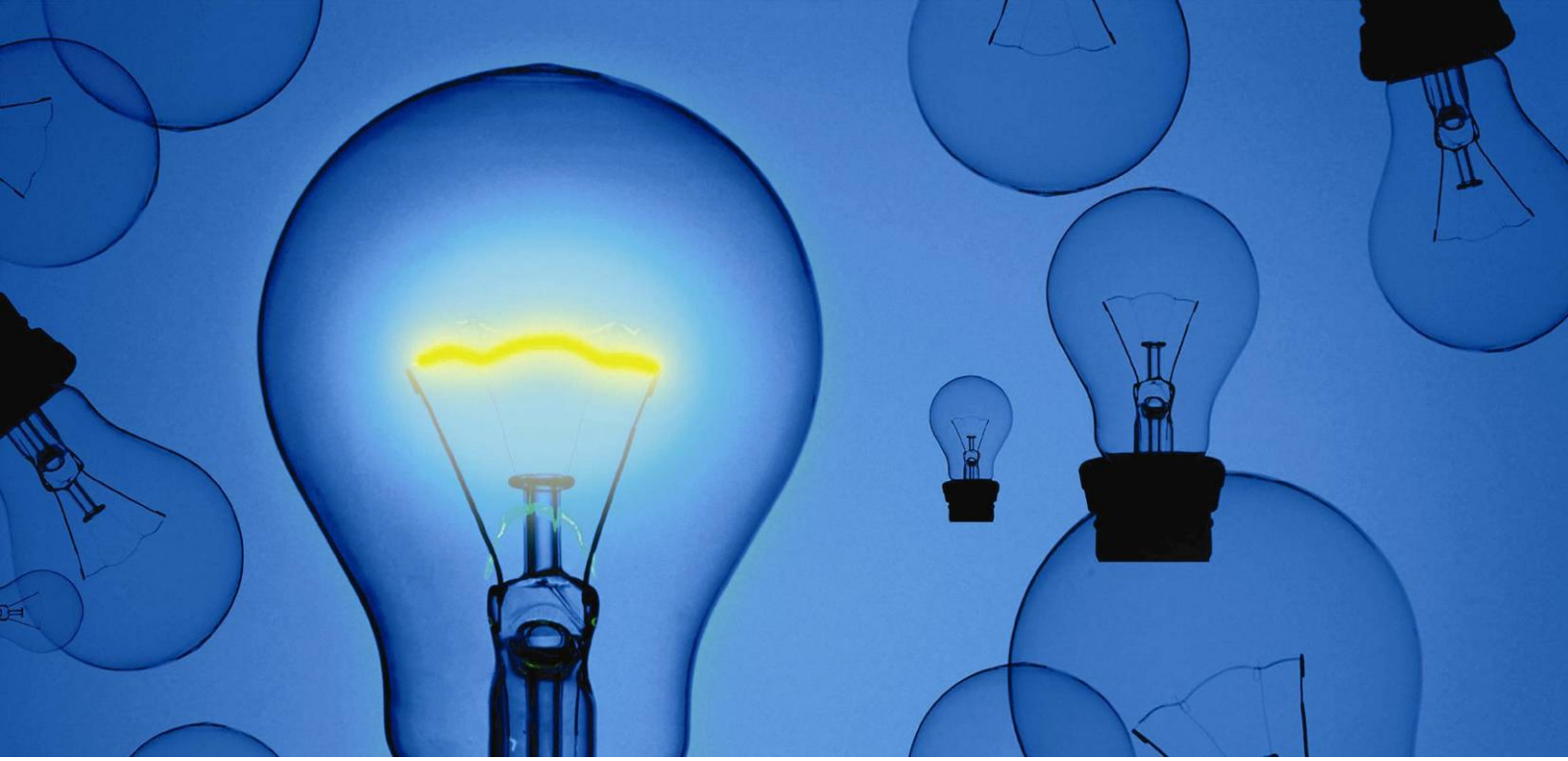


IGEL Clever Clients

Terminal User Guide

For IGEL Thin Clients with IGEL Flash Linux

- **2110 LX Smart**
- **3210 LX Compact**
- **4210 LX Winestra**
- **5210 LX Premium**
- **5310 LX Premium**
- **7302/04 LX PanaVeo**
- **9317 LX Elegance**
- **1110 Legacy**
- **5110 X-Term**
- **2210/2810 Netvista**
- **TC 5200-CF LX TC Card**

IGEL® TECHNOLOGY

Important Information

- ***Copyright***

- ***Disclaimer***

The information in this document is subject to change without notice. IGEL Technology GmbH makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, IGEL Technology GmbH reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of IGEL Technology GmbH to notify any person of such revision or changes.

- ***Trademark Recognition***

IGEL is a registered trademark of IGEL GmbH.

SAPdb is a trademark of SAP AG.

Windows, Windows 95, Windows NT, Windows 2000, Windows XP and Windows 2003 are either registered trademarks or trademarks of Microsoft Corporation.

Java is a registered trademark of Sun Microsystems, Inc.

All other products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owner's benefit.

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice, and should not be construed as a commitment by IGEL Technology GmbH.
IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including the products and software described in it.

Table of Contents

1 Introduction

- **Welcome**

Congratulations on purchasing one of the IGEL Linux-based Thin Client models.
The IGEL Thin Clients are composed of state-of-the-art hardware and an operating system based on the IGEL Flash Linux Technology. We have done our best to deliver an excellent product and we promise to provide support and service of the same quality.
Please refer to the "Software Feature Comparison List" on page 2 to get an overview of the supported software features and protocols of the different IGEL Thin Client models.

- **How to use this Guide**

In this IGEL User Guide we describe the setup screens and options as well as the boot procedure. We do not describe common functionalities like TCP/IP, NFS, SMB, XDMCP, DHCP, and BOOTP, etc. If you have any questions concerning these matters please ask your system administrator or, if you would like to know more about protocols, please refer to the corresponding documentation

This guide is divided into the following chapters:

IMPORTANT NOTE:

Chapter 4 "Boot Procedure" and the major part of Chapter 5 "Setup" are valid for all IGEL Linux-based Thin Clients without separation into device-specific sections.
Please refer to the list of supported Software features (better known as "Software Feature Comparison List"; see next page) to see which sections of Chapter 6 ("Application Launcher") are relevant for your particular IGEL Thin Client model.

Since the IGEL 5300 LX Premium model supports nearly all available features, we have used it as the reference for screenshots of windows and dialog-boxes.

All shown screenshots and descriptions are based on firmware version 3.05.500.

In case you need further support that your dealer or distributor cannot provide, you may use our online support form at www.igel.de (section "Service & Support").

2 Quick Overview of Supported Software Features

	IGEL Series Name	Smart	Compact	Winestra	Netvista Upgrades
	IGEL Models Name	2100 LX	3200 LX	4200 LX	2210 / 2810
	Embedded Operating System	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux
CONNECTIVITY	ICA Client Version	9.0	9.0	9.0	9.0
	Citrix Program Neighborhood	Full PN	Full PN	Full PN	- / Full PN
	RDP Client Version	5.1	5.1	5.1	5.1
	PowerTerm Emulation Suite	-	✓	✓	✓
	Kerberos (within PowerTerm)	-	✓	✓	-
	SAP Gui	-	-	-	-
	X11R6	✓	✓	✓	✓
	XDMCP (max. displays)	2	2	4	4
	Extended Local Xfonts	-	-	-	-
	Font Service (XC + NFS)	✓	✓	✓	✓
	SMB / NFS Mounting	✓	✓	✓	✓
	Devicemapping Daemon	✓	✓	✓	✓
	ThinPrint Client	✓	✓	✓	✓
	Printing via Line Printer (LP)	✓	✓	✓	✓
	Printing via TCP/IP	✓	✓	✓	✓
INTERNET	Local Browser	-	Firefox	Firefox	- / Firefox
	Java Runtime Environment (JRE)	-	-	-	-
	Acrobat Reader	-	✓	✓	- / ✓
	Mediaplayer	-	-	-	-
	Flashplayer	-	✓	✓	- / ✓
	Realplayer	-	-	-	-
	PPTP (VPN)	✓	✓	✓	✓
	PPPOE (DSL)	✓	✓	✓	✓
	Cisco VPN	✓	✓	✓	✓
MISC	Smartcard Application	✓	✓	✓	✓
	VoIP (Voice over IP)	-	✓	✓	-
	USB Hotplug Automount Feature	✓	✓	✓	- / ✓
	KVK Support	✓	✓	✓	✓
ADMIN	Full Remote Manageability	✓	✓	✓	✓
	Shadowing / VNC	✓	✓	✓	✓
	Remote RSH / SSH Access	✓	✓	✓	✓
	Setup via Bootp / DHCP	✓	✓	✓	✓
	PXE Netboot	✓	✓	✓	dependent on hardware

	IGEL Series Name	Premium		Legacy Terminals		TC Cards
	IGEL Models Name	5200 LX	5300 LX	1100 Legacy	5100 X-Term	TC 5200-CF LX
	Embedded Operating System	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux
CONNECTIVITY	ICA Client Version	9.0	9.0	-	-	9.0
	Citrix Program Neighborhood	Full PN	Full PN	-	-	Full PN
	RDP Client Version	5.1	5.1	-	-	5.1
	PowerTerm Emulation Suite	✓	✓	✓	-	✓
	Kerberos (within PowerTerm)	✓	✓	✓	-	✓
	SAP Gui	-	✓	-	-	-
	X11R6	✓	✓	✓	✓	✓
	XDMCP (max. displays)	4	4	2	4	4
	Extended Local Xfonts	-	-	-	✓	-
	Font Service (XC + NFS)	✓	✓	✓	✓	✓
	SMB / NFS Mounting	✓	✓	✓	✓	✓
	Devicemapping Daemon	✓	✓	✓	✓	✓
	ThinPrint Client	✓	✓	✓	✓	✓
	Printing via Line Printer (LP)	✓	✓	✓	✓	✓
	Printing via TCP/IP	✓	✓	✓	✓	✓
INTERNET	Local Browser	Firefox	Firefox	-	-	Firefox
	Java Runtime Environment (JRE)	-	✓	-	-	-
	Acrobat Reader	✓	✓	-	-	✓
	Mediaplayer	-	MPlayer	-	-	-
	Flashplayer	✓	✓	-	-	✓
	Realplayer	-	✓	-	-	-
	PPTP (VPN)	✓	✓	✓	✓	✓
	PPPOE (DSL)	✓	✓	✓	✓	✓
	Cisco VPN	✓	✓	✓	✓	✓
MISC	Smartcard Application	✓	✓	✓	-	✓
	VoIP (Voice over IP)	✓	✓	-	-	✓
	USB Hotplug Automount Feature	✓	✓	✓	-	✓
	KVK Support	✓	✓	-	-	✓
ADMIN	Full Remote Manageability	✓	✓	✓	✓	✓
	Shadowing / VNC	✓	✓	✓	✓	✓
	Remote RSH / SSH Access	✓	✓	✓	✓	✓
	Setup via Bootp / DHCP	✓	✓	✓	✓	✓
	PXE Netboot	✓	✓	✓	✓	dependent on hardware

Note: Hardware Configuration
In the appendix you will find a detailed overview of the hardware configurations and technical specifications of the individual types of device series.

3 Quick Installation

If you carry out the following steps, the terminal can be installed in your network environment within a few minutes.

- Connect the terminal to a VGA monitor, an AT compatible keyboard with PS/2 or USB connector, a PS/2 or USB mouse, the LAN via RJ45 and AC power.
- Turn on the terminal and wait until the graphical desktop has started (around 30 seconds) and the window of the application launcher appears on the screen. Highlight the setup entry and start the setup either by pressing the START button or double clicking on the setup entry.
- Select your keyboard layout in the “Input/Keyboard” menu.
- Select your display settings in the “Display” menu.
- Complete the terminal setup program by entering a local IP address in the “Network” section or keep the default DHCP mode for automatic network configuration.
- Finally “save” the settings, press “ok” and confirm with “yes”.

The unit will reboot now and will come up with the new settings.

Note:
For detailed session configuration refer to Chapter 6.4.

Virtually every setting is “equipped” with a meaningful Tool Tip. Simply move the mouse pointer over the setting/option you want to know more about and wait a second.

4 Boot Procedure

4.1 System BIOS

The BIOS looks for extensions in the appropriate memory area.
If there is a DOC (Disk On Chip) in use, the BIOS extension will be detected and executed.
If there is a DOM (Disk On Module) or CF (Compact Flash) in your unit, they are IDE devices and directly treated as hard disks.
The next step is the execution of the master boot record, which starts a secondary stage loader.

4.2 Secondary Stage Loader and Boot Menu

The secondary stage loader provides the user with a menu, which is reached by pressing the "ESC" key when the "Loading Kernel …" message appears on the screen.

You can then choose between 3 boot options and the option of resetting the Thin Client to its factory defaults.

- ***Quiet Boot***
- ***Verbose Boot***
- ***Emergency Boot (setup only)***
- ***Reset to factory defaults***

4.2.1 Quiet Boot

"Quiet Boot" is the standard boot mode; it suppresses all messages from the kernel and starts up the graphical desktop.

4.2.2 Verbose Boot

If the "Verbose Boot" is chosen, the boot messages are shown and you will have a diagnostic shell, from which common debug commands (like "ifconfig", etc) can be executed. To leave this shell type "init 3" and the boot process continues.

4.2.3 Emergency Boot

If you choose "Emergency Boot" (setup only with standard parameter values), the secondary stage loader looks for a bootable system in the flash and continues the boot process as in the other boot modes. Emergency Boot basically starts the X Server without the network driver at a resolution of 640 x 480 – 60 Hz and finally starts directly into the setup. This is very useful if you selected a too high screen resolution or chose a wrong mouse type.

4.2.4 Reset to Default Factory Settings

All your personal settings including your password and configured sessions will be lost if you choose this option. Before the reset is applied, a warning message is displayed on the screen, where you have to explicitly confirm your decision.
If the terminal is protected by an administrator password, you will be prompted to enter it.
In case this password is not known anymore, you will have to contact us by using the online support form on our web page www.igel.de in the "service" section.
Provide the displayed "terminal key" and the stated firmware version and, of course, your contact data.
Our support will provide a so-called "reset to factory defaults key" for this specific unit.
(Every key is valid for one single unit only, to keep this process at its most convenient, but still secure.)

4.3 Networking

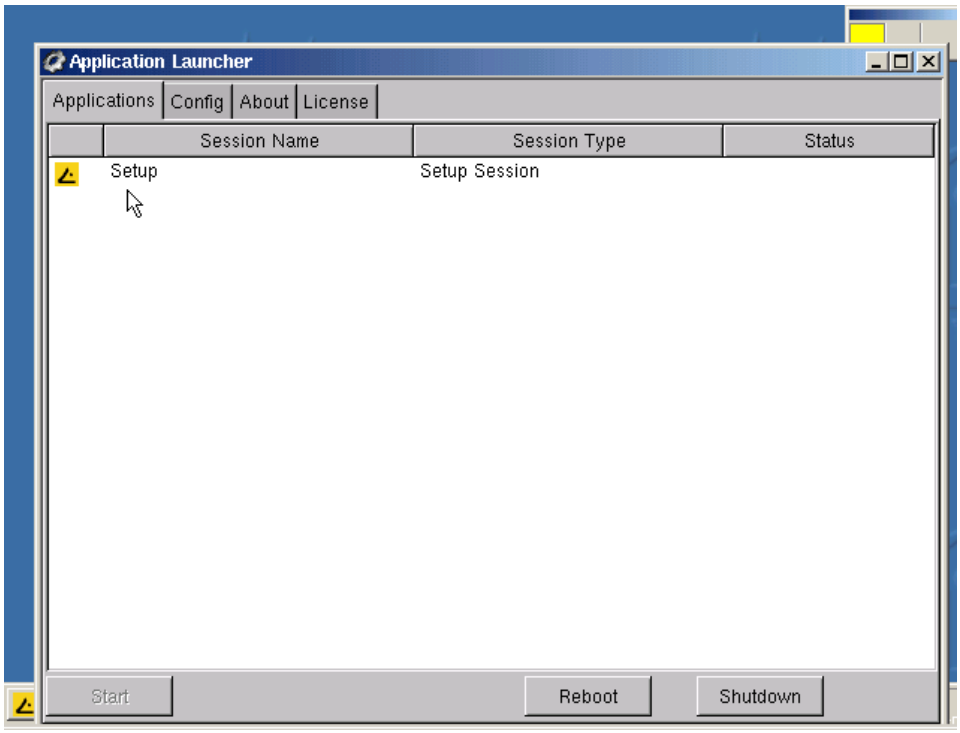
After loading the kernel the network configuration follows. Three different ways can be chosen to include the terminal in the network environment. According to the settings of the terminal, DHCP, BOOTP or manual configured IP address can be used.

4.4 X Server

The last step of the boot procedure is the start of the X-Server and the local window manager.

5 Setup (Global Settings)

After the boot procedure has completed, a desktop such as the above will be displayed on the screen.



The "***Application Launcher***" starts automatically because it's set to "autostart & restart" by default. Because the "Setup" program is the central configuration tool for all global settings of the Thin Client, a "Setup" session is also predefined.

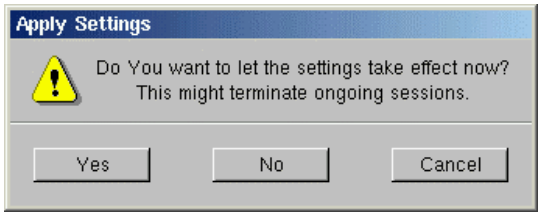
5.1 Starting the Setup

You can reach the setup in three different ways:

- Select the "*Setup*" entry in the "*Application Launcher*" and double click it or press the "Start" button in the lower left corner of the window.
- Click on the "IGEL" icon in the very lower left corner and in the pop-up select "Setup".
- Clicking on any free space on the desktop with the right mouse button will cause a drop-down list to appear; again select the "Setup" entry to proceed.

These are the default settings to reach the setup. You can configure it to be reachable in every combination of these three possibilities within the *"**Application Launcher**" (*see Chapter 6).

5.1.1 Leaving the Setup

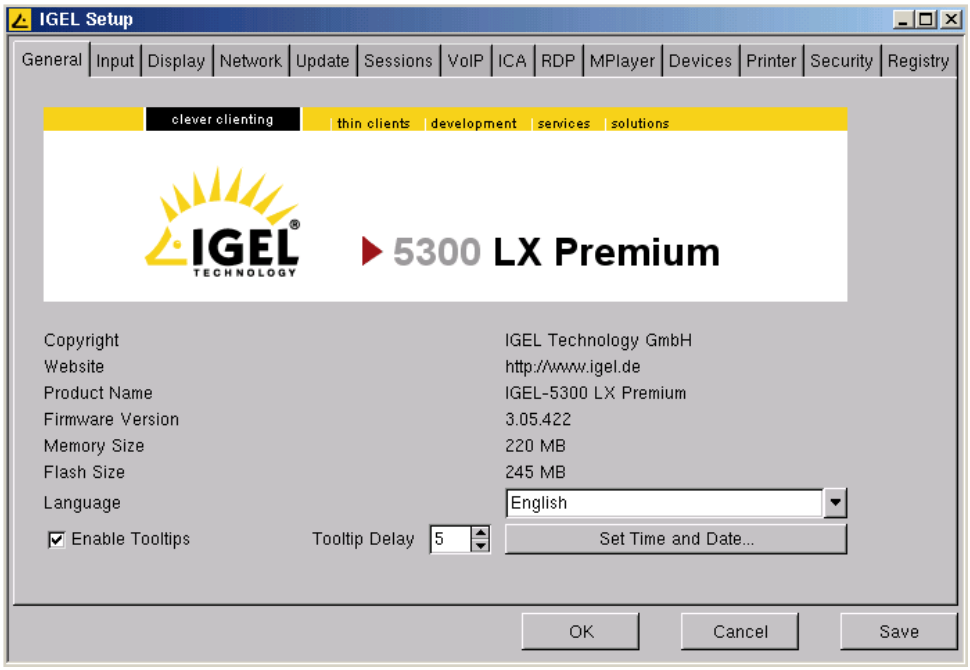


In general, every particular setup page provides an "*OK*", "*Cancel*" and "*Save*" button.

After all configurations in a particular setup section have been made and you want to save your settings without leaving the setup program, click on the "*Save*" button.

If you did not change any settings and you want to exit the setup, click on the "*Cancel*" button. In case you changed settings, leaving the setup with "*OK*" will prompt you with the above "*Apply Settings*" popup. Decide if you want to let the changes take effect immediately ("*Yes*"), save and let it become effective on next reboot ("*No*"), or "Cancel" to stay within setup.

5.2 General



When the “IGEL Setup” has been started, first the “General” page appears on the screen.

Some system information in additional to the product name is provided on this page along with some vital information like the firmware version, the memory size (RAM) and the flash size.

- ***Language***

Select the appropriate language from the list. (Currently “German” and “English” only.)

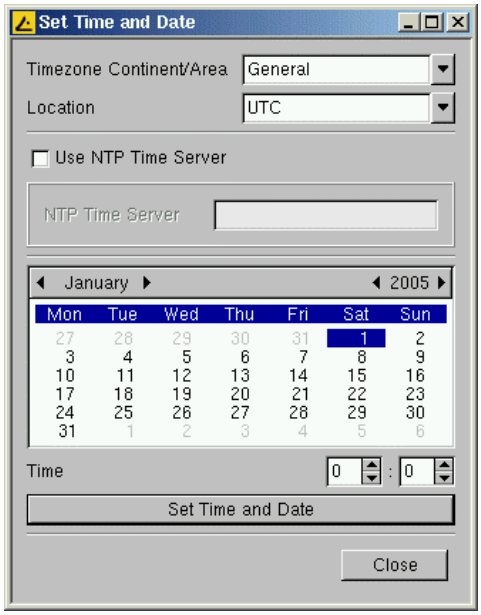
Note: The chosen language is the user interface language, so it’s valid for all local applications.

- ***Tooltips***

These are small dropdown windows with a short description of the pointed menu entry. These tooltips open up if you stay on a menu entry with your mouse pointer for the entered amount of “*Tooltip Delay*” time (in tenth of seconds).

- ***Set Time and Date*** …

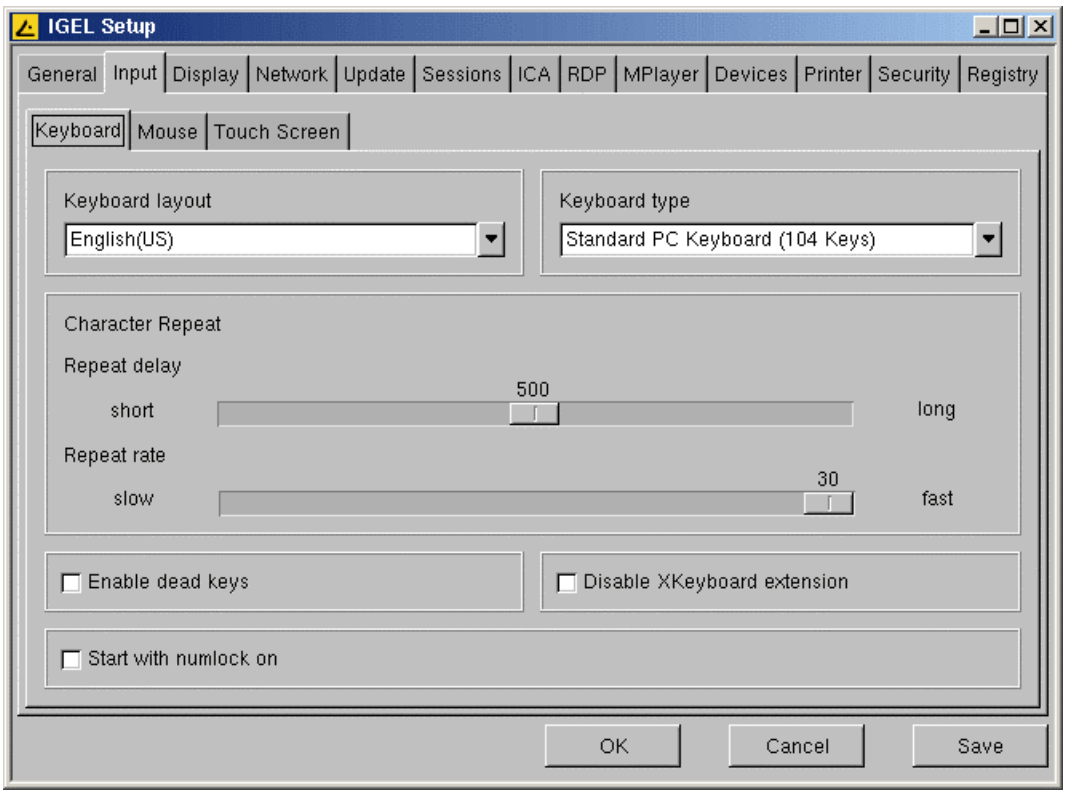
Click on the “Set Time and Date” button to open up this dialog-box.
Make your changes and confirm them by pressing the “Set time and Date” button once, then close this page.



If a Time Server such as this is available in your network, you may also use the “Network Time Protocol” (NTP) to request the proper time and date automatically during each boot up

5.3 Input

5.3.1 Keyboard



- ***Keyboard Layout***

Select your "Keyboard layout" here. The layout will be valid for all parts of the system including emulations, window sessions and X applications. (Table to the right shows all currently supported layouts.)

English(US)
English(UK)
English(International)
English(South Africa)
German
German(Switzerland)
French
French(Switzerland)
French(Belgium)
French(Canada)
Dutch
Dutch(Belgium)
Danish
Norwegian
Swedish
Finnish
Italian
Spanish
Portuguese
Slovenian
Croatian
Polish
Polish(Programmers)
Slovak
Czech
Hungarian
Turkish(Q)
Turkish(F)

- ***Keyboard Type***

Choose your keyboard type from the available from this drop box:

Standard PC Keyboard (104 Keys)
IBM Keyboard (122 Keys)
Trimodal Keyboard
Sun Type 6 Keyboard

- ***Character Repeat***

In this section you can set the auto repeat behavior for the keyboard:

  - ***Repeat Delay***
    Sets the delay time (in milliseconds) between pressing a key and the start of the auto repeat mode.

  - ***Repeat Rate***
    Sets the number of repeated characters per second.

- ***Enable Dead Keys***

Enable this function if the chosen keyboard layout uses dead keys for special characters.

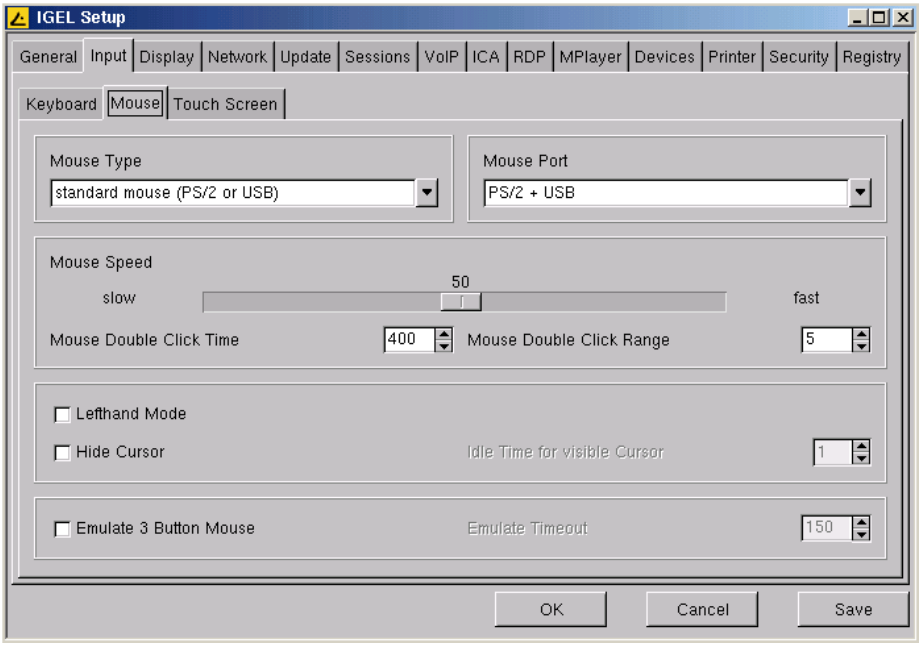
- ***Disable Xkeyboard extension***

Activating this button disables the language-specific keymappings of the local X-Server. (Thus you will in fact have US keyboard layout.)
Within an XDM connection, though, keys may be mapped by the server.

- ***Start with Numlock on***

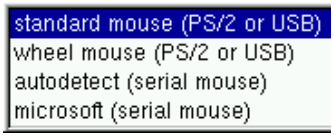
Enable this checkbox if you want Numlock to be automatically activated during the boot process.

5.3.2 Mouse



- ***Mouse Type* and *Mouse Port***

Set the type and port of the attached mouse device from these two dropdown boxes:



- ***Left-hand mode***

Changes the orientation of the mouse to left handed by swapping the mouse buttons.

- ***Emulate 3-Button Mouse*** (not supported with serial mouse)

Enable/disable the emulation of the third (middle) mouse button for mice which only have two physical buttons. The third button is emulated by pressing both buttons simultaneously.

- ***Emulate 3-Button Timeout***

Sets the timeout (in milliseconds) the driver waits before deciding if two buttons where pressed "simultaneously", if 3-button emulation is enabled.

- ***Hide Cursor***

In case you don't use a mouse or you want to show some self-running presentations, you may set a mouse cursor idle timeout. To completely disable the mouse cursor, set timeout to zero.

- ***Mouse Resolution***

Here you set the resolution of your mouse in counts per inch.

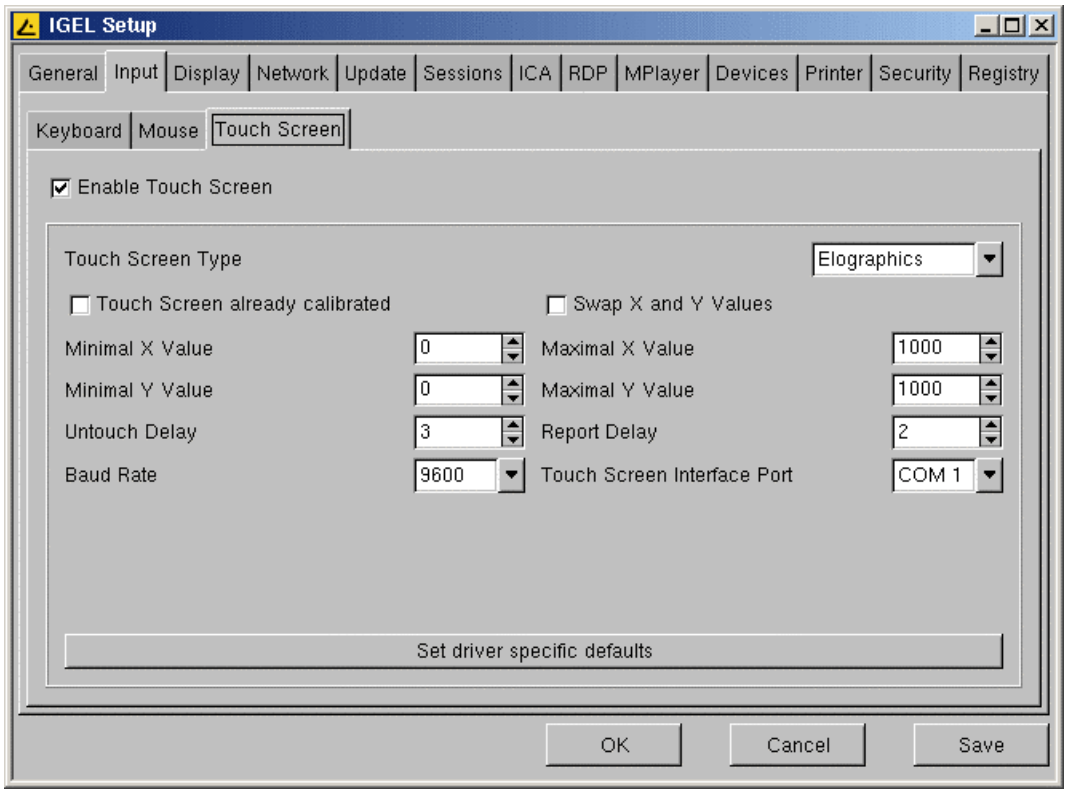
- ***Mouse Double-Click Time***

The maximum interval (in milliseconds) between two successive mouse clicks to recognize a double click may be altered here.

- ***Mouse Double-Click Range***

The maximum distance (in pixels) between two successive mouse clicks to recognize a double click may be altered here.

5.3.3 Touch Screen



Note: To get into and navigate within the setup, it's recommended to do the initial configuration with an attached mouse. You may also use the "Emergency Boot" and navigate through the setup with the keyboard by using the cursor arrows, tab and space bar.

- ***Touch Screen Type***

The supported types are currently "Elographics" and "MicroTouch".

- ***Touch Screen already calibrated***

After enabling the touch screen functionality, you have to calibrate it minimal once. As long as you do not activate this checkbox, the calibration will automatically start at every boot up.

- ***Swap X and Y Values***

Activate this option in case you rotate the panel by 90 degrees (portrait mode).

- ***Minimal and Maximal X and Y Values.***

These will be set by the calibration tool. (You may also manipulate them manually)

- ***Untouch Delay***

The maximal time (in milliseconds) allowed between two touch events still being interpreted as one. E.g. while moving Windows by drag&drop, unintentional untouch events may occur. Increasing this value prevents the Thin Client from interpreting this as two separate touches.

- ***Report Delay***

Defines the time (in milliseconds), the screen must be touched to recognize it as a touch event.

- ***Baud Rate***

Set the communication speed via the selected port. (In doubt, refer to your panel's manual.)

- ***Touch Screen Interface Port***

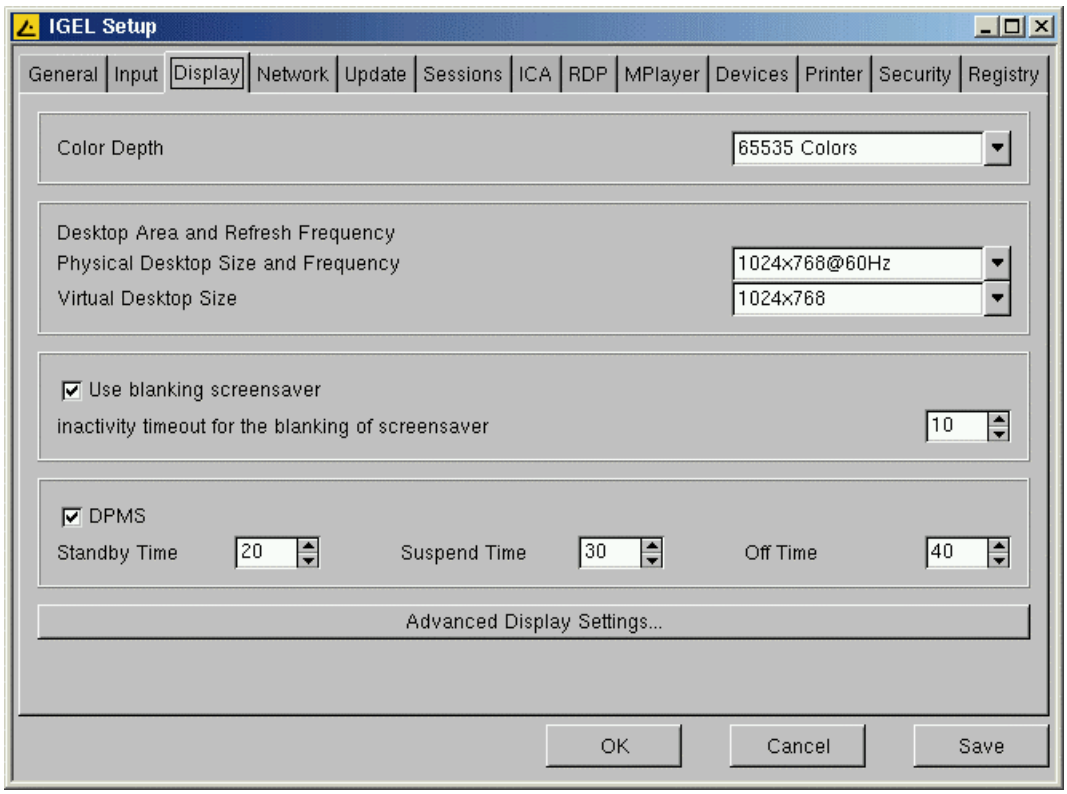
You can attach the Touch Screen to either COM1 or COM2. Set the selected port here.

- ***Set Driver-Specific Defaults***

Click here once after changing the Touch Screen type or to reset the settings to its defaults.

5.4 Display

5.4.1 Global Display Settings



- ***Color Depth***

This menu allows you to specify the desktop color depth from these available:

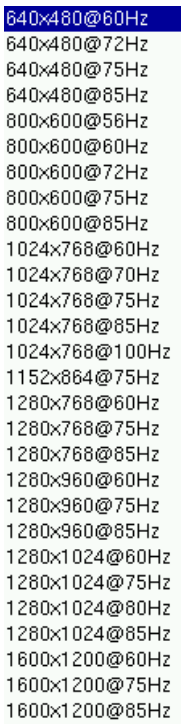
- 8 bits per pixel (256 colors)
- 16 bits per pixel (High color / 65k colors)
- 24 bits per pixel (True color / 16,7million colors).

Note: Make sure that the display unit connected to the Thin Client supports the selected settings! (In case you accidentally set it too high, refer section 4.2.3 “Emergency Boot”.)

Desktop Area and Refresh Frequency

- ***Physical Desktop Size and Frequency***

Select the needed resolution from this menu. The available resolutions depend on the previously chosen color depth and the hardware model of your thin client.



- ***Virtual Desktop Size***

The virtual resolution is used for panning. That means that the virtual screen is bigger than the physical screen. So the “Virtual Desktop Size” can never be smaller than the chosen entry of the “Physical Desktop Size”.

Note: Both of the desktop size entries but also the value of the color depth depend on each other, as well as the used hardware (Thin Client model).

Screensaver and DPMS

- ***Blanking Screensaver***

If the screensaver function is activated a blanking screensaver is used after the period of time (in minutes) you have defined.

- ***DPMS***

See 5.4.2.2.

