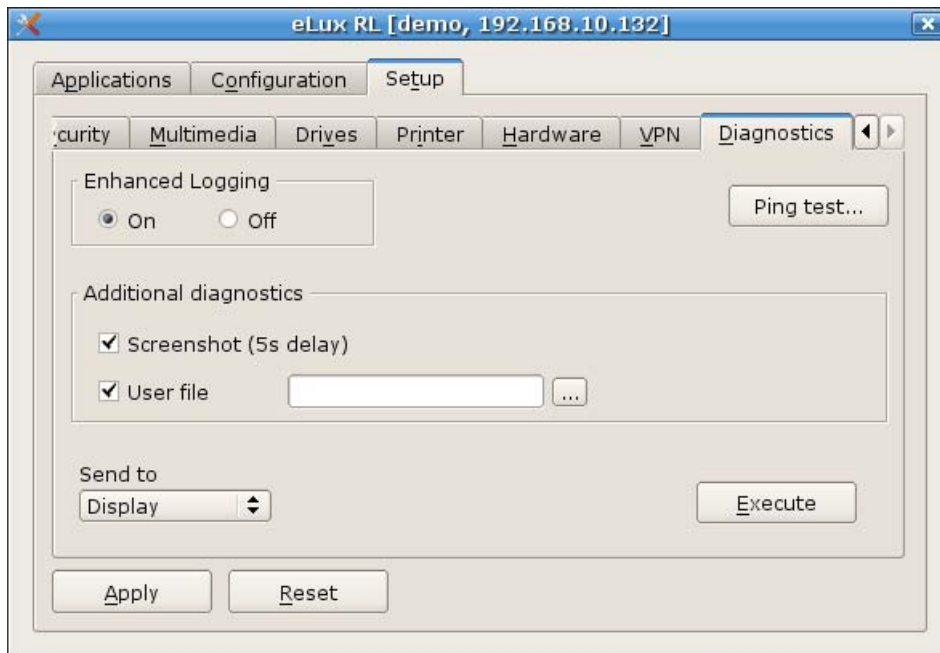
Figure 44 Setup – Diagnostics

Example for a Ping dialog:
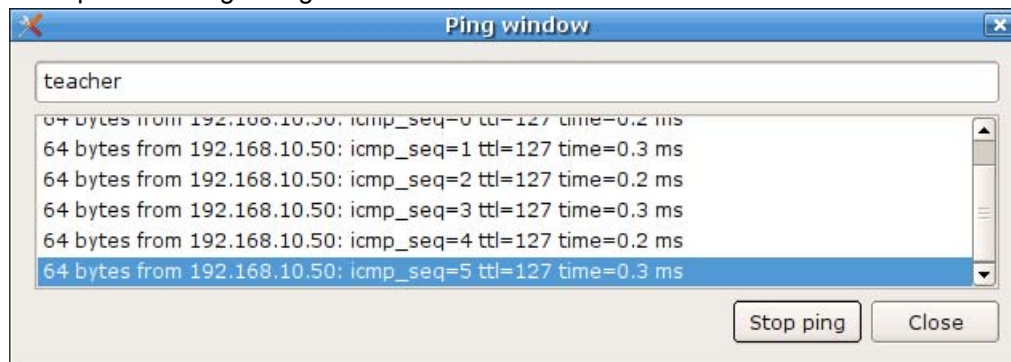
Figure 45 Setup – Diagnostics – Ping test

Send to: **Display**, Click on **Execute**

to open the **Log Viewer**.

The Log Viewer shows the automatically created diagnostic files sorted by date.

Select send to:

Scout, Click on **Execute**

The created diagnostic files are stored within the Scout installation folder.
The **Scout** menu option **View** > **Logging** > **Server files** leads directly to these folders.
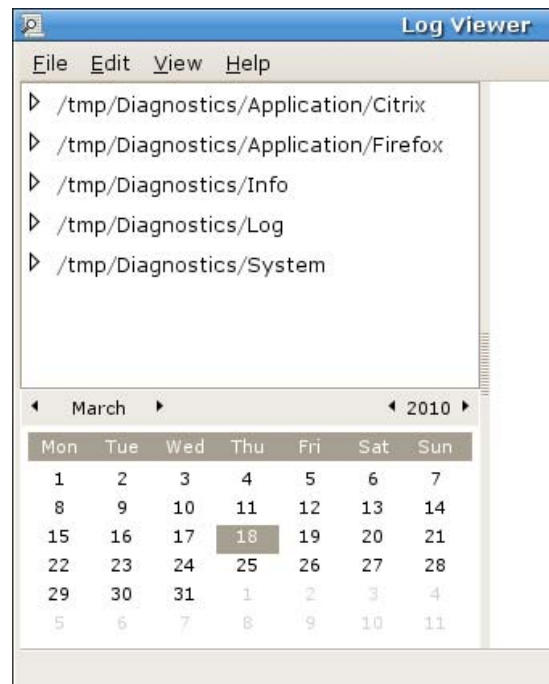
The management tool Scout Enterprise offers further diagnostics. Please consult our latest version of the *Scout Enterprise Administrator's Guide* on www. myelux.com.

4 Configuration of Applications

This chapter describes how to define an application that runs locally or how to connect to a remote server.

4.1 Introduction

eLux® *RL* offers you two types of applications:

- remote
- local

The main employment area of a Thin Client is as a terminal in server based computing. "Remote" means the application runs on a server, such as a Windows application on a terminal server. Even when an application runs remotely, client-side software is still required to initiate and maintain a session.

By nature, the Thin Client has limited resources, meaning the majority of applications will be server based. However, in addition to server applications eLux® *RL* also offers a variety of local applications. "Local" means the application runs locally on the Thin Client. Local applications include browser software (e.g. Firefox, local shell (XTerm)), and desktop tools (resource information, Explorer, Picture Viewer, CD player). This software is provided free of charge and can be downloaded from www.myelux.com or copied from the eLux® *RL* CD-ROM.

This chapter describes how to configure both local applications and session clients. In addition, further configuration may be required in the application itself. For further information on configuring session clients (such as SAPGUI or Citrix ICA), please consult the manufacturer's product documentation.

⇨ To configure a local application or session client

1. From the **Configuration** tab, click **New**. This opens the **Application definition** dialog box, which contains a number of sub tabs.
2. Click the tab for the application you want in the **Application definition** dialog box.

   Note: If the application you want does not appear as a tab, the required firmware is not installed on the Thin Client. Contact your network administrator.

3. Configure the application (see details in the following sections).
4. Click **Finish** in the **Application definition** dialog box.

4.2 Standard Options:

- **Application restart** The session will be reconnected after a user has logged off (so-called "terminal mode"). In addition, the session will be started when the terminal starts.
- **Start automatically** The session will be started when the terminal starts.
- **Desktop icon** Creates a desktop shortcut for this application on the eLux *RL* desktop.
  Note: Not available for Program Neighborhood Agent.

Additional options are application specific.

As long as the dialog box **Application Definition** is open, you cannot start any applications or activate the **Setup** tabs.

Use the task hotkey CTRL + ALT + <*cursor*> to jump between open eLux *RL* dialog boxes:

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

To start an application, from the **Applications** tab either double-click the application you want, or click to select the application and click **Connect**.

When the user shuts down the device, remote applications continue to run on the server. For this reason, it is important that the administrator either set a server-side time-out for logging off inactive accounts or instruct users to quit from within the session rather than click the eLux *RL* **Disconnect** button.

You can modify an existing application configuration by clicking **Edit**. Click **Delete** to remove an application configuration.

4.3   ICA Terminal Session

Independent Computing 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.

You have the following two configuration possibilities when connecting to a specific XenApp Server: remote desktop or Windows application. In addition, this chapter discusses the Citrix ICA Client for Linux, which allows you to set advanced ICA client settings.

Configuring a session to connect to a **Published application** is discussed in chapter… "Accessing Citrix Published Applications".
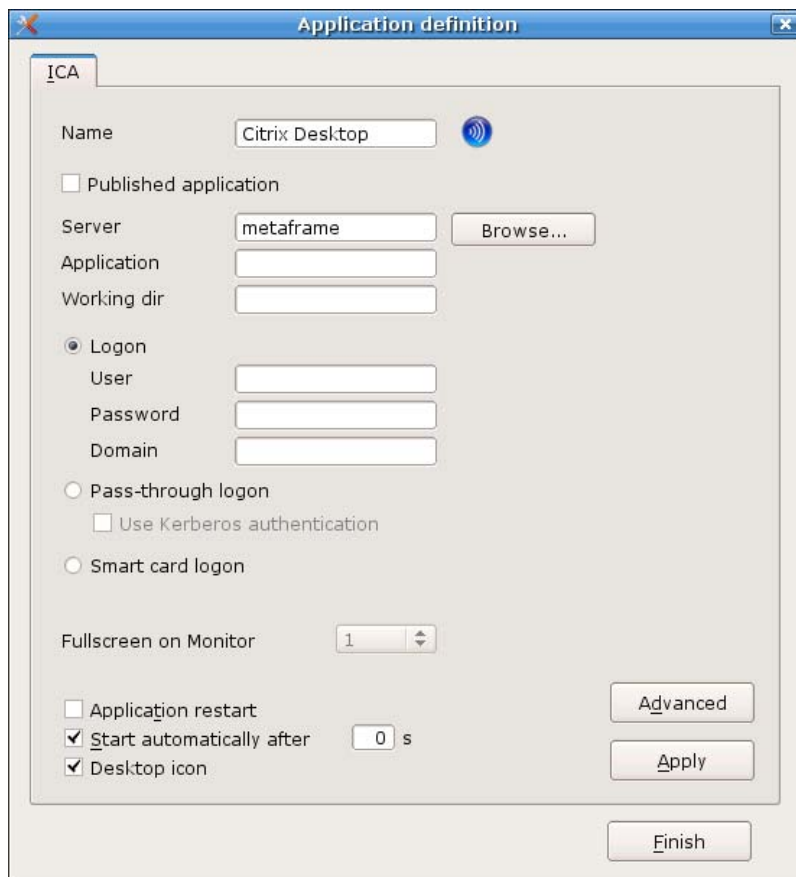
Figure 46 Configuration – ICA Remote Desktop

⇨ **To configure a remote desktop session via ICA**

In the **Application Definition** dialog box click the **ICA** tab.

- **Name**: Enter an appropriate name for this application, such as "XenServer".

- **Published application**: Leave deselected.

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

- **Working dir:** Leave deselected

- **Application:** Leave blank or enter an arbitrary name

- **User, Password, Domain:** Optional; enter to automatically log on to the terminal server

- **Pass-through-Logon:**

- **Smart card logon:**

- **Fullscreen on Monitor:**

⇨ **To configure a connection to a Microsoft Windows application via ICA**

In the **Application Definition** dialog box click the **ICA** tab.

The parameters are the same as above with the following exceptions:

- **Name**: Enter an appropriate name for this application, such as "MS Excel" for Microsoft Excel.
- **Application:** Name of the Windows application (for example, notepad.exe), including path, for example,
  `c:\Program Files\Microsoft Office\Office\EXCEL.EXE`
- **Working dir:** (optional) Enter the working directory of the Windows application.

4.3.1 Advanced Citrix ICA Settings

Using Citrix ICA, you can access server-specific applications or published applications. Other features include:

- Client drive mapping
- Client printer mapping
- COM port mapping
- Low bandwidth requirements
- Citrix ICA Client hotkeys
- Seamless Windows support
- Program Neighborhood Agent
- 128-bit SSL support

Note that some of these features are server-specific.