5.4.2 Advanced Display Settings

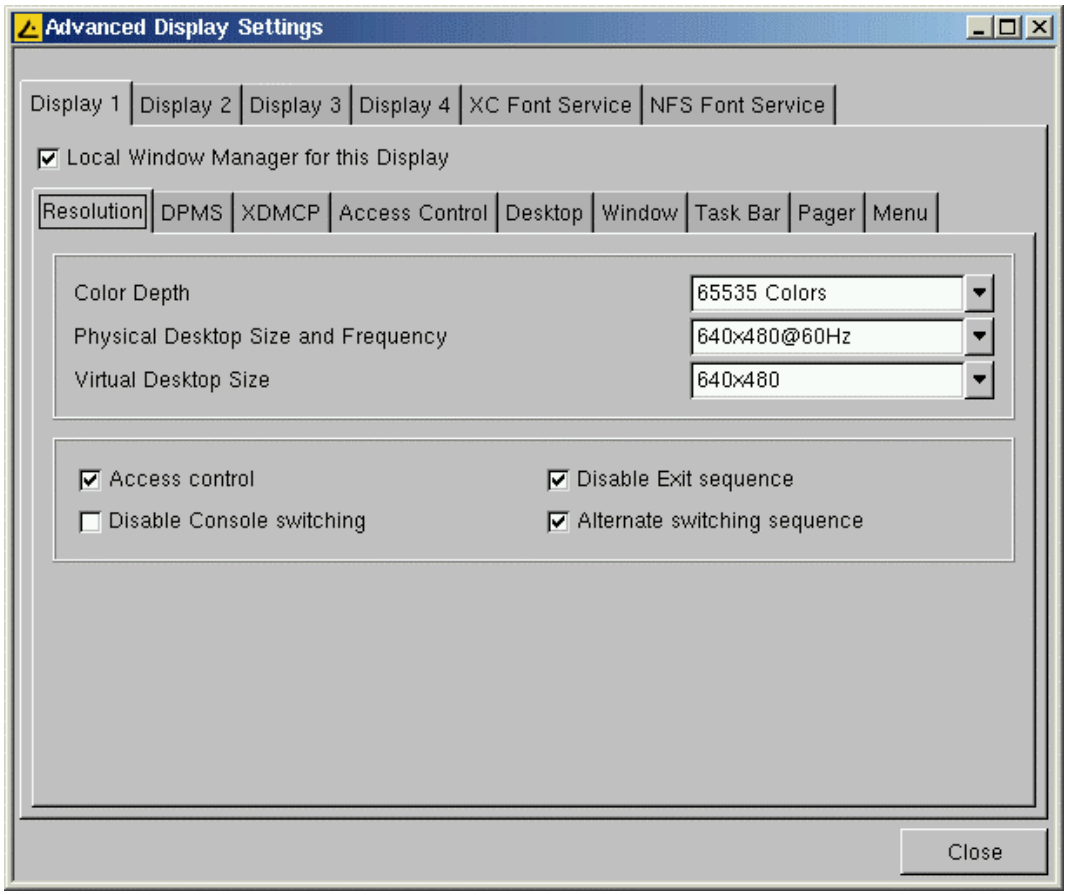
Depending on the Thin Client model, you may start up to four local X servers.

By default, the first X server is enabled and preconfigured. The settings in the dialog-box "***Display 1***" are identical with the global display settings (see previous page).
Changes in display 1 will automatically be set in the global display page and vice versa.

"***Display 2***", "***Display 3***" and "***Display 4***" are the corresponding pages of the three additional X servers, which are disabled by default. (Not all models do in fact have four but only one additional.)
The available dialog-boxes are all the same for the four displays (except the "Enable Display" checkbox), so we used "Display 1" as reference for the descriptions.

Note: Remember that every display consumes a certain amount of memory! If your unit is low on RAM, you must be careful here! In doubt, upgrade the installed RAM.

Resolution



- ***Access Control***

If enabled (default) this option prevents other hosts to have access to your display.
(See also section 5.4.2.4 for details on how to grant access for specific hosts.)

- ***Exit Sequence***

This option allows you to disable the sequence <Ctrl>+<Alt>+<Backspace> to exit the X server.

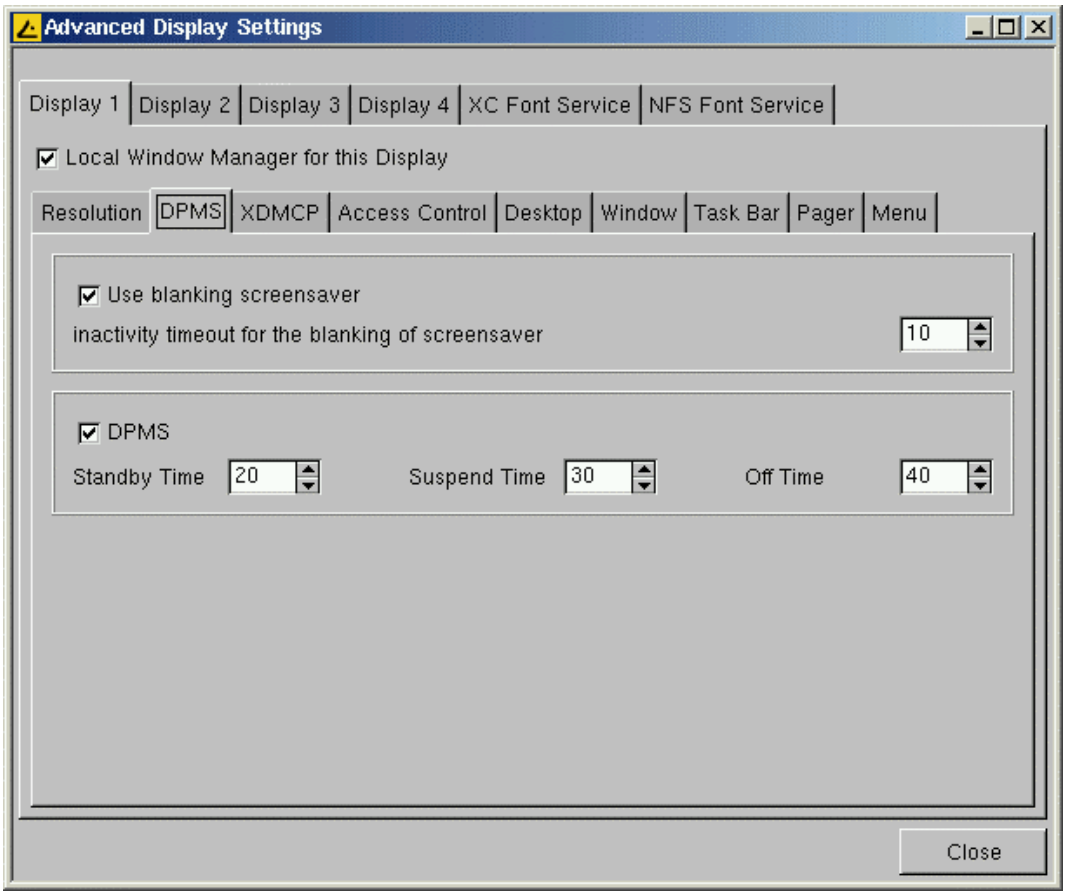
- ***Console Switching***

Press this button to disable the console switching with <Ctrl>+<Alt>+<Fx>

- ***Alternate Switching Sequence***

Here you can choose between <Alt>+<SysRq>+<Fx> and <Ctrl>+<Alt>+<Fx> to switch between displays.

DPMS



If your monitor supports “Display Power Management Signaling” it allows more functions (energy saving) than just a screensaver.

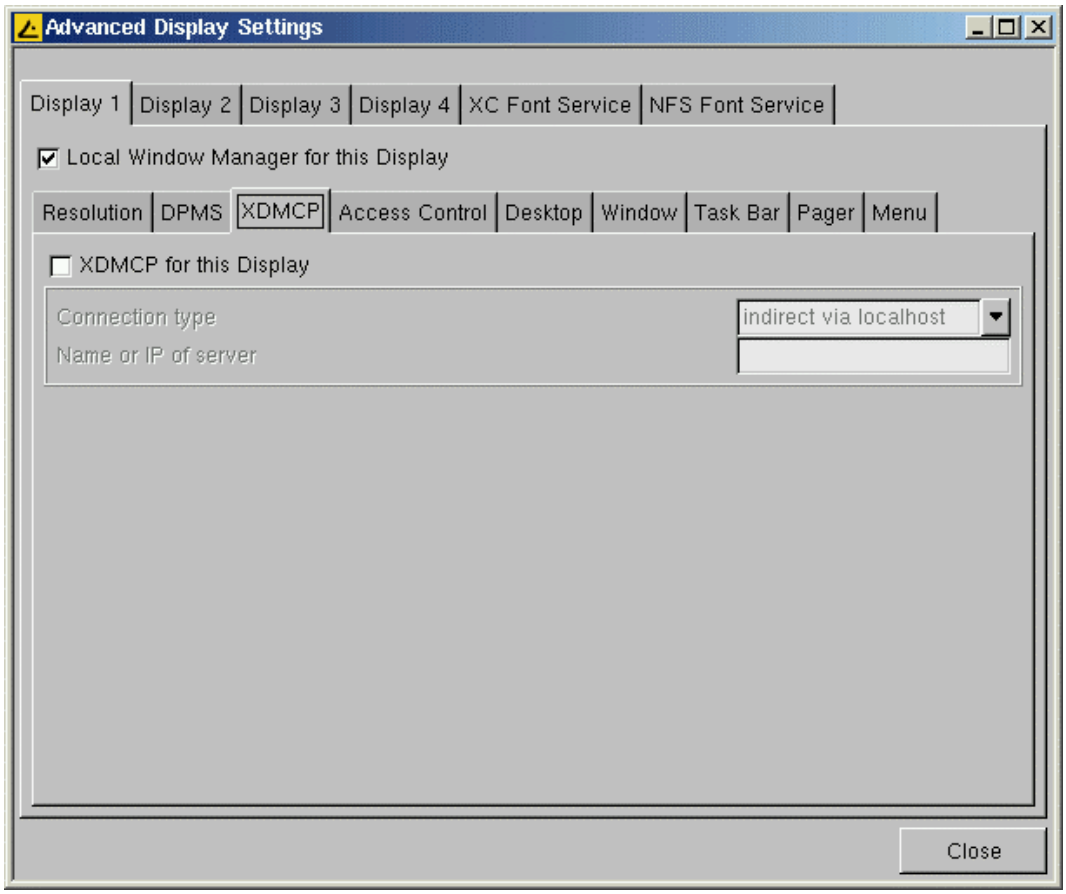
There are three different modes called “***Standby mode***”, “***Suspend mode***” and “***Off mode***”, which are activated after their adjustable time loops (in minutes) ran off.

Enabling DPMS with the default time settings activates the “power off mechanism” of the monitor as follows:

After 10 minutes the display switches to "blank" (standby mode), after a further 10 minutes it sets the first current savings level (suspend mode: Switch off the high voltage), and after further 10 minutes the monitor changes into the "Off" mode.

Note: All levels are passed through naturally only if the X server receives no new inputs during this runtime.

XDMCP



Click the corresponding button to enable the XDMCP functionality for the “Display 1”.

- ***Connection type***

Select the appropriate “Connection Type” here.

If you select “**broadcast**” the “Graphical Logon” will be provided from the first XDMCP server answering on the broadcast request.

In the case that you select “**indirect via localhost**” connection type a list of XDMCP hosts is displayed at boot-up time. From this list you must select the host which provides the “Graphical Logon”.

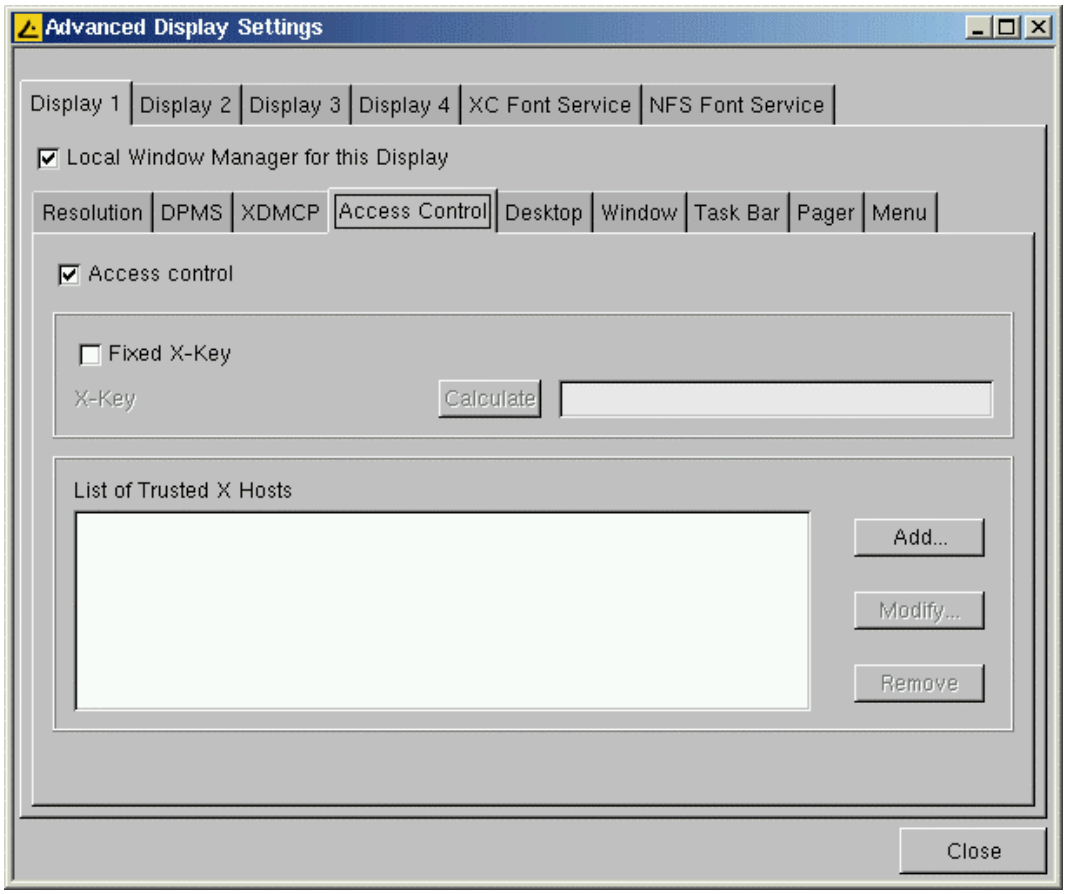
- ***Name or IP of Server***

If you select “**direct**” or “**indirect**” connection type, the “Name or IP of Server” field is enabled. Specify the name or the IP address of the XDMCP server you want to use.

In the “direct” mode you will get your “Graphical Logon” directly from the XDMCP server you have specified in the entry field, in the case that you have selected the “indirect” mode a list of available XDMCP servers will be provided from the server you specified.

Note: Make sure that your Display Manager Daemon (XDM, KDM, GDM, …) is running and the access permission is given on the remote host.

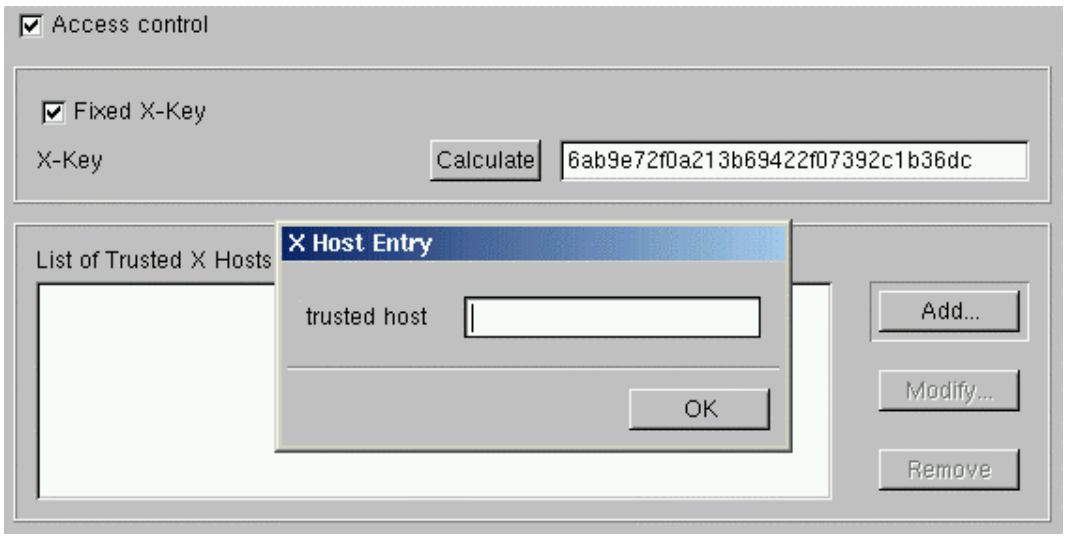
Access Control



The Thin Client provides an access control that is activated by default. If you disable this "Access Control" it will be possible for everybody from any UNIX host to have access to your terminal's display.

- ***Fixed X-key***

You can allow specific users to get permanent remote access to the Thin Client. Therefore you need to activate this option, press the "calculate" button and enter that 32-digit key into the Xauthority file of the user's machine.



List of Trusted X Hosts

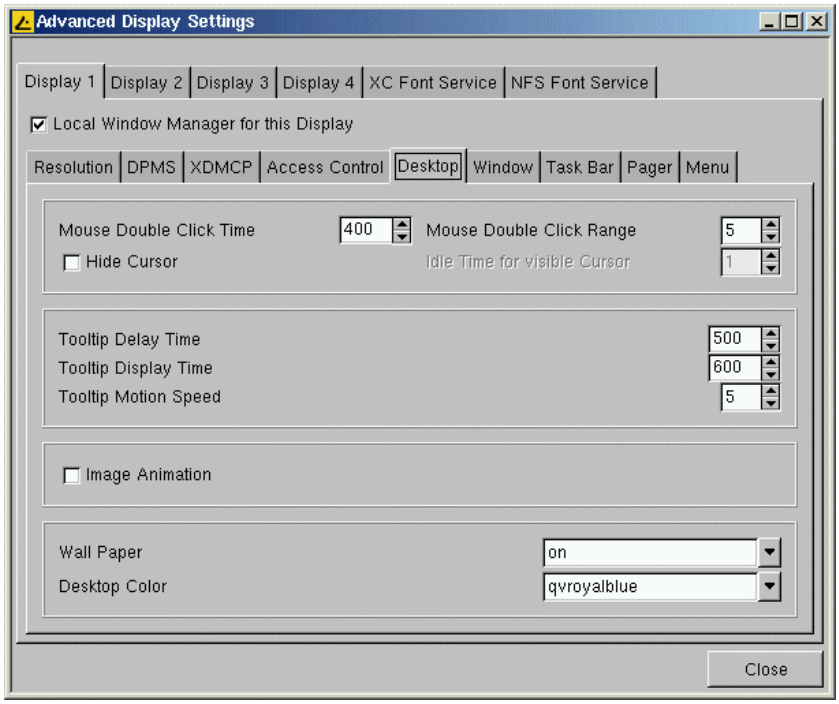
Click the "***Add…***" button to open the "X Host Entry" box. Enter the name of the remote host (**not the IP address**) you want to add and confirm with "ok".

Appearance

The following five dialog-boxes allow you to configure the appearance and the behavior of the “Desktop”, “Windows”, “Task Bar”, “Pager (Virtual Screens)” and the “Start Menu”.

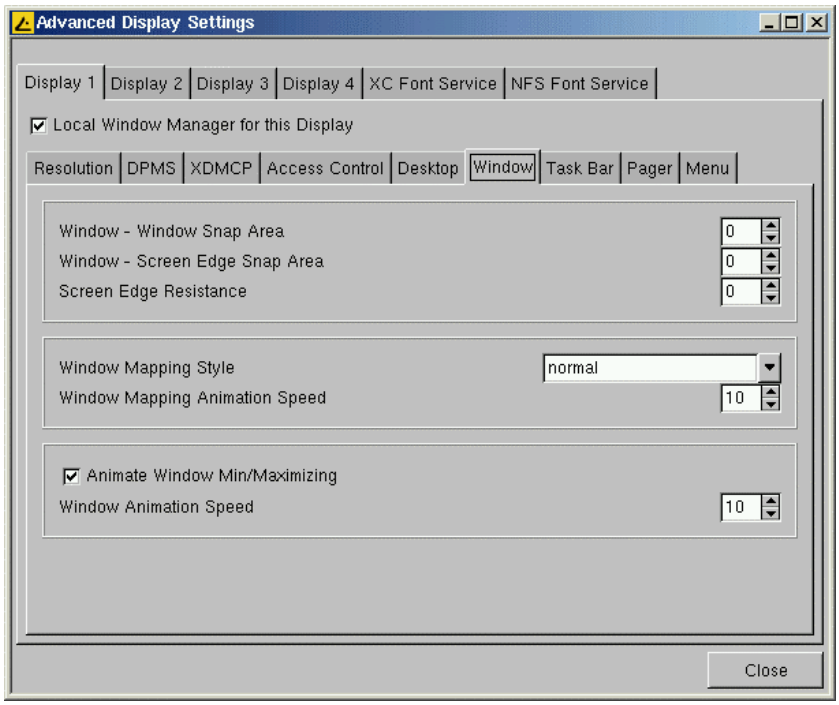
Note: Except the “Pager”, these masks are not described in detail, please refer to the tooltips.

Desktop



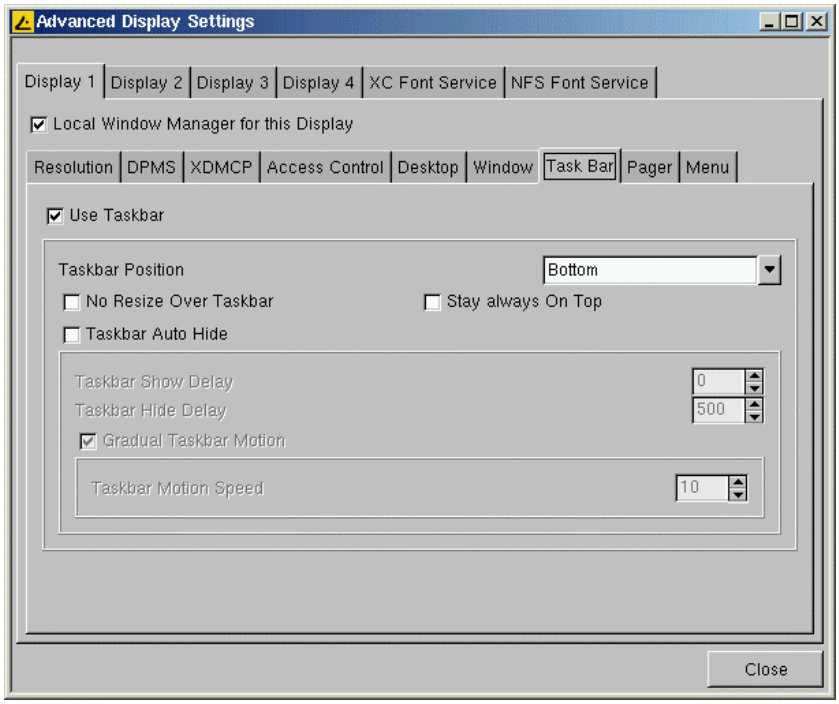
The “Desktop” dialog-box contains two additional properties of the mouse behavior, and allows you to manipulate the tool tip timings and the appearance of the desktop.

Window



The “Window” dialog-box enables you to define the window snap behavior, the style how to map/unmap windows and to enable/disable the animation of window minimizing and maximizing.

Task Bar

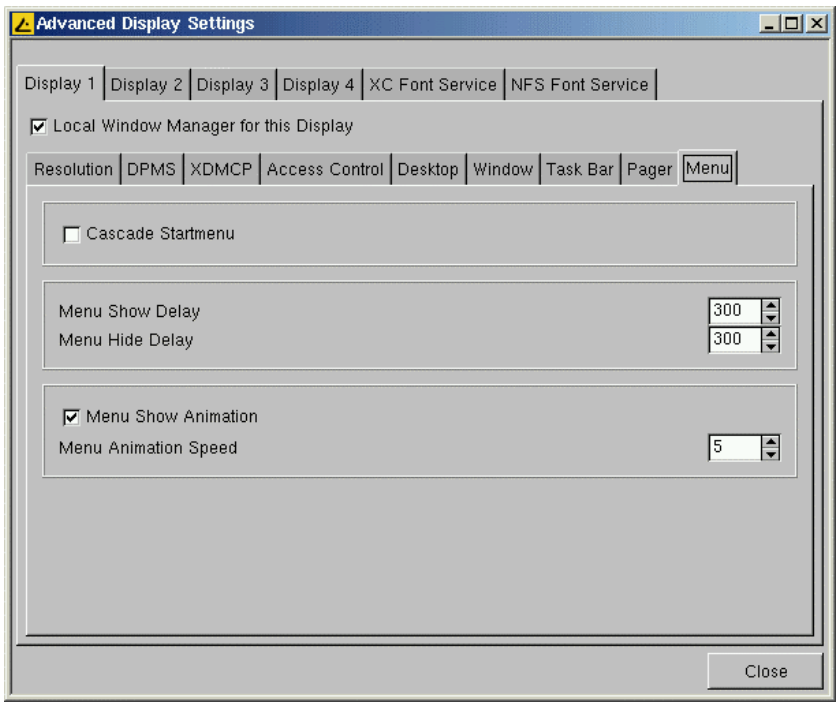


The ”Task Bar” dialog-box allows you to enable/disable the usage of the task bar and to define its behavior.

Pager

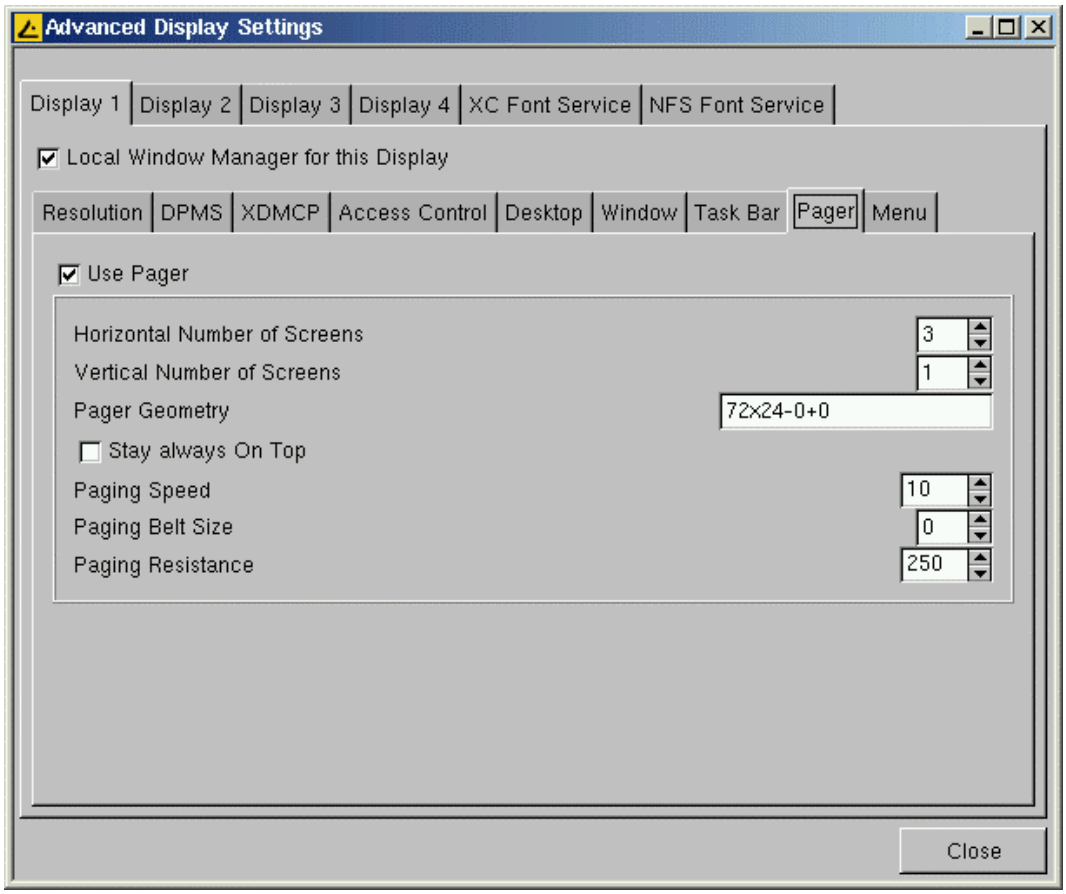
(See next page, please)

Menu



The ”Menu” dialog-box allows you to define the behavior of the start menu.

Pager



The “Pager” dialog-box allows you to enable/disable the usage of multiple “Virtual Desktops” like it is common in Linux.

The “Pager“ is a window with “Virtual Screens” that you can use to easily move from one open application to another. This window is displayed in the upper right corner of the desktop screen. It could contain a single “Virtual Screen”, or a higher number of “Virtual Screens”.
By using the pager, you can for instance switch between full-screen Applications by one sole mouse click.

To give a little example:

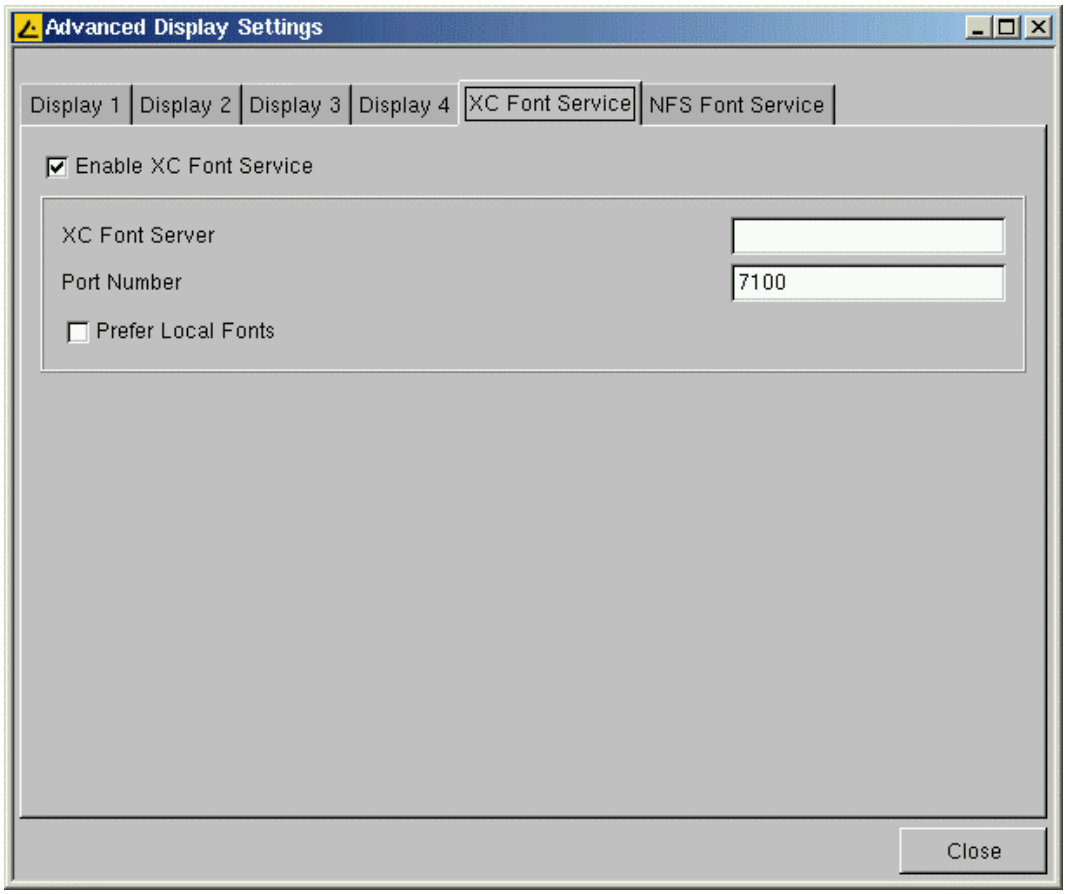
This exemplary pager contains three virtual desktops.
The first of them is active (dark gray) and shows the “*Application Launcher*” and the “Setup”. On the second one is a full-screened browser window.
Two different local shells are running on number three.

Now instead of minimizing and maximizing all that sessions or toggling them via key combinations, you simply mouse-click on the desired Screen and get back to it exactly like you left it before (except after reboot).

Have a look at the tooltips in order to modify the pager to your needs.

Note: Enable the option “Stay always on top” to always have it on top of every window.
Note: All running sessions of all virtual screens will be accessible via the task bar in each of the screens.

XC Font Service



If you require fonts in addition to those that the Thin Client provides, the XC Font Service can be used.

Note: This is a service that has to be installed and completely configured on the server.

The advantage of using the XC Font Service instead of NFS is the better performance of XC Font Service.

Click the "***Enable XC Font Service***" button to enable the following entry fields.

- ***XC Font Server***

Specify the server on which the XC Font Service is running.

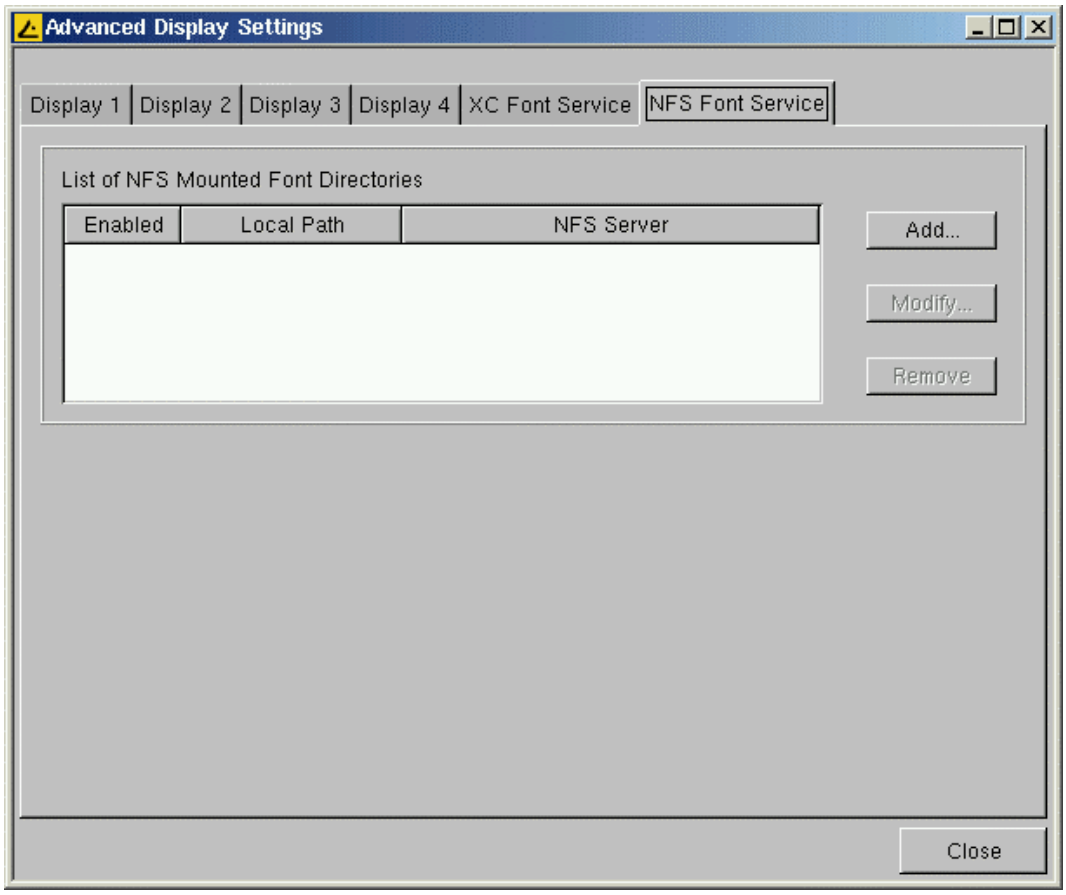
- ***Port Number***

Specify the port number where the font service is listening. (Default is port number 7100)

- ***Prefer Local Fonts***

Enable this option to use local fonts before asking the font server.

NFS Font Service



Another way of importing additional fonts is the usage of the NFS Font service. In addition, there is the advantage that the mount point for the fonts is configurable, which is necessary for certain remote applications that search for their fonts in a specific path.

If you want to use the “NFS Font Service”, you have to define and enable an “NFS Font Path Entry”, which will be added into “***List of NFS Mount Font Directories***”.

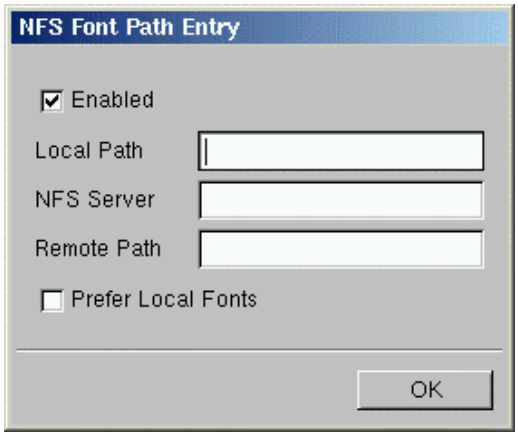
To do so, click the “***Add…***” button to open the following “***NFS Font Path Entry***” dialog-box:

- ***Local Path***
Specify the “Local Path” to the mount point.

- ***NFS Server***
Enter the name or the IP address of the server which provides the font directories via NFS.

- ***Remote Path***
Specify the path on the server side where the fonts are available.

- ***Prefer Local Fonts***
Enable this option to use local fonts before asking the font server.

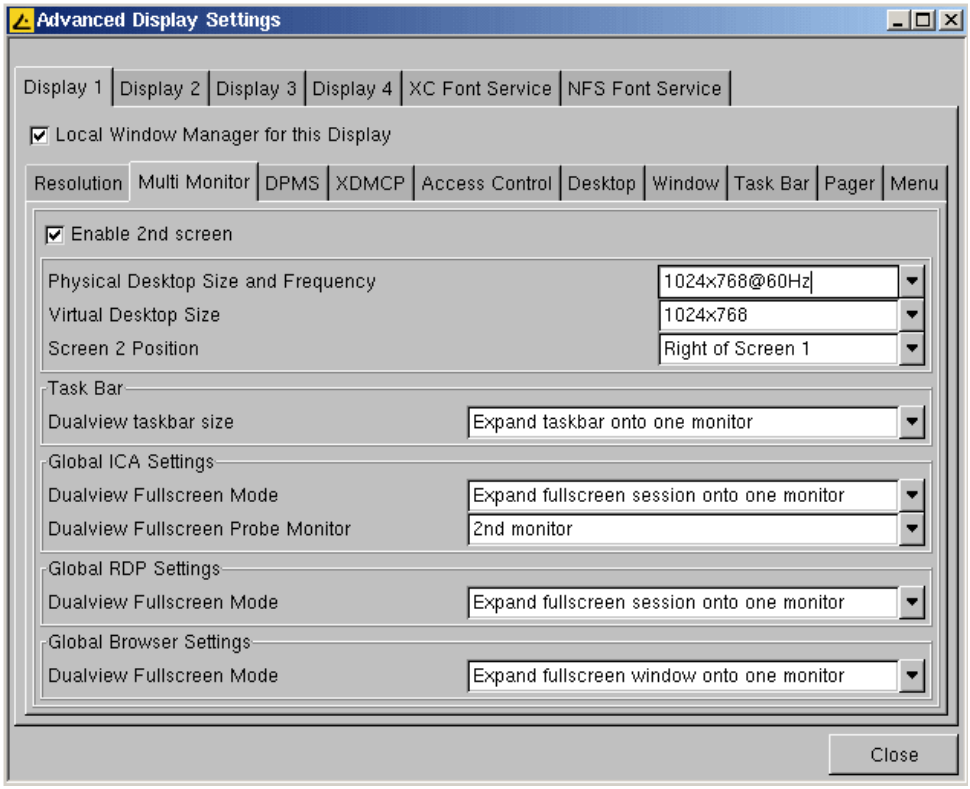


Note: Don’t forget to click the “Enable” button to activate your entry.
Note: On server side you have to export the font directory via NFS read only for the Thin Client.

5.4.3 Multi Monitor Mode

IGEL Thin Clients of series 5000 allow a Multi Monitor mode with the internal VGA chipset. You can attach one analog and one digital monitor.

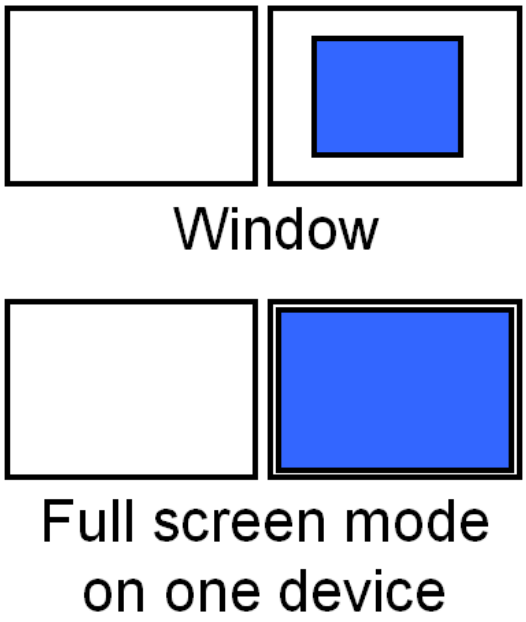
You can activate the Multi Monitor mode and change its settings on the „*Multi Monitor*“ page of the *Advanced Display Settings*.

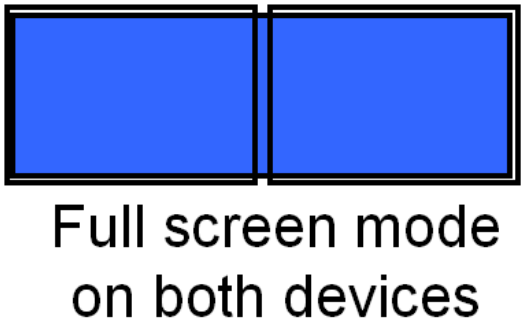


The resolution of the second display can be set independent from the first display’s resolution while the color depth will be the same. The second monitor can be positioned above or below and left or right besides of the first one.

Basically the second screen will be used as extended desktop on which you can position your application windows.

Possible display options are:



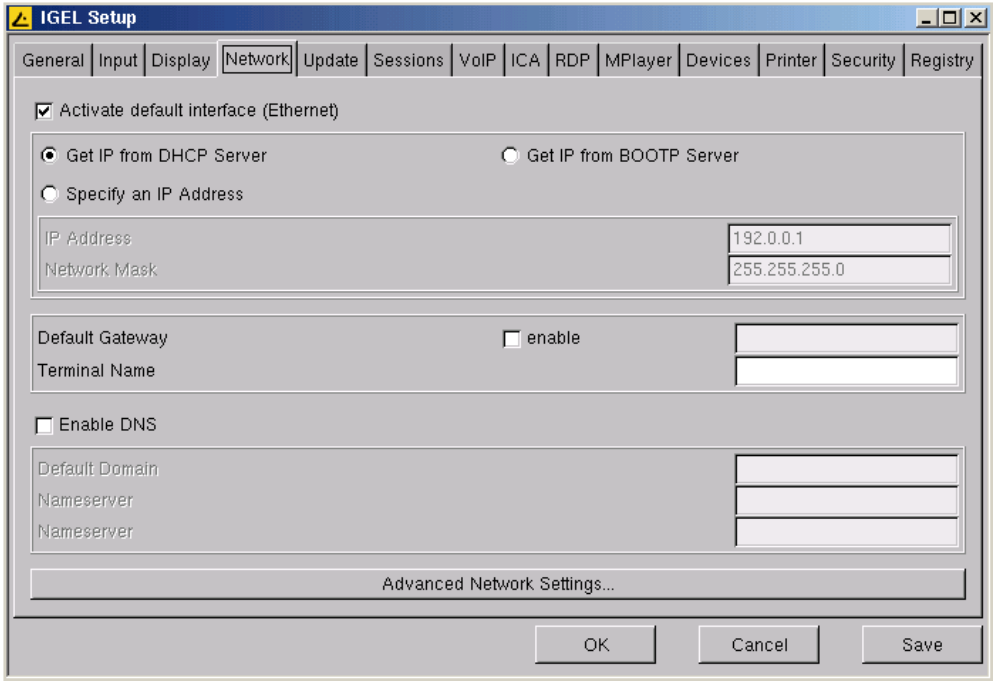


Note: If one of the screens does show no picture you should check in the BIOS of the Thin Client if both adaptors (CRT+DVI) are active (*Advanced Chipset Features -> Select Display Device*) and if enough graphic memory is reserved (*Advanced Chipset Features -> VGA Share Memory Size*). Usually 8 MB are enough for single screen mode, high resolution settings in Dual Monitor mode can require 16 to 32 MB.

5.5 Network

5.5.1 Main Network Settings

The main “Network” page allows you to configure the network settings on the Thin Client side. Automatic network set up by using DHCP and BOOTP protocols, but also manual network configuration can be chosen.



- ***DHCP***

DHCP stands for “Dynamic Host Configuration Protocol” and enables the Thin Client to extract its IP-address, network mask, DNS, gateway and other network configurations from a DHCP server.

- ***BOOTP***

Using BOOTP allows the Thin Client to obtain the IP address, network mask, DNS, gateway and other network configurations from a BOOTP server database.

Note: The transfer of either a setup.ini or boot script is supported. BOOTP is not used to get a boot image from a server and to boot this image as the classical meaning of using BOOTP suggests.

- ***Specify an IP Address***

Click this button to set the network settings manually instead of looking for a DHCP server.
Make sure that the fixed IP you enter is not occupied by another machine in your network.
If you have to use a “***Gateway***” to route the data packets to and from the target network, click the “***enable***” button and enter the gateway IP address.

- ***Terminal Name***

Enter the local name of the Thin Client, otherwise the name “IGEL-<MAC-address>” will be generated.

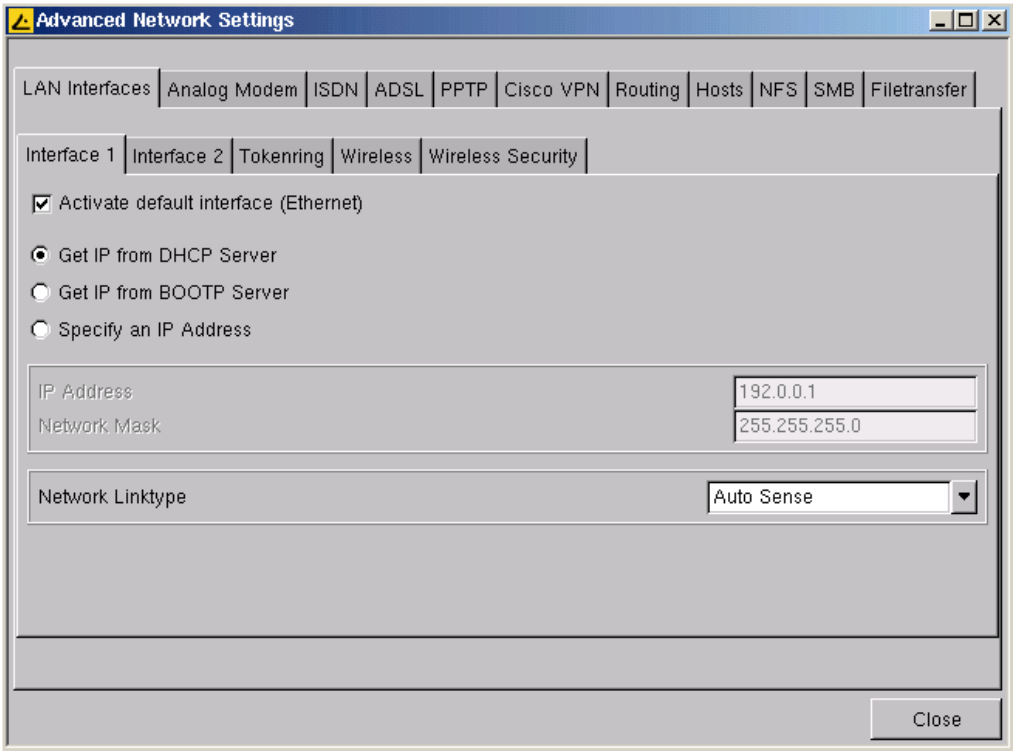
- ***DNS***

Click “**Enable DNS**” button to configure the Domain Name System. Set the “Default Domain” the unit should work in and the IP of up to two name servers, which will be queried one after the other.

5.5.2 Advanced Networks Settings

LAN Interfaces

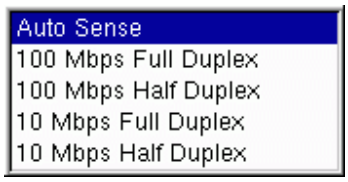
By default the “onboard” network hardware is used and you have configured the basic network settings in the “Network” page described before.
Now after you have entered the “Advanced Network Settings” section these settings are taken over to the corresponding “***Interface 1***” dialog-box of the “***LAN Interfaces***” page.



There are three additional dialog-boxes to configure the optional “LAN Interfaces” as there are: The configuration masks of Interface 2 and Tokenring are exactly the same as Interface 1 (except the network speed).

- ***Interface 2***

If you installed an optional ethernet card in the available PCI/ISA slot (only available in IGEL Thin Client series 400 and 500), use this dialog-box to configure the LAN interface called “Interface 2”.
In case you encounter problems with the auto sense function in your network, you can set a fixed network speed.
See the box to the right for possible speeds for both, Interface 1 and Interface 2.



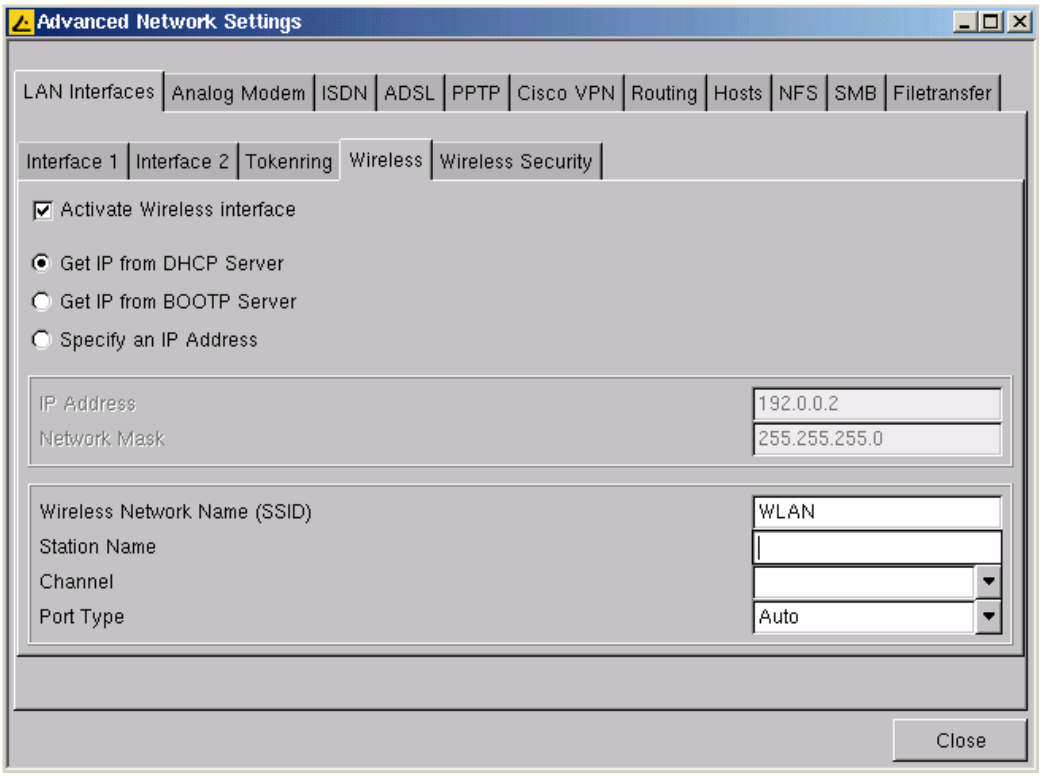
- ***Tokenring***

If you have installed an optional Token-Ring card in the available PCI/ISA slots (only available in IGEL Thin Client series 400 and 500) use this dialog-box to configure the LAN interface called “Tokenring”.
As described above (“Interface 2”), you may set a fixed speed for Token Ring as well.

- ***Wireless Network***

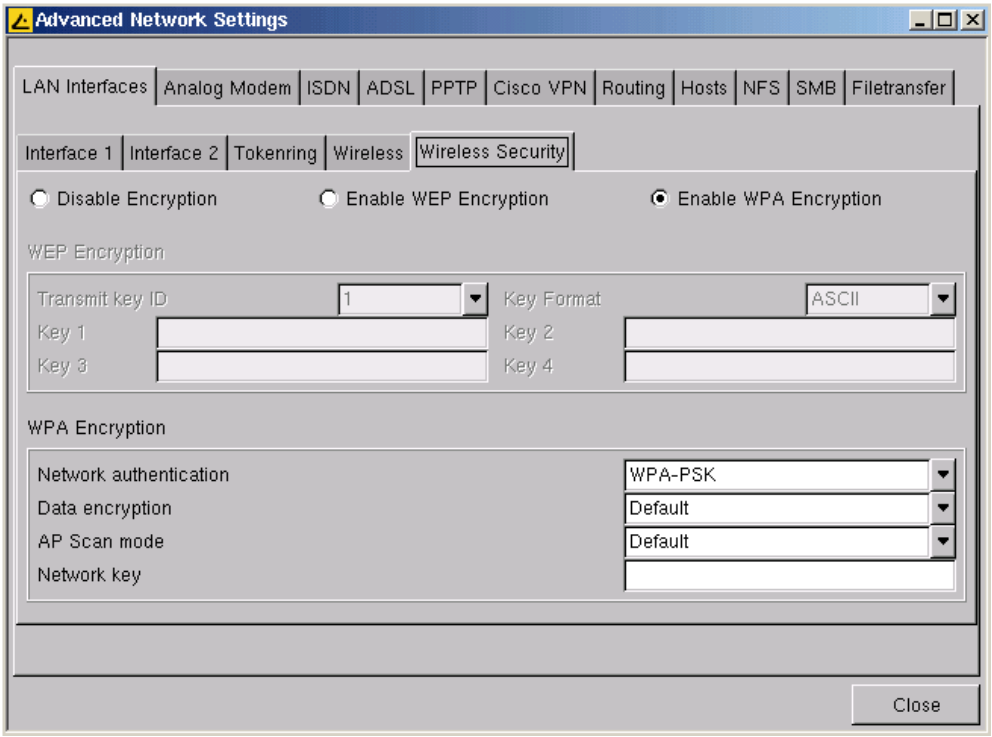
(see next page)

Wireless LAN Configuration



If you have installed an optional Wireless-LAN card in the available PCI/ISA slots (only available in IGEL Thin Client Series 4000 and 5000) use this dialog-box to configure the LAN interface called “wlan0”.
In case you want to use a Wireless-LAN PCMCIA card, you’ll need the proper IDE-to-PCMCIA adapter for units of the 4000 series. The 5000 series models are already equipped with an onboard PCMCIA adapter. On the Wireless Security page you can change the encryption settings, the highest available encryption is WPA-2.

Note: These dialog-boxes are not described in more detail, because they are well explained by the available tooltips. Please also refer to the manual of your WLAN equipment.

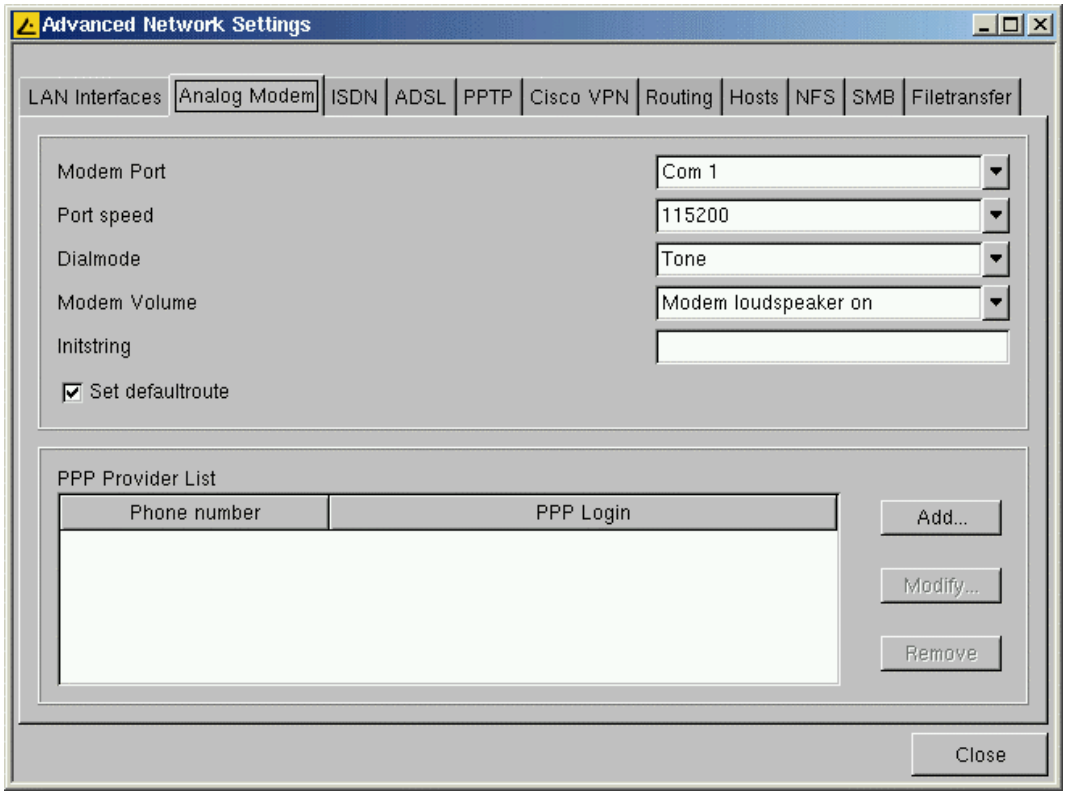


Analog Modem

To set up a WAN connection with the Thin Client you can use an analog modem.
There are different modem types that can *not* be used with our Thin Clients. Especially so-called WIN modems will *not* work. All external modems that are connected to the COM ports or internal modems that can be configured to behave like an external modem will work. (If possible, prefer modems with a “Rockwell” chip)

Note: *Internal* modems are only supported by IGEL Thin Clients Series 4000 and 5000.

The following dialog-box allows you to configure the basic modem settings and specific PPP connections:



- ***Modem Port***

Specify the serial port where the modem is connected. (Use COM 1 + COM2 for external modems and COM 3 + COM 4 for internal modems)

- ***Port Speed***

Specify the speed of the port where the modem is connected.

Note: This is not the speed of the modem, but the speed of the communication between modem and Thin Client in baud. This means this speed should be set higher than the modem speed to guarantee that data transfer can run at full modem speed.

- ***Dial Mode***

Specify the dial mode of your phone line.

- ***Initstring***

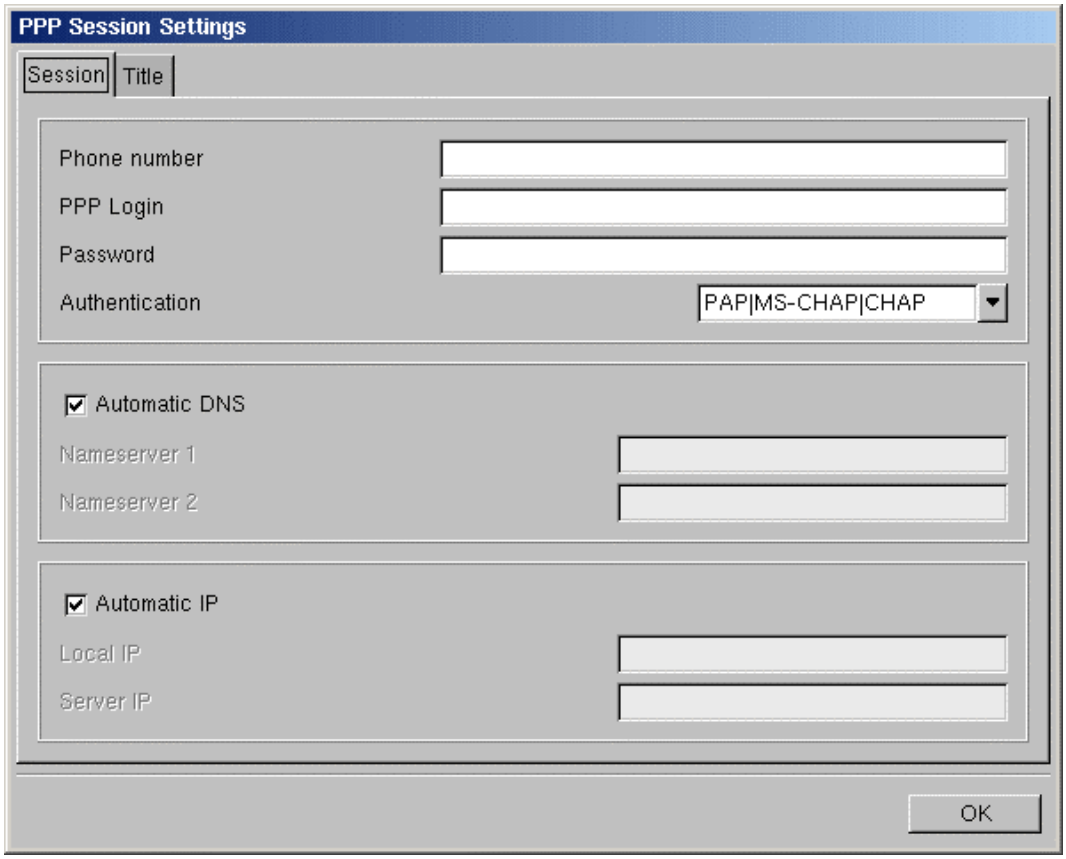
Specify a special initstring for your analog modem if the standard initstring does not work.

- ***Set Default Route***

This option can be used to set the default route to the PPP connections.

To create a new PPP connection, click the “***Add…***” button and the following dialog-box will appear on the screen (see next page):

PPP Provider Settings



- ***Phone Number***

Specify the phone number of your provider.

- ***PPP Login*** and ***Password***

Specify the login and the password of your provider account.

- ***Authentication***

Select the authentication type for this modem connection from this list:
(Only a few providers use the CHAP method although it is the safer one because of the usage of encryption.)

- ***Automatic DNS***

This option allows you to choose between automatic or manual DNS configuration.
If you choose manual configuration you have to enter the IP address of your provider's "***Nameserver***".

- ***Automatic IP***

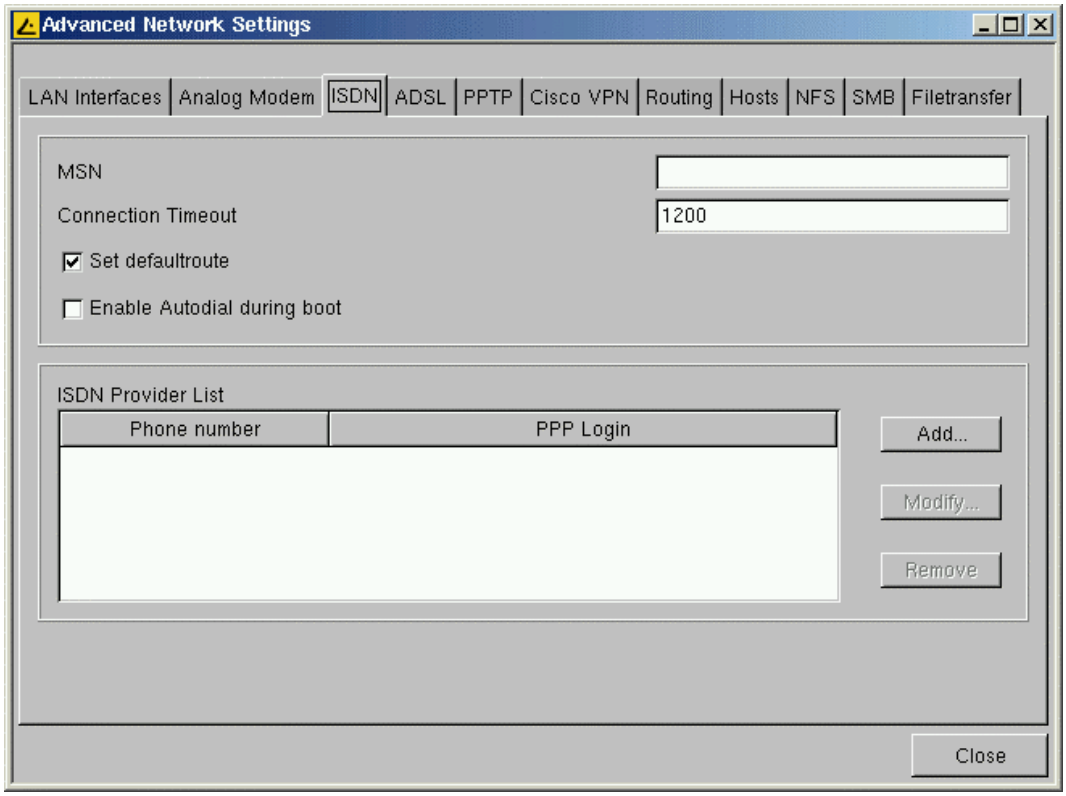
This option allows choosing between automatic or manual IP address configuration. The default setting is set to automatic, which means that the Thin Client gets its IP address dynamically from the provider's DHCP server. In case you have deactivated the automatic mode, you have to enter the Thin Client's "***Local IP***" and your provider's "***Server IP***" manually.

For details on the "**Title**" tab, please see Chapter 6.4.

ISDN

The second way to set up a WAN connection with the IGEL Thin Client is using an ISDN card.

Note: The currently supported ISDN cards are the AVM Fritz (version 1.0 and 2.0 as well as the ISDN/DSL combi card) and the U.S. Robotics PCI card. This feature is available only for the IGEL Thin Client Series 4000 and 5000, which provide the additional PCI slot.
Note: Because the ISDN configuration is nearly the same as the modem configuration, we only describe the differing or additional features / options below.



- ***MSN*** (Multiple Subscriber Number)

In this field you have to provide the MSN of your ISDN installation. This number is the phone number being used for the device without predial.

- ***Connection Timeout***

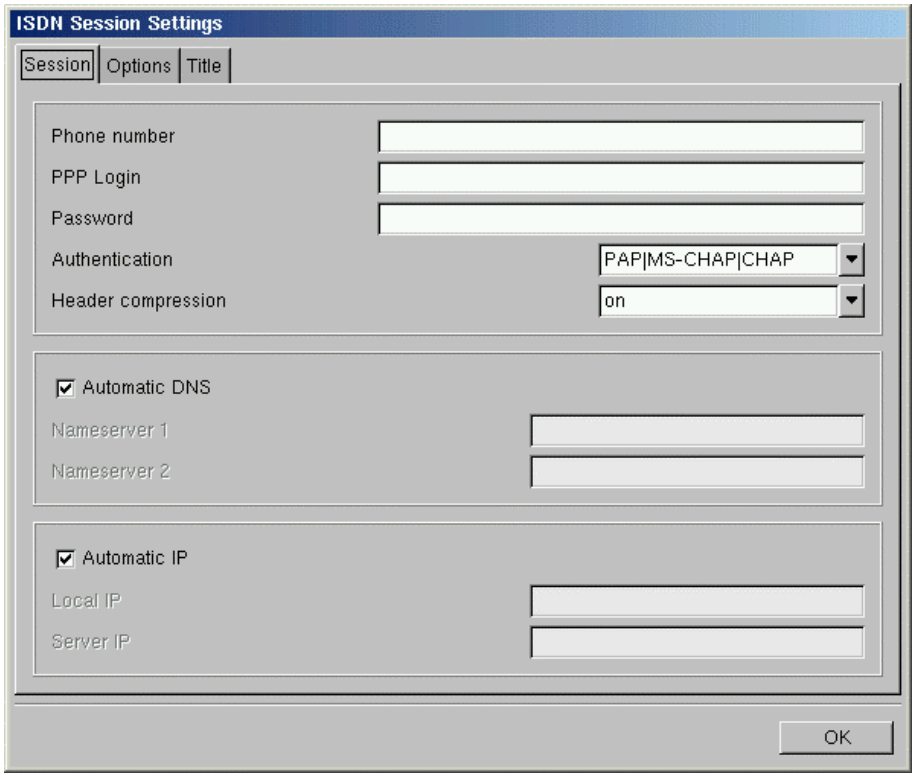
Specify the period of time (in seconds) of inactivity after which the ISDN connection will be disconnected automatically by the Thin Client.

- ***Enable Autodial during Boot***

Enable this checkbox to make the client connect to your host before the desktop boots up.

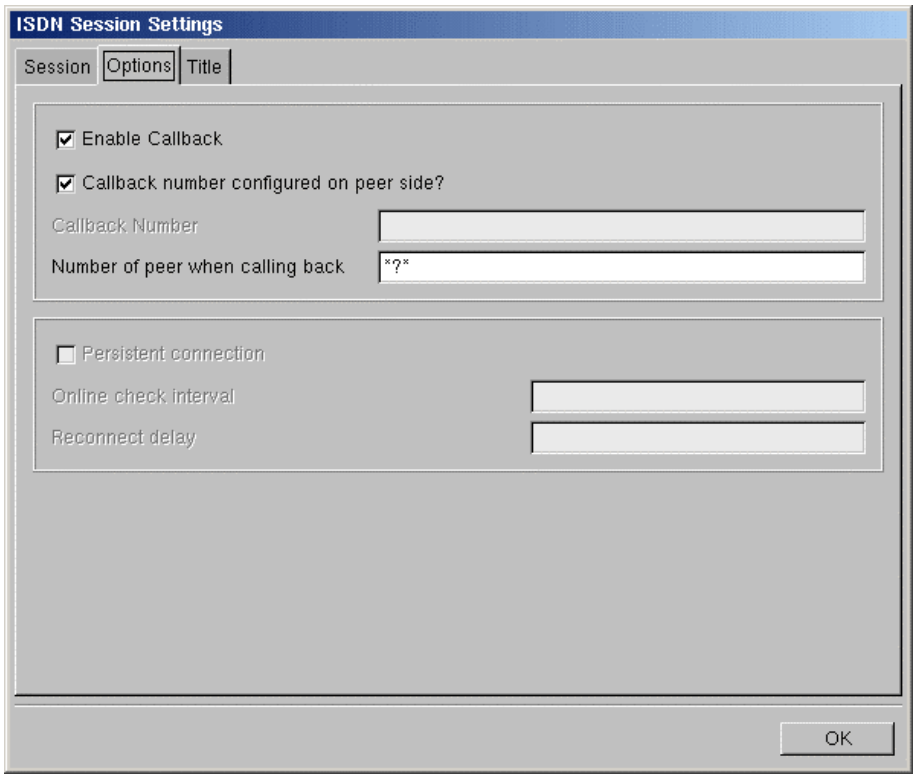
To create a new connection, click the "***Add...***" button, and the following dialog-box will appear on the screen (see next page):

ISDN Provider Settings



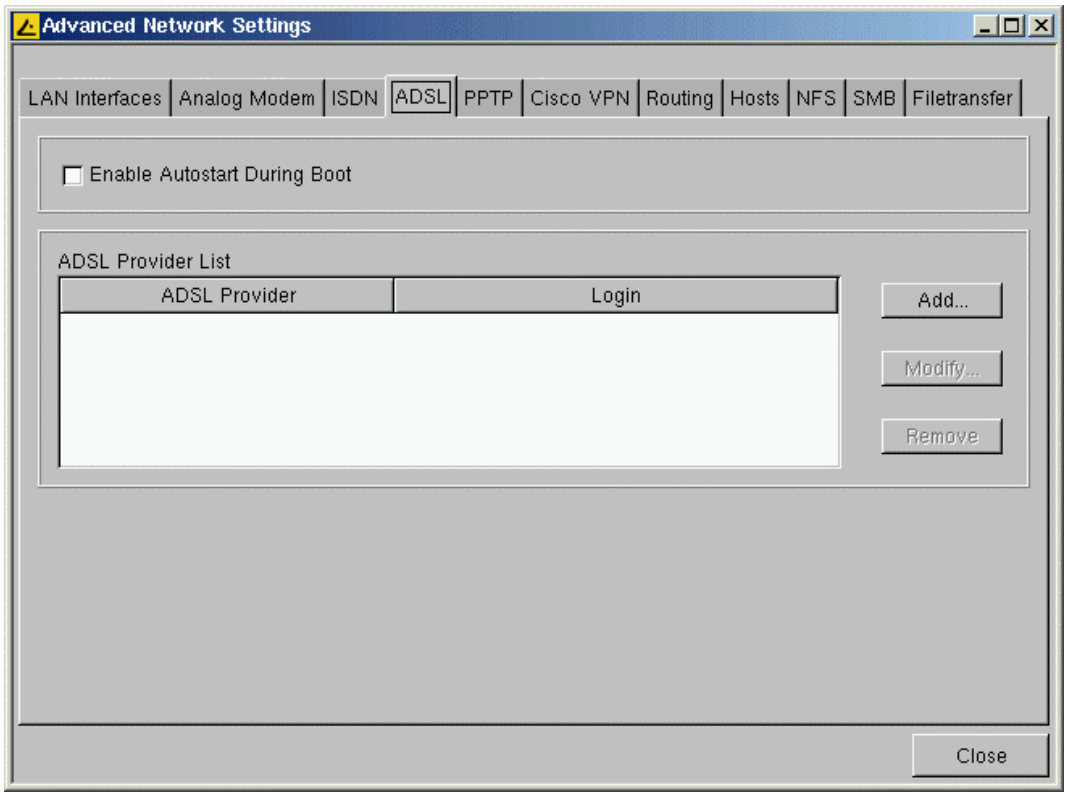
Enter your provider settings here.

Options (Callback)



The callback feature enables your provider to call back the Thin Client (mainly used for home workers). Please refer to the meaningful tooltips for details and syntax.

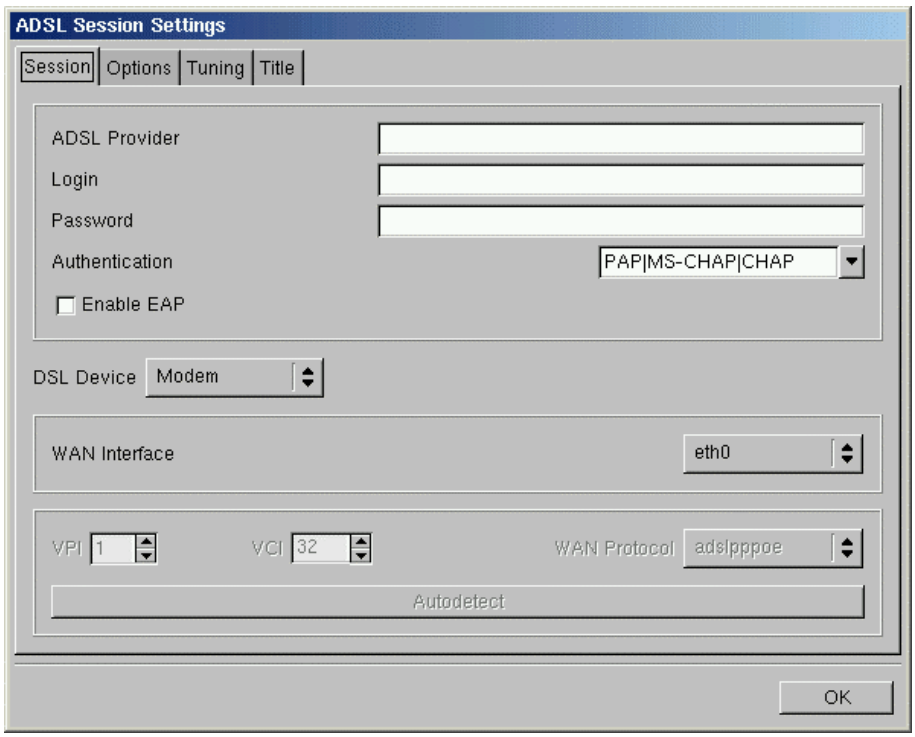
ADSL



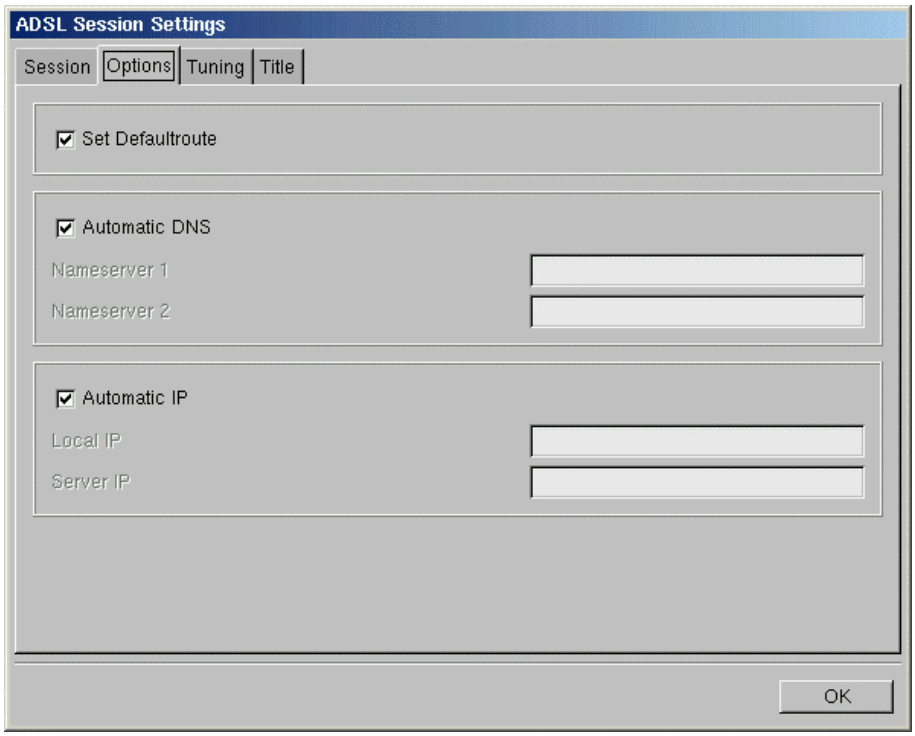
- ***Enable Autostart during Boot***

In order to set up a fully autostart-configured client, you may need to dial in first. Enable this checkbox to make the client connect to your host before the desktop boots up.