Configuration of advanced ICA settings is done by clicking the **Advanced** button in an ICA application definition.
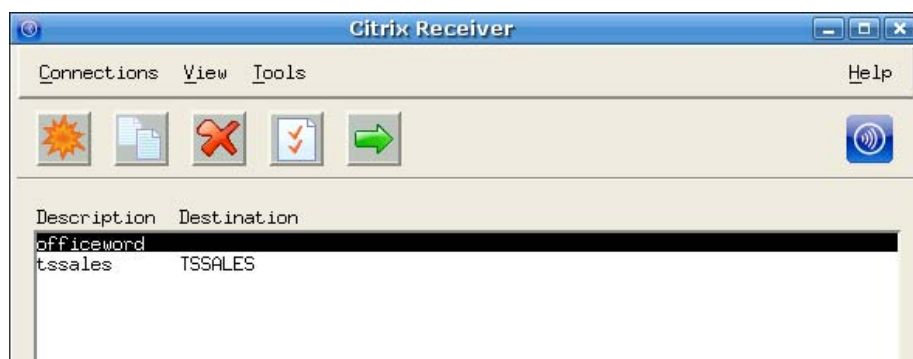
Figure 47 Configuration > ICA > Advanced > Citrix Receiver

This opens the Citrix Receiver, which is software from Citrix and has a different look than the eLux *RL* control panel.

If you do not see a list of ICA connections, you may not be in Connection view. In the **View** menu, click **Connection View**. ICA sessions defined in eLux RL are automatically entered in the Citrix ICA Client. You do not have to redefine them here.

PNAgent view is described in chapter 5.3.3 PN Agent.

Warning Do not define a new ICA session in the Citrix Receiver! Define new sessions in the eLux RL **Configuration** tab. If you define new sessions in the Citrix Receiver, they will not be accessible via the eLux RL **Applications** tab!

The configuration file for the Citrix Receiver is named "wfclient.ini" and resides on the Thin Client under: `/setup/ica/wfclient.ini`

This file can easily be viewed using the **Diagnostics** tab > **ICA files**.

Published applications, a feature commonly in use with Citrix server farms, are discussed in the following chapter.

For further information on configuring the Citrix ICA Client, such as **drive mapping**, **COM port mapping** and **server location**, please consult the Citrix documentation "*Citrix Client Administrator's Guide*" which you find on www.myelux.com > Manuals & Documentation > Misc.

4.3.2 Accessing Citrix Published Applications

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, the eLux taskbar must be enabled in the **Desktop** tab. Only then is it possible to maximize minimized windows again.

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

4.3.2.1 Via ICA Application Definition

You can configure a session to access a published application via the eLux *RL* control panel.

Note: The application name must correspond exactly to the name published on the server.
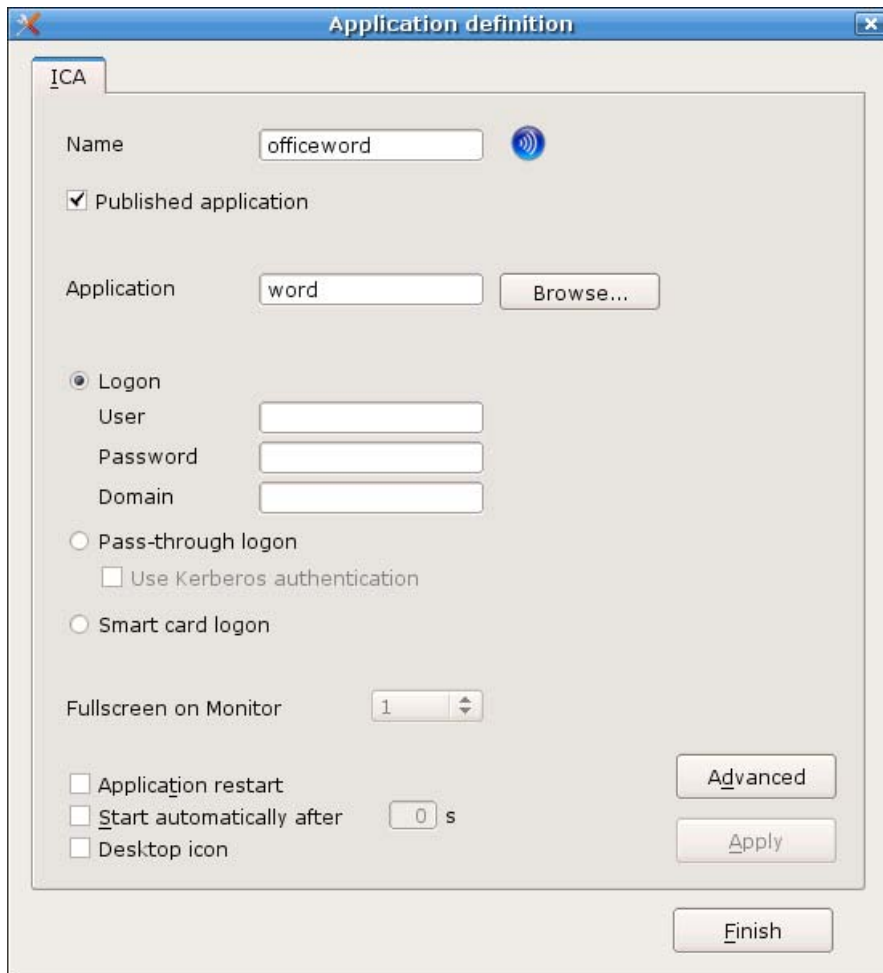
Figure 48 Application Definition – ICA – Published Application

- **Name:** Enter an appropriate name for this application.

- **Published application:** Select

- **Browse…:** You can browse for published applications or servers. The first listed address of the connection options is used as browser address.

- **Application**: Name of the published application

- **Pass-through logon:** If enabled an ADS logon is required on the Thin Client

4.3.2.2 Via Citrix Receiver

Alternatively, you can search for available published applications in the **Citrix Receiver.** When you are done, the parameters will automatically be transferred to eLux *RL*.
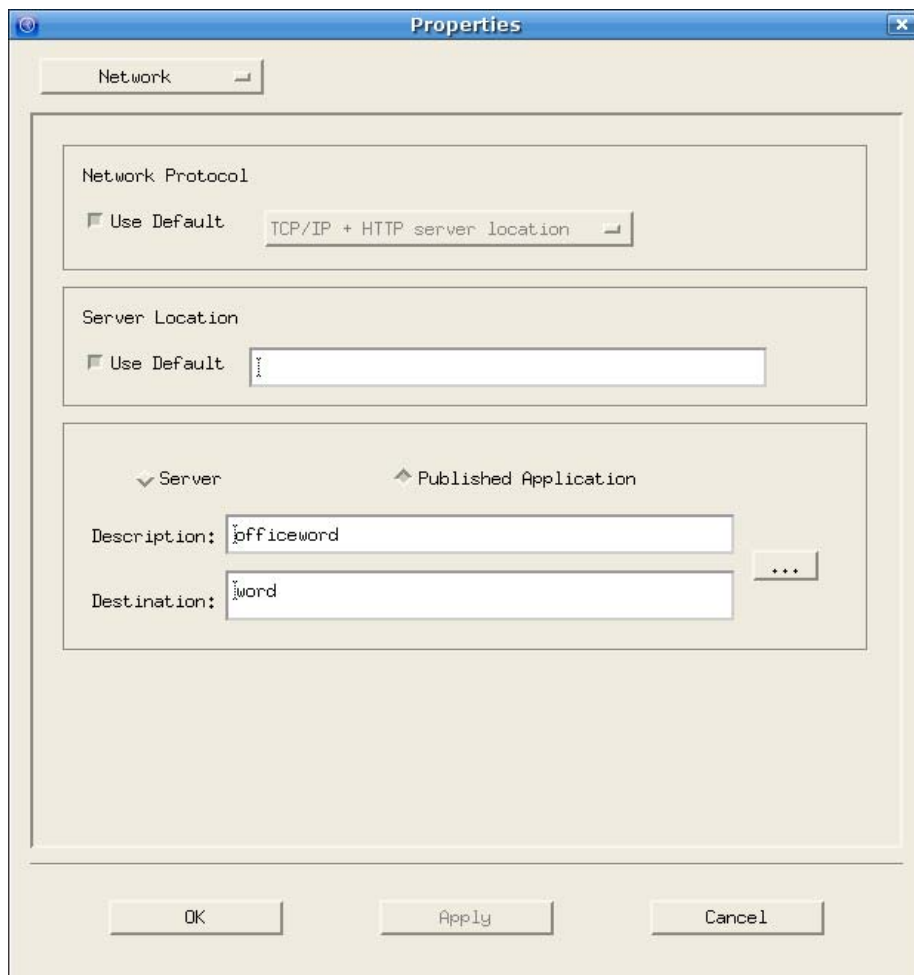
Figure 49 Citrix Receiver – Connection Properties

⇨ **To configure a published application in Citrix Receiver**

1. In the **Application Definition** dialog box click the **ICA** tab.
   Name: Enter an appropriate name for this application.
2. Click **Advanced**. The **Citrix Receiver** opens.
3. Select the session you want to configure.
4. Click **Connections** > **Properties** > Network
5. Select the check box **Published Application**. Type the name of the published application or select the name from the pop-up menu to the right of the **Server** field.

   Note If no applications appear, check that the browser protocol is correct.

6. In the **Properties** dialog box, click **OK**.
7. Exit the **Citrix Receiver** to return to the eLux *RL* ICA application definition. The published application parameters are automatically entered in the eLux *RL* ICA application definition.
8. Click **Apply** and **OK**.

4.3.2.3 Via Web Interface

You can launch published applications from a local browser using the Web Interface.

Required software: browser software and Citrix ICA Client version 7.x

⇨ **To access a published application via local browser**

1. Configure a local browser.

   - **Name**: Enter an appropriate name for this application.

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

   - **Proxy type** Choose one of the following:

     No proxy: If you don't use a proxy server.

     Manual (Proxy:Port): If you use a proxy server, enter it in the format:
     <proxy server IP address or name>:<port number>.

     Auto (URL): If you use an automatic proxy configuration file.
     Example: `http://www.yourserver.com/autoproxy.pac`

   - **Browser type:** Select the browser you want: Firefox (for the time being)

   - **Kiosk mode:** Leave unchecked.

2. Start the browser from the eLux RL **Applications** tab. The Web Interface appears. Enter your credentials to log on.

3. After successful logon, a list of published applications is displayed. Click on an application to start it.

For an overview and detailed information on the **Citrix Receiver** see the Citrix documentation *Citrix Client Administrator's Guide* which you find on www.myelux.com > Manuals & Documentation > Misc.