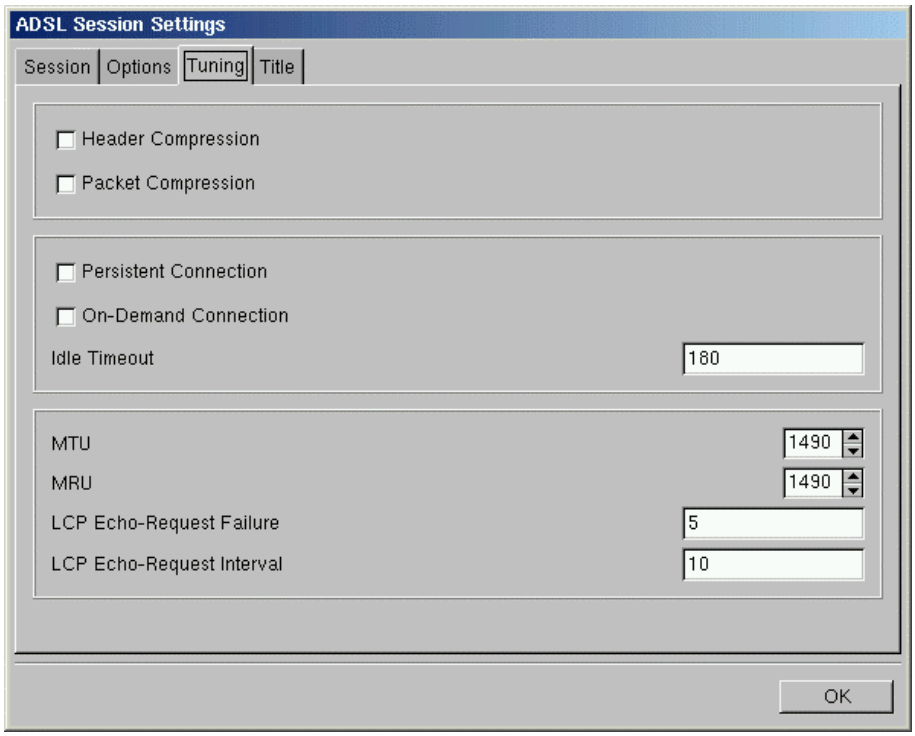
Via the "***Add...***" button, you set up new connections:



First, enter your account's configuration. Next, select if you connect via a DSL modem connected to the network interface or if you use an internal PCI device.
Also, set if the DSL connection should be network interface eth0 or eth1 and the protocol to be used.



The options tab enables you to define name service and IP configuration for the DSL connection. Usually, this will be handed over by the RAS server of the provider, so by default, both DNS and IP are set to “automatic”.



The tuning tab lets you basically set two things, the connection’s duration and network packet size and error handling.

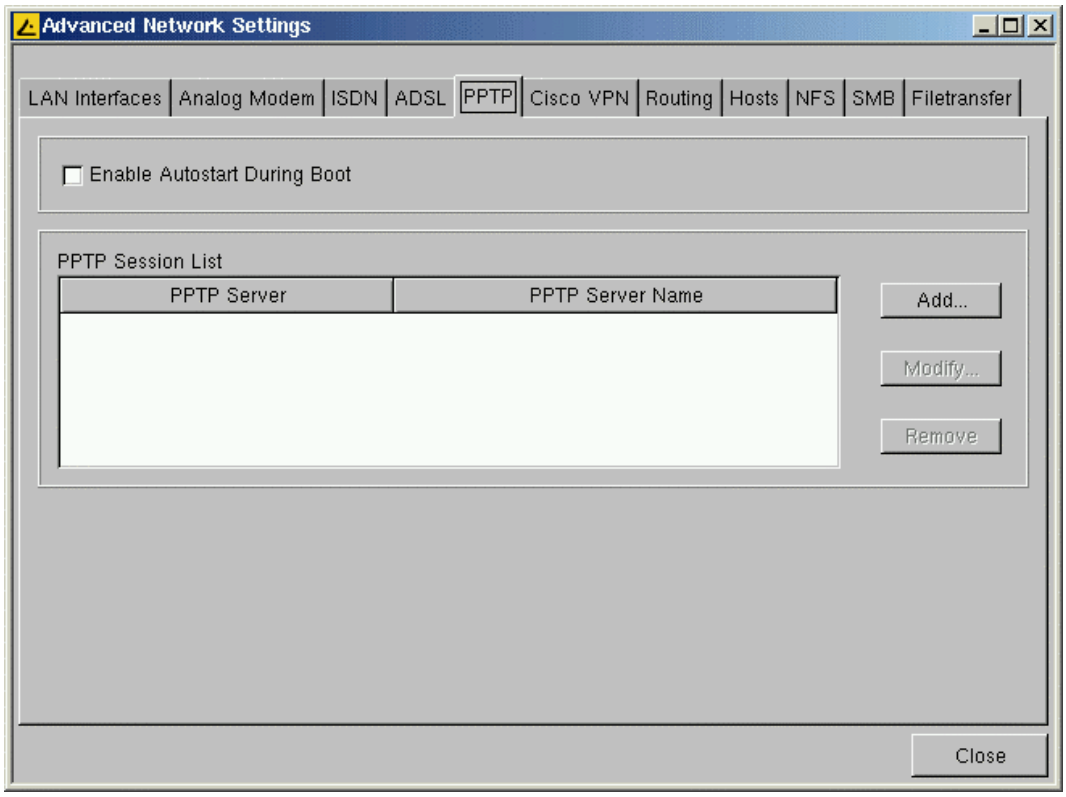
- ***Persistent Connection*** and ***On-Demand Connection***

Select if your connection should be kept or only be used on demand only if needed.
If on-demand is chosen, the connection will disconnect after the given timeout (in seconds).

- ***MTU*** and ***MRU***

Set the maximum size of packets (maximum transfer units and maximum receive units).

PPTP

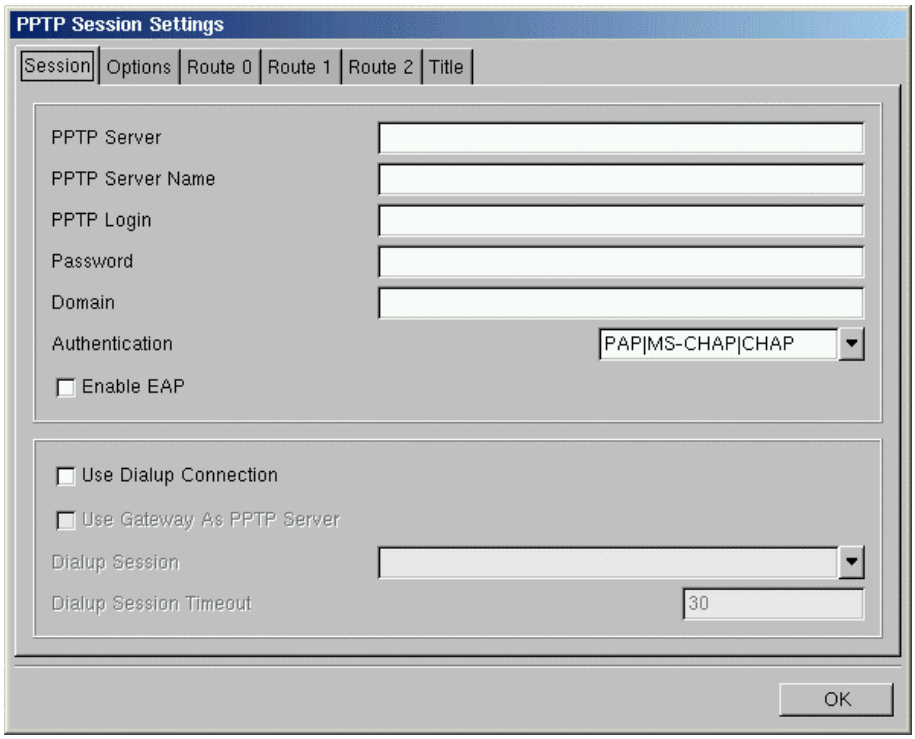


PPTP (Point-to-Point Tunneling Protocol) is one of the most common virtual private networks (VPN) protocols enabling remote users to access corporate networks securely.

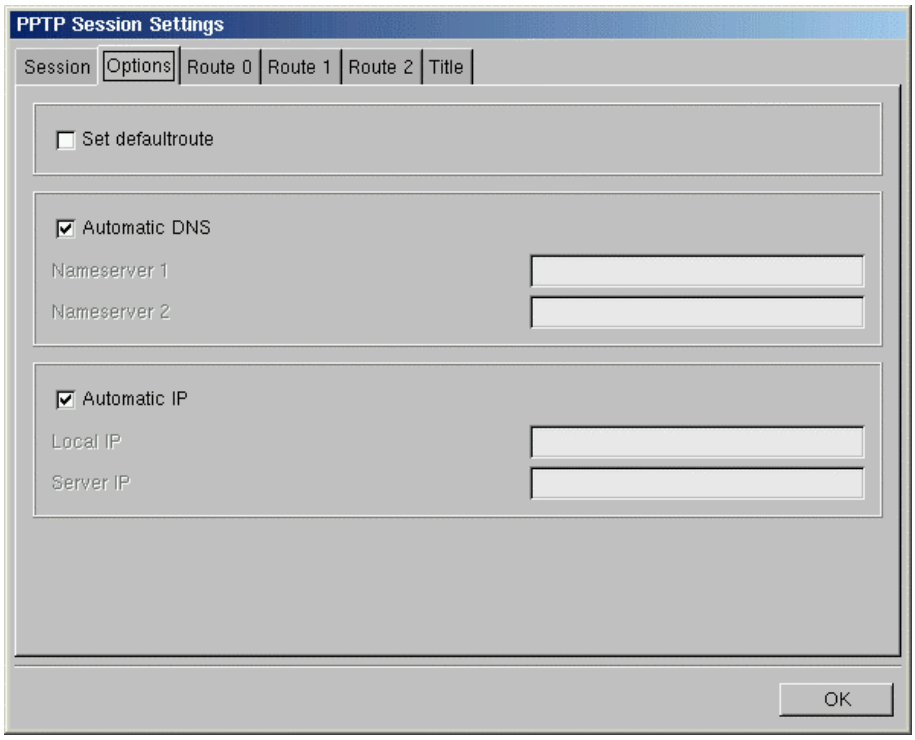
- ***Enable Autostart during Boot***

In order to set up a fully autostart-configured client, you may need to dial in first. Enable this checkbox to make the client connect to your host before the desktop boots up.

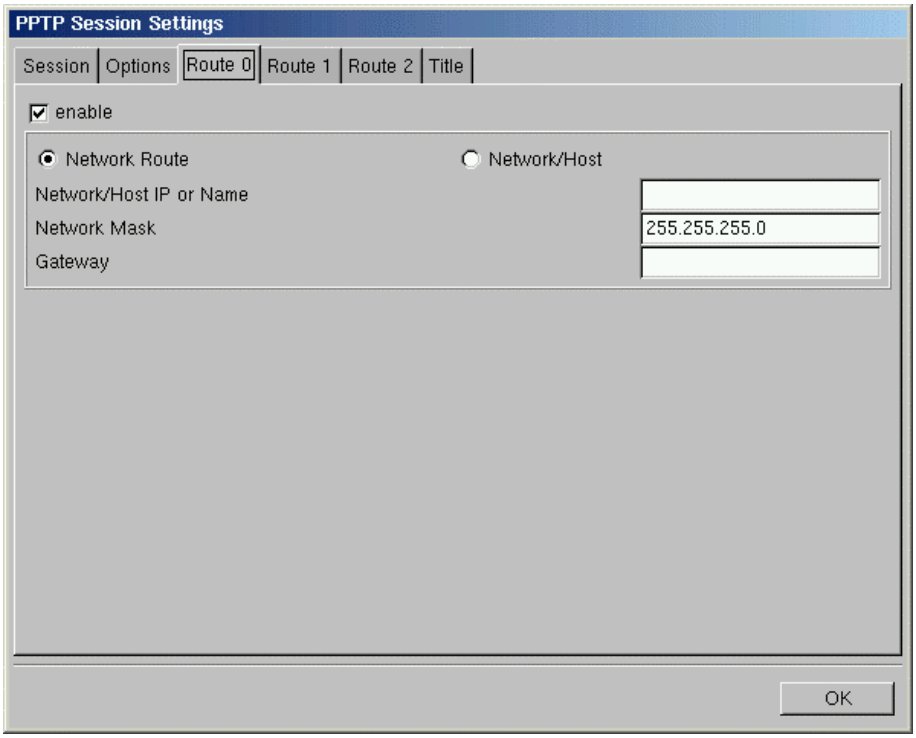
Click the "***Add...***" button to set up new connections:



Enter the necessary settings to dial in to the RAS server on the desired remote station. Further, you select the network device and if a dialup connection should be used.

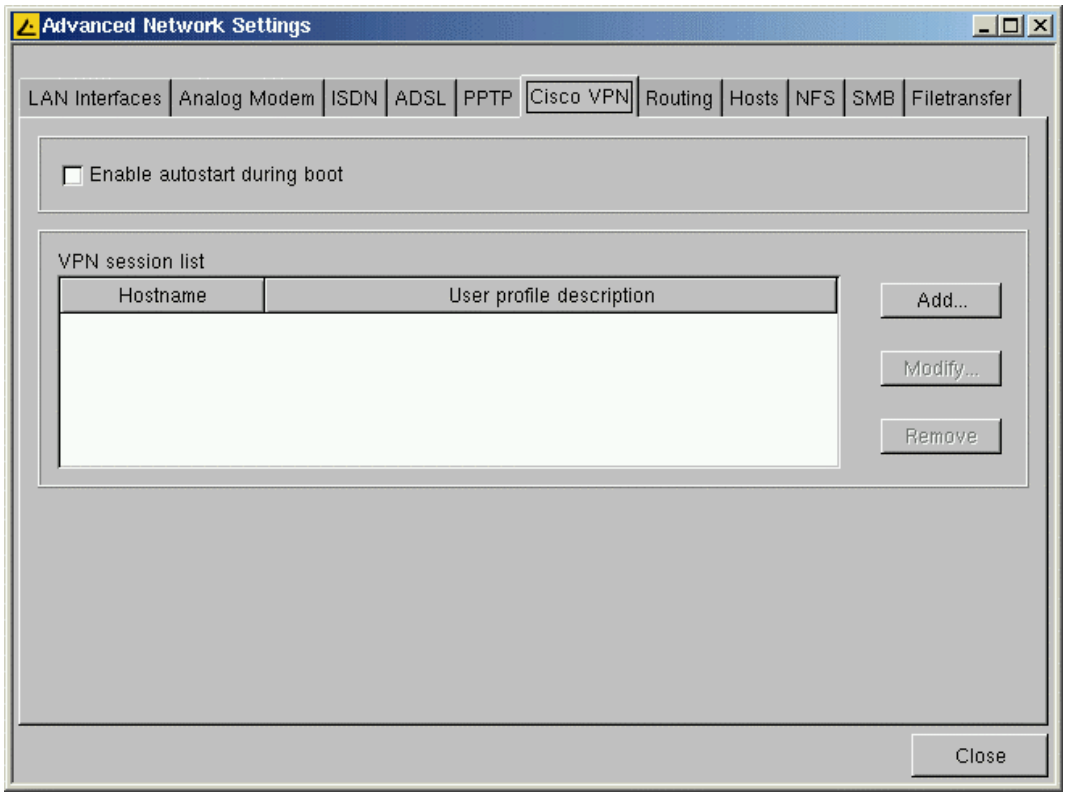


In the options tab you define name service and IP settings for the PPTP connection.
As this will usually be handed over by the RAS server of the remote station, both DNS and IP are set to “automatic” by default.

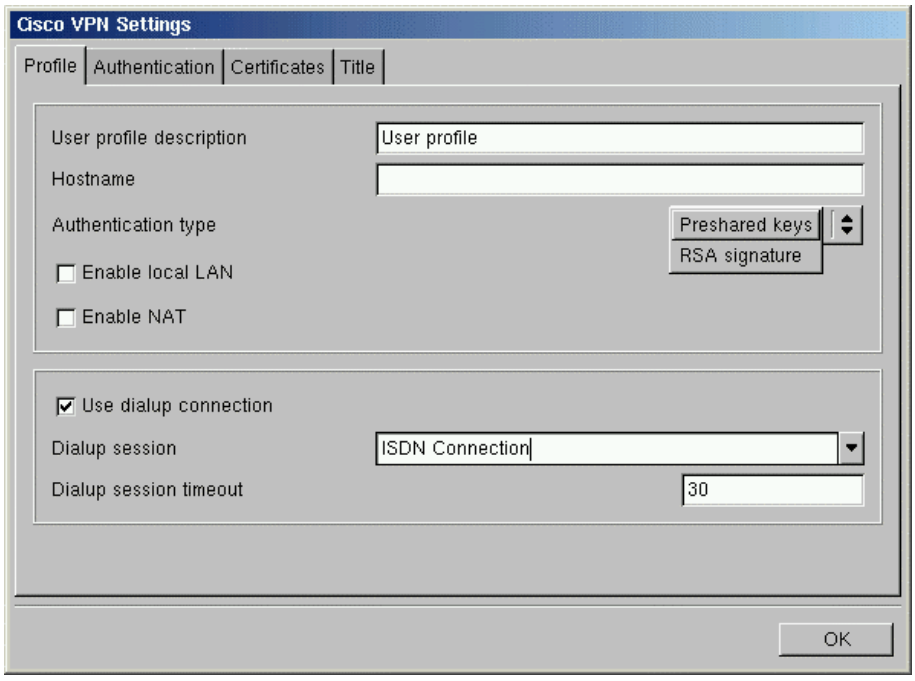


The following three setup pages let you set up additional network routes.

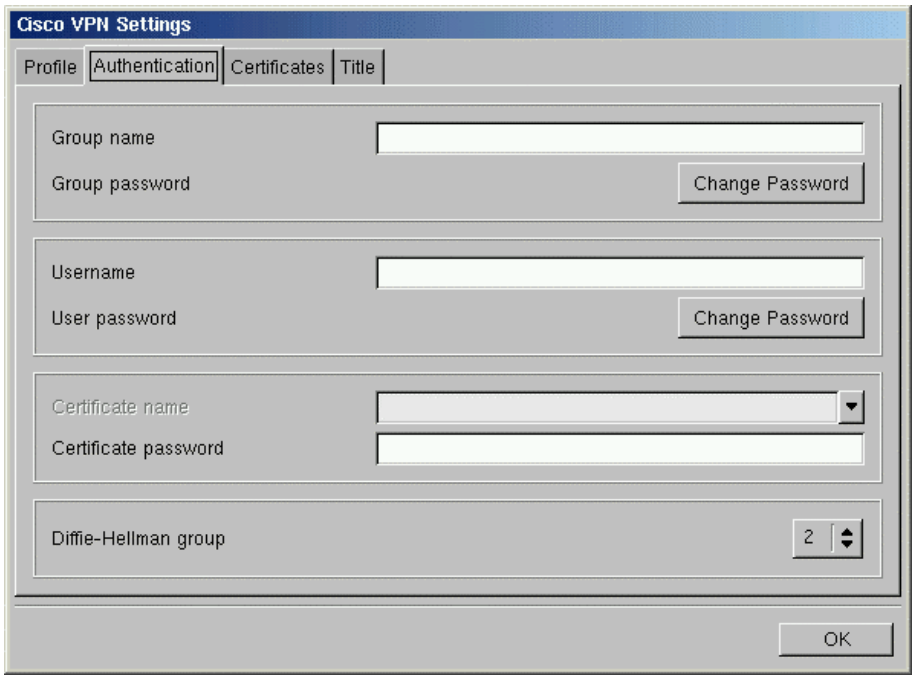
Cisco VPN



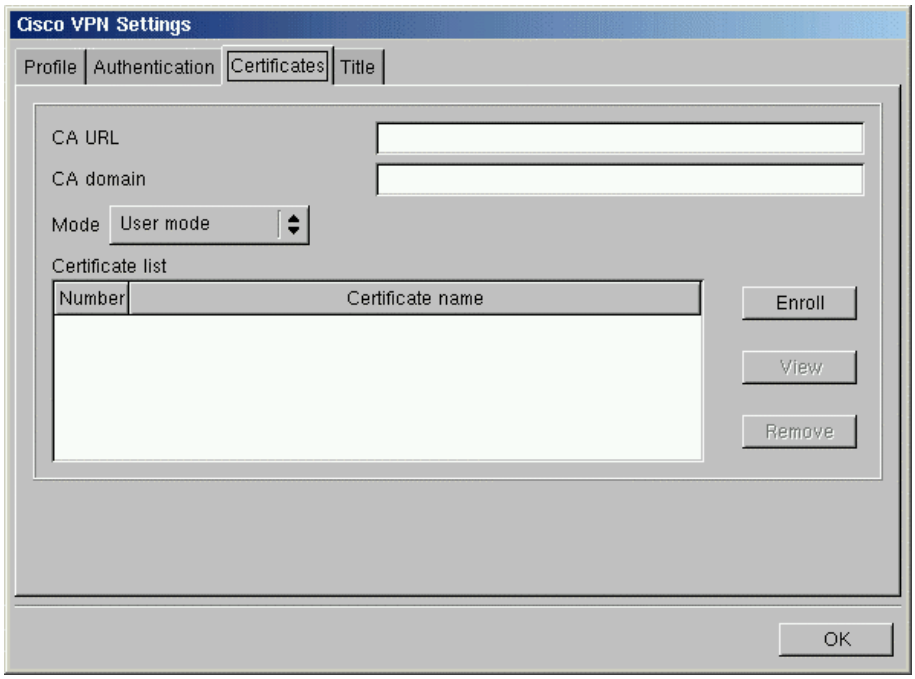
Please refer to the third party documentation “Cisco_VPN_Client_User_Guide.pdf” for details on proper configuration and syntax details.
We only show the corresponding setup pages and give a rough description here.



Initially, set the host to authenticate against.
You also set the desired connection to be used here.

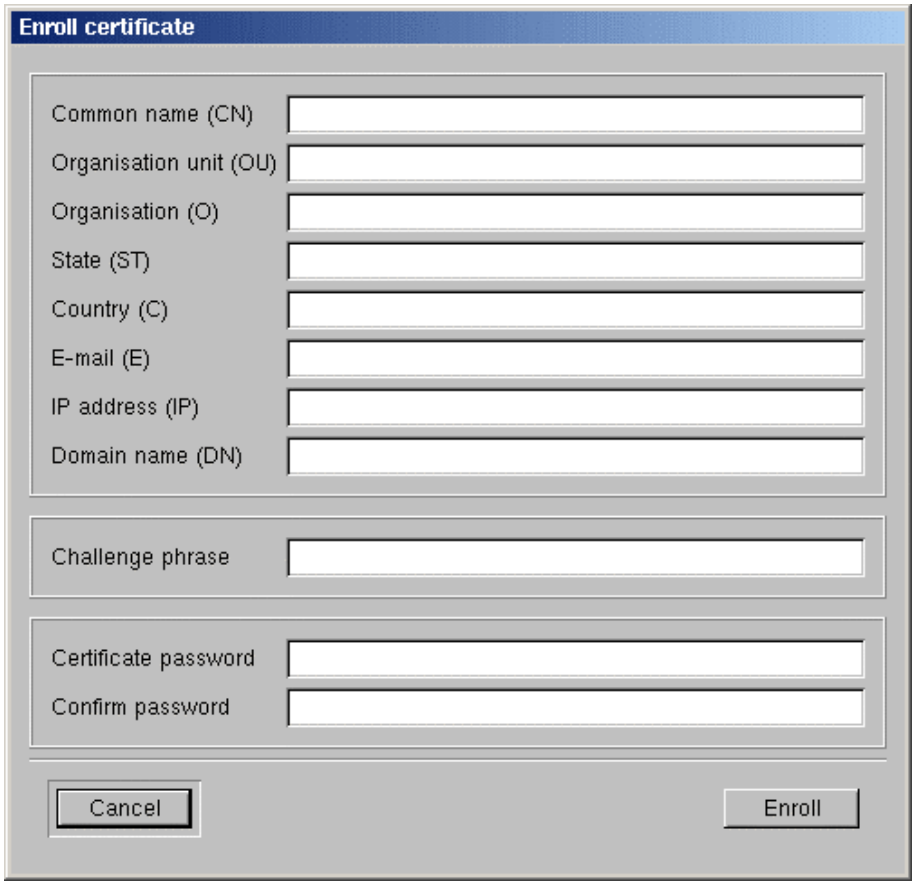


Enter the account's details here.



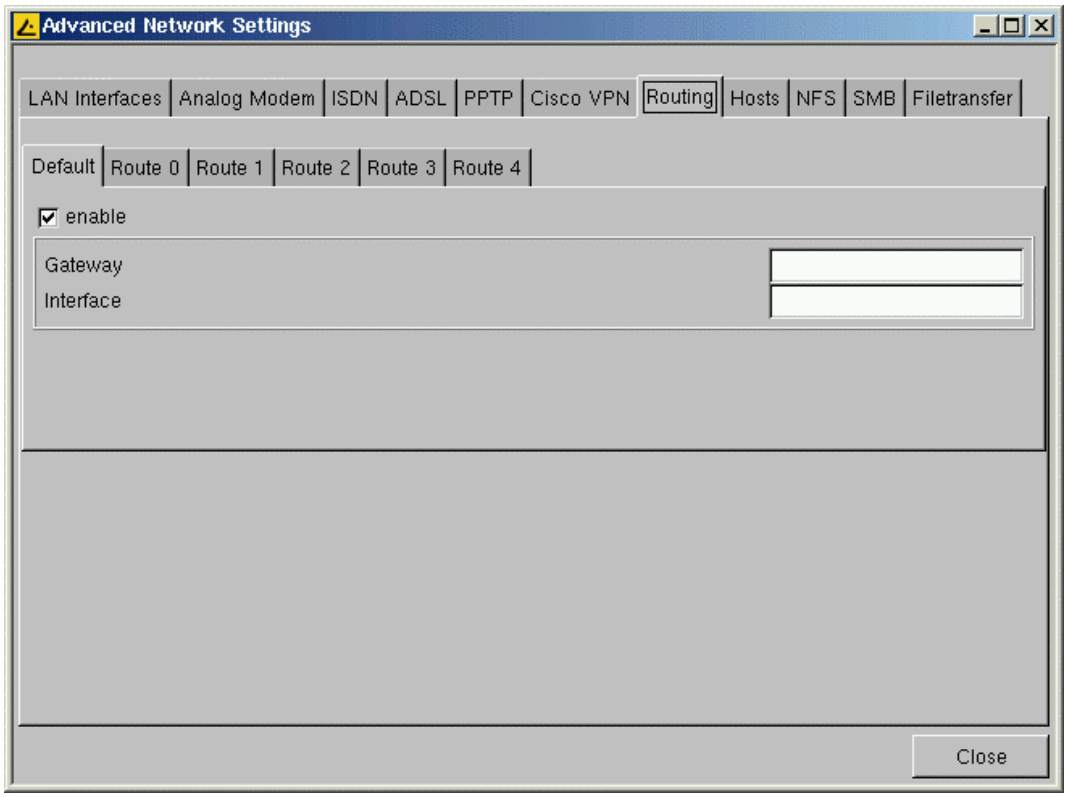
Certificate global settings like the URL and domain for them have to be set in this tab.

Click the "***Enroll"*** button for the certificate's details (see next page).

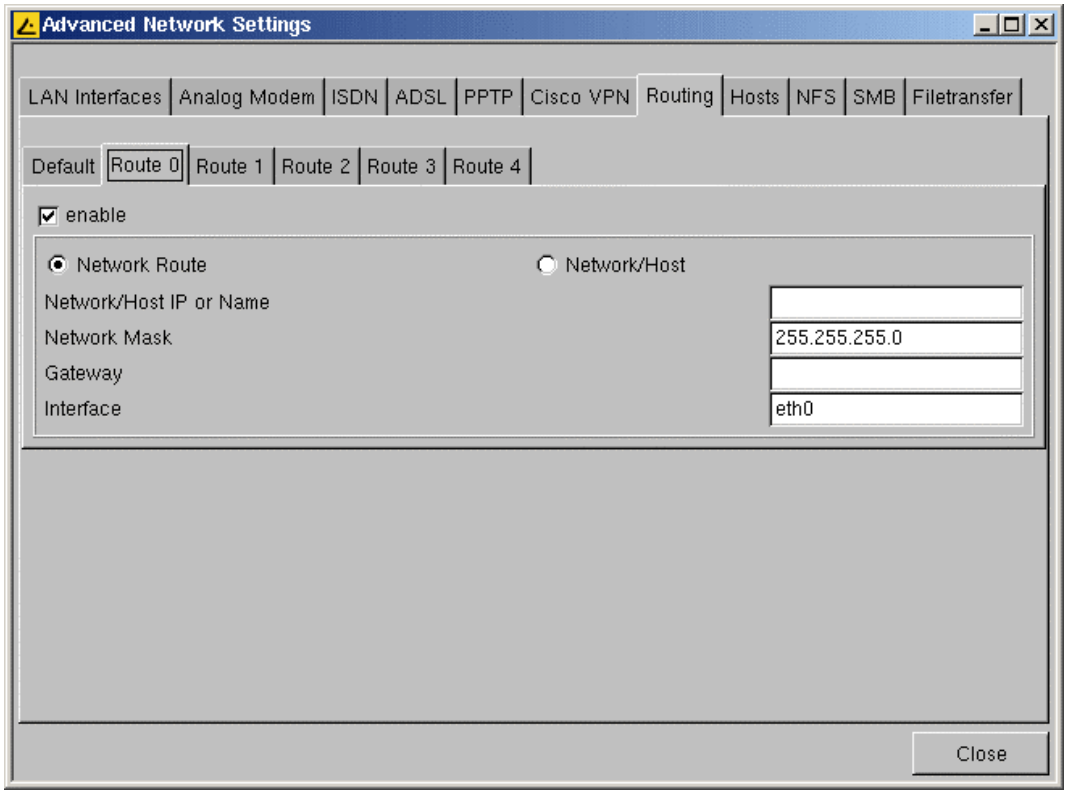


This tab is for the certificate's actual details.

Routing



Use this dialog-box to specify additional network routes if necessary.
(The Interface field needs “eth0”, “eth1”, “tr0” or “wlan0” meaning Interface 1+2, Tokenring and Wireless Lan.)

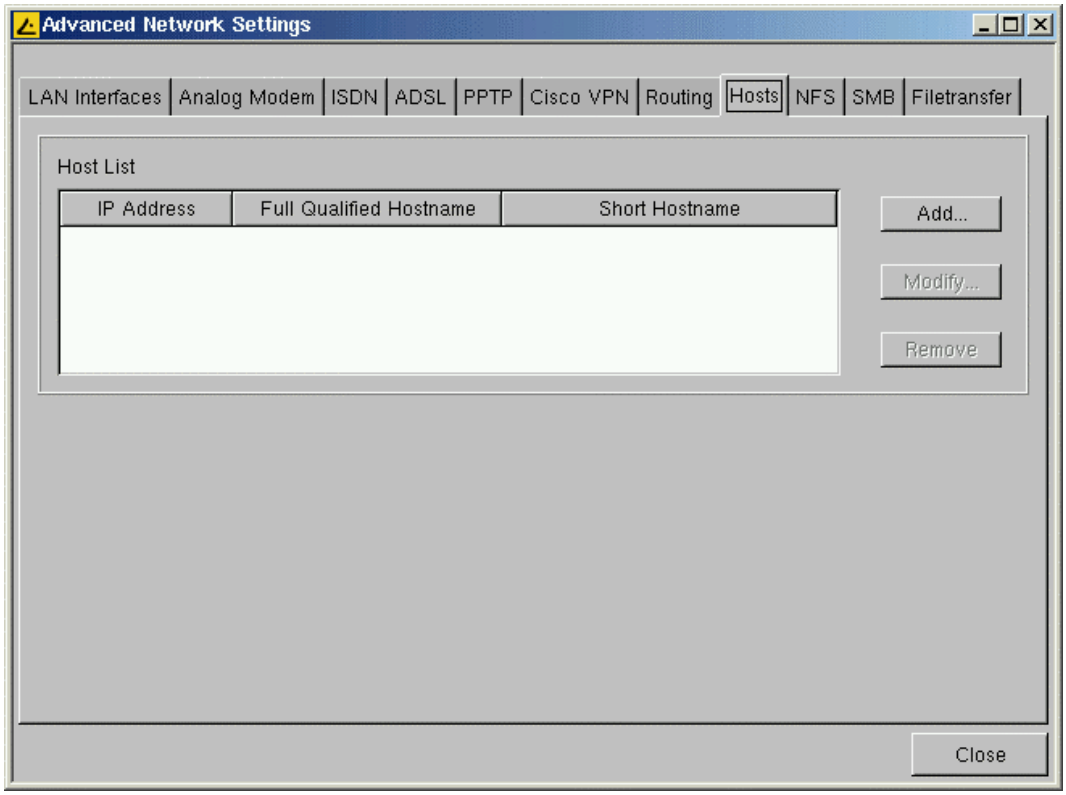


Altogether you can define up to 5 additional routes.

Hosts

If no DNS (Domain Name Service) is used you can provide a list of hosts to translate between their “IP addresses” “Full Qualified Hostname” and “Short Hostname”.

Use this dialog-box to create this ”***Host List***”.



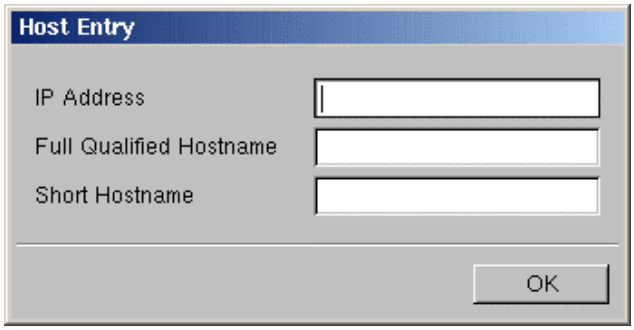
Click “Add…” to open the following “Host Entry” dialog-box:

Host Entry

- ***IP Address***
Enter the IP address of the host you want to add.

- ***Full Qualified Hostname***
Enter the “Full Qualified Hostname” (e.g. <mailserver.igel.de>).

- ***Short Hostname***
Enter the “Short Hostname” (e.g. <mailserver>).



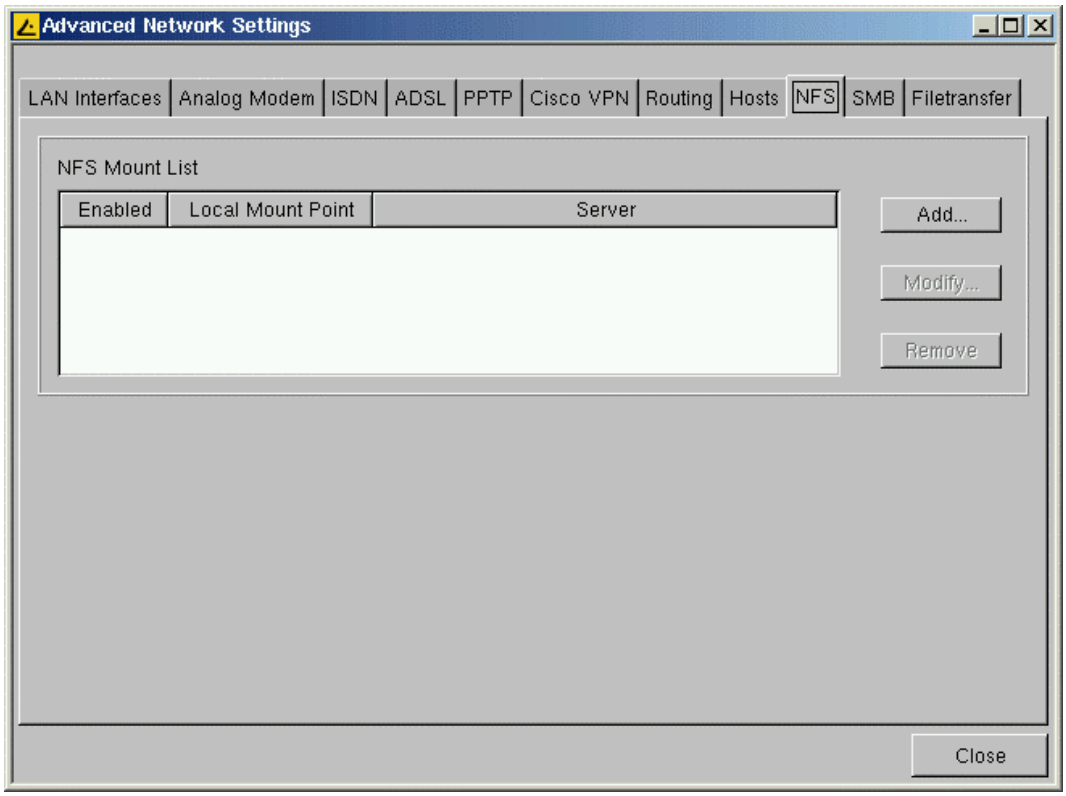
After all entries have been made please confirm this by clicking “***OK***”.
Now the specified host will be added to the “Host List”.

NFS

NFS (Network File System) enables you to share files via the network. The NFS server exports a file system, and the NFS client (your Thin Client) associates this to a mount point of its own file system. So afterwards the exported file system will be a logical part of the Thin Client's file system, while it physically remains on server side.

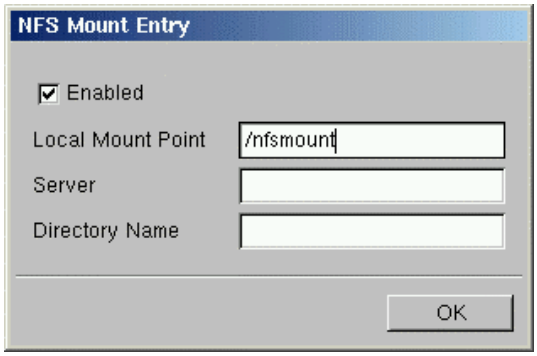
Note: To set up NFS mount, the server has to be configured first. For detailed information about "NFS" refer to the corresponding "man pages" of your server operating system.

Use this dialog-box to define NFS mounts on the Thin Client side:



Click "**Add…**" to open the following "**NFS Mount Entry**" dialog-box:

NFS Mount Entry



- ***Enabled***

By default the "NFS Mount Entry" is enabled and mounted at every system start.
(Disable the entry if the shared file system is not needed permanently.)

- ***Local Mount Point***

Specify the "Local Mount Point" where the share should be mounted in the local file system of the Thin Client.

- ***Server***

Enter the name or the IP address of the NFS server that provides the share.

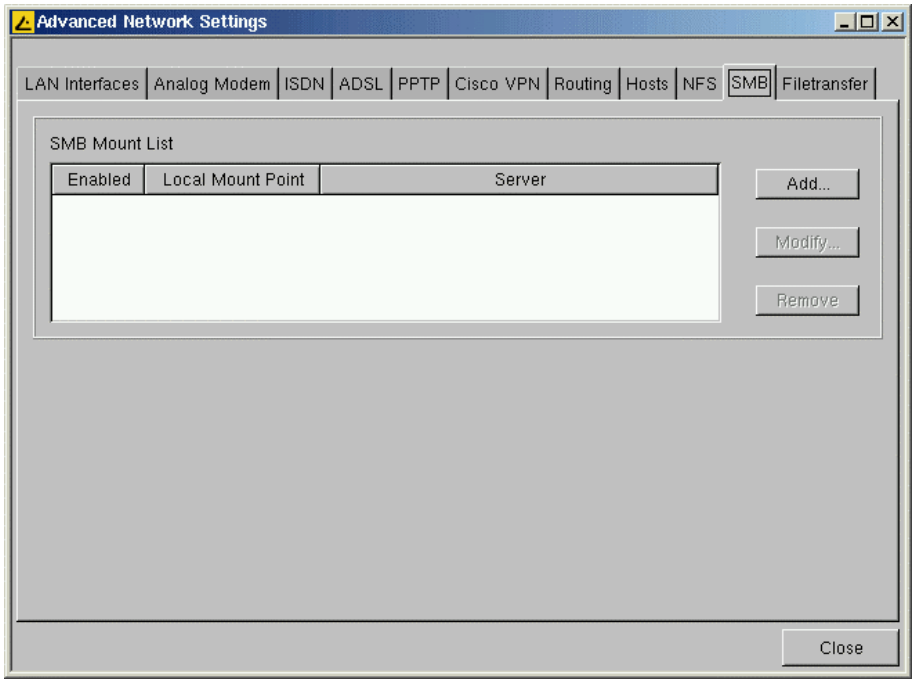
- ***Directory Name***

Enter the directory name as it is exported by the NFS server.

SMB

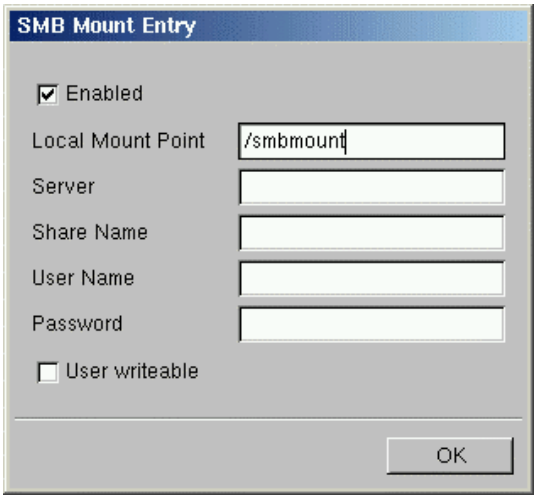
The SMB protocol is very useful because it is used by Microsoft Windows NT, Windows 95/98, Windows 2000 and Window XP to share disks and printers. So as Unix (including Linux) can also handle this protocol with the Samba suite tools, it is possible to share disks and printers with Windows hosts.
So it is possible on the Thin Client to mount SMB shares from Windows or Unix Samba hosts.

Note: The SMB (Server Message Block) protocol is only used for sharing files over the network (no printers). It is necessary that the shares you want to mount be created on the Windows or Unix host first!



Click "**Add…**" to open the following "**SMB Mount Entry**" dialog-box:

SMB Mount Entry



- ***Local Mount Point***

Specify the "Local Mount Point" where the share should be mounted in the local file system of the Thin Client.

- ***Server***

For a Windows host, the NetBIOS name has to be entered here. In the case of a Unix samba host, the host name or IP address is to be used .

- ***Share Name***

Enter the directory name as it is exported by the Windows or Unix samba host.

- ***User Name / Password***

Enter the user name and the password of your account on the Windows or Unix samba host.

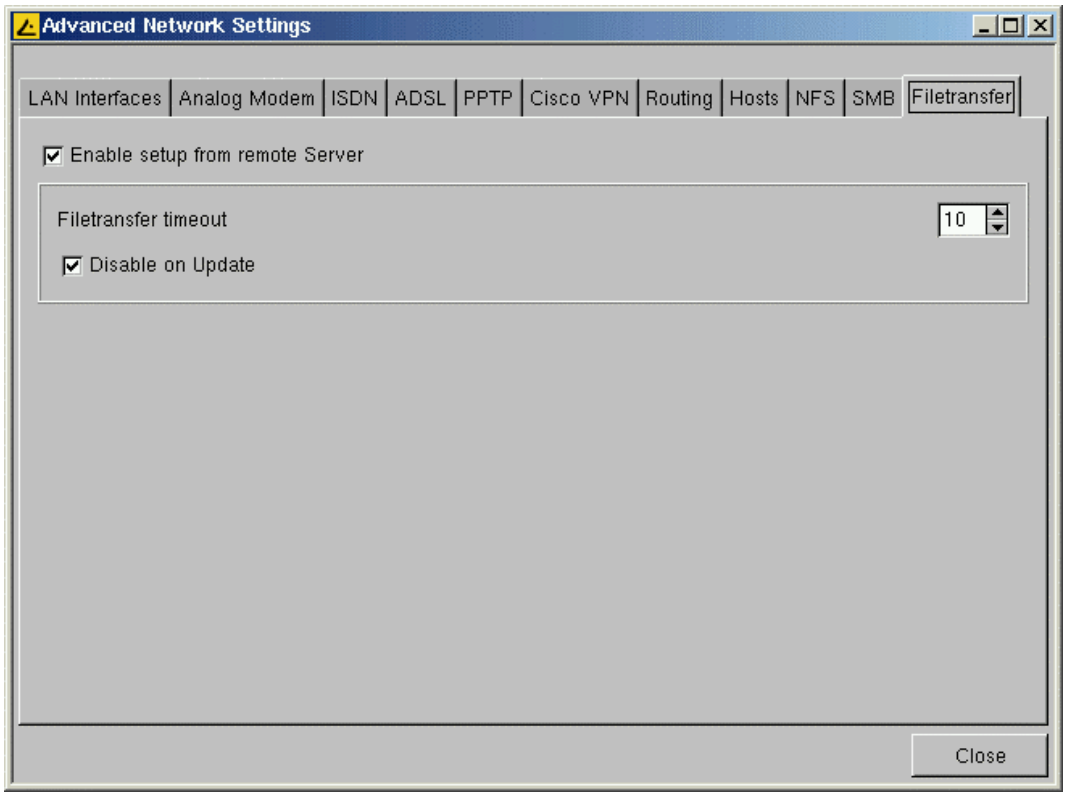
- ***Enabled***

By default the "SMB Mount Entry" is enabled and mounted at every system start.

- ***User writeable***

Activating this also enables the desktop user to write data (otherwise, only "root" is).

Filetransfer



- ***Enable Setup from Remote Server***

In case you use BOOTP+TFTP or DHCP+TFTP to spread the 'setup.ini' or boot scripts, this option enables the transfer from a remote server at boot time.

- ***Filetransfer Timeout***

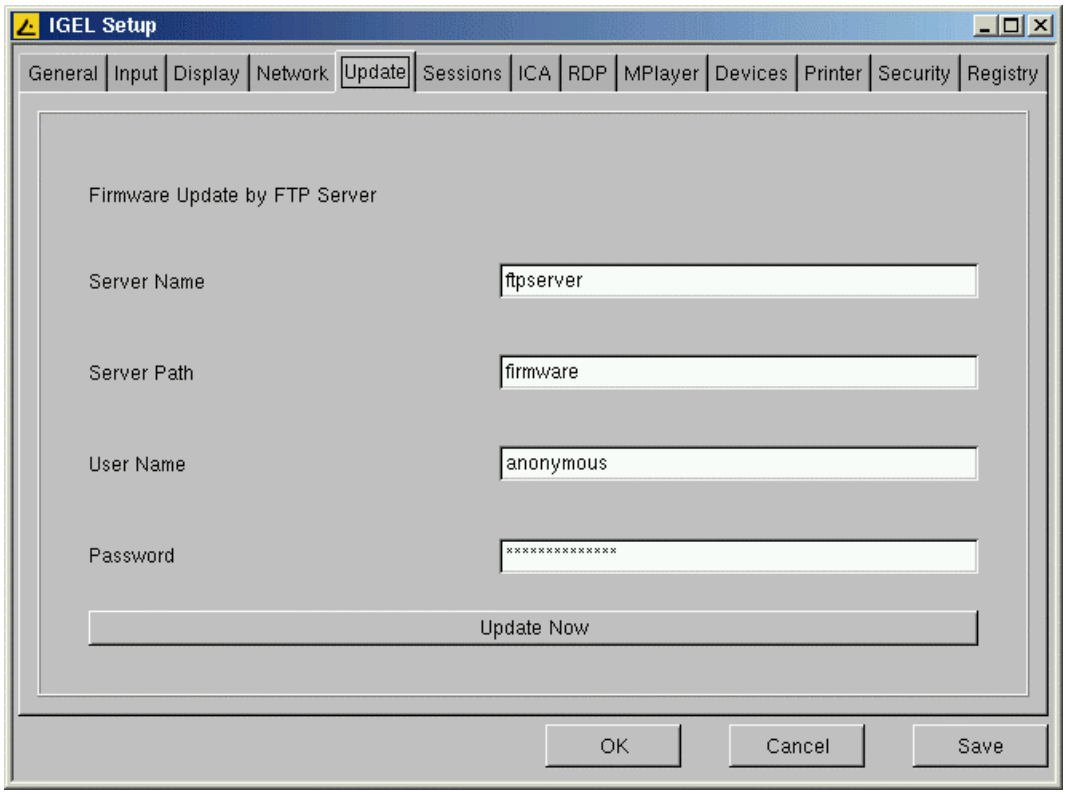
Defines how long the Thin Client should try to get its configuration from the server (in seconds). In case it does not succeed within the chosen time, the local configuration is used

- ***Disable on Update***

This option is important for firmware updates.
Because a reboot takes place during the update process, there might be a serious mix-up of configurations if the Thin Client still got its setup from remote. This could end up in a half updated unit that has to be reconfigured completely or even worse.

Note: Leave the "***Disable on Update"*** option untouched as long as you do not completely understand the interactions of the update and the filetransfer processes.

5.6 Update



The “Update” page shows you a simple dialog for updating the Thin Client’s firmware via FTP.
The common procedure to update your Thin Client(s) is as follows:

1) Download the wanted firmware image from our FTP server ftp://ftp.igel.de/pub/firmware (there are sub-directories named after the models, e.g. “3200_Compact” or “5300_Premium”).
2) Unpack the *.zip file, as this is the usual way we provide updates.
3) Put all files into the designated directory on your local FTP server.
4) Enter the necessary settings (see below for details) and press “Update now”.

Now the update process will advance automatically.

Note: The default values ‘update.igel.de’ etc are exemplary only, you will not be able to update directly from our FTP server!
The update procedure cannot be done via PPP /ISDN connections.

The following information must be provided in order to start the update process:

- ***Server Name***

Enter the name or the IP address of the used FTP server.

- ***Server Path***

Enter the name of the directory you stored the update files in (relatively from the FTP root directory).

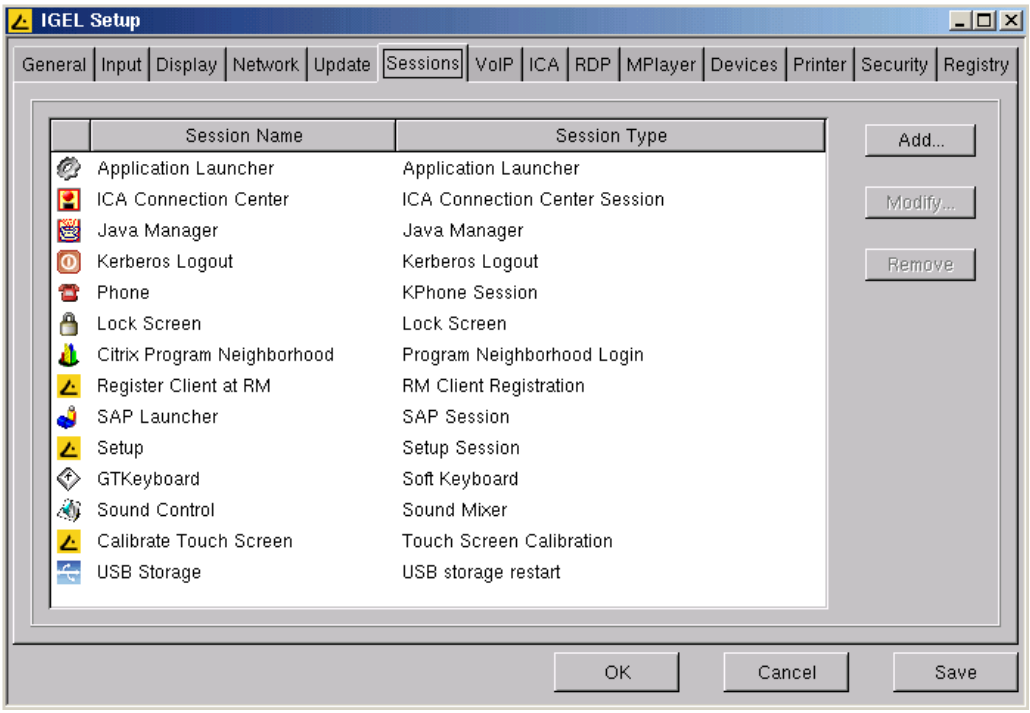
- ***User Name***

Enter the User ID / FTP account name.

- ***Password***

Enter the corresponding password of that user / account.

5.7 Sessions



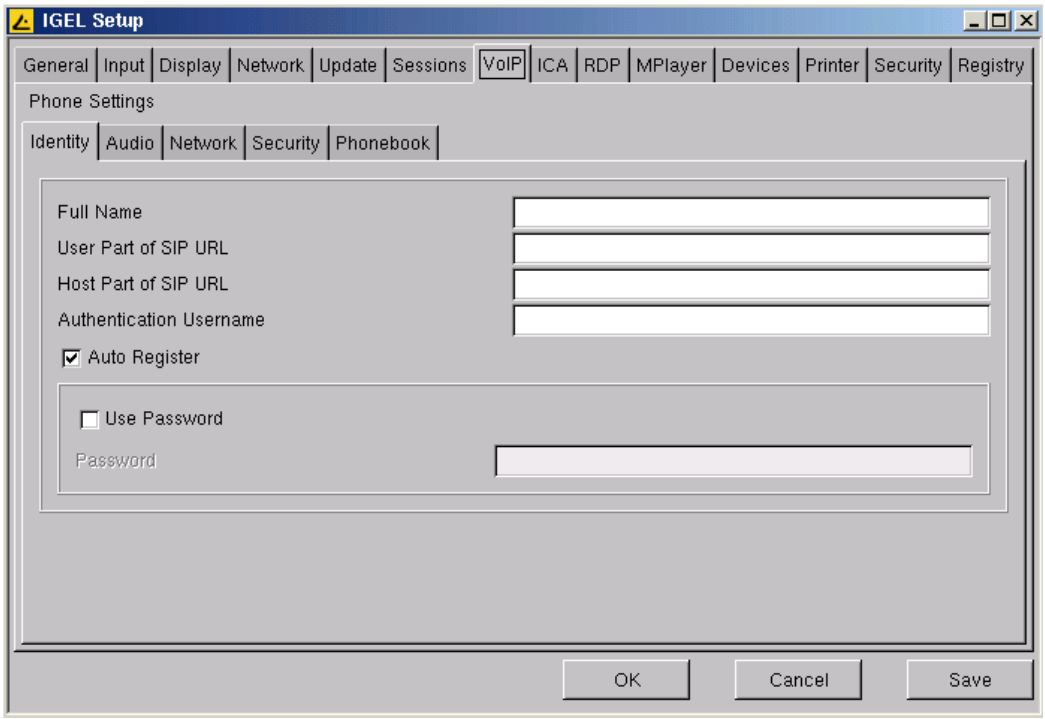
In circumstances when the “Application Launcher” itself is inaccessible, you may manipulate your sessions directly via the setup here.

Refer to Chapter 6 “Application Launcher” for details on how to configure your sessions.

5.8 VoIP

This section describes how to configure Voice over IP telephony (VoIP).

5.8.1 Identity



- ***Full Name***

Describing name of subscriber, this name will be displayed at remote station.

- ***User Part of SIP URL***

First part of SIP URL (before '@').

- ***Host Part of SIP URL***

Second part of SIP URL (after '@').

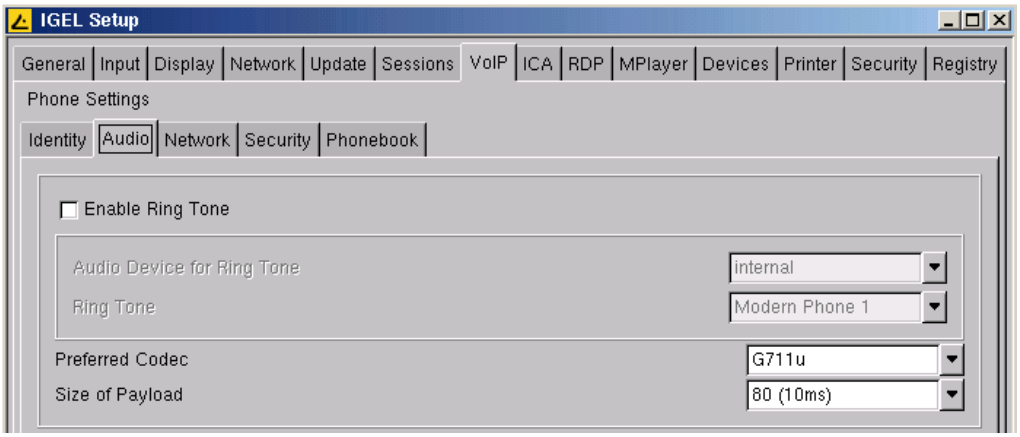
- ***Authentication Username***

Identifier to register at Location Server, usually the user part of SIP URL is used.

- ***Auto Register, Use Password***

At start of application the registration window will be displayed automatically. The password can be filled in automatically as well.

5.8.2 Audio



The section ***Audio*** allows to set coding options and package size for audio data.

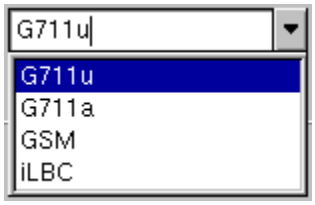
- ***Ringing Tone***

Activate the ringing tone to be notified with an acoustic signal at incoming calls. If not activated only the notification window will pop up.

- ***Preferred Codec***

Choose a procedure for encoding of audio data from the list. The required bandwidth for each of the available codecs is as follows:

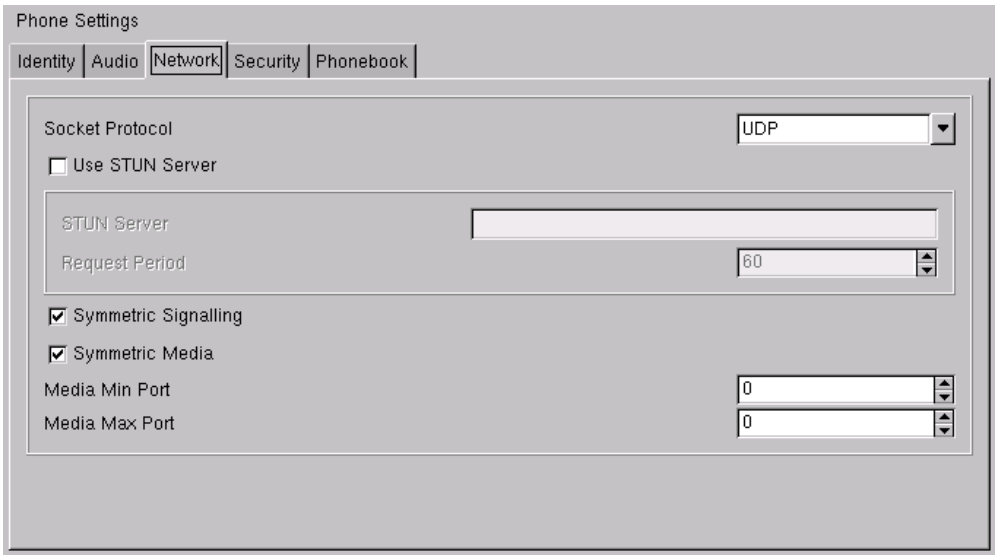
G.711u	:	ca. 80 kBit/s - provides audio quality comparable with ISDN (G.711a for US)
GSM	:	ca. 13 kBit/s - provides audio quality comparable with mobile phones
iLBC	:	ca. 15 kBit/s - high compression with still good quality



- ***Size of Payload***

Choose 80 or 160 milliseconds for size of data packages. A bigger payload decreases the overhead during transmission (and increases the net data rate), but causes higher latencies as well.

5.8.3 Network



- ***Socket Protocol***

Choose a protocol from the list (UDP or TCP).

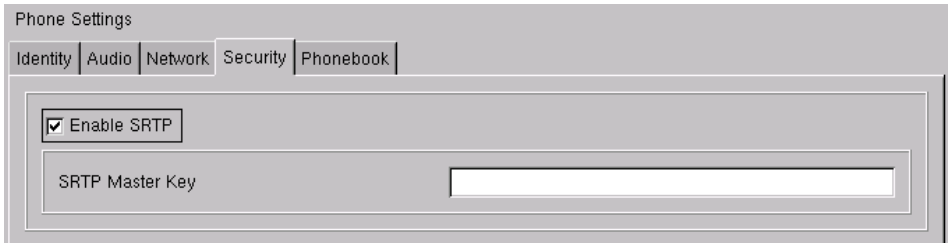
- ***STUN Server***

When using a STUN server activate this option and fill in the address and port number of the server and define the interval for requests as well (in seconds).

- ***Port Usage***

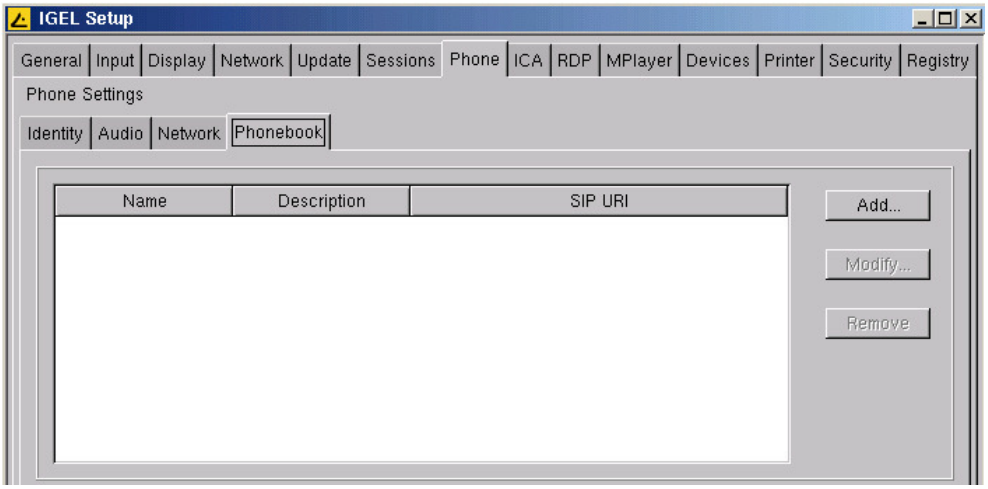
Define if the same port number should be used for incoming and outgoing signaling and media streams and assign a range of port numbers for media channels as well.

5.8.4 Security



On Security page you can activate SRTP (Secure RTP) to encrypt communication via VoIP.

5.8.5 Phonebook



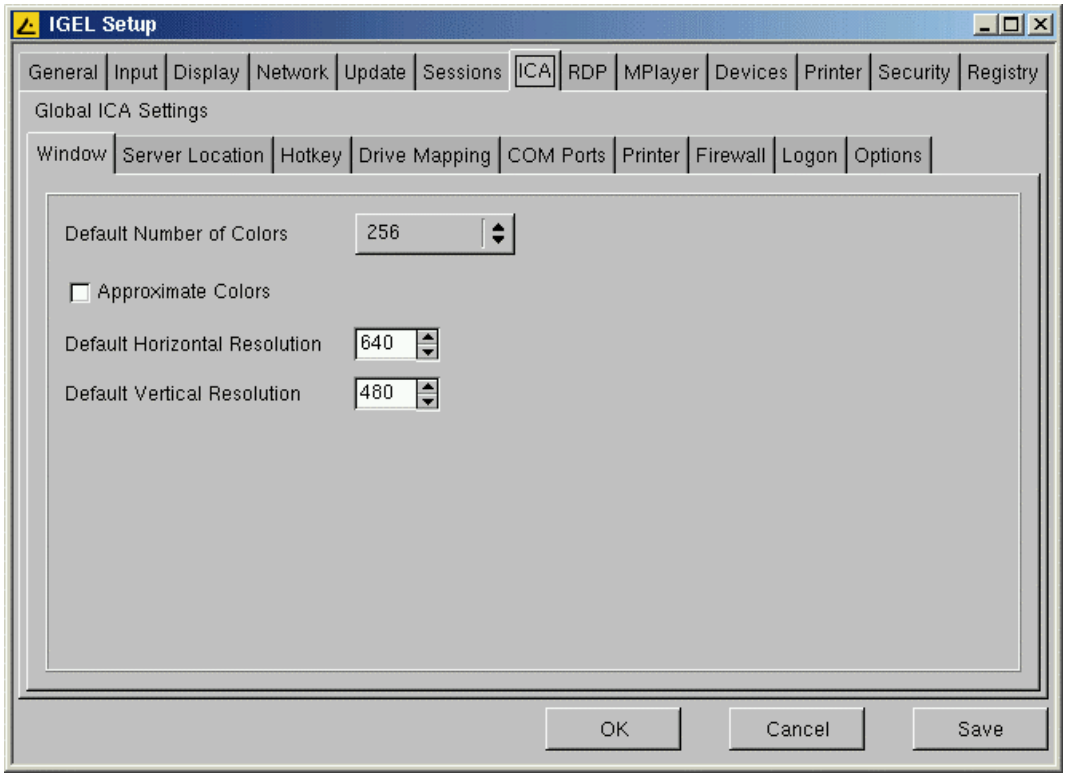
Maintain your contacts in phonebook with related SIP URL.

5.9 ICA (Global ICA Settings)

This section describes how to configure the “Global ICA Settings” that will be valid for all ICA sessions.

Note: These are the default values for all ICA sessions. Most of these properties (especially color depth, resolution and server IP or name) can be altered for each session separately (see Section 6.4.6).

5.9.1 Window



- ***Default Number of Colors***

You are allowed to set the default number of window colors to 256 (default), thousands (High Color) or millions (True Color). The color depth your sessions can run in also depends on your Metaframe server.

- ***Approximate Color***

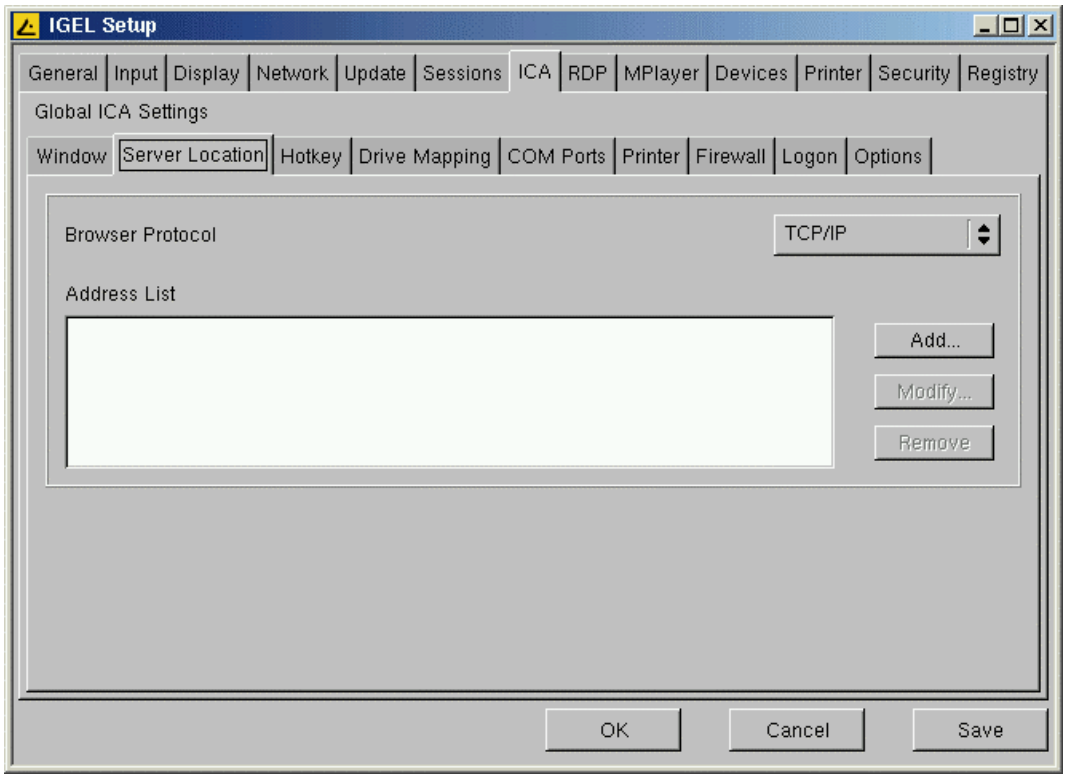
Because of differences in the color palettes used between the ICA Client (and the application it displays) and the “Thin Client” desktop, an annoying flashing can occur when switching context on a pseudo-color display. The ICA Client’s color approximation scheme eliminates this flashing by using colors from the local desktop palette to display the ICA window session.
Enable “Approximate Color” to eliminate color flashing when switching context.

Note: This only applies if the X server is running in 8-bit color mode.

- ***Resolution***

Set the default window size by adjusting the values for the “***Default Horizontal Resolution***” and the “***Default Vertical Resolution***”.

5.9.2 Server Location



- ***Server Location***

The "Server Location" (also called server browsing) provides a method for a network-connected Citrix ICA Client to view a list of all Citrix servers and Published Applications that are accessible on the network and using the chosen browsing protocol.

The default functionality for server location is "Auto-Locate" (broadcast). With the "Auto-Locate" function the ICA Client broadcasts a "Get nearest Citrix server" packet. The address of the first Citrix sever to respond then functions as the master ICA browser.

You can also specify a separate "***Address List***" for each network protocol (***Browsing Protocol***), which could be "***TCP/IP***","***TCP/IP + HTTP***" or "***SSL/TLS + HTTPS***".

- ***TCP/IP***

If your network configuration uses routers or gateways, or to eliminate additional network traffic by the broadcasts, you can set specific server addresses for the Citrix servers from which the list of available servers and/or published applications should be requested.

Note: You can place more than one address in the "Address List" to continue allowing clients to connect and function even if one or several of the servers is/are not available.

- ***TCP/IP + HTTP***

You can also retrieve the information of available Citrix Servers and Published Applications across a firewall by using TCP/IP + HTTP server location.

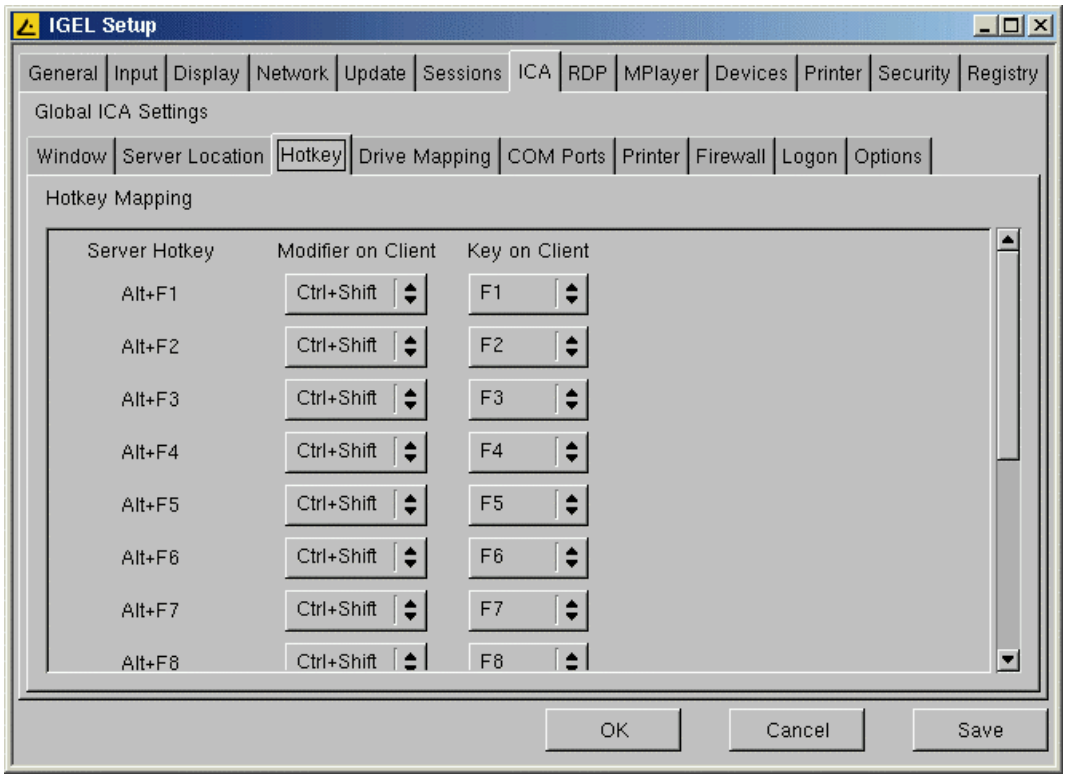
Note: "TCP/IP + HTTP" server location does not support the "Auto-Locate" function.

- ***SSL/TLS + HTTPS***

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption provide server authentication, encryption of data stream and message integrity checks.

Note: If you attempt to make a non-SSL/TLS connection to a SSL/TLS server, you will not be connected and a "connection failed" message will be displayed.

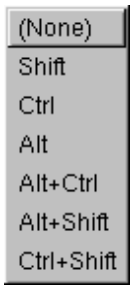
5.9.3 Hotkey



Use the “Hotkey” page to define alternative key combinations for the common hotkeys used within ICA sessions.
For example in MS Windows, the key combination <Alt>+<F4> closes the current window. It also works within ICA sessions.

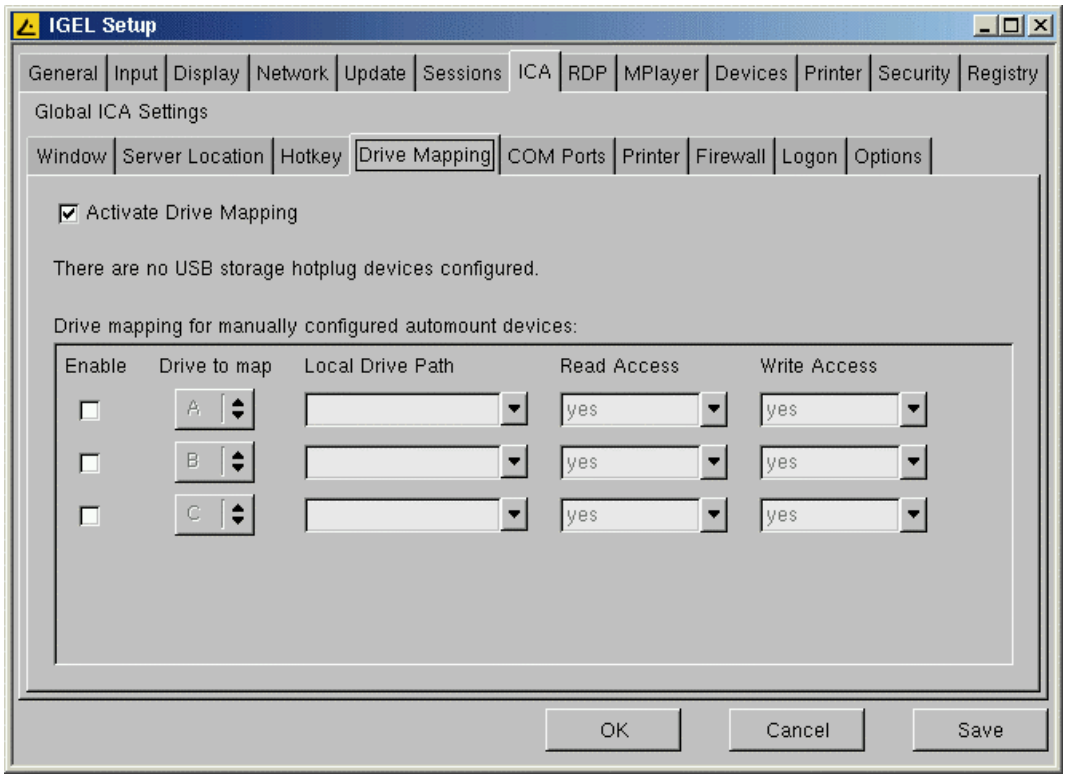
If you choose to disable the “Alternate switching sequence” (see 5.4.2.1), many of these hotkey combinations will be occupied by the X Server (esp. <Alt>+<Fx>). Therefore you will have to use the alternate sequences or map the affected combinations to different ones here to keep them available.
Any <Alt> key combination not used by your X Window manager may still be used as usual within the ICA session.

By default, the key alternatives are mapped to <Ctrl><Shift>+Key, but you can change the definitions by clicking on the drop-down box “Modifier on Client” and/or “Key on Client” of the particular combination.
The two graphics to the right show the possible keys.



Note: If you want to use the PC key combination <Ctrl><Alt><Delete> during the ICA session, use the key combination <Ctrl><Alt><Enter> or <Ctrl><Alt><Return>.

5.9.4 Drive Mapping



"Drive Mapping" makes any directory mounted on your Thin Client (including CD-ROMs and floppy disk drives) available to you during ICA sessions on Citrix servers.
Use this page to specify which folders or drives to map at logon. This applies for all ICA connection sessions.

- ***Activate Drive Mapping***

This option allows you to temporarily enable/disable the drive mapping.
This gives you the advantage of not losing your stored settings, but being able to switch them on/off.

Note: Local devices that are to be used for drive mapping first have to be configured as device! (See 5.12.)

How to configure a "***Drive Mapping***":

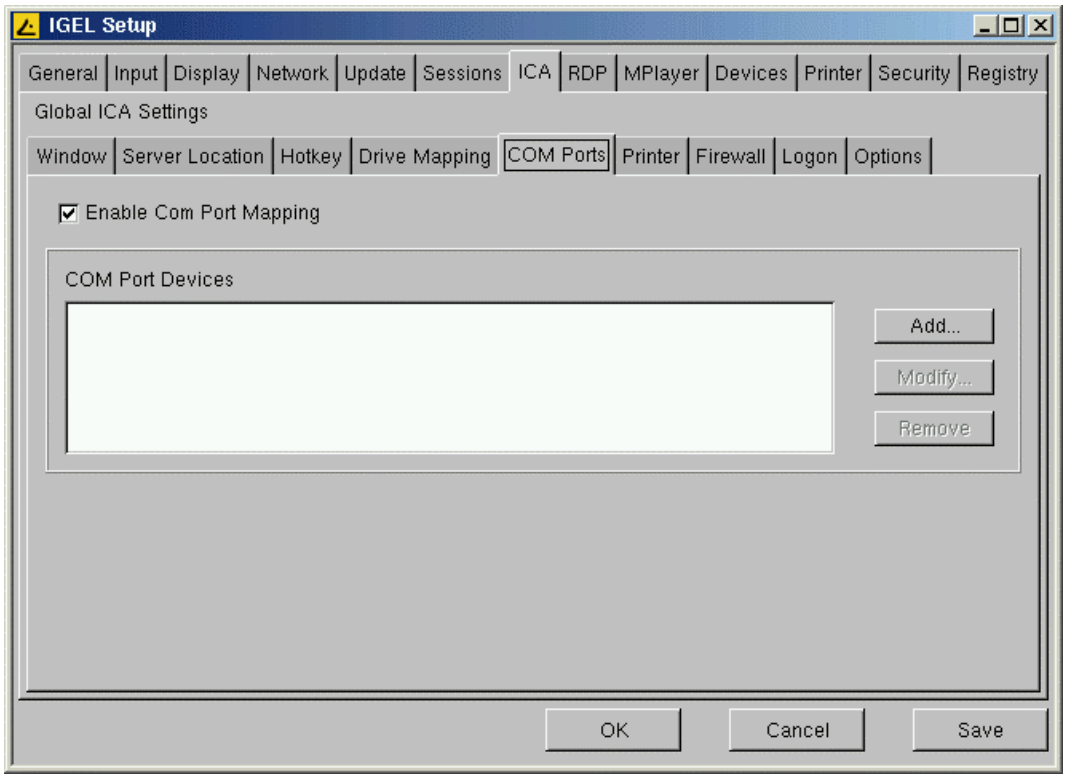
Enable one of the three mappings to activate the corresponding entry fields.
Then click on the corresponding button in the "***Drive to map***" column.
Now select the drive letter under which the local device or folder should be mapped.
In case the drive letter you selected is not available on the Citrix server anymore, the specified directory or local drive will be mapped to the next free drive letter at logon.