4.3.3 Citrix Secure Gateway
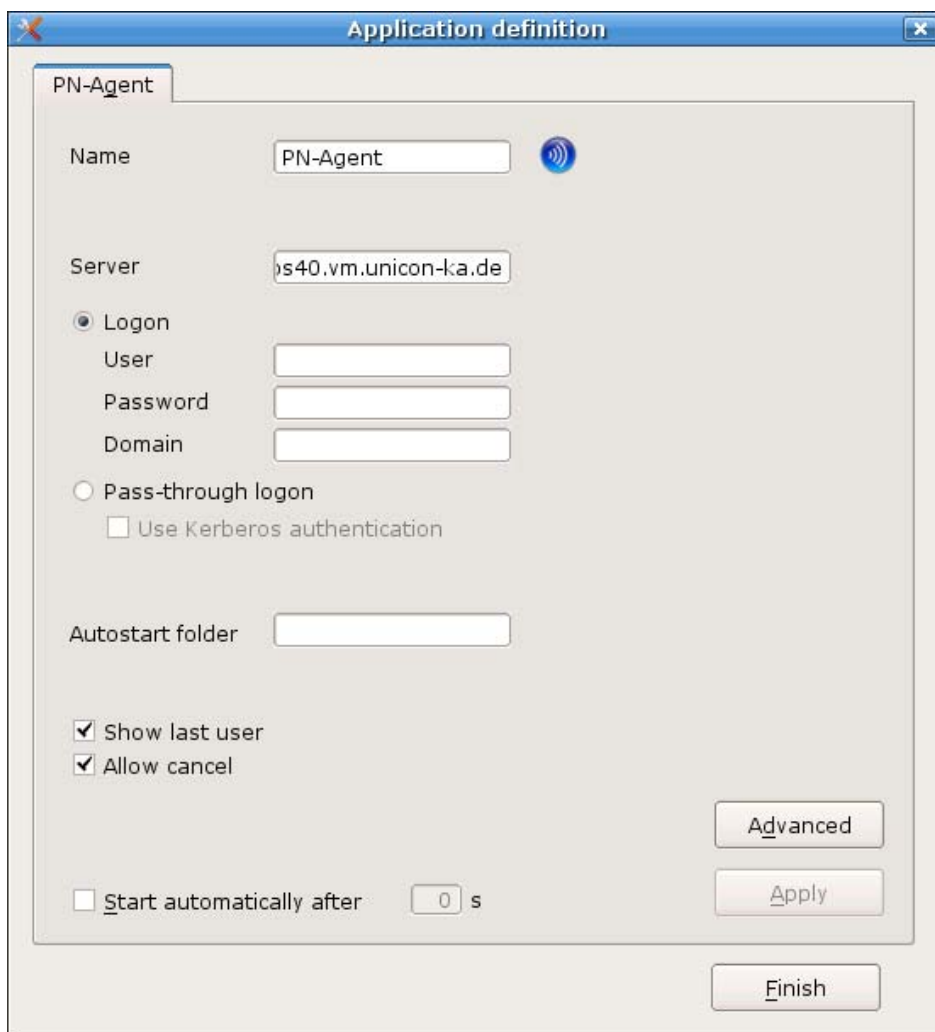
By means of a certificate-based server authentication it can be secured that the server you are connecting to is the right one.

For details please consult the Citrix documentation *Citrix Client Administrator's Guide* which you find on www.myelux.com > Manuals & Documentation > Misc.

4.3.4 PN-Agent

The Program Neighborhood Agent enables users to connect to published resources (i.e. published applications and published content) through a server running the Web Interface. The configuration for all users is defined in the configuration file *config.xml*, stored on your server running the Web Interface. The default location for *config.xml* on a server is //Inetpub/wwwroot/Citrix/PNAgent. The PN-Agent downloads its configuration data from the server running the Web Interface when it is started, and can be configured to update settings and the user interface periodically.

Administrators should use the Web Interface to customize users' PN-Agent options, rather than editing *config.xml* manually. For more information about editing config.xml using the Web Interface, see the *Citrix Web Interface Administrator's Guide*.

Figure 50 Configuration – PN-Agent

⇨ **To configure Program Neighborhood Agent settings on the Thin Client**

- **Name**: Enter an appropriate name for this application.

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

- 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
  ```

- **User, Password, Domain:** Enter to automatically log on to the terminal server.

- **Show last user** 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** When activated, allows the user to close the XenApp logon dialog box.

- **Autostart folder** On the server, in Program Neighborhood Agent create a folder (or subfolder) with published applications. Enter the name of the folder here. All published applications in this folder will automatically be started when the session connects.

- **Start automatically:** Click this check box to open the session when the terminal starts.

Click **Apply** and **Finish**.

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 51 Advanced PNAgent settings

⇨ **Reconnect Applications**

There are 3 options to connect automatically:

- None (default)
- Disconnected
- Active and Disconnected

⇨ **Timed Logoff**

You can schedule logging off from a PN Agent session by a given period of time (in seconds), and without having to wait for the last PN Agent application to close.

For manual logoff you have the options to define whether to log off from server only, from server and applications or logoff from server and disconnect applications.

⇨ **Manual Logoff**

- Log off only server
- Log off server and applications
- Log off server and disconnect applications

When this session connects, the Thin Client will retrieve all applications from the defined XenApp server which were published for the given user credentials. The published applications will be displayed in the eLux RL control panel and taskbar menu (in addition to the other defined applications) in a tree-like structure: the top-level name is the PNAgent application definition name, second level are the published applications or folders from the server (both applications and folders are defined server side).
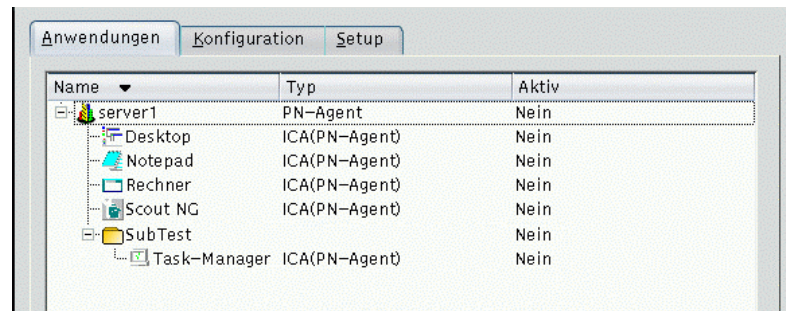
For detailed information on configuring the PN-Agent see the Citrix documentation *Citrix Client Administrator's Guide* which you find on www.myelux.com > Manuals & Documentation > Misc.

4.3.4.1 Domain list

A domain list can be created for the PN-Agent to offer the user a selection.

1. Create a text file "icadomains".
2. Enter the domains you want (one domain per line)
3. Save the file in the Scout Enterprise installation folder.
4. Transfer the file to "/setup/icadomains" (without the .txt extension) on the Thin Client using the Scout Enterprise file transfer functionality.

When you start a PN-Agent session a dialog will open to logon to a Citrix XenApp web server. The domains are offered for selection in a dropdown list (domain1, domain2, domain3). Also, you can preset a domain during the PN-Agent application definition (e.g. "work.myelux.com").

4.3.4.2 Troubleshooting

If you get the error message when logging on using the PN-Agent:

```
One or more fields are incorrect
```

Check if your logon credentials are correct.

Note: In our experience, the PN-Agent will not always accept an empty domain name field. If your server does not belong to a Citrix domain, we recommend entering the Windows domain at logon.

4.3.5 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 Presentation Server Client for Linux includes a helper application, xcapture, that allows 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 desktop (including non-ICCCM-compliant applications) and an application running in an ICA Client window.

⇨ **To configure xcapture**

1. In the Application Definition dialog box click the **Local** tab.

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 RL desktop.

2. Click **Finish**.

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

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.

4.4   RDP Remote Desktop and RDP Windows Application

This connection corresponds to the ICA functionality using Microsoft Remote Desktop Protocol (RDP). It is used to connect to a Microsoft Terminal Server. The application type is a native RDP client with the free software "rdesktop." For further information see www.rdesktop.org.

There are two configuration possibilities: Windows desktop or individual application.

 A remote desktop session allows you access to the desktop of a terminal server. You can run any applications available on the desktop, in any order.
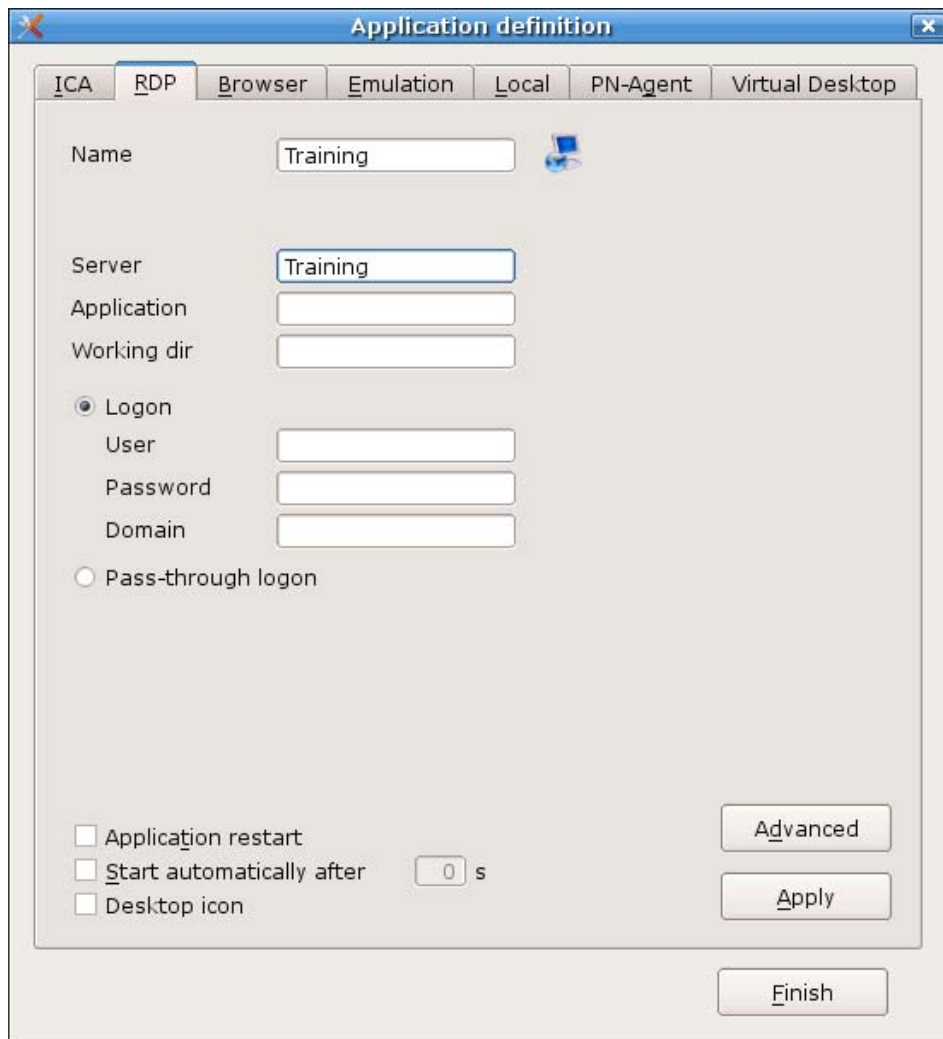
Figure 52 Application Definition – RDP Remote Desktop

⇨ **To configure a remote desktop session via RDP**

> In the **Application Definition** dialog box click the **RDP** tab.

- **Name**: Enter an appropriate name for this application, such as "RDP Desktop"
- **Server**: Enter the IP address or name of the terminal server.
- **Application**: Leave blank.
- **Working dir**: Leave blank.
- **User, Password, Domain:** Enter to automatically log on to the terminal server.
- **Pass-through-Logon:**

⇨ **To configure a connection to a Microsoft Windows application via RDP**

In the **Application Definition** dialog box click the **RDP** tab.

The parameters are the same as in the last chapter with the following exceptions:

- **Name**: Enter an appropriate name for this application, such as "MS Word" for Microsoft Word.

- **Application**: Enter the name of the Windows application (for example, notepad.exe), including path, for example,
  `c:\Program Files\Microsoft Office\Office\Winword.exe`
  Note: System variables are allowed, for example: `%SystemRoot%\system32\notepad.exe`

- **Working dir**: (optional) Enter the working directory of the Windows application. Do not end the parameter with a backslash. Note: System variables are allowed, for example:
  `%HOMEDRIVE%%HOMEPATH%`

4.4.1 Advanced RDP Settings

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.
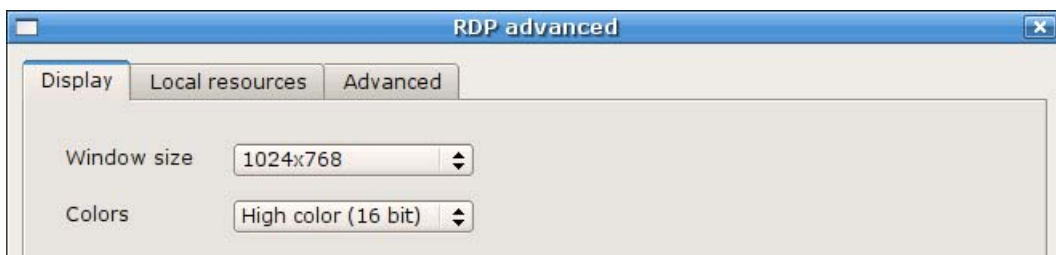
Figure 53 RDP Advanced - Display

The **Local resources** tab offers additional settings for terminal servers that support RDP 5.2 or higher. **Note**: This tab is only visible if you have the native RDP client version 1.3.1 or higher installed ("rdesktop52"). 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 a terminal server that supports RDP 5.2 or higher.
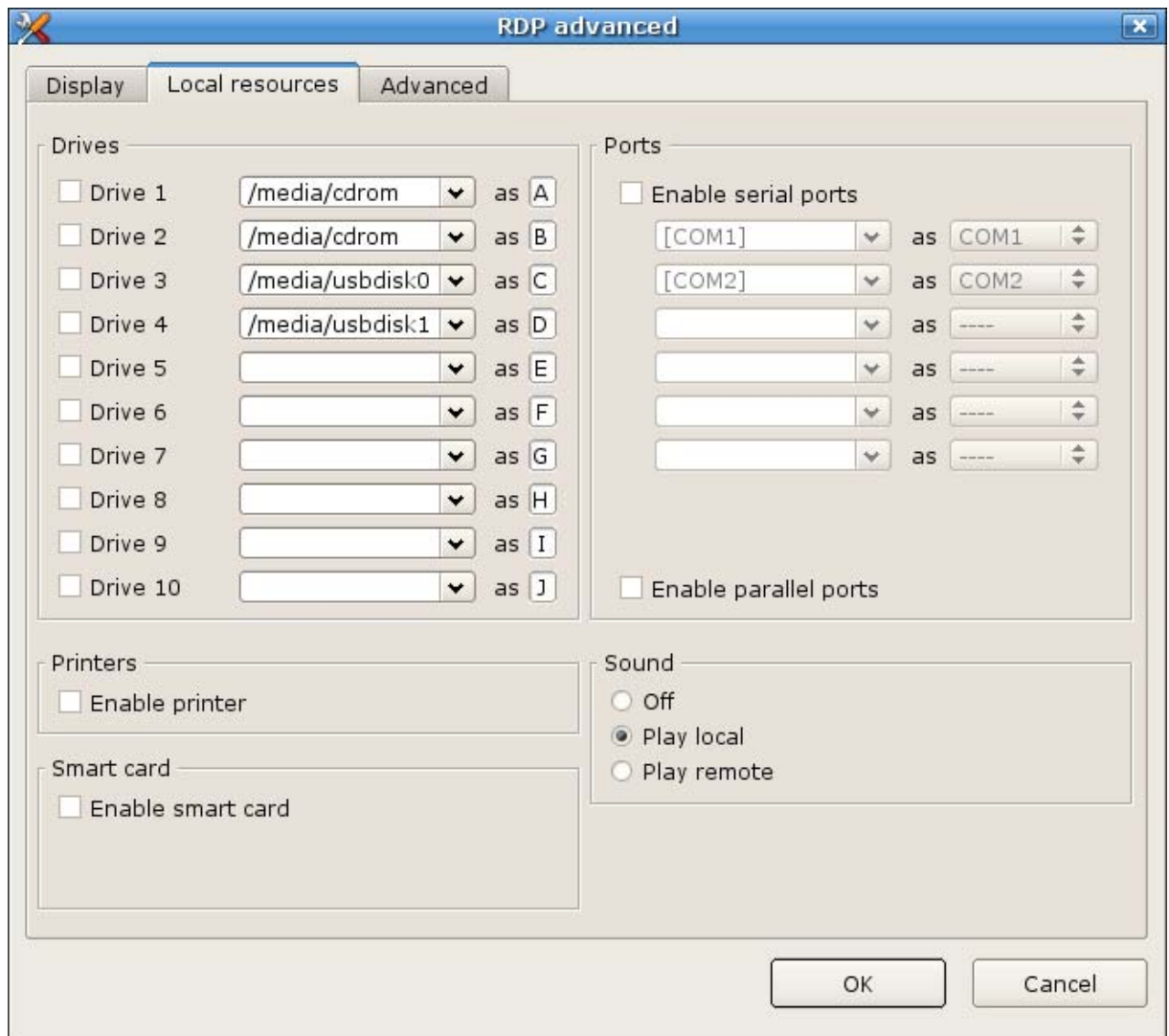
Figure 54 RDP Advanced – Local resources

- **Drives** 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. 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.
- **Printers** Allows you to automatically create up to four printer definitions for this session. The printers must be defined in the eLux *RL* 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" check box in the eLux *RL* printer profile.
- **Sound** "Play local" means 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**
  Enabling the check box means that smart cards can be used for certificate-based logon.

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

Figure 55 RDP Advanced – Advanced

- **Protocol** Allows you to set the protocol to 4 or 5. By default, the RDP protocol 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 *RL* control panel will be used.
  Warning: The keyboard language set in RDP advanced settings may not differ from the keyboard language set in the eLux *RL* control panel.
- **Disable window manager decorations** The border that appears on eLux *RL* 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.
- **Bandwidth:** You can select between default, Modem, Broadband, LAN

4.4.2 Command RDESKTOP

Advanced users have the possibility of calling the native RDP client from a local shell.

To see command line parameters, enter the command `rdesktop -h` in a shell. You can then define a session with any rdesktop parameter in the tab **Local** > **Local application** > **Customized**. See also section "Notes to Custom-defined Applications".

4.4.3 Invisible RDP Application

An RDP application which is to be invisible for the users can e defined by entering RDP_TEMPLATE (capital letters) in the **Name** field.
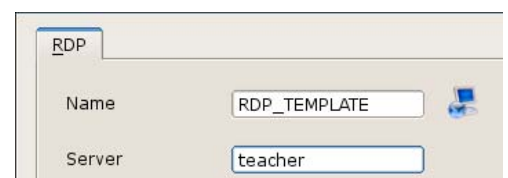
Figure 56 RDP – Definition of an invisible application

4.5   Virtueller Desktop → VMwareView

The parameters must be correctly set 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.
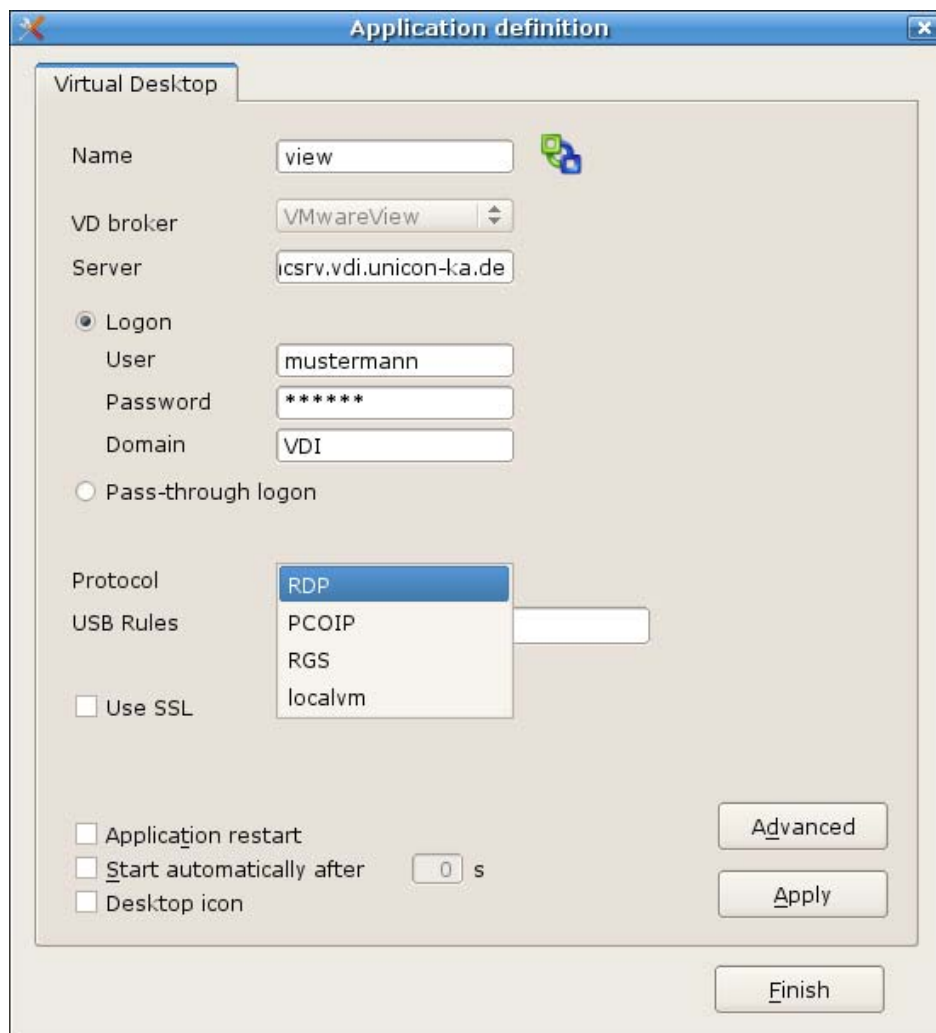
Figure 57 Virtual Desktop – Configuration of VMware view

⇨ **Configuration of the Virtual Desktop at the Thin Client**