In the "***Local Drive Path***" field, set the path name of the local directory the mapping should point to.
When mapping a locally attached device, use the pre-defined path names as offered by the drop-down box. These are the directories the devices are mounted to by default at boot up.
(e.g. /autofs/floppy for a built-in floppy disk drive)

Finally specify the access rights for the mapping.
You can choose to grant "***Read Access***", "***Write access***" or to "***Ask User***" for each mapping separately.
("***Ask User***" will prompt for read/write access on first access per ICA session.)

Note: The same drive mappings and access settings will apply to all ICA connections.

5.9.5 COM Ports

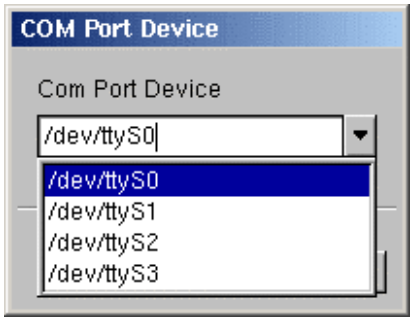


You can perform bi-directional mapping between serial devices that are attached to the Thin Client (e.g. scanners, serial printers) and the Citrix Server's COM ports.
This enables programs running on the server to exchange data with the local devices.

- ***COM Port Devices***

Select the COM port your device is attached to from this drop-down box:
/dev/ttyS0 stands for the local COM1 and /dev/ttyS1 stands for the local COM2. ttyS3 and ttyS4 are for potential add-on cards plugged in the PCI/ISA slot, e.g. internal modem (series 400 and 500 only).

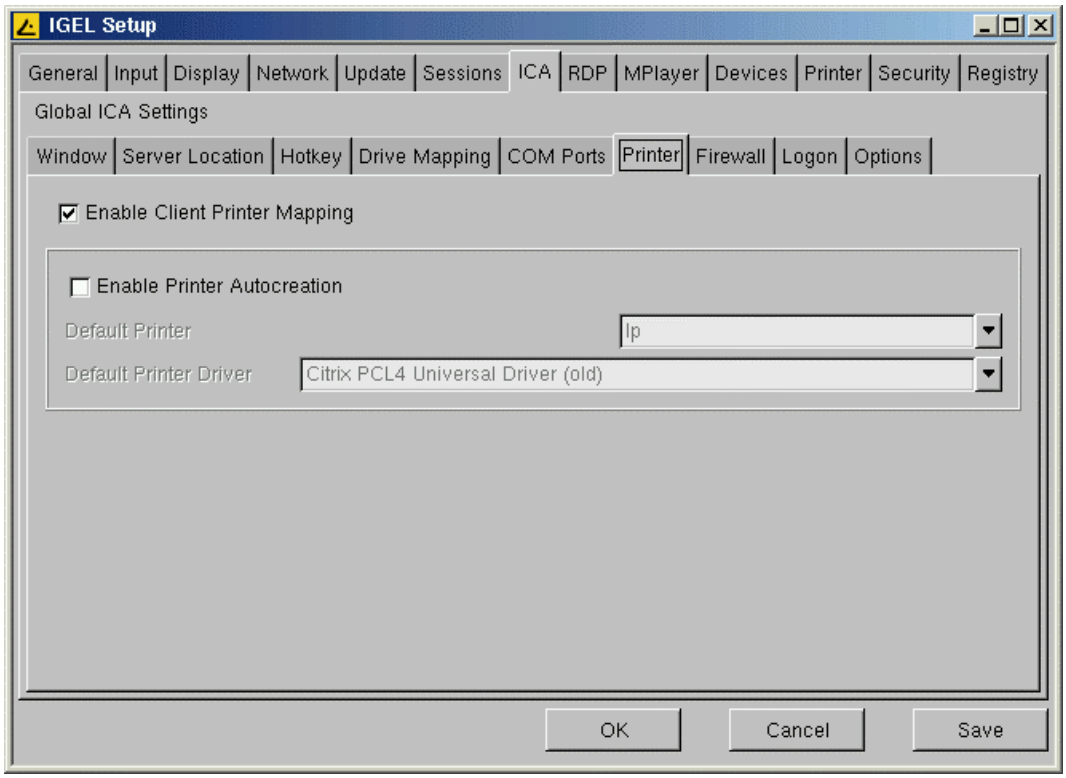
Your selection will be mapped to the virtual COM1, a second one will become virtual COM2 and so on.



Note: The behavior details of the local COM port have to be configured in "***Devices***" (see 5.12). The configuration and its assignment on server side has to be done within Metaframe.

5.9.6 Printer

In this tab, you configure the printer for ICA sessions.
(For general printer configuration, see Section 5.13)



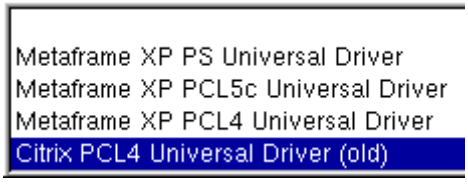
- ***Enable Client Printer Mapping***

This feature makes the locally attached printer of the Thin Client available within your ICA sessions (assuming that it's not disabled from server side).

Because the Thin Client will only spool the incoming print jobs, you have to install the printer on the server. This is done in the familiar way ('Start' –> 'Settings' –> 'Printer' and so on…).
The only thing you have to take care of is that you have to be logged in from the terminal the printer is connected to as Administrator.

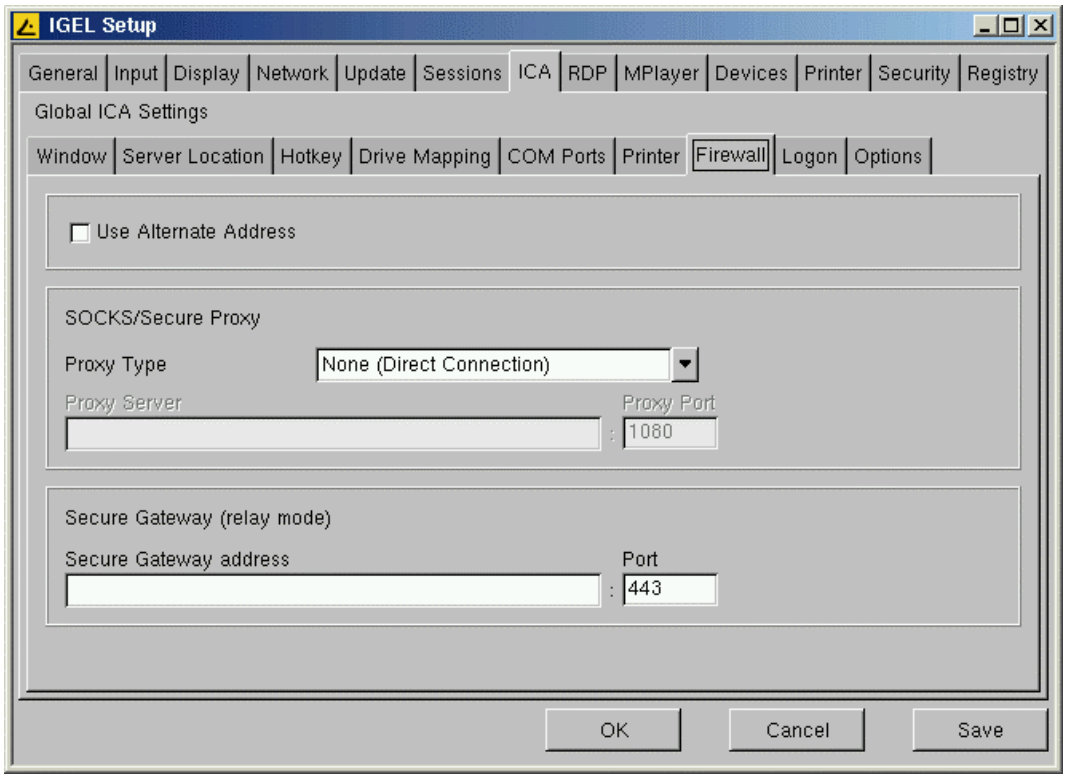
- ***Enable Printer Autocreation***

Metaframe XP on Windows Servers provides the feature to automatically create the printers when connecting to the server.
To use this function, the Thin Client has to provide information about the chosen local printer (see 5.13) and the Microsoft Windows printer driver name for it.
The default value for the driver name here is "***Citrix PCL4 Universal Driver***", because that works fine for most printers and is usually installed on the Metaframe Server anyway.



Note: Verify the configuration of the attached printer itself first (see 5.13)!

5.9.7 Firewall



This "***Firewall***" page allows you to configure ICA connections through a firewall or a SOCKS proxy server. (Firewalls and SOCKS proxy servers are used on networks to improve security.)

- ***Use Alternate Address***

If you are using ICA sessions to connect to a specific Citrix server behind a firewall, you have to activate this option. The Citrix server (usually) has a different IP in the local network than from the outside world.
(For details on server configuration, look up the "***altaddr***" command in your Metaframe admin manual.)

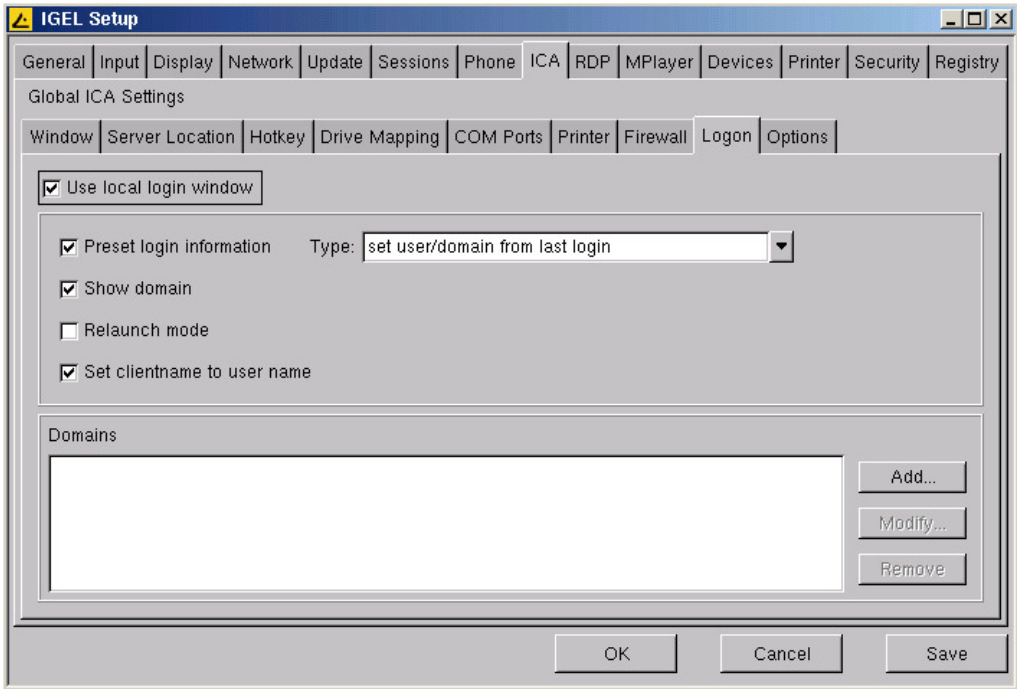
Note: After enabling the alternate address, add the server in the "***Address List***" in the "***Server Location***" box of the "***Global ICA Settings***" (see 5.9.2).

- ***Connect via SOCKS or Secure Proxy Server***

You can configure the ICA sessions to connect to a Citrix server through a SOCKS proxy server or a Citrix Secure Gateway (in relay mode).

Note: To make the "***Secure Gateway***" field accessible, the "***Browser Protocol***" in the "***Server Location***" tab (see 5.9.2) has to be set to "***SSL/TLS + HTTPS***"

5.9.8 Logon



In some environments you may encounter problems with load balancing.
Use this local login module in order to avoid this.
(User credentials will already have been transmitted when connecting the Metaframe master browser.)

- ***Set login information***

After you have logged in successfully once, you only have to re-enter the password to log in if this box is enabled.

- ***Show Domain***

Check this box

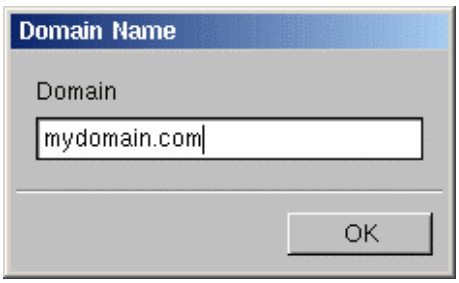
- ***Relaunch Mode***

As long as this feature is enabled, the login module will automatically restart after it was exited.

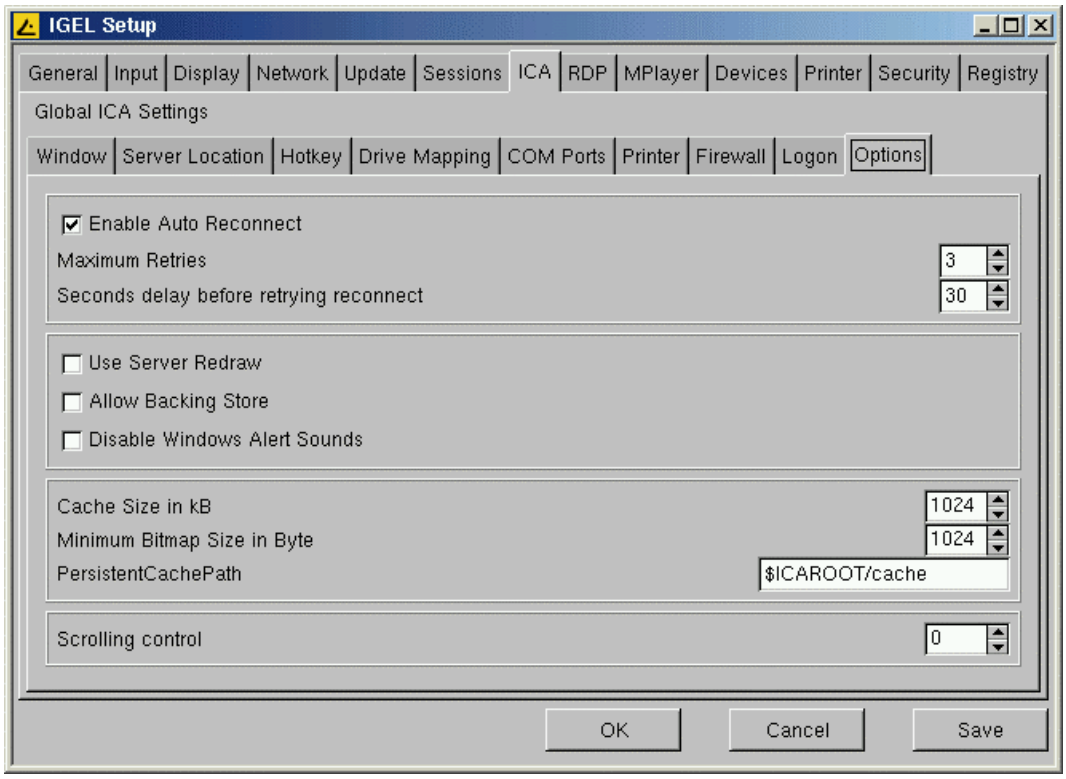
- ***Set Clientname to User Name***

Take over the client's name as ICA user name.

Domains
Add the domain(s) to be available. Multiple domains entered here will be available in the login module's domain drop box.



5.9.9 Options



This page allows you to set additional options to tweak the general behavior and performance.

- ***Use Server Redraw***

This option enables the Citrix server to control the screen redraws.

- ***Allow Backing Store***

Press this button to use the X server backing store functionality for hidden desktop windows.

- ***Disable Window Alert Sounds***

Use this option to disable Windows Alert Sounds.

- ***Caching***

Here you can manipulate the settings for the Bitmap Cache.
This may considerably improve the performance of your ICA session(s) if you are working with pictures that are displayed over and over again.
Set the maximum size of local system memory (in kilobytes) to be used for caching and the minimum size of bitmaps to be cached and the directory the files should be stored locally.

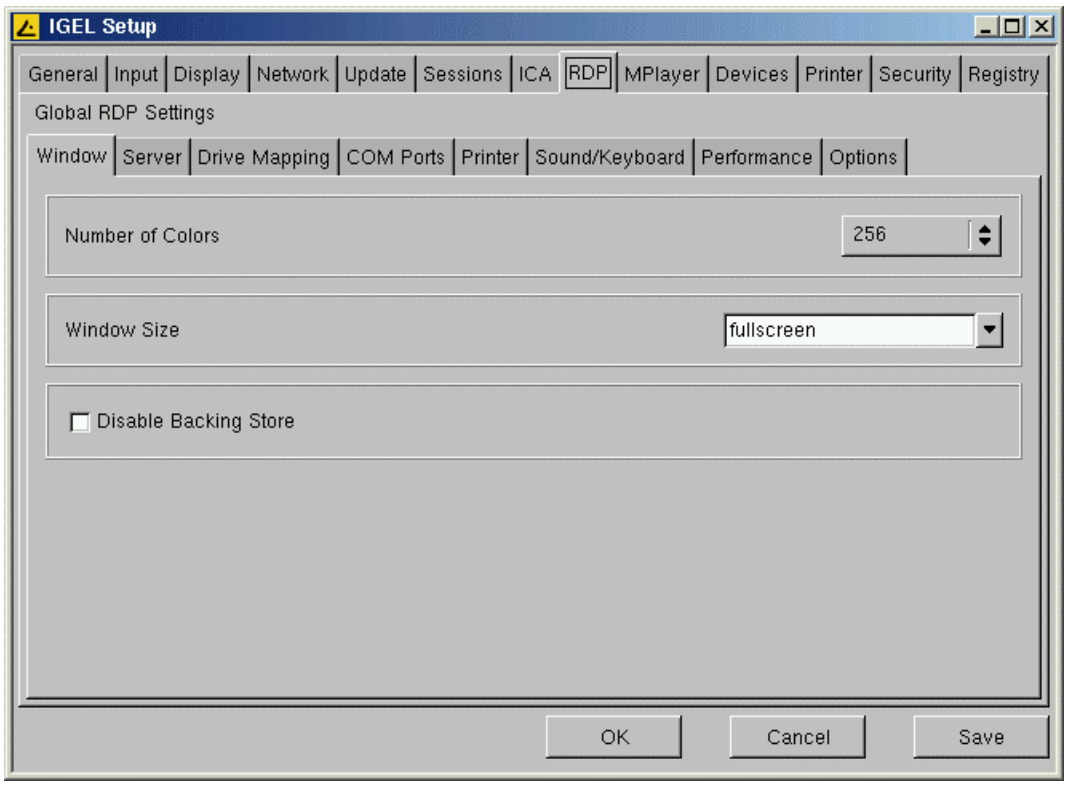
Note: A too high setting might leave the Thin Client with too low memory for its system and other applications! In doubt, you have the possibility of adding RAM to your Thin Client.

- ***Scrolling Control***

Depending on the speed of your network or answering time of your server, you may encounter the effect (e.g. in EXCEL) that there is a delay between releasing the mouse button from a scroll bar and stopping scrolling locally.
Setting a value of 100 or above here will probably eliminate this.

5.10 RDP (Global RDP Settings)

5.10.1 Window

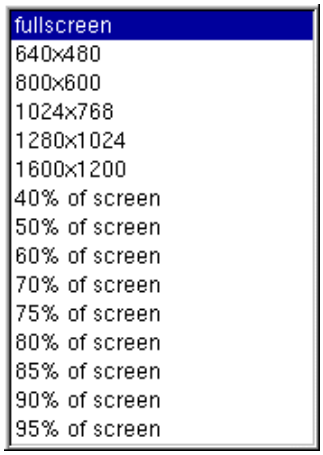


- ***Number of Colors***

This default applies to all your RDP sessions as long as you do not have any or a differing color depth. Set the default number of colors to 256 (default), thousands (High Color) or millions (True Color).

- ***Window Size***

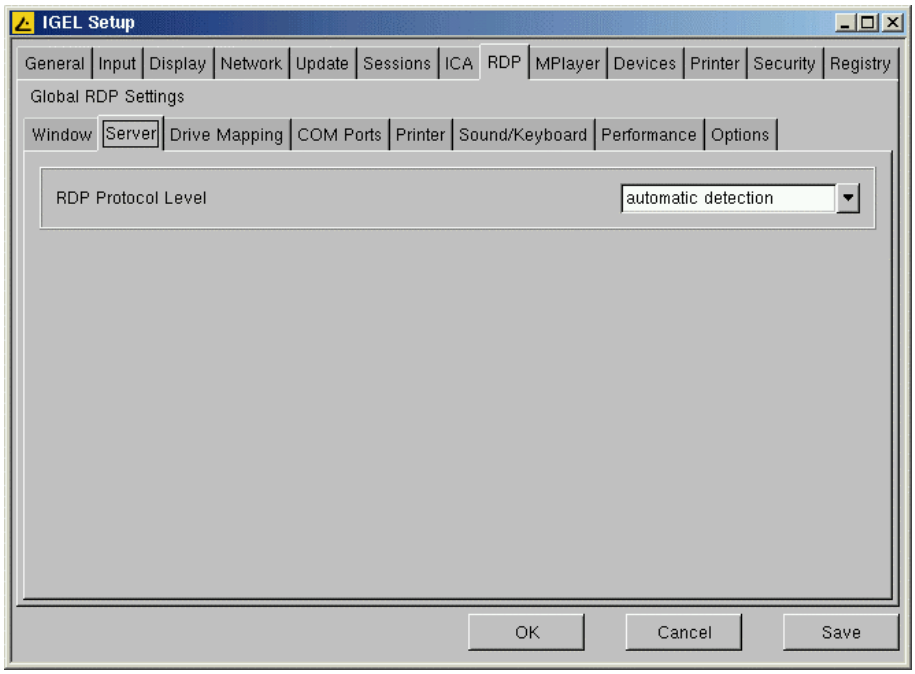
You can choose between a full screened session, a specific static resolution or a percentage between 40% and 95%.



- ***Disable Backing Store***

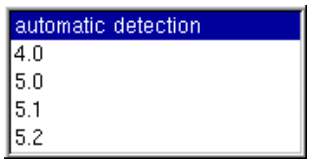
This option allows you to choose the Backing Store mechanism for hidden session-windows.

5.10.2 Server

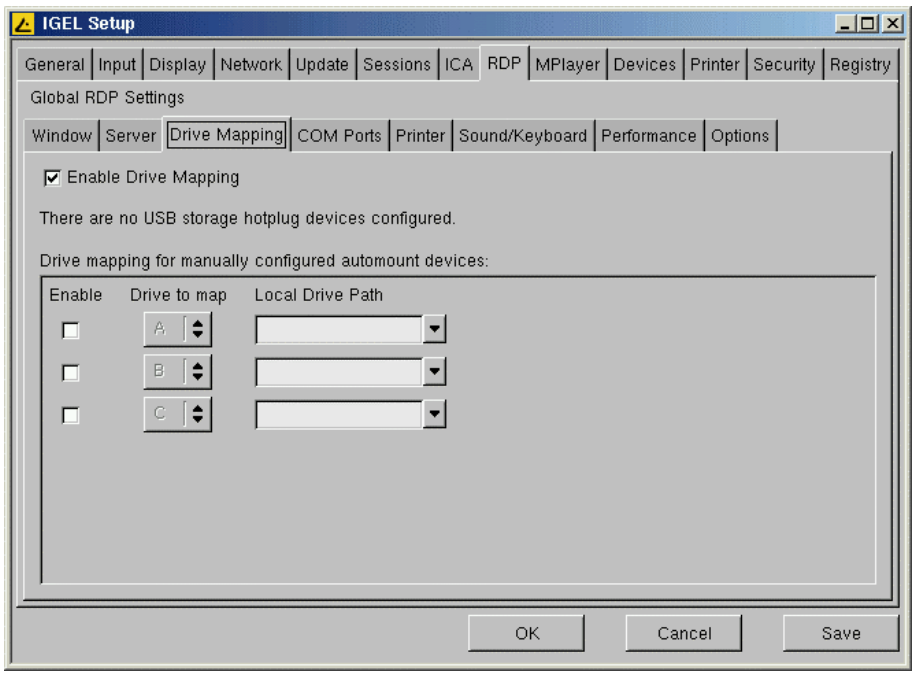


- ***RDP Protocol Level***

Set the protocol level according to the server you are going to connect to.

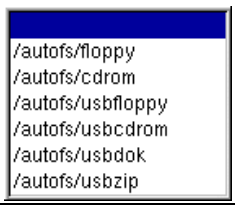


5.10.3 Drive Mapping



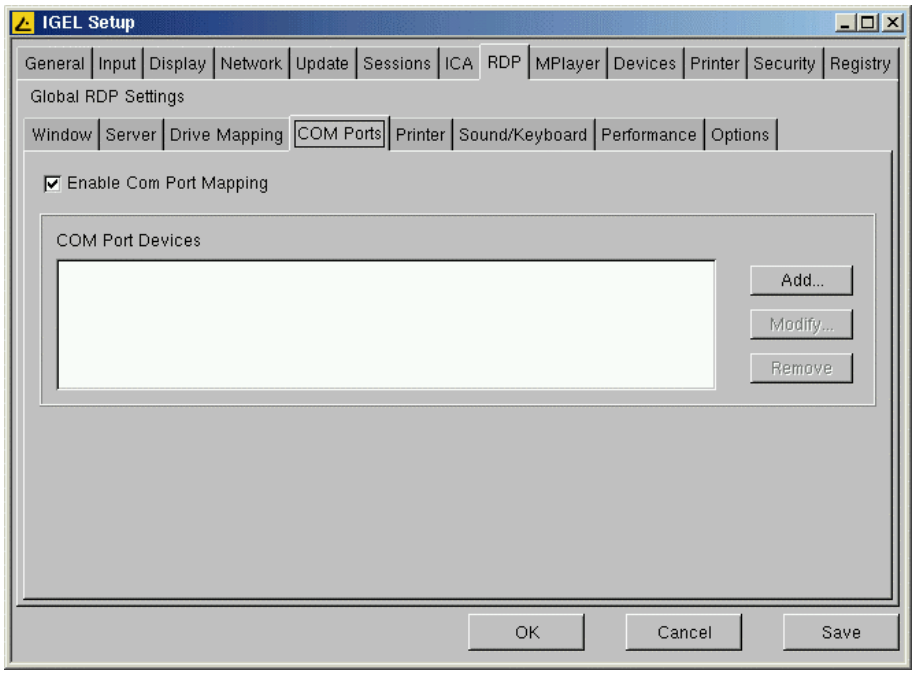
If you have mass storage devices attached, make them available to the user by mapping them here.

Check the “Enable” box, select the drive letter to be used and finally choose the device to map (see picture to the right).



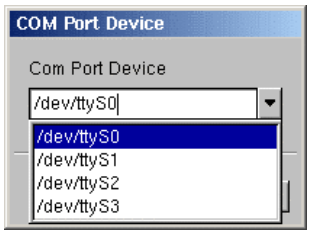
Note: Refer to Chapter 5.12 on how to set up the device(s) to map.

5.10.4 COM Ports

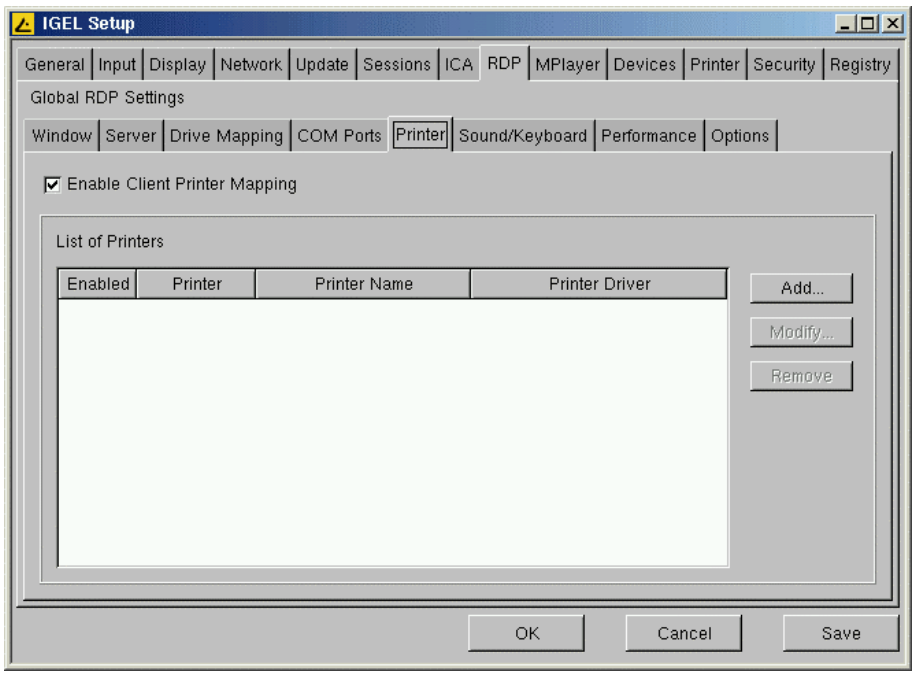


As well as locally attached mass storage devices, you may also map the local COM ports of the Thin Client into the RDP session.

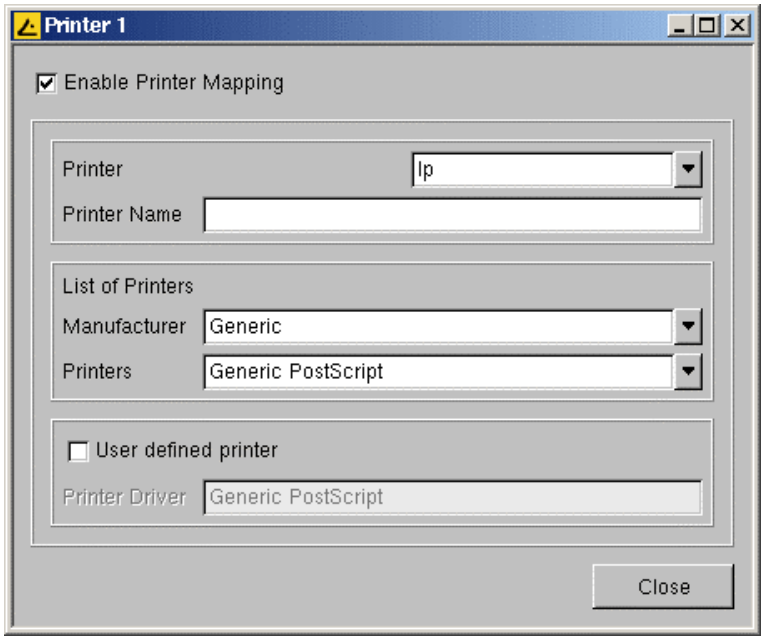
Enable COM port mapping and add the wanted port.
/dev/ttyS0 stands for COM1 and /dev/ttyS1 for COM2.
In the case your unit has an add-on multiport PCI card, you may have more than 2 ports.



5.10.5 Printer



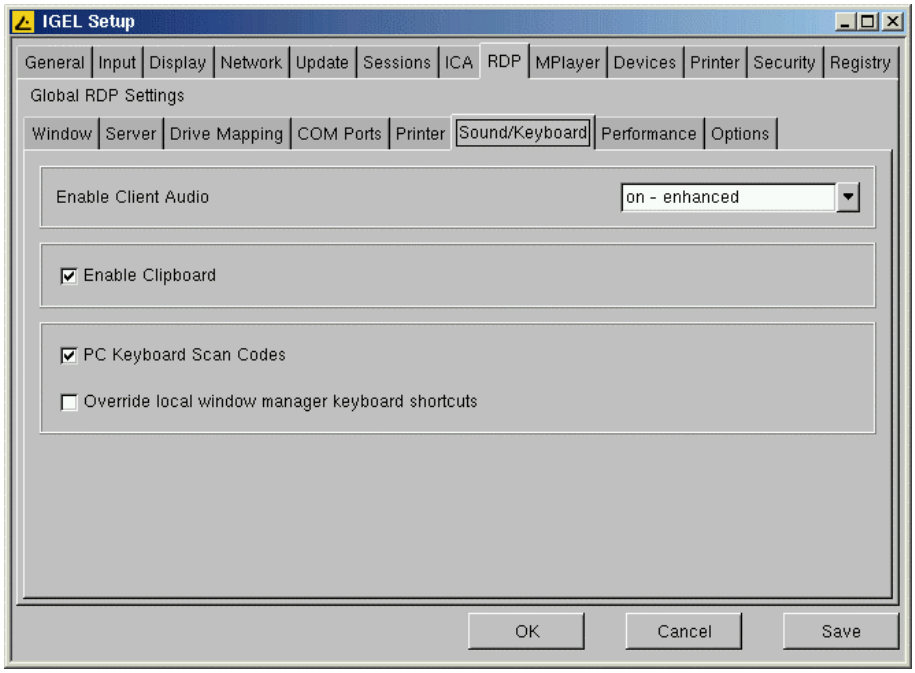
Set up the printer to be used within RDP session here. (Please see next page for details.)



Choose the printer queue (***lp+lp_lp***, ***lp_com1***, ***lp_com2*** or ***lp_usb***) and set the printer's name.

List of Printers
Here you can select your printer's brand and model.
This sets the proper Windows driver name for the printer to be mapped.
(The most common printers are available.)
Alternatively or in the rare case your printer is not in the list, define the printer driver manually.

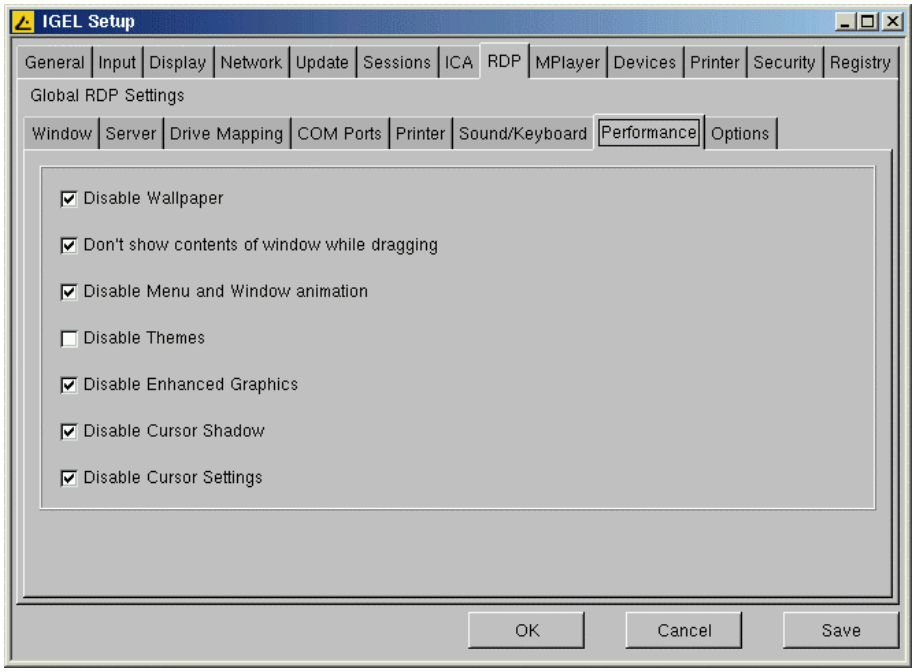
5.10.6 Sound/Keyboard



Set the sound quality level you want to use (the higher the quality, the higher the network traffic caused!)

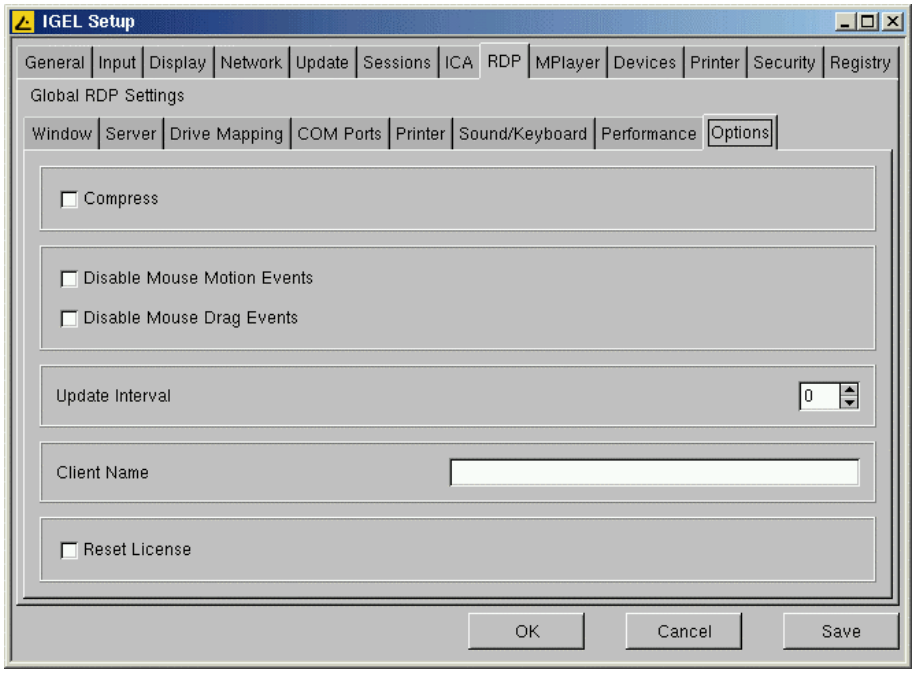
Also, you decide here how to deal with keyboard strokes.

5.10.7 Performance



In case of performance problems, disable some not necessarily needed graphical features.

5.10.8 Options



- ***Compress***

In low bandwidth environments, it's recommended to use compression in order to lower network traffic. (Be aware that this consumes CPU power.)

- ***Disable Mouse Motion Events*** and ***Disable Mouse Drag Events***

Tell the client not to send "unnecessary" mouse moves to save performance.