- **Name**: Enter any logical name for this application

- **VD Broke**r: Select VMwareView from the dropdown list

- **Server:** Enter the IP address or the name of the server

- **Login Data** enables the automatic login to the terminal server (user, password, domain)

- **Passthrough Login** Enabling this option sends the following parameters to the client:
  $ELUXUSER
  $ELUXPASSWORD
  $ELUXDOMAIN

- **Protocol**: Preset are: RDP, PCOIP, RGS, localvm

4.6 Browser

At the time of publishing this manual the following browser is available with eLux *RL*.

4.6.1 Firefox

Required Software

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.

For a description of EPMs and FPMs, see the *ELIAS Administrator's Guide.*

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, see www.mozilla.org.
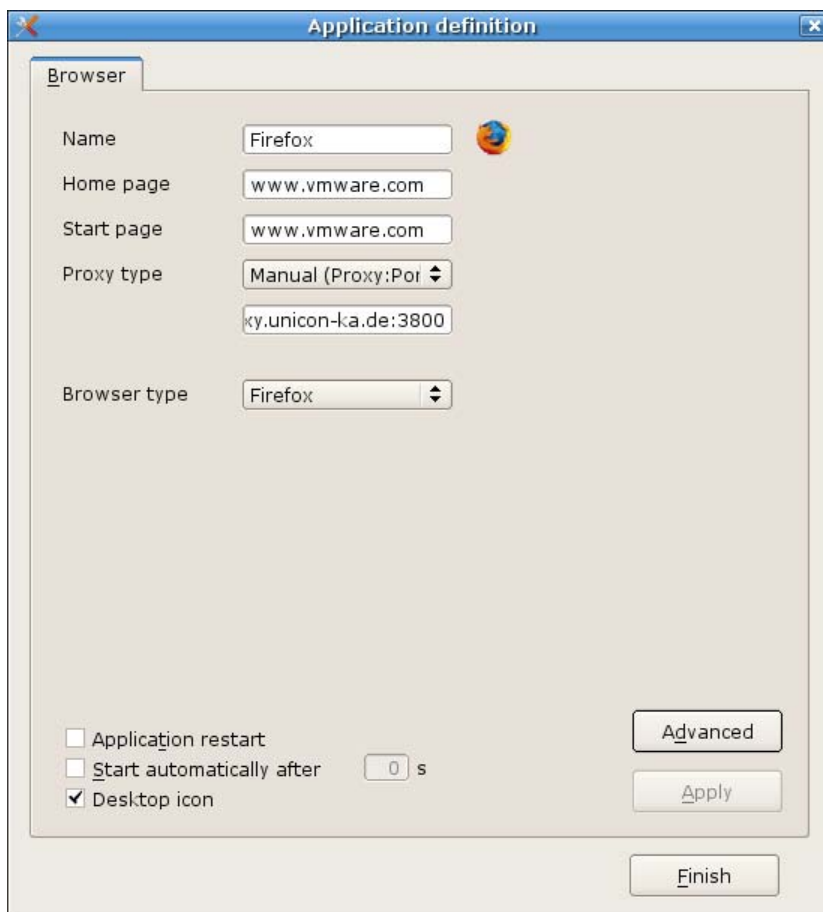
Figure 58 Application Definition - Browser

⇨ **To configure a browser application**

1. In the **Application Definition** dialog box click the **Browser** tab. A series of fields appears.

   - **Name**: Enter an appropriate name for this application, such as "www."

   - **Homepage**: Enter a home page for the browser.

   - **Start page**: Enter the first Web page to be called when the system starts.

   - **Proxy type**

        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 nam*e>*:<port number>*.

        Auto (URL): If you use an automatic proxy configuration file.
        Example: `http://www.yourserver.com/autoproxy.pac`

   - **Browser type**

     Required Software

     A selection of browsers will only be given if the software for **several** browsers has been installed.

2. Click **Apply** and **Finish**.

Note By default, all browser files (cache, history, bookmarks, etc.) are saved to the device flash memory, which is limited. This can quickly use up available memory and interfere with work. To avoid this, configure the browser to save files to a network drive.

You can make additional settings configurations in the browser itself. For further information consult the respective browser documentation at www.mozilla.org/products/firefox.

4.6.1.1 Kiosk Mode

Firefox comes with a default kiosk mode with the following features:

- URL bar has been blended out
- Toolbar cannot be customized by user
- "Save to disk" is deactivated (downloads still allowed)
- Preferences cannot be customized by user
- Not in full screen mode

The following options can be configured easily when clicking **Advanced** in the Browser definition dialog:

To make additional changes, you will have to customize kiosk mode yourself. The JAR archive that comes with Firefox can be used as a template. It contains all XUL documents used to describe the user interface.

⇨ **To customize kiosk mode for Firefox**

1. Install the kiosk mode software (in the respective browser package).

2. Copy the following file to a machine with unzipping software:

   `/opt/MozillaFirefox/lib/chrome/modes/kioskmode.jar`

Tip On the Thin Client, you can use the UNIX copy command ("cp *<file directory> <target directory>*") to copy the file to an NFS or SMB drive, or in the eLux *RL* control panel the FTP function available in **Setup** > **Diagnostics**.

3. Unzip the file.

Windows: Winzip tool

UNIX: unzip tool (command: `unzip kioskmode.jar`)

The directory "content" with the subdirectory "browser" will be created.

Warning Do not change the directory structure. This will make your rezipped JAR file unusable.

4. Edit the appropriate files using Notepad or an XUL editor. Comment out functions you want to deactivate and interface elements (menus, toolbars, etc.) you do not want displayed. For an example, view the document "browser.xul" from "/opt/MozillaFirefox/lib/chrome/modes/kioskmode.jar", which mainly describes the browser interface.

Tip A description of what to edit exceeds the scope of this document. For more information, there are many tutorials available on the Web, for example, http://tln.lib.mi.us/~amutch/pro/phoenix/kiosk.htm.

5. Zip the file to the name "kiosk.jar".

Windows: Winzip program

UNIX: "zip" command with the "-r" option (recursive) (`zip -r kiosk.jar`)

6. Copy the file to the following directory on the Thin Client:

   `/setup/firefox/kiosk.jar`

7. Set the homepage and start page in the application definition (**Configuration** > **New** > **Browser**). Use full URL format: "http://*<domain name>*". The Web page can be on the Internet, on your thin client, or on another computer on the network. Click to select **Kiosk mode**.

Firefox uses the *.jar file according to the following selection rules:

1. /opt/MozillaFirefox/lib/chrome/modes/normalmode.jar

   This file is used if the **Kiosk mode** check box in the browser definition is deactivated (always the case when the „Kiosk mode" software has not been installed).

2. /setup/firefox/firefox.ini

   The following entry in the Firefox initialization file is used if the **Kiosk mode** check box in the browser definition is activated, "File=*<path>*/*<file>*", where *path* is the complete path of the *.jar file and *file* is the file name. The default value "/setup/firefox/kiosk.jar" can be customized to the path and name of your choosing, for example "/smb/smith/browser/testkiosk.jar".

3. /opt/MozillaFirefox/lib/chrome/modes/kioskmode.jar

   This file is used if the **Kiosk mode** check box in the browser definition is activated and the *.jar archive specified in the Firefox initialization file (/setup/firefox/firefox.ini) does not exist.

4.7   Emulation

Use the **Emulation** tab to connect to mainframes or UNIX systems.

For the time being the following emulations can be configured:

- **X11**: for X applications on remote (Unix) systems which use the local X server
- **Powerterm**: for IBM mainframes, IBM AS/400, UNIX, VAX/Alpha OpenVMS, Tandem (NSK), HP-3000 and Data General (to be licensed).

4.7.1   X11 for X Applications Using the Local X Server

The X11 server developed by The XFree86 Project, Inc (http://www.xfree86.org/) and its contributors is included in the base OS. No additional software must be installed.
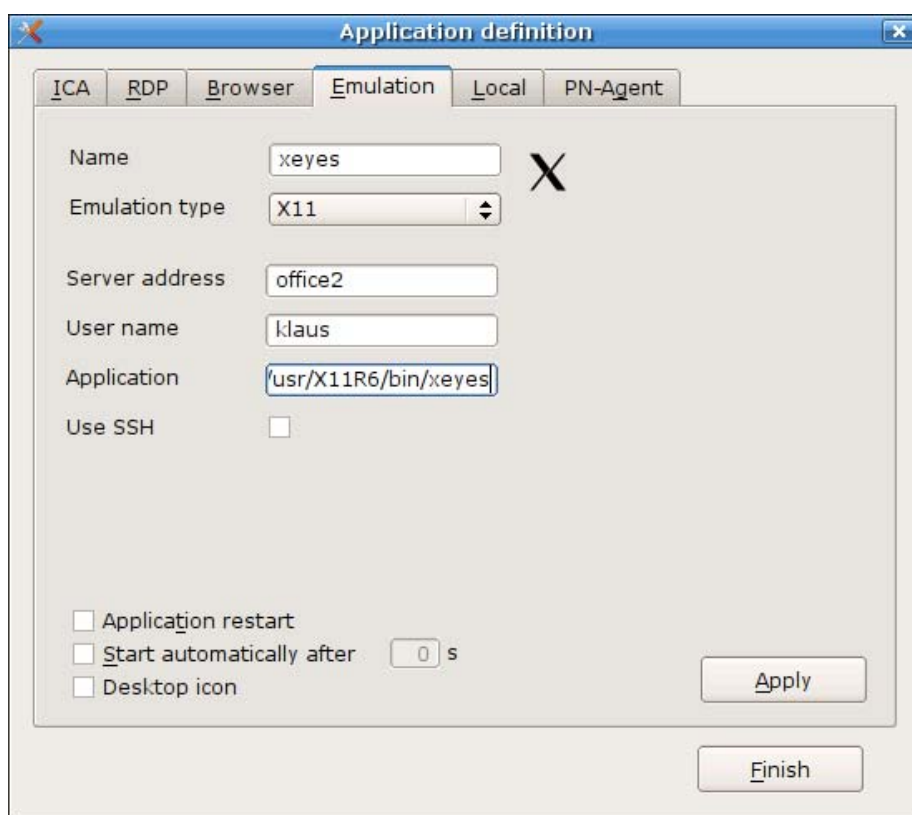
Figure 59 Application Definition – Emulation

⇨ **To configure an X11 session**

1. In the **Application Definition** dialog box click the **Emulation** tab.
2. Click **X11** in the **Emulation type** list. A series of fields appears.
   - **Name**: Enter an appropriate name for this application, such as "X11."
   - **Server address**: Enter the IP address (or name) of the UNIX server.
   - **User name**: Enter the username on the UNIX server.
   - **Application**: Enter the X application name with its complete path.
   - **Use SSH**: If selected, the X11 session is started via the Secure Shell (SSH) protocol. Only the public key authorization is permitted).
3. Click **Finish**.

4.7.2 PowerTerm InterConnect

To use this software, you must have the "PowerTerm InterConnect" (powerterm) package installed.

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 product has to be licensed. The software includes a 30-minute trial period. To purchase a license, please contact sales@myelux.com or order via the Fujitsu Siemens distribution channel.

⇨ **To start PowerTerm InterConnect**

1. In the **Application Definition** dialog box click the **Emulation** tab.
2. Click **PowerTerm** in the **Emulation type** list. A series of fields appears.
    - **Name**: Enter an appropriate name for this application, such as "PowerTerm."
    - **Parameter**: (optional) If you leave this field blank, the default setup file (ptdef.pts) will be used. Alternatively, you can 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""`

      See the PowerTerm documentation for more information on PowerTerm parameters and scripts.
3. Click **Finish**.
4. From the **Applications** tab, double-click or use the **Connect** button to run the application.
5. 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"). To create a new configuration file, start PowerTerm, configure your settings and save the file using a different name (**File** menu > **Save terminal setup as**). When you open a connection (**Communication** menu > **Connect**), you can select the configuration file by clicking on the browse button next to "Setup File" in the "Upon connection run" area. Initially only the default configuration file (ptdef.pts) is available.

You can transfer a configuration file to many Thin Clients using the "File Transfer" feature of Scout Enterprise – see the *Scout Enterprise Administrator's Guide* for more information.

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

4.8 Local

eLux *RL* offers an easy-to-use graphical user interface (the control panel). All configuration settings and application definitions can be made using point-and-click. No Linux knowledge is required.

Because eLux *RL* is Linux-based, you also have the option of entering commands directly in the command-line interface (CLI). It helps if the administrator has experience either with Linux or using a CLI (such as the Windows CLI). Selected commands are provided in this manual.

The command line does not replace the GUI, rather it extends the options available to experienced administrators.

The following applications can be configured in the **Local** tab:

XTERM, File Manager, Movie Player, Thunderbird Mail Client, ICA Connection Center. No Machine,Custom

As an example, we describe the local applications XTERM and Custom.

4.8.1 XTerm (Local Shell)

The local shell is useful for troubleshooting and for defining applications interactively. For example, if you are experienced with using the command line, you can type in the command line for the application, see if it works correctly and test different options. You can then configure that application using the eLux RL GUI or by entering that same command line into the control panel. Using UNIX commands and the UNIX editor vi, you can browse local directories, edit configuration files, or move files between the Thin Client and mapped SMB drives (such as log files to send to your support team).

The predefined command **XTerm** opens a local shell. The user is `elux` and has no root authorization.
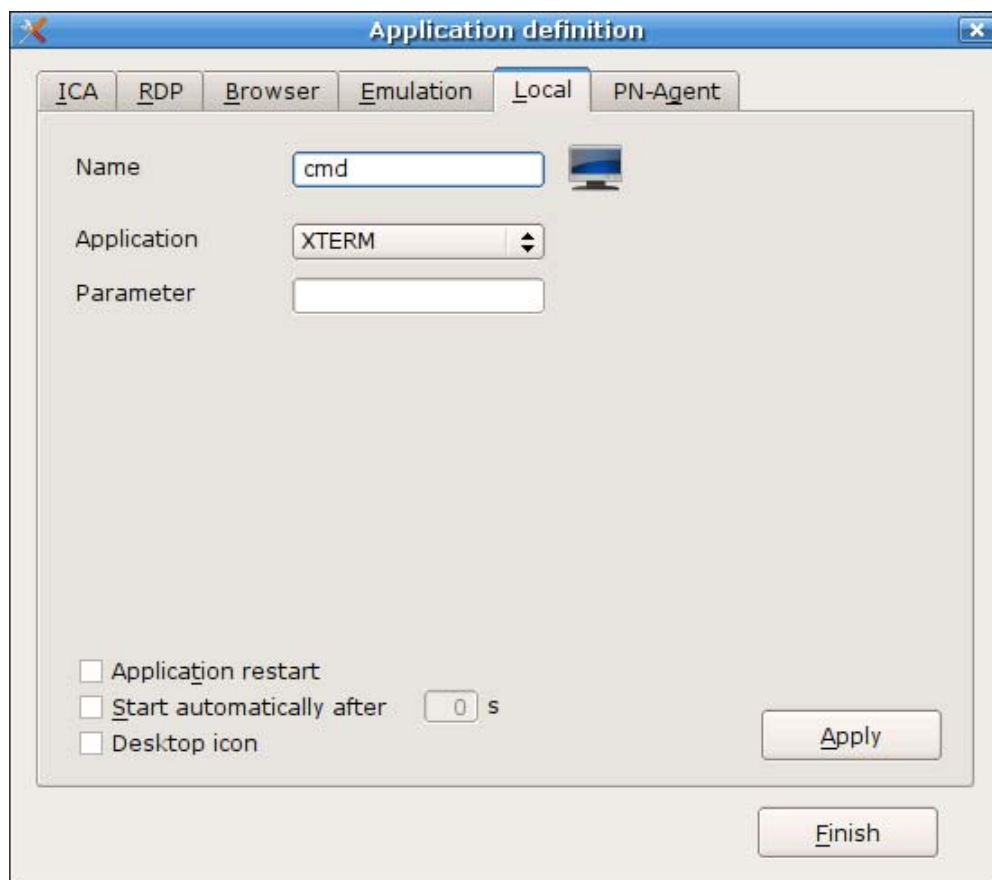
Figure 60 Application Definition – Local

⇨ **To configure a local shell**

1. In the **Application Definition** dialog box click the **Local** tab.

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

- **Application**: Select **XTERM**.

- **Parameter:** (optional) Enter the desired parameter. See the examples below.

2. Click **Finish**.

Example 1: Setting font and color parameters

Enter the following in the **Parameter** box:

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

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

Example 2: Setting font and color parameters and calling a program

Enter the following in the **Parameter** box:

```
-fn 10x20 -bg navy -fg white -e telnet -l schmidt myhost
```

fn	font
10x20	font size (big)
bg	background color
fg	foreground color
-e	parameter to call a program
telnet	ASCII program
-l schmidt	program-specific parameter
myhost	host required by telnet program

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

Tip: To copy in XTerm, click the middle mouse button.

The properties for all X applications are set in the resource file "Xdefaults" located in /setup. For more information on Xdefaults, see the *Scout Enterprise Administrator's Guide.*

4.8.2 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**

From the **Configuration** tab, click **New**.

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`.

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 and www.millenux.de.

4.8.3 Notes to "Custom" defined Applications

Defining local commands is special – it allows you to define applications which can be called within a shell. (Note that the average user may not have the required knowledge about commands.)

The user must be authorized to start the applications. All commands are carried out by the UNIX user "eLux RL" (UID = 65534).

We recommend that you test whether the command works by calling it from within an XTerm session before entering it in the **Application definition** dialog box. This is the only way you will receive feedback via error messages. You will not receive feedback when you enter it in the **Local** tab, as no error messages are displayed when it is called from eLux *RL*.

If you enter a command that does not call an X-capable application, you will not see anything when it is carried out.

⇨ **To enter a command**

- In the **Application Definition** dialog box click the **Local** tab.
    - **Name**: Enter an appropriate name for this application.
    - **Application**: Click **Customized**.
    - **Parameter:** Enter the desired command, including all program parameters. See the examples below. For more information see the man pages of a Linux system.
    - **Hidden:** Does not display the application in the **Application** tab.
- Click **Finish**.

If you select the option "Hidden," you must select "Start automatically" (or "Application restart") for the command to run.

Example 1: Retrieve any file from an FTP server automatically

Enter the following:

`wget [-O <outputfile>] <URL>`

The command

`wget –help`

offers all the parameters.

Files can also be retrieved from a Web server.

Example 2: Retrieve any file from a Web server automatically

`ftp –o /setup/local/eterm/eterm.map http://mywebserver/confiles/eterm.map`

This command is entered on one line. Keep in mind that files can only be transferred to the local directories `/setup/public` and `/setup/local/`*<application>*. Further, the memory area is restricted.

To see the current memory usage, enter the shell command `df` (=disk free) to see free disk space and `df –i` to see the number of I nodes. For example on a 32-MB flash, data saved in `/setup` cannot exceed 512 KB or 100 files.

Further line commands and parameters can be found in the product's online documentation or the Internet.

"Start automatically" with "Customized command"

You can use the customized command features to retrieve a configuration file, as in the examples above. However, the order in which applications are started automatically (**Start automatically** check box) is not defined. If both the application and a local command to get its configuration file are set to "Start automatically," this application may be started before the configuration file arrives. If this conflict occurs upon start, restart the desktop.

5 Administration Functionality

5.1 eLux® *RL* Desktop

- A desktop icon can be created for all defined application. The icons are also stored in the start menu, so that the application can be opened via the start menu as well. When using USB storage devices, the files can be moved to the desktop by "Drag&Drop".
- PDF files can simply be opened by a double click.
- On special request further Gnome applications can be added, such as CD burning software, Open Office, skype.
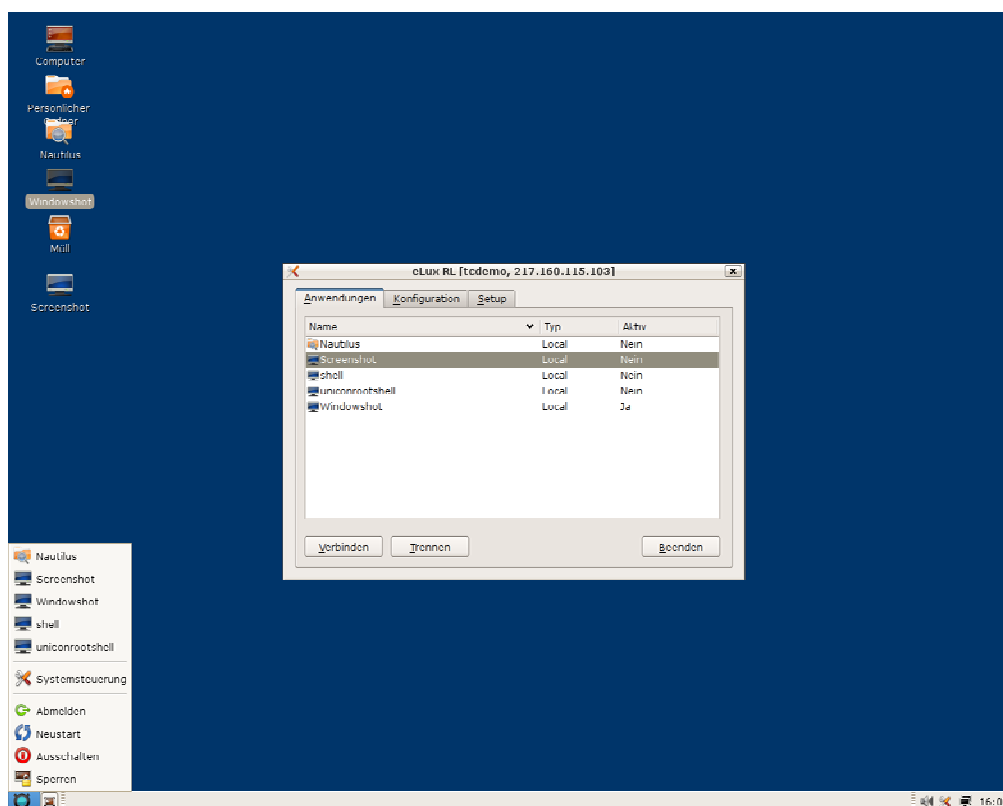
Figure 61 Desktop - Example with eLux® *RL* Main Window (Control Panel), Start Menu and Systray.

5.2 Taskbar – Start Menu and Systray

The taskbar contains the start menu, displays open applications and the systray icons allow to view and/or modify settings very quickly. The icons are:

- USB Device Info
- Info Control
- Mouse/Keyboard
- Screen Control
- Network Connections
- Volume Control
- Control Panel
- Time
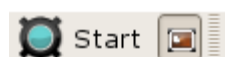
Requirements: Enable the check boxes in the area "Systray" in the **Setup** tab **Desktop** > Advanced.

The start menu, the systray icons as well as the control panel can be closed by the ESC key.

5.2.1 USB Device Info

When inserting an USB device the USB icon appears in the systray of the taskbar.

Right click this icon to display the USB device info:
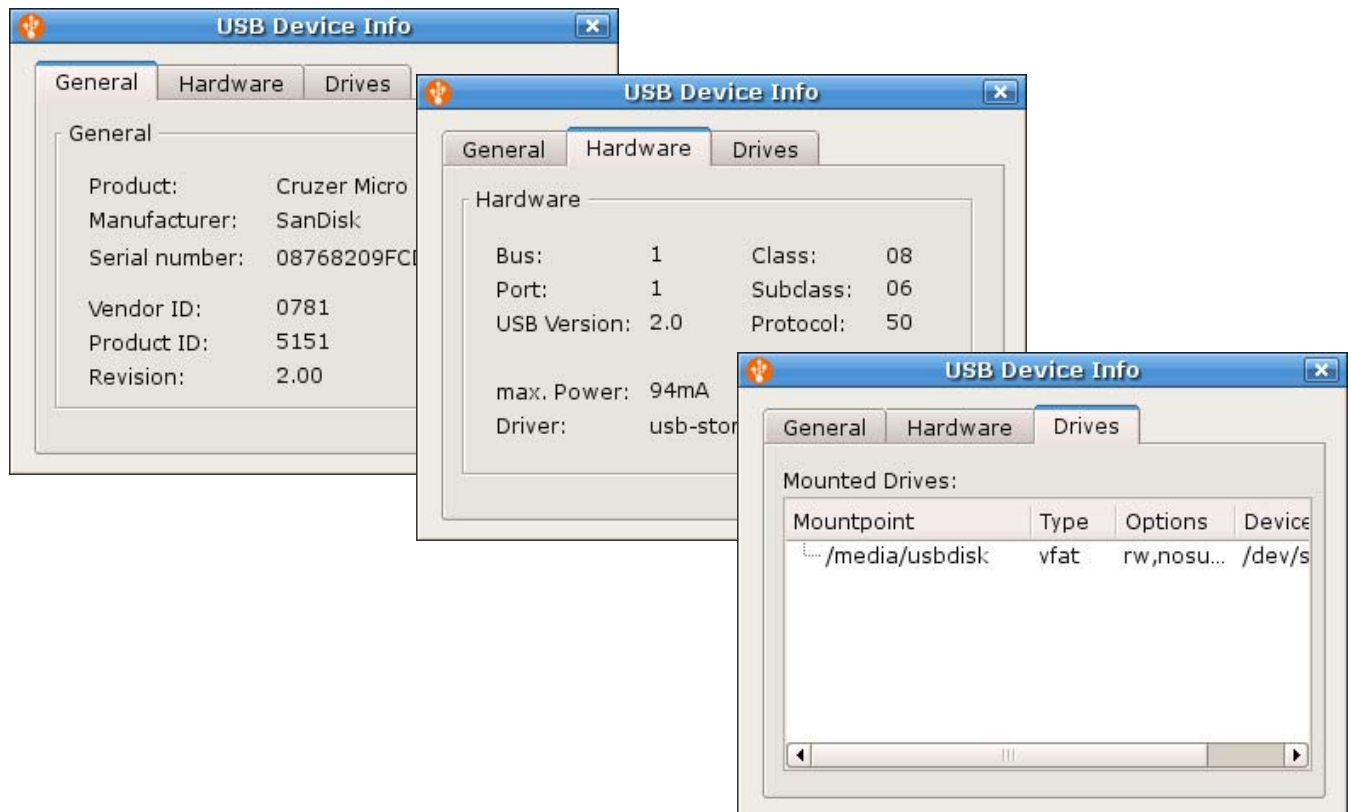
Figure 62 Systray – USB Device Info

To enable an USB memory stick for RDP or ICA applications, set the mountpoints corresponding to this device info (see the section "Advanced RDP settings" and "Citrix Receiver").

5.2.2 Info Control

The Info Control displays the device information.

Data can be entered – or modified – in the fields Info1, Info2, Info3.

This information can be sent to Scout provided that the option "client info" in the "desktop tools" software package (see *Scout Enterprise Administrator's Guide*, chapter ELIAS) is enabled.

The Info Control can also be opened by the shortcut
<Windows key> + Alt + i.

Figure 63 Systray – Info Control

5.2.3 Mouse/Keyboard

The Mouse/Keyboard icon in the systray shows the settings as defined in the Setup.

Changes can be made here. No confirmation is needed.