- ***Client Name***

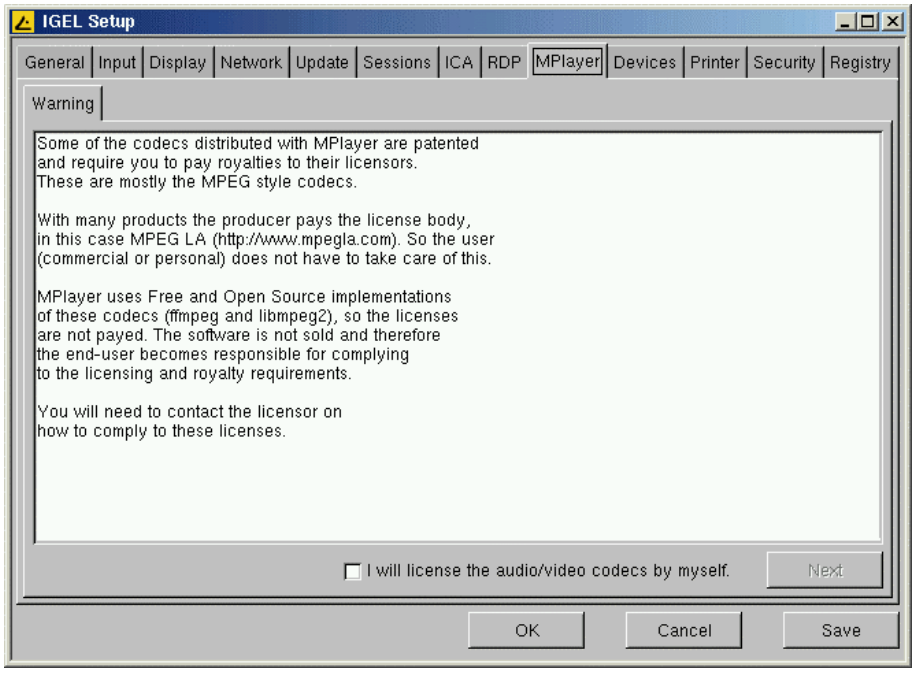
Specify a client name for TS identification (by default the machine's hostname is set).

- ***Reset License***

In case you need to remove the MS license from the unit, activate this checkbox and reboot.

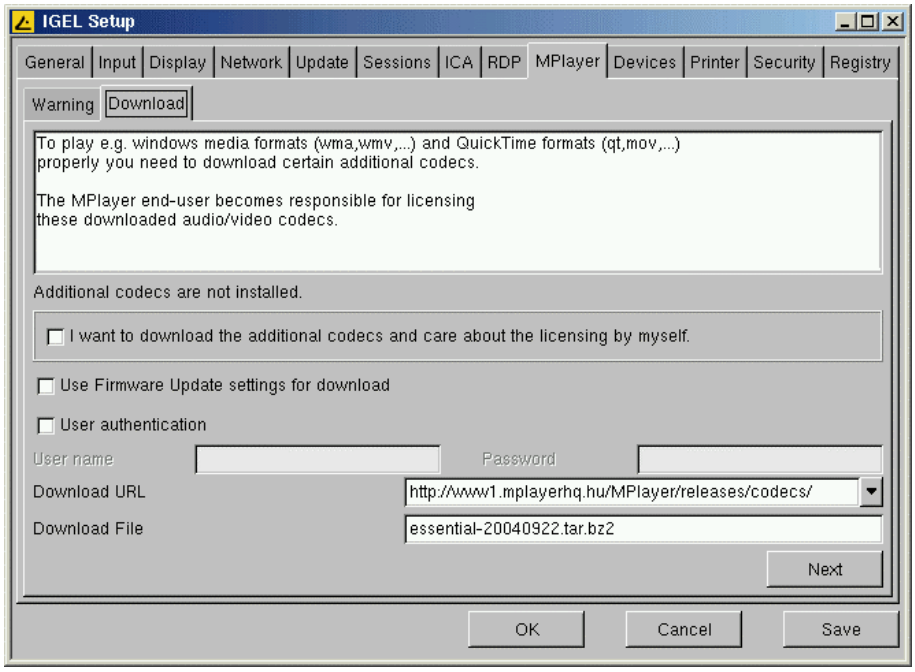
5.11 MPlayer

5.11.1 License



Before using the local Mplayer application, please make yourself familiar with the codec license disclaimer (as shown above)!
Without proper licensing, it's illegal to use the MPlayer application!

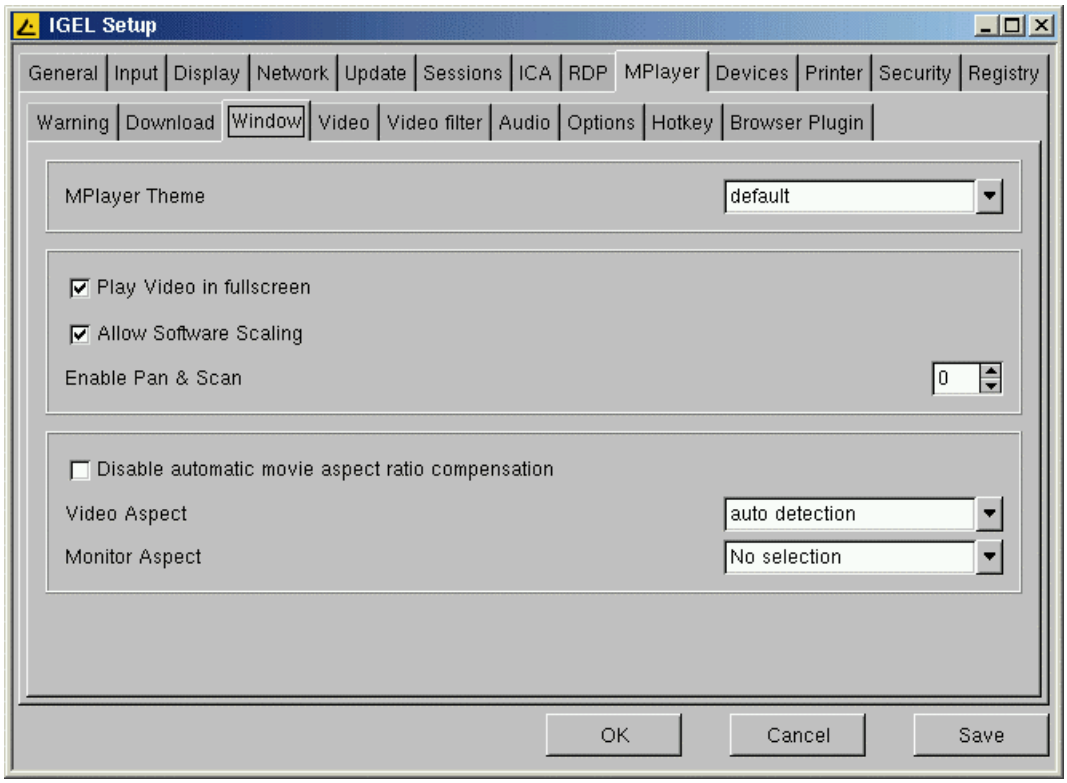
5.11.2 Codecs



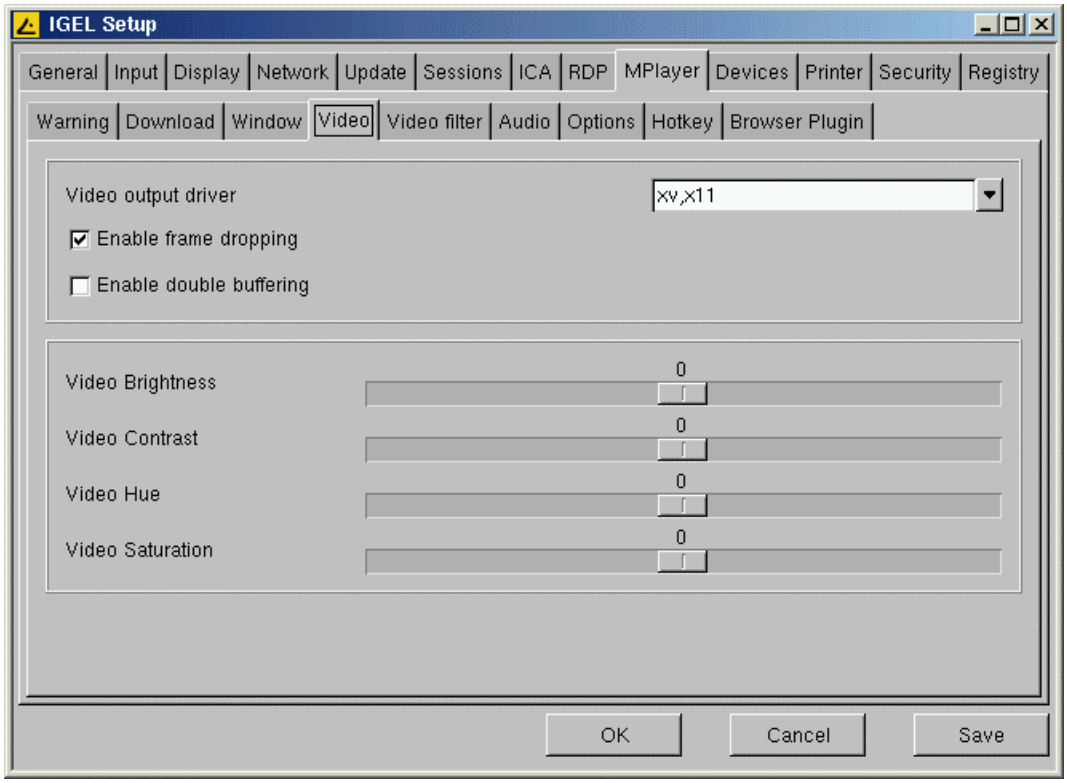
To install further codecs, you need to download them directly from the vendor's or his distributor's site.
In order to avoid multiple downloads from the Internet, you may locate the codecs on your local ftp server and use the client's firmware update mechanism to spread them (see Chapter 5.6 for update settings).

5.11.3 Appearance & Video Tuning

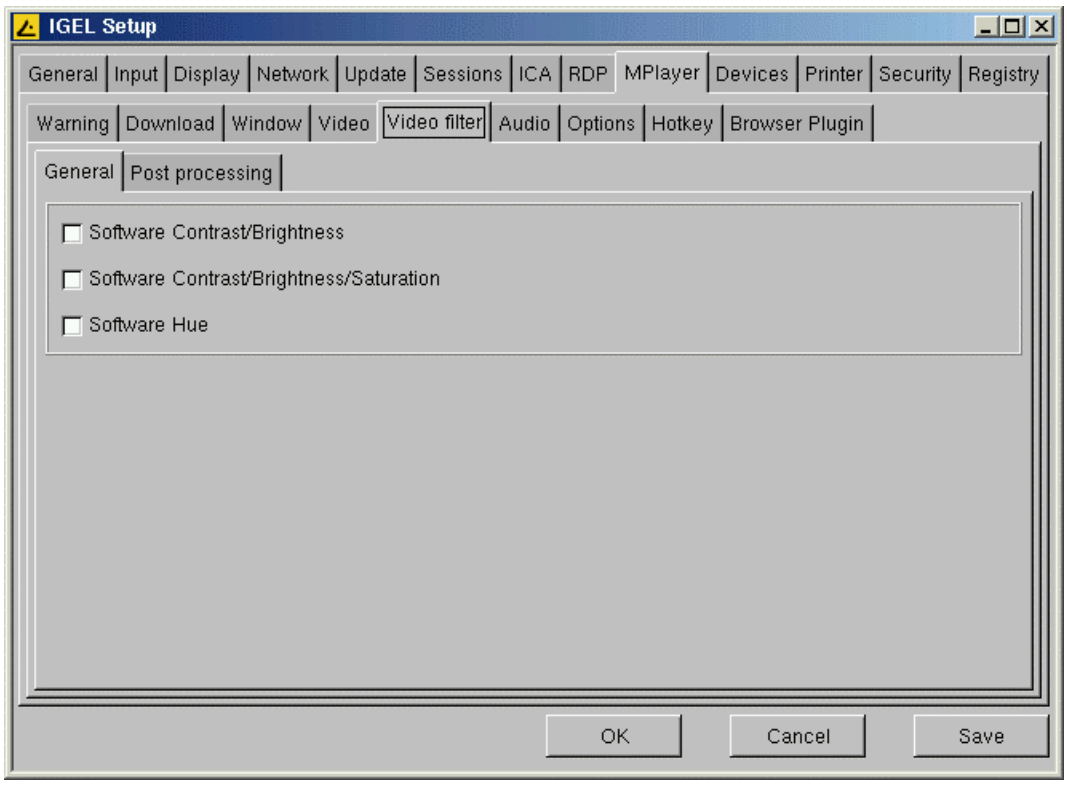
Because of the diversity of settings, not every single one will be explicitly described here. (Most of them will only be used in rare cases anyway.)



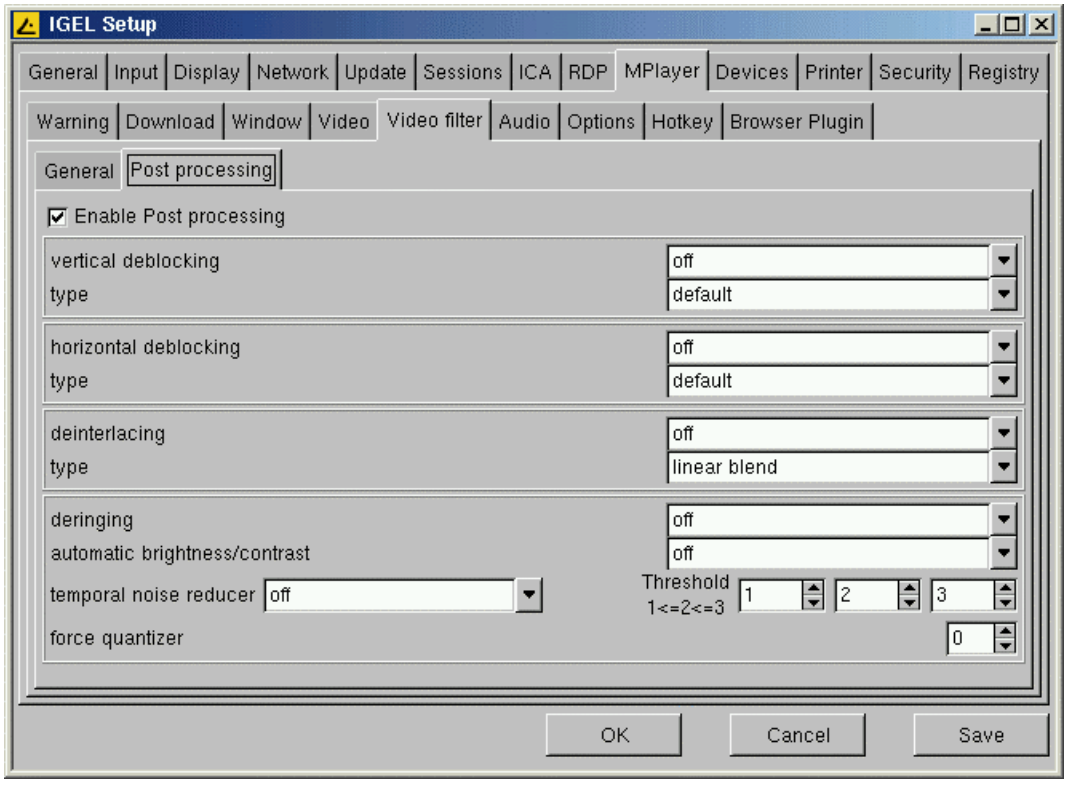
Set up the look of the Mplayer window in this tab.



For video fine-tuning use the controllers here.

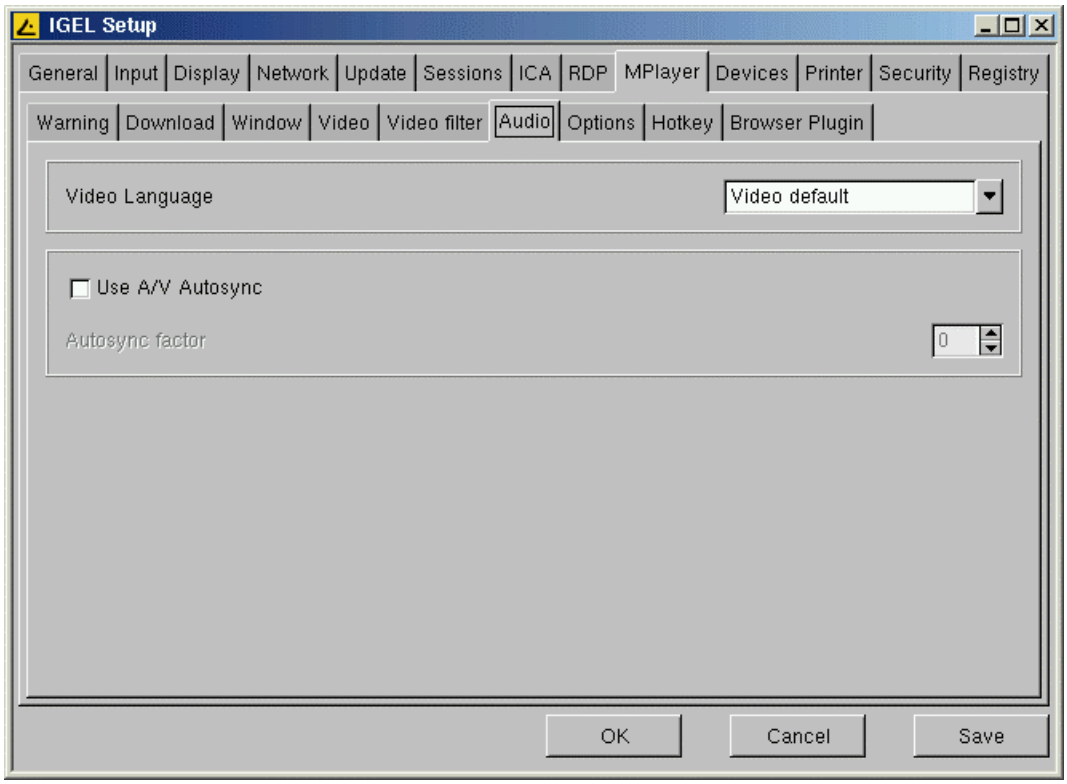


Switch between hardware and software handling here.



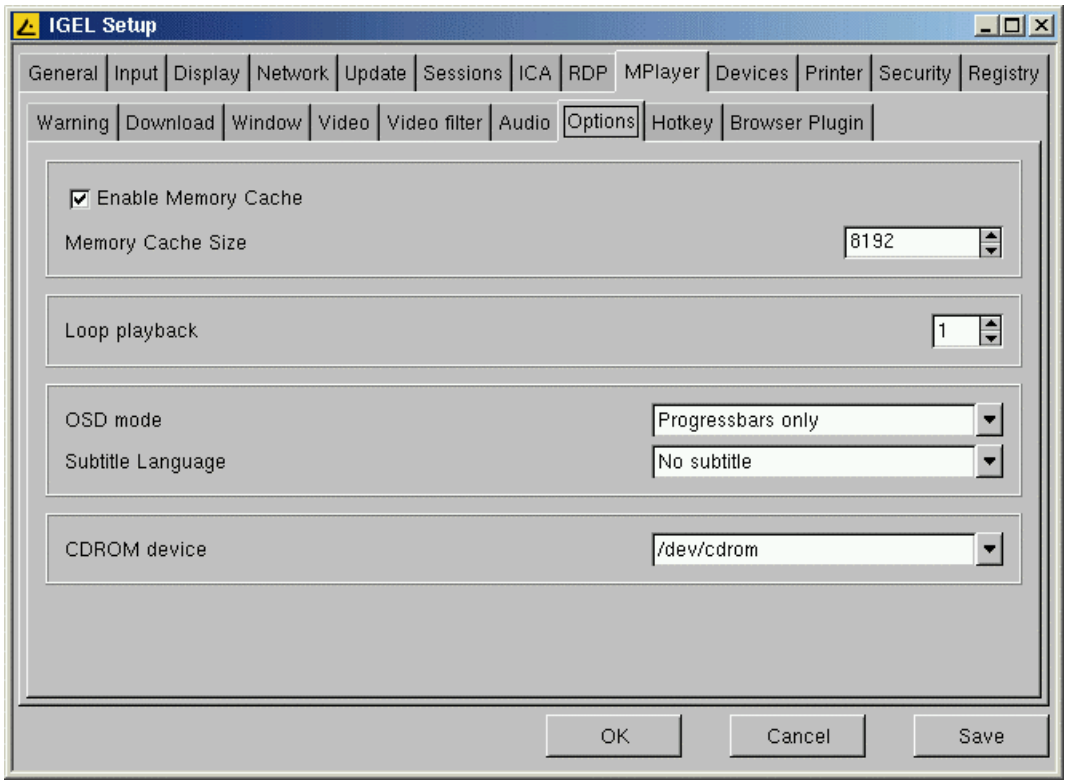
For some media files, you may need to tweak these advanced video-processing options.

5.11.4 Audio



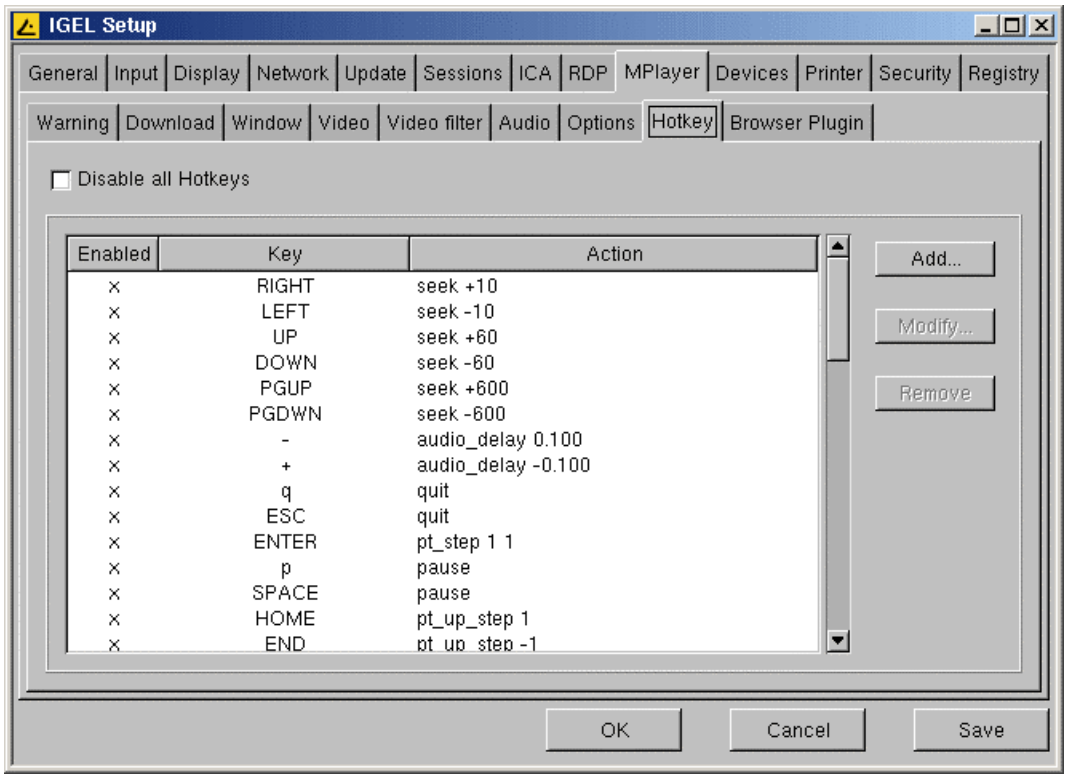
Choose the video language. Available are: English, German, French, Italian, and Spanish.

5.11.5 Options



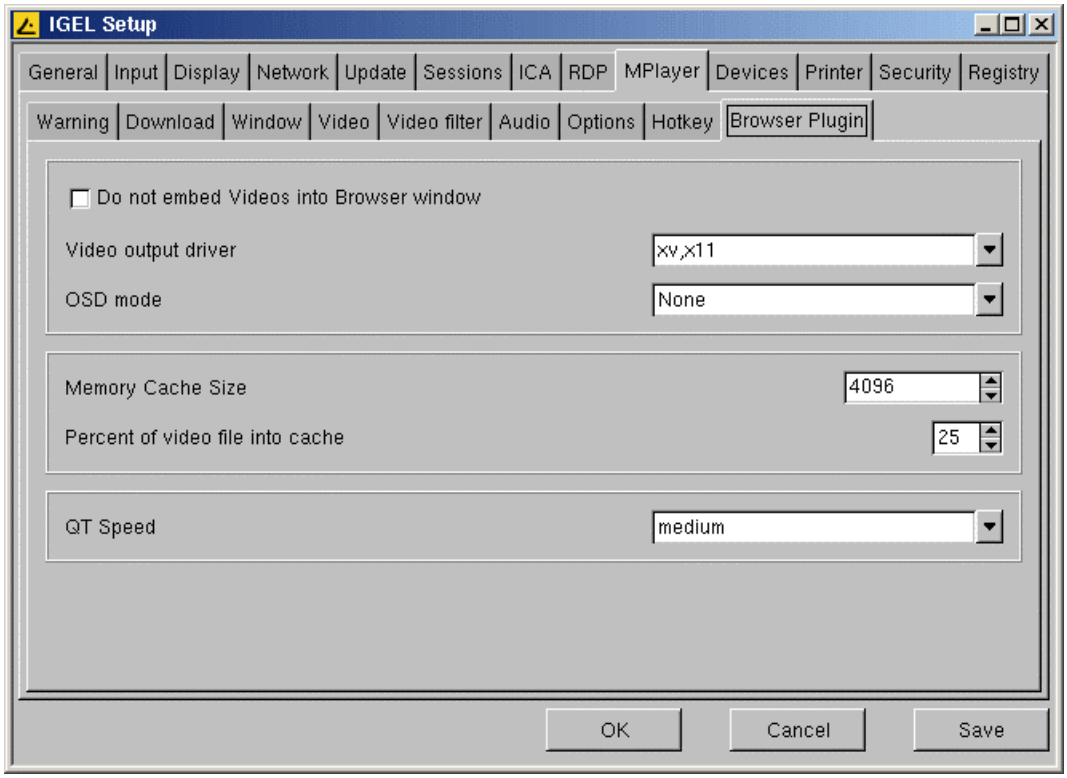
In this tab, you can configure how much RAM should be used to cache the media file(s), how often it should loop, the OSD mode, the subtitle language and the source device.

5.11.6 Hotkeys



Here you can reassign the hotkeys for the Mplayer's GUI functions.

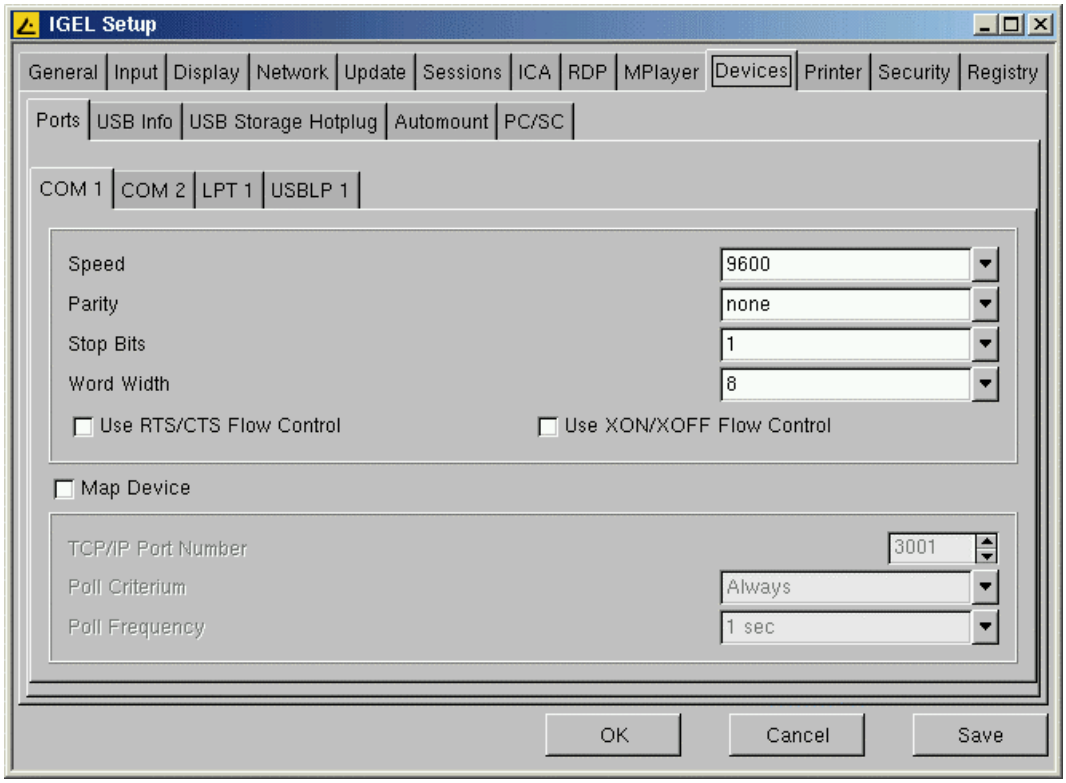
5.11.7 Plugin



If you want to use the MPlayer as browser plugin, you can set configuration values differing from the previous ones which affect manually configured Mplayer sessions (see 6.4.9.1).

5.12 Devices

5.12.1 Serial Ports



This page allows you to define the parameters of the serial ports COM 1 and COM 2.
You can also enable port mapping for them and LPT1.

- ***Speed***

Select your input and output communication speed from the list.
(Depends on the attached device and the program communicating with this port.)

- ***Parity***

If a parity bit is used, select the type of parity bit from the list.

- ***Stop Bits***

Decide whether one or two “Stop Bits” are used.

- ***Word Width***

Select how many bits are used per byte.

- ***Use RTS/CTS Flow Control***

Enable this flow control type if you have to use hardware handshake.

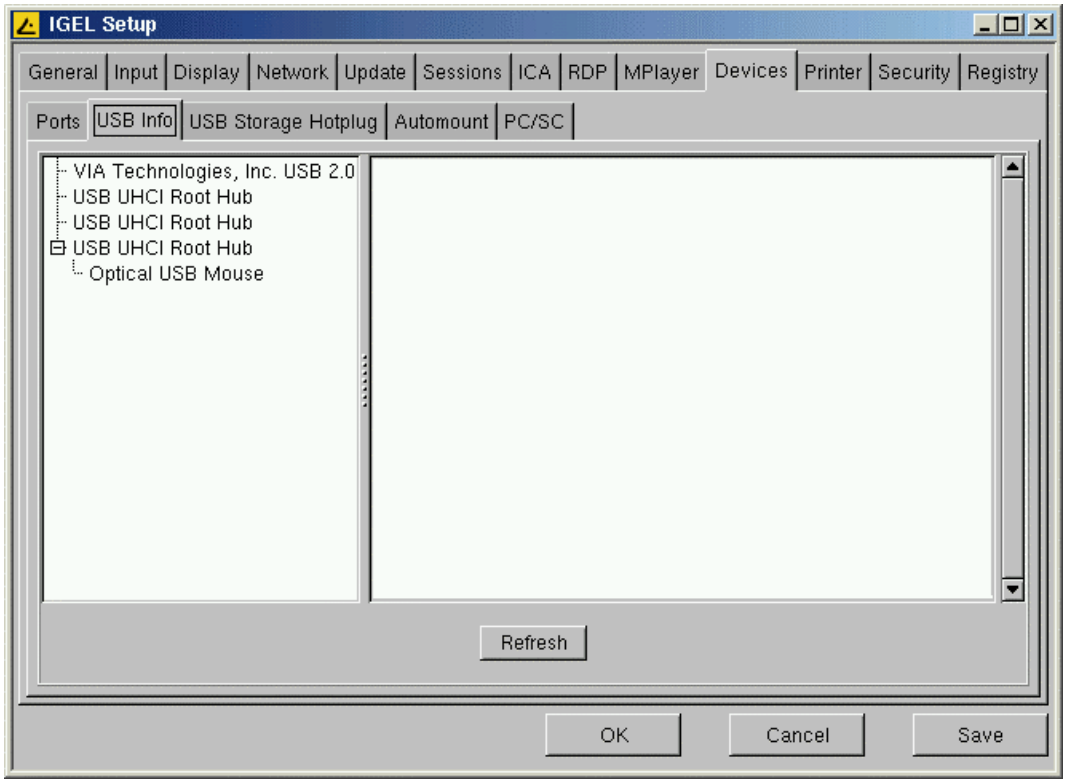
- ***Use XON/XOFF Flow Control***

Enable this type of flow control if you want to use software flow control by using start/stop characters.

- ***Map Device***

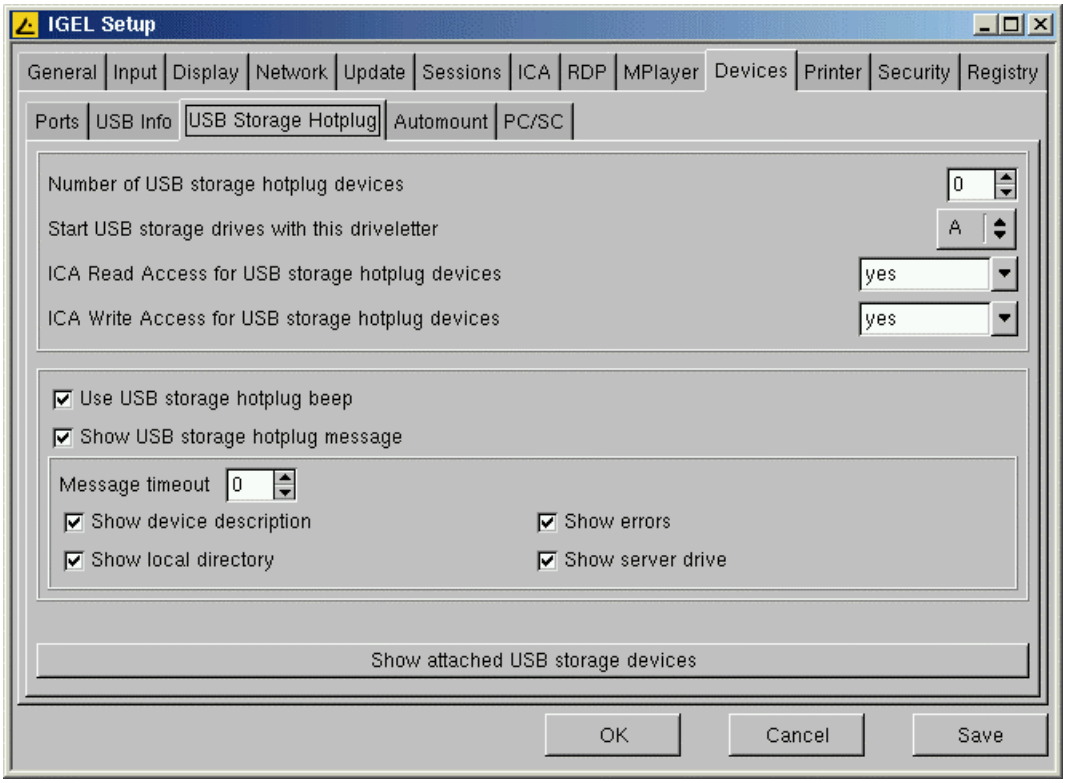
You can map the four interfaces directly to a TCP/IP port.
This feature is useful to access the Thin Client’s interfaces directly from remote.
(The default values here are: 3001 for COM1, 3002 for COM2, 3003 for LPT1 and 3004 for the USBLP1.)

5.12.2 USB Info



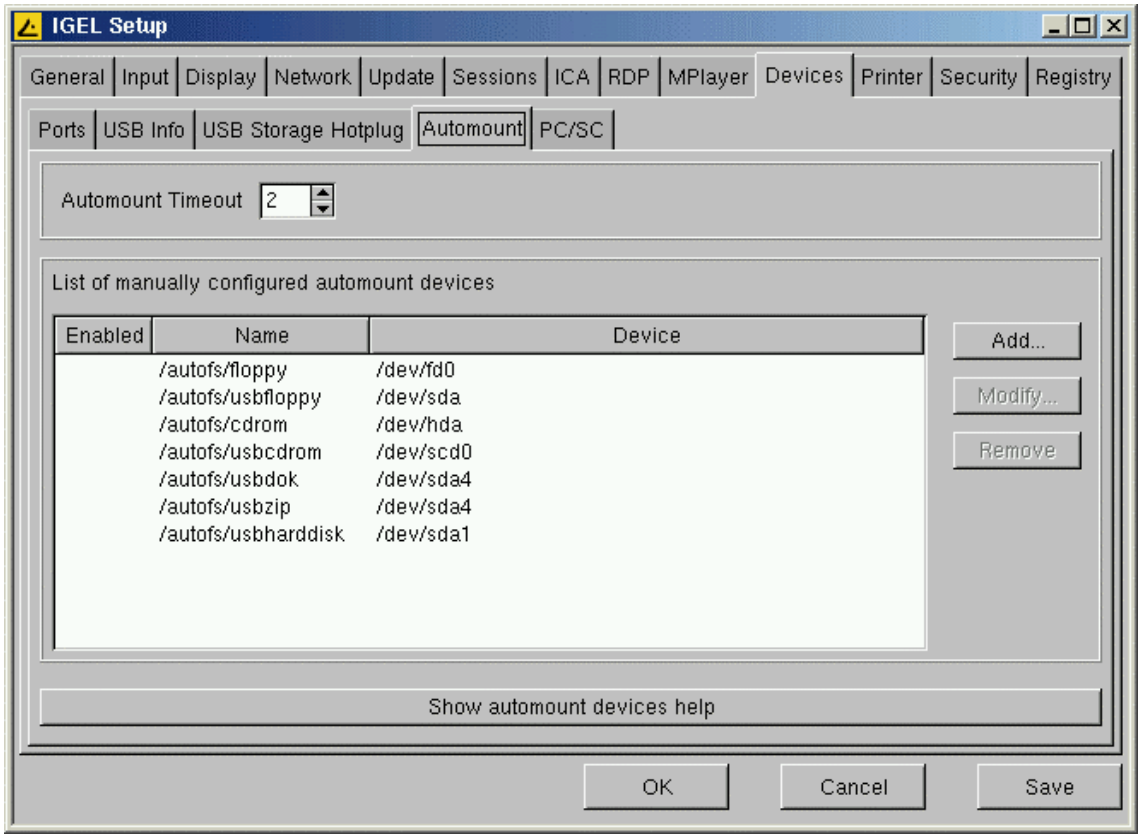
Attached USB devices will be shown here. In very rare cases, you need to press “Refresh” once.

5.12.3 USB Storage Hotplug



Specify the details on how to set USB devices. Most important is the number of potential devices, the drive letter assignment and what access (read and/or write) should be available to users within ICA sessions.
By default, new attached devices will be auto-detected, the terminal will beep once and a pop-up stating that a new device has been found will come up.

5.12.4 Automount Devices



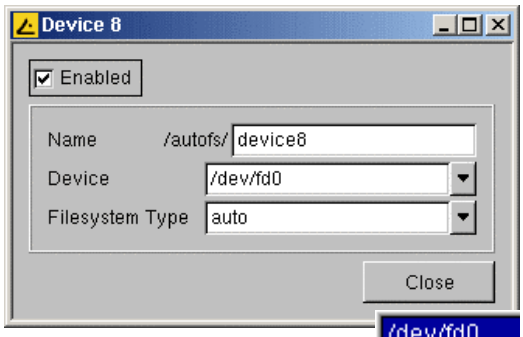
This page allows you to define and configure devices which will be mounted automatically when accessed.

- ***List of Automount Devices***

This list gives you an overview of the “Automount Devices”.
The most common devices (like floppy, CD- ROM, etc) are already pre-configured here for you.

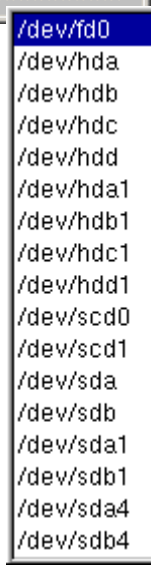
- ***Modify…***

To activate one of the pre-defined devices, click here and simply check the “Enabled” checkbox.