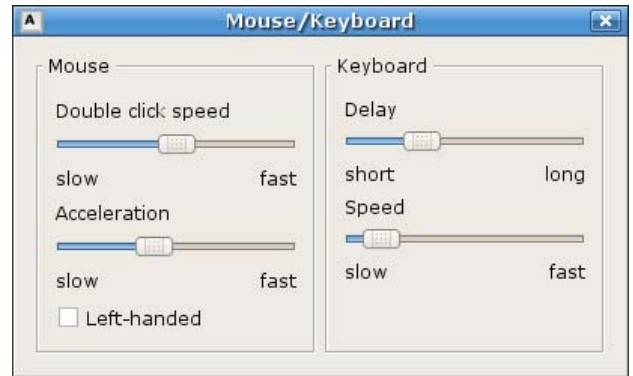
Figure 64 Systray – Mouse/Keyboard

5.2.4 Screen Control

The screen control shows some information on the screen settings.

The settings may be changed. Confirm by clicking **Apply**.
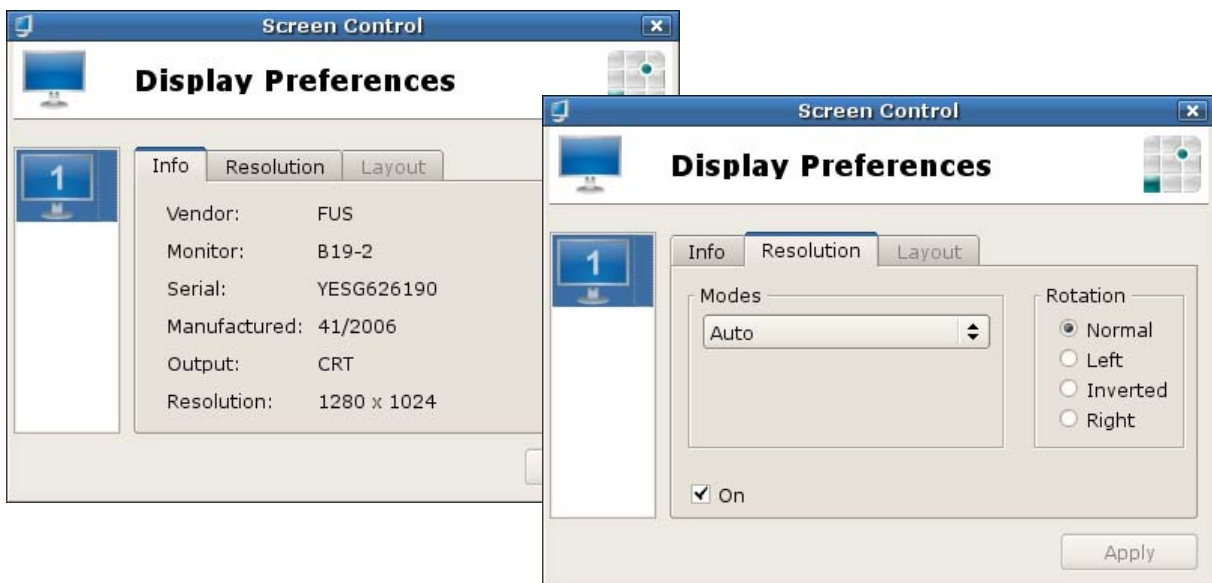
Figure 65 Systray – Screen Control

5.2.5 Network Connections

In the systray click this icon

to show the definied **network profiles**, add new ones or modify existing profiles.

Rightclick the systray icon to get information on the **current connection**, which can be repaired this way.
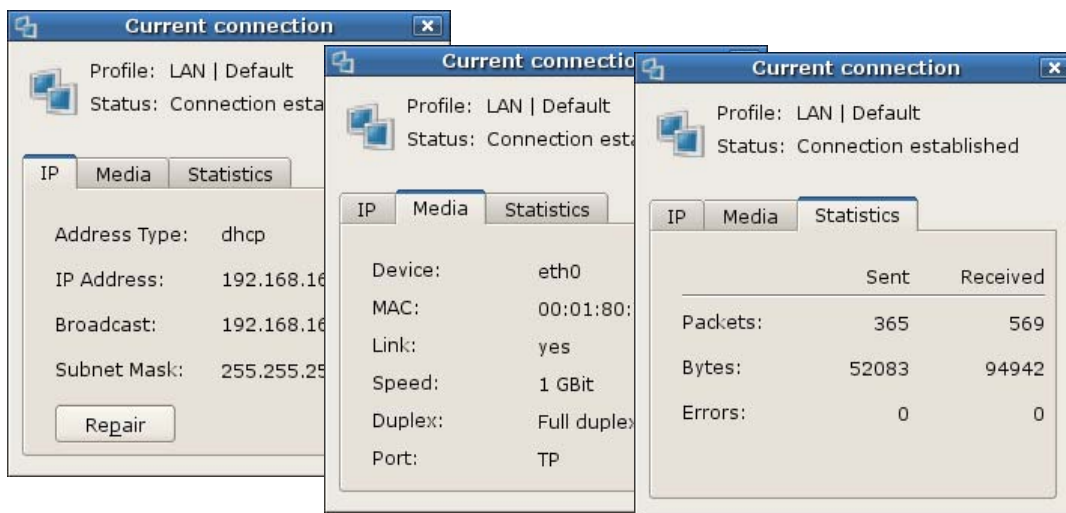
Figure 66 Systray – Network Connections

Requirement: The option "Show network status" in Setup > **Desktop** > **Advance** must be activated.

5.2.6 Volume Control

This helps to change the settings quickly.

Figure 67 Systray – Volume Control

5.3   eLux® *RL* Control Panel

Having completed the first configuration wizard, the eLux® *RL* interface appears. The main window is referred to as the "eLux® *RL* control panel". (eLux NG users have experienced the main window as "starter"). If not in English, screen elements can only be displayed in German. For all other desktop languages, the screen elements appear in the default language, English (US). However, the desktop language setting is required for local applications to run correctly.

The control panel contains three tabs: **Applications, Configuration** and **Setup**.
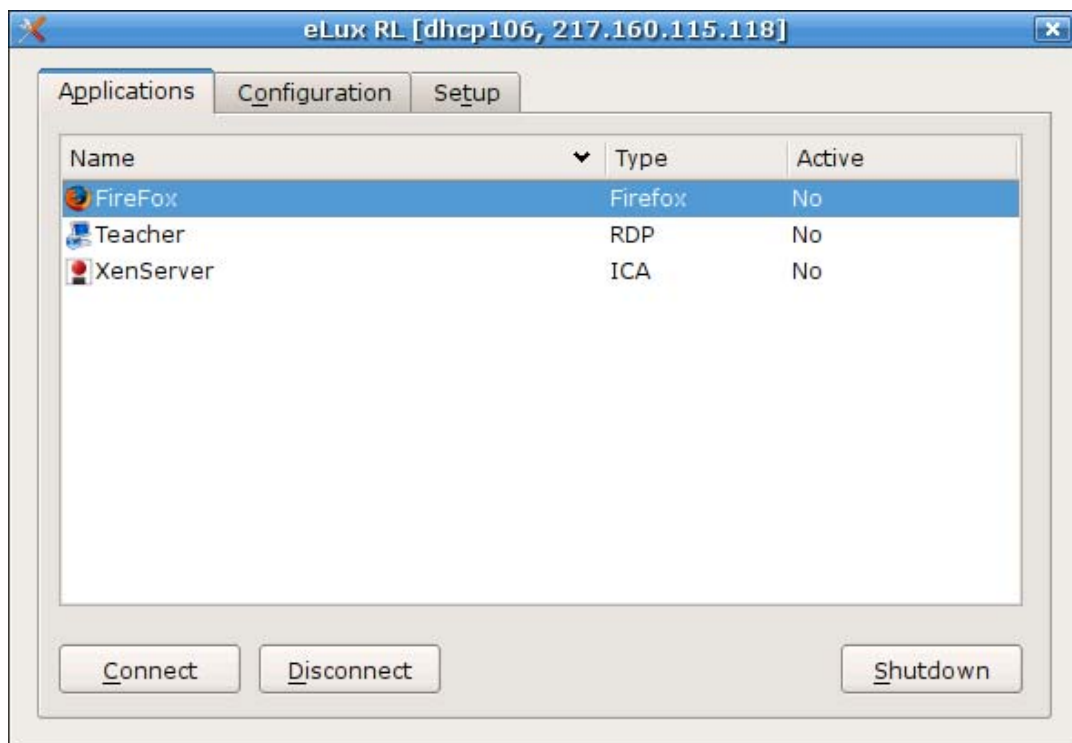
Figure 68   eLux® *RL* Control Panel

Initially, the **Applications** and **Configuration** tabs are empty, and the **Setup** tab contains a default configuration.

The eLux® *RL* control panel is mouse based. However, it is possible to navigate through the eLux® *RL* control panel using the keyboard by pressing ALT + <*underlined letter*>. For example, press ALT + T to jump to the **Setup** tab.

You can use the **ESC** key to close the Control Panel.

5.4 File Explorer

With the Nautilus Explorer files and folders can be displayed in different views. Some examples of the "eLux® *RL* File Browser":
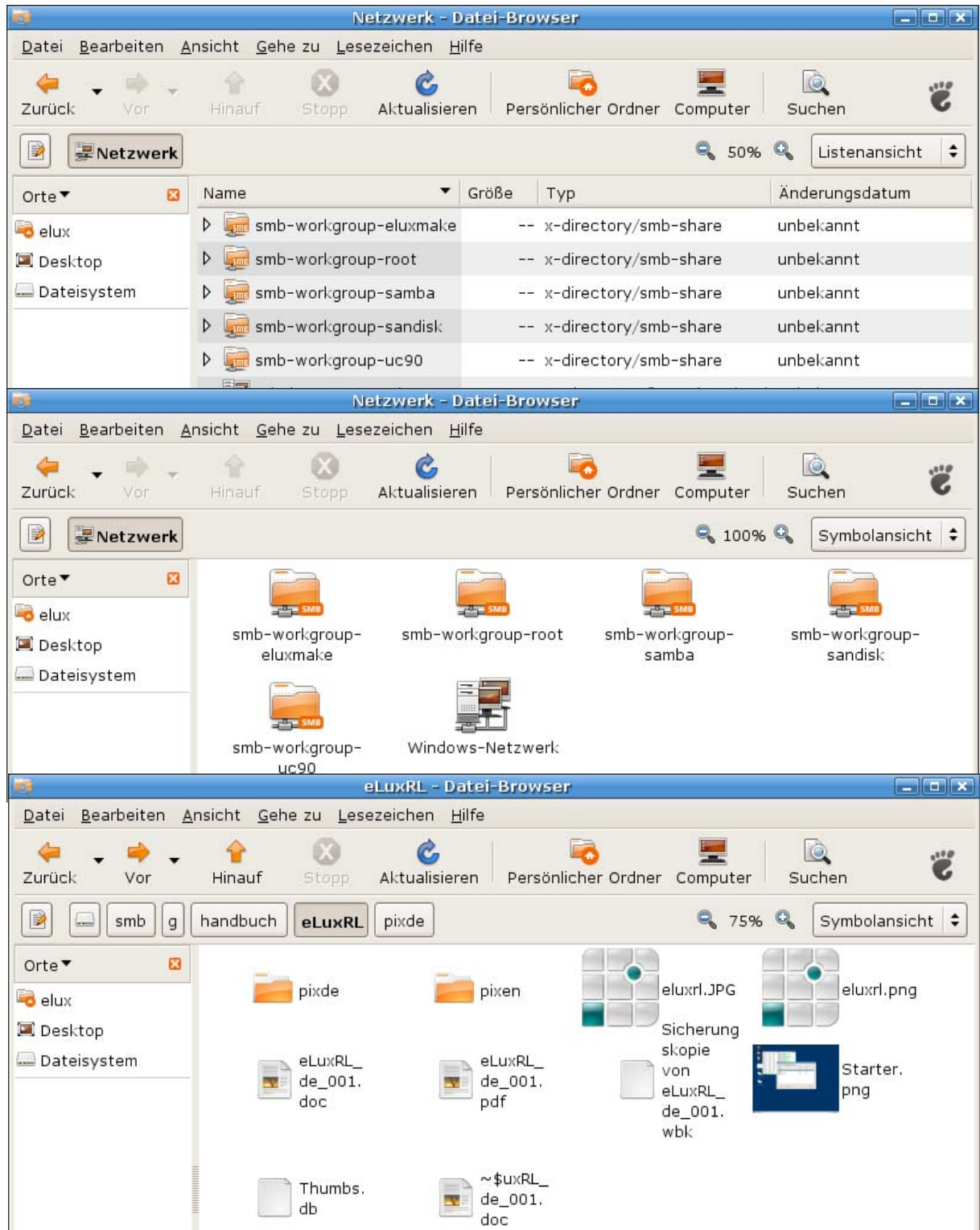
Figure 69 eLux® *RL* File Explorer (Nautilus)

5.5   Magnifier

The magnifier can be selected in the software package "Desktop Tools" and appears – if installed – in the eLux control panel as a local application.
The following command line parameters may be entered in the field "Parameter":

--notop	don't stay always on top
--nocross	disable cross
--size SIZEX SIZEY	magnification window size
-u TIME	update interval in ms
-m FACTOR	magnification factor as float
-cs SIZE	cross size in pixel
-cb SIZE	cross boldness in pixel
-cl SIZE	cross line width in pixel

"cross" is a kind of reticule which highlights the mouse position to be magnified.

Figure 70 Magnifier

5.6   Gnome Configuration

Management of advanced gconfm settings
In the "Advanced file entries" of the device properties in Scout Enterprise now values can be directly entered into the terminal.ini for the configuration of the Gnome desktop. The syntax is as follows:
File: terminal.ini
Section: gconfm
Key/Parameter name: <gconfkey>:<type>
value: <value>
Example:
Key: /desktop/gnome/background/primary_color:string
value: #ffff00
or
Key: /apps/metacity/general/reduced_resources:bool
value: false

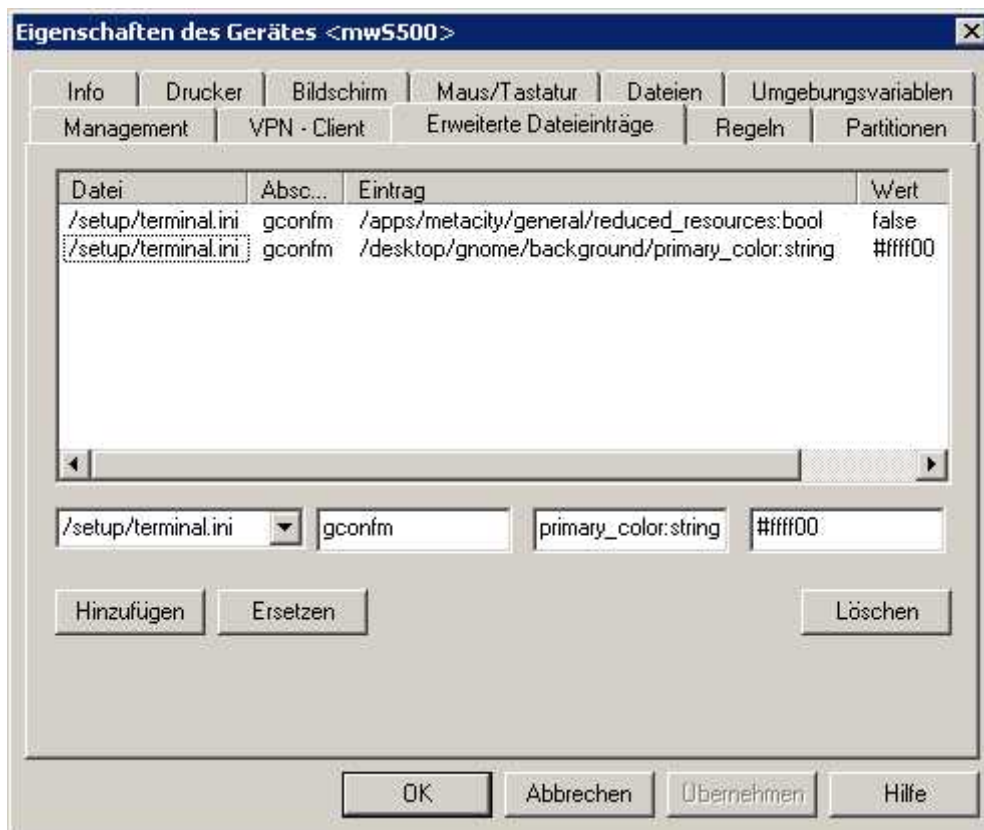The **Scout** dialog "Properties of device":

Figure 71 Scout Enterprise – Properties of Device – Advanced File Entries

NOTE: The values set this way are prior to all other management values !!!

5.7 Safe Boot

Once the BIOS has been scanned press the ESC key to go to the **Safe Mode**. (The TAB key has been used for this purpose up to now.) The client password is requested (value by delivery is: "elux").

Default screen settings are set to values all monitors support. If after configuring the Thin Client you have massive screen distortion, resolution, frequency and color depth are most likely set to values your monitor does not support. In this case, switch off your monitor to avoid damage. Start the Thin Client in Safe Boot mode. Safe Boot allows you to start the terminal in a mode which does not damage hardware. You can then correct screen settings.

Warning: In the Safe Mode you don't have network support. If you should have made the desired changes, please restart the terminal.

5.8 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.

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 , removing the management address in **Management**, and changing the password of LocalLogin (click **Apply**).

Note: If you do not want users to be able to remove themselves from management, do not share the client password.

5.9 LocalLogin

"Help! I'm locked out!"
If you activate directory services and settings are incorrect, you will be locked out. However, you can still log on to the Thin Client locally using the login name "LocalLogin" and the Thin Client password. You can then correct the settings by going to **Setup** > **Security**.

5.10 Factory Reset

The factory reset is an important troubleshooting function.

During a factory reset the Thin Client's firmware setup as well as applications and any locally created files are being deleted. However, licenses and management settings are **not** deleted.

After a factory reset the client restarts. If management settings had been stored the client connects to the Scout server, is automatically entered into the organization unit as it was before, and is assigned the configuration and the applications from this organization unit.

In particular, a factory reset is useful in case a Thin Client had been configured locally and eLux configuration errors had slipped in which the administrator might not find out quickly.

Expert tip:
All files in the directory /setup/public are deleted during the factory reset.