- ***Add…***

In case your device is not already predefined in the “***List of Automount Devices”***, use the “***Add…***” button to open up this window and configure it manually:



- ***Name***

Type in a meaningful name for your device.
(This will also be the name of the subdirectory that will be created in /autofs/)

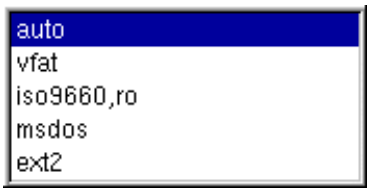
- ***Device***

Select the proper device synonym from the dropdown box (you may also type it in manually).

Note: Make sure that this fits to the rules of the “***List of Possible Automount Devices***” (see page below)!

- ***Filesystem Type***

Set the filesystem that will be used here.
In general, you should choose “auto”, but if you use “ext2” or encounter any other trouble, set the filesystem you are using explicitly.

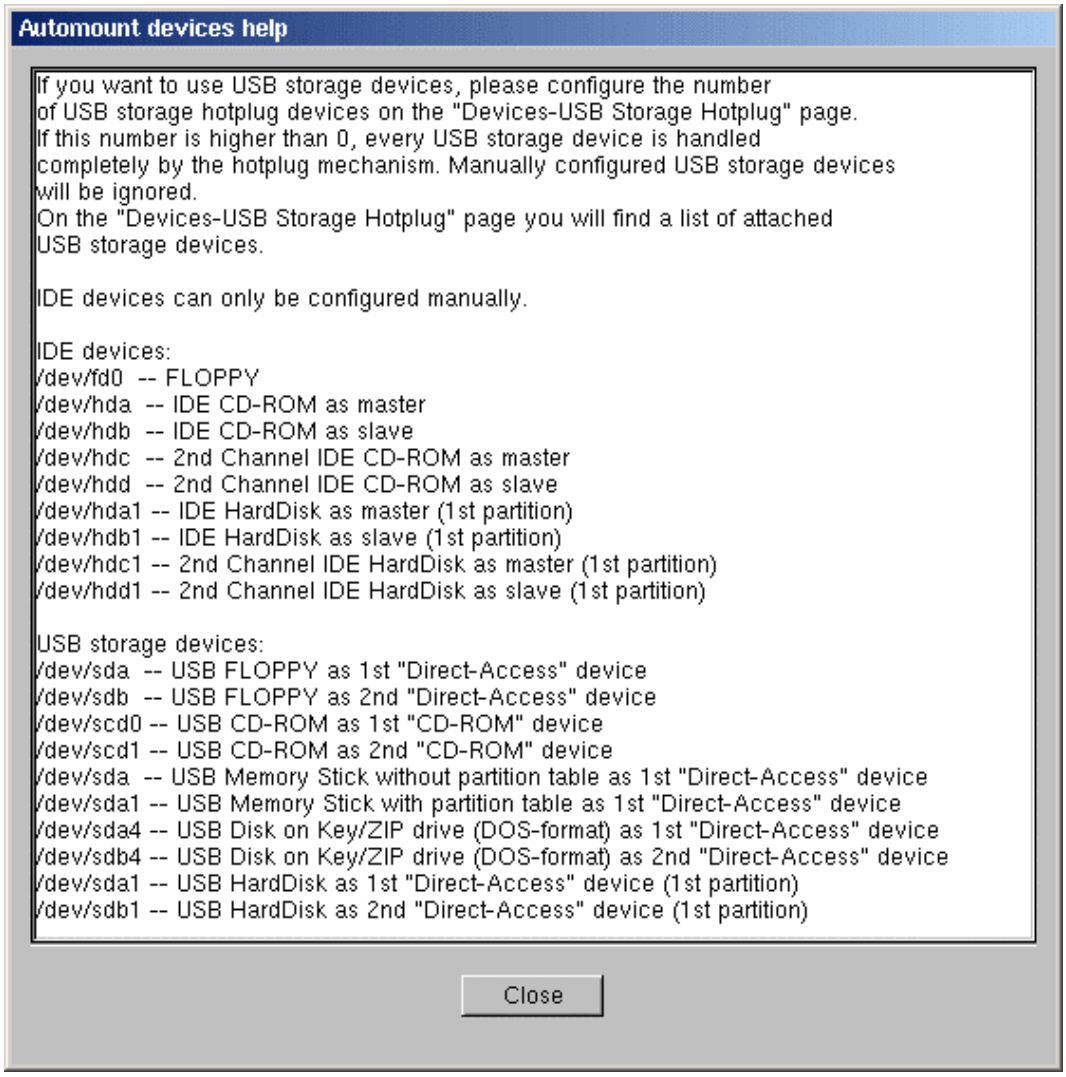


- ***Automount timeout***

Set the time (in seconds) the system should wait after an access to your devices, before unmounting it. The range of this timeout reaches from 0 to 600 (10 minutes).

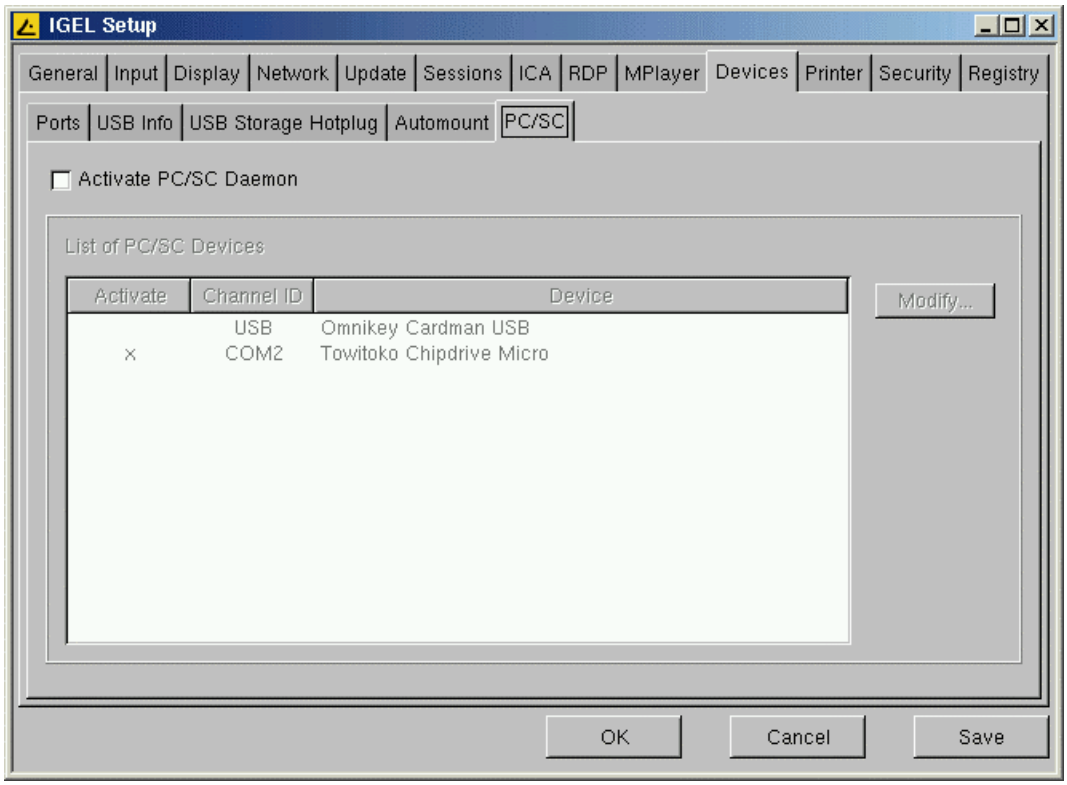
Note: It is strongly recommended **not** to set the timeout to zero, because this can cause data loss!

- ***List of possible Automount Devices***



Note: The Linux device synonyms or their sequentials have to be used as stated in this table!

5.12.5 PC/SC



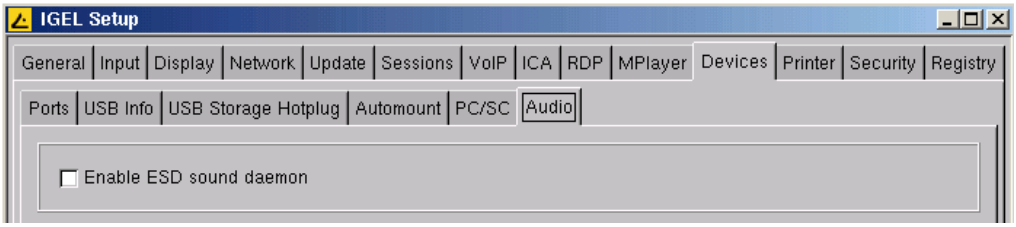
- ***Activate PC/SC Daemon***

In order to use the PC/SC interface of the thin client, check the “Activate PC/SC Daemon” box.

By default, the internal card reader is set. Some models already have one built-in as well as the reader being available separately.
You may also use an external Cardman reader attached to the USB port.

5.12.6 Audio

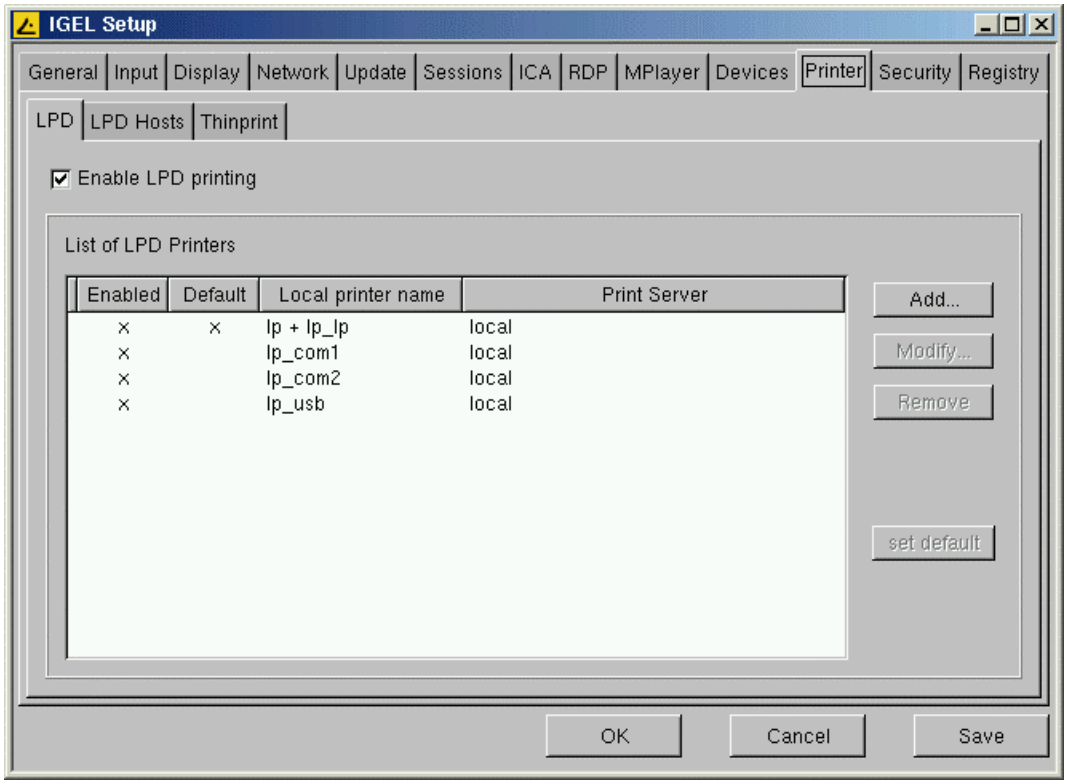
If you want to have an audio output with XDMCP you can activate the ESD Sound Daemon.



5.13 Printer

This tab is the central tool to configure the properties of your LPD and/or “ThinPrint” printers.

5.13.1 LPD Printer



LPD (Line Printer Daemon) printers are used by the BSD print system, which is the standard printing method in UNIX environments and is also supported by Windows NT and Windows 2000.

- ***List of LPD Printers***

There are four pre-configured LPD printers by default, named ***lp+lp_lp***, ***lp_com1***, ***lp_com2*** and ***lp_usb***. These queues belong to the corresponding interfaces of the Thin Client and are “ready-to-use”.
Usually, there is no further configuration needed here, especially if your printer is attached to the LPT1 interface (default printer).

- ***Add…***

You can add a network printer here. Provide the print server’s name or IP and the name of the remote printer / print queue (for details on all printer settings, see next page).

- ***Modify…***

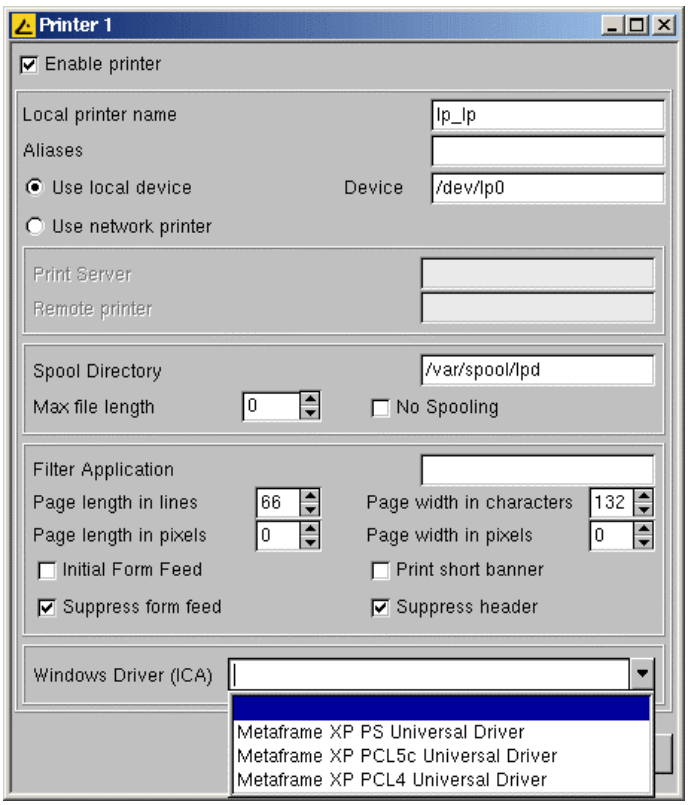
Click here to manipulate the pre-configured printers or potentially added ones (see next page).

- ***Set default***

Mark the printer that’s supposed to be your default output device within the “***List of LPD Printers”*** and click on “set default”. The selected printer will automatically be assigned to the queue “***lp***” within /etc/printcab. You may use “***lp***” when printing to your default printer.

Note: In Linux you normally have to make these changes within the file /etc/printcab manually. This is not necessary with your Thin Client; all changes can be made in the setup masks here and will be transferred into the /etc/printcab almost immediately.
Do not edit the /etc/printcab manually anymore! Your changes will be overwritten by further changes made via the setup or get lost at the latest during the next reboot of the Thin Client.

Printer Properties



- ***Local Printer Name***

Enter the name of the printer that can be used with the *lpr* command.

- ***Aliases***

If needed, enter the alias names of the printer here. Separate by | if you enter more than one.

- ***Use Local Device***

Use this setting if the printer uses a local device, and enter the name of the "***Device***" which handles the printing.

- ***Use Network Printer***

If you are using a network printer, click this button and enter the name of the "***Print Server***" and the name of the "***Remote Printer***" queue in the corresponding entry fields.

- ***Spool Directory***

Enter the path of the local spool directory.

- ***Max File Length***

Define the maximum size allowed for a print job in blocks of 1KB (0=no size restriction).

Note: Files bigger than the set size will be truncated.

- ***Filter Application***

This option allows defining the name of a filter script which is used over, e.g., an NFS mount.

Note: There are no local filter scripts available on the Thin Client.

- ***Page Length in Lines***, ***Page Length in Pixels***, ***Page Width in Characters*** and ***Page Width in Pixels***

These options allow you to adjust the page size. You can either assess it in lines by characters (like the defaults do) or in pixels by pixels.

- ***Form Feed***

Enables / disables the print of a form feed when the device is opened.

- ***Suppress Form Feeds***

This button switches form feed suppression on / off.

- ***Print Short Banner***

Click this button to print a short banner, one line only.

- ***Suppress Header***

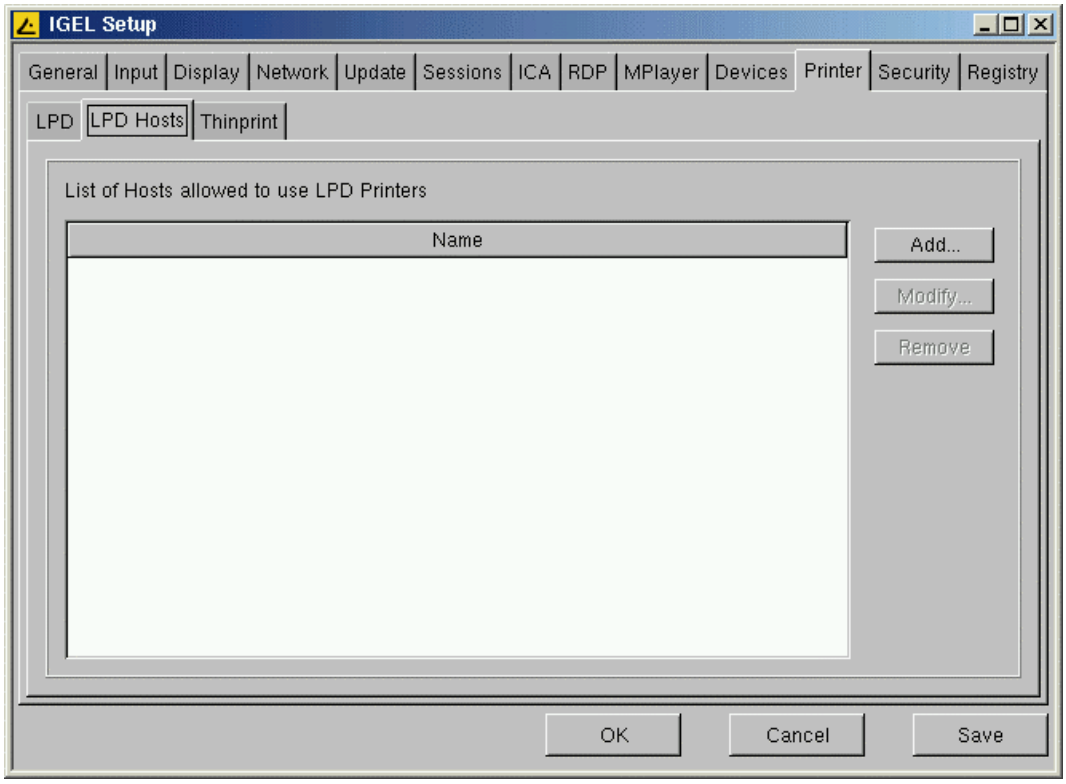
The suppression of printing a burst page header can be toggled here.

- ***Windows Driver (ICA)***

Enter the (very exact) windows driver name of a printer to be used for ICA connections. Alternatively, use one of the Metaframe universal printer drivers via the drop box.

5.13.2 LPD Hosts

The permissions to print on the Thin Client can be configured in this page.



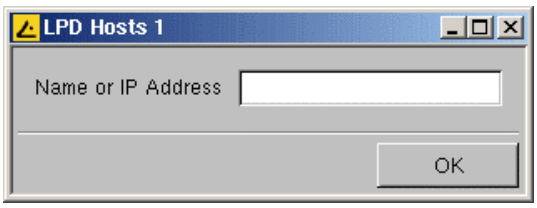
As long as you have not granted print permissions here, no LPD host will be able to print to the Thin Client but will get a “permission denied” error.

- ***List of Hosts allowed to use LPD Printers***

All hosts that are allowed to print on the Thin Client will be displayed in this list.

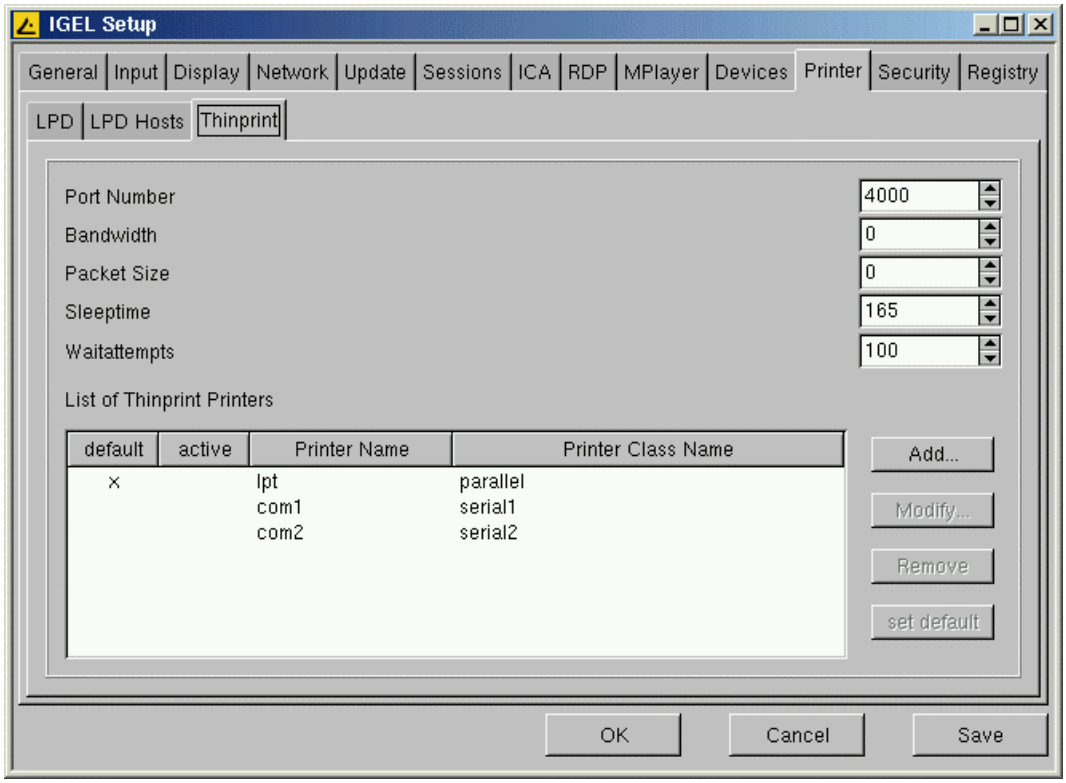
- ***Add…***

To define print permissions, click “add…” and provide the host’s IP or name in this mask:



Note: If you want to grant access for every LPD host, enter + (plus sign) and click OK.
This disables the access control for LPD.

5.13.3 ThinPrint Client



ThinPrint offers resource-oriented reduction of bandwidth allocated for print job transfers. The ThinPrint Client does not use preexisting queues on the Thin Client. Instead, it sends the decompressed print jobs directly to the printer.

- ***Port Number***

Enter the port number the ThinPrint daemon should communicate over. Ensure that the port number is the same on both the ThinPrint Client and the ThinPrint Server (otherwise communication will fail).

- ***Bandwidth***

Enter a bandwidth value (in bits per second) which is the same or smaller than that set on the ThinPrint server. A larger value, disabled Client Control or no entry here means that ThinPrint Server values will apply.

- ***Packet Size***

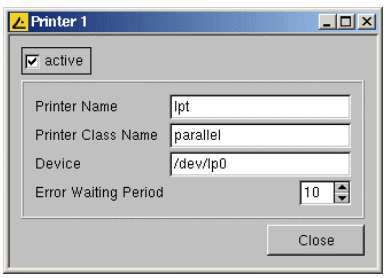
Like bandwidth, packet size is given in bytes here. (No entry means that ThinPrint Server values apply.)

- ***Timeout***

Maximum waiting period in case of blocked printer (in seconds).

- ***List of ThinPrint Printers***

This list gives you an overview of the pre configured ThinPrint printers.
Except for minor differences, this menu is designed and works like the LPD printer menu (see 5.13.1):



- ***Class***

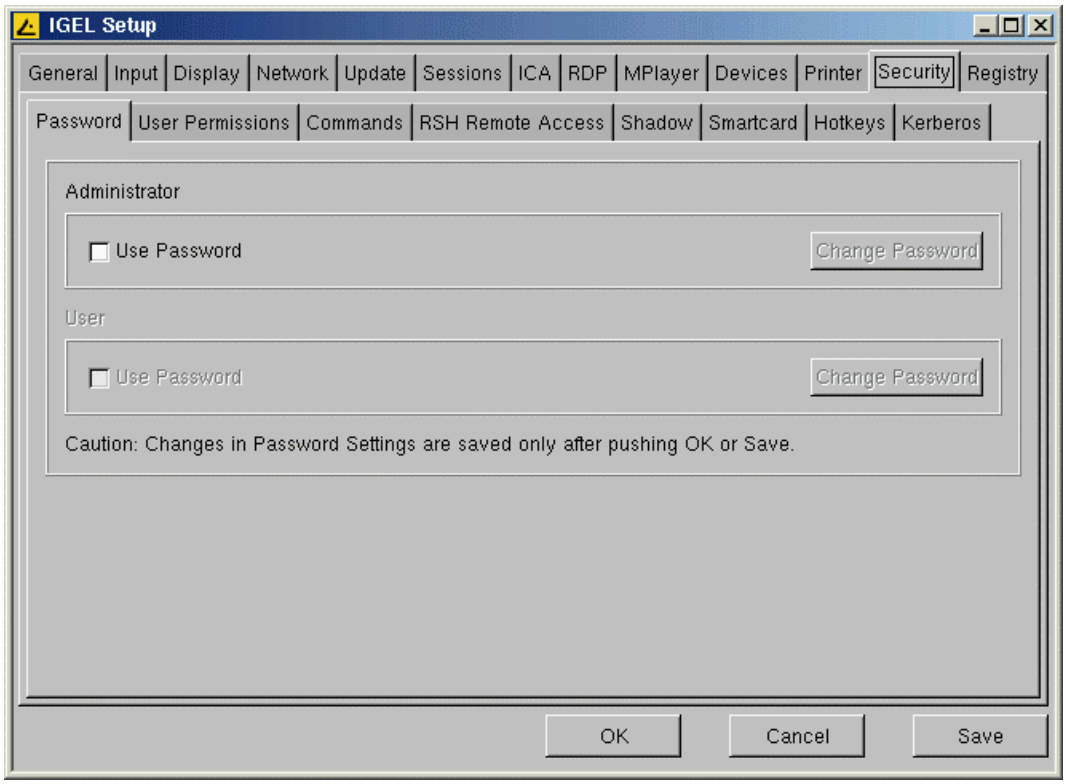
Enter the printer class name (optional).

- ***Active***

Enable / disable network visibility for this printer.

Note: For more detailed information about setting up your "ThinPrint" components, please refer to your "ThinPrint" manual.

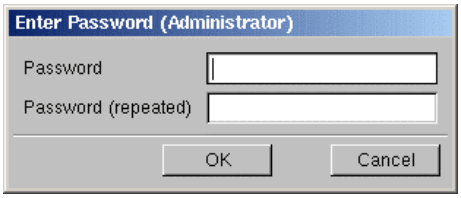
5.14 Security



To prevent any unauthorized 'trespassing' into the Thin Client's setup (which could enable to intrude deeper into your network), it is highly recommended to set an administrator password after the initial configuration.
To allow limited configurations by the user, you can use an additional user password that offers most variable options (explained in detail in 5.14.2 on next page).

5.14.1 Password

The "Password" page allows you to set an administrator password and a user password.



- ***Administrator Password***

By clicking on "User Password", this dialog box will pop up prompting you to enter the administrator password.

Note: Enabling this password will restrict the "***Config***" tab of the "***Application Launcher***", the shell access in an "***Xterm***" and on the console to the administrator at once!

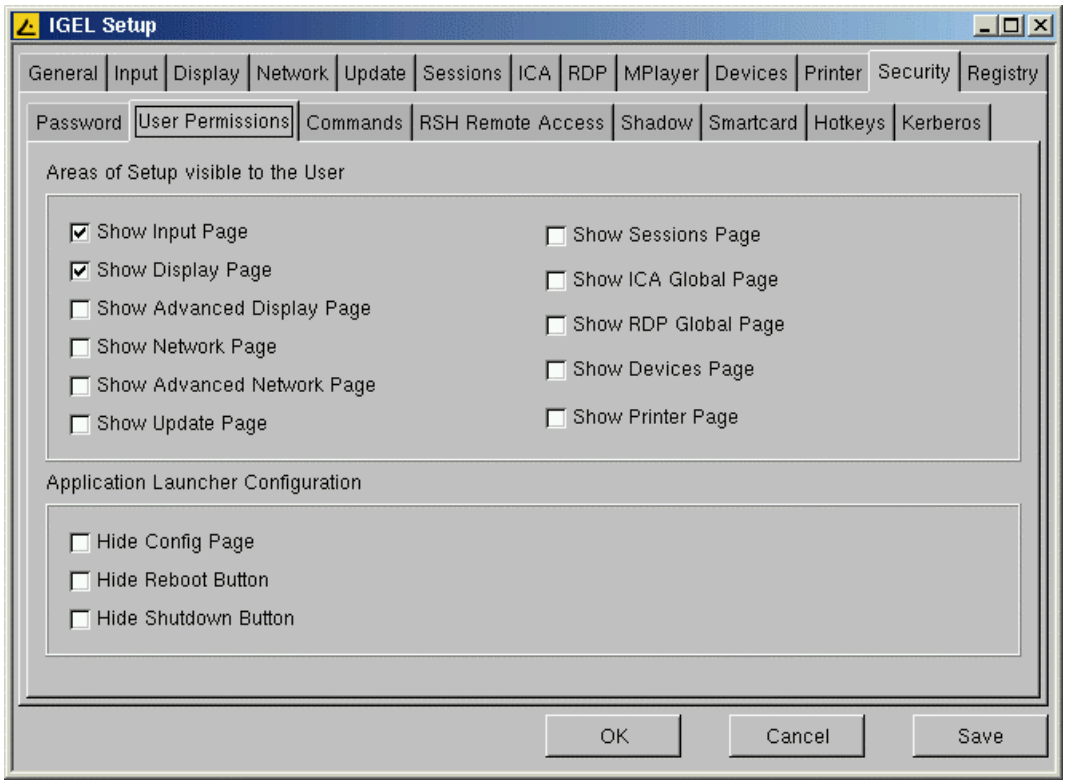
- ***User Password***

The same procedure as for the administrator password applies here.
See the dialog-box to the right; it comes up when entering the setup after both passwords have been set.

Note: To enable the user password option, an administrator password has to be set first.

Attention: Make sure that the right key mapping is enabled when typing in any password! Because the typed characters in the password fields are masked by asterisks, you will not see if, for instance, 'x' and 'y' are mixed up. After changing the key mapping later on, you will wonder why your password is not accepted anymore…

5.14.2 User Permissions

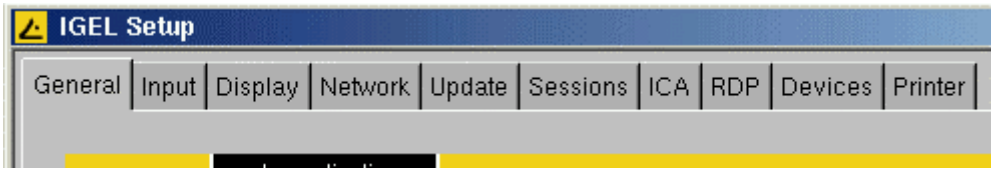


- ***Areas of Setup visible to the User***

The administrator can completely define which areas of the setup are visible and configurable by the user. The “Input Page” and the “Display Page” are enabled by default. “Advanced Display Settings” and “Advanced Network Settings” are sub-menus of these but have to be enabled separately.

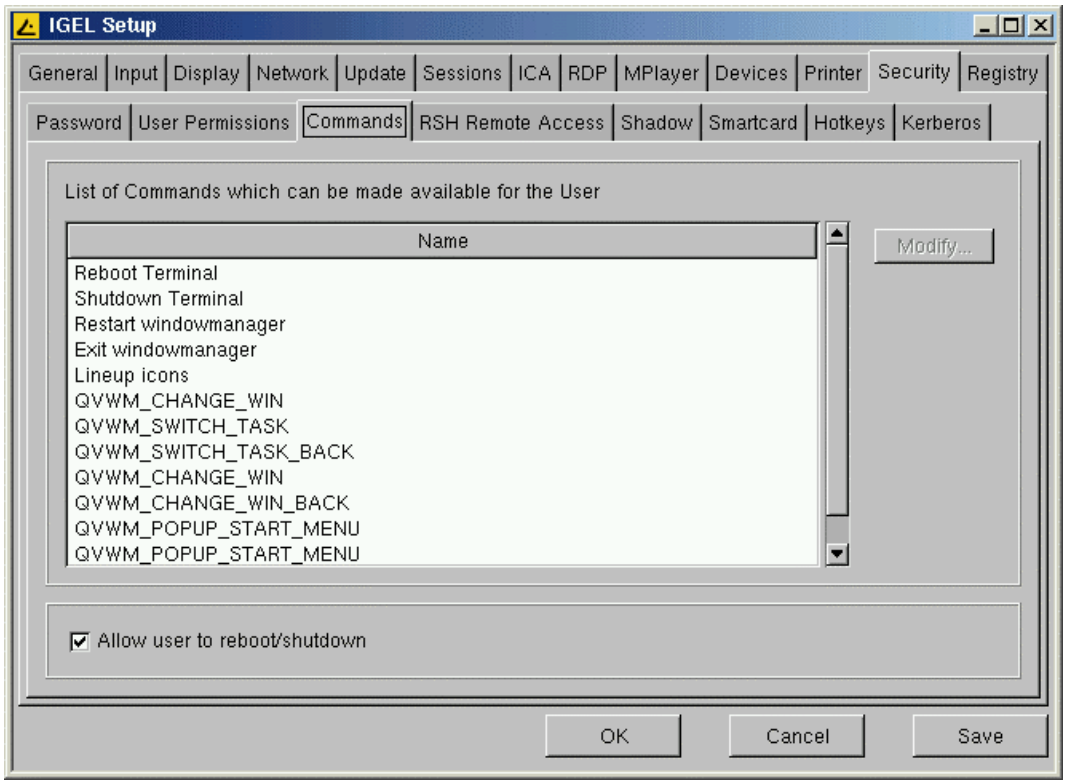
Without further configuration, the user’s default setup will look like this:

Enabling all options giving the user the most influence possible will look like this:

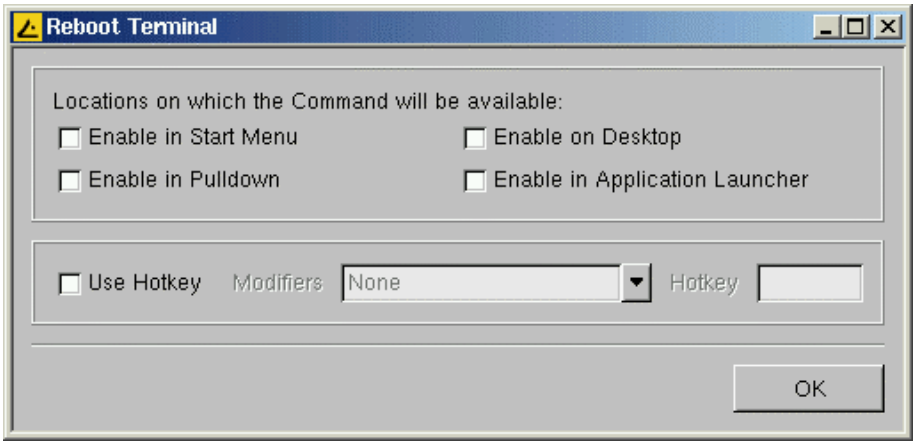


“*Security*” and “*Registry*” will always be restricted to the administrator only!

5.14.3 Commands



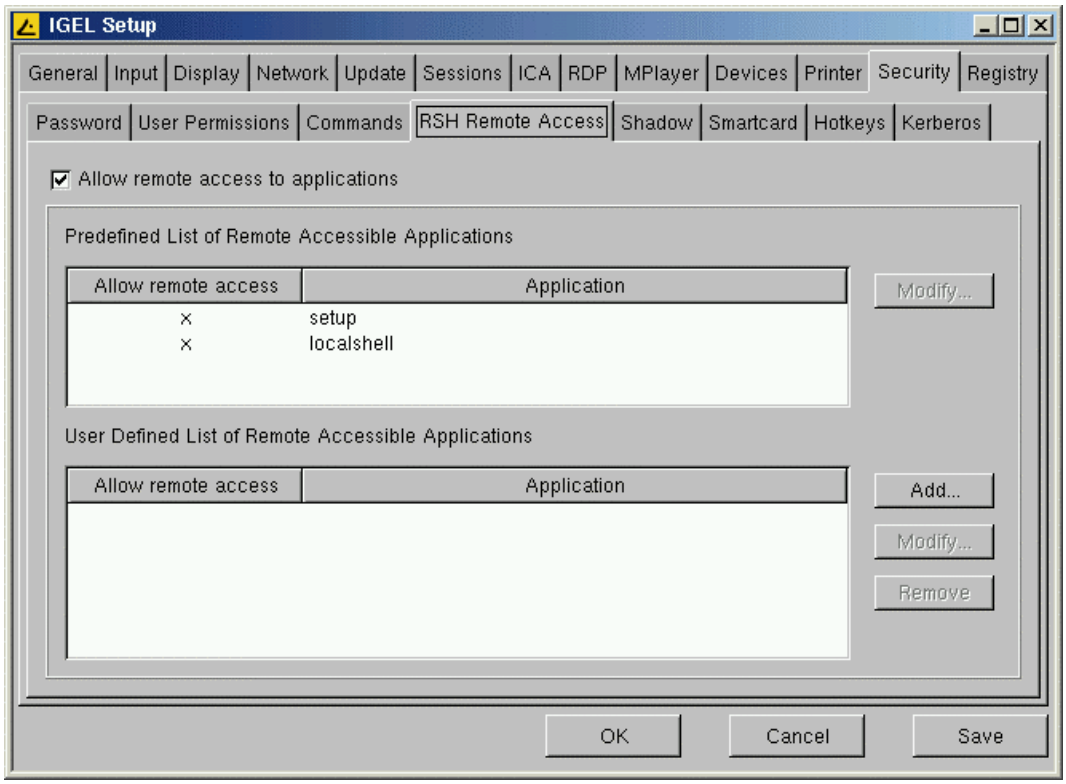
You have further configuration / limitation options here concerning the menu items shown in the main window.
They can be associated to any combination of the three main access areas as there are the "***Start Menu***", the "***Desktop***" and the "***Pulldown***" menu.



Additionally, it is possible to assign a hotkey sequence to those commands for better and quicker access.

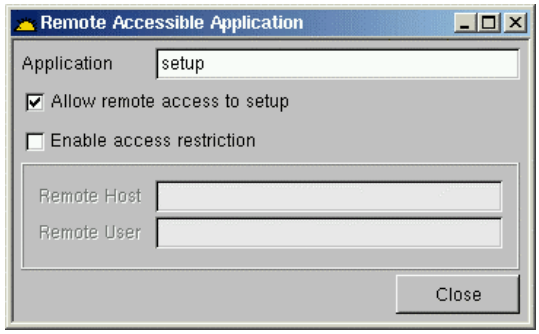
As soon as you activate the "***Use Hotkey***" option, this Drop down box will be accessible (every common modifier is available):

5.14.4 RSH Remote Access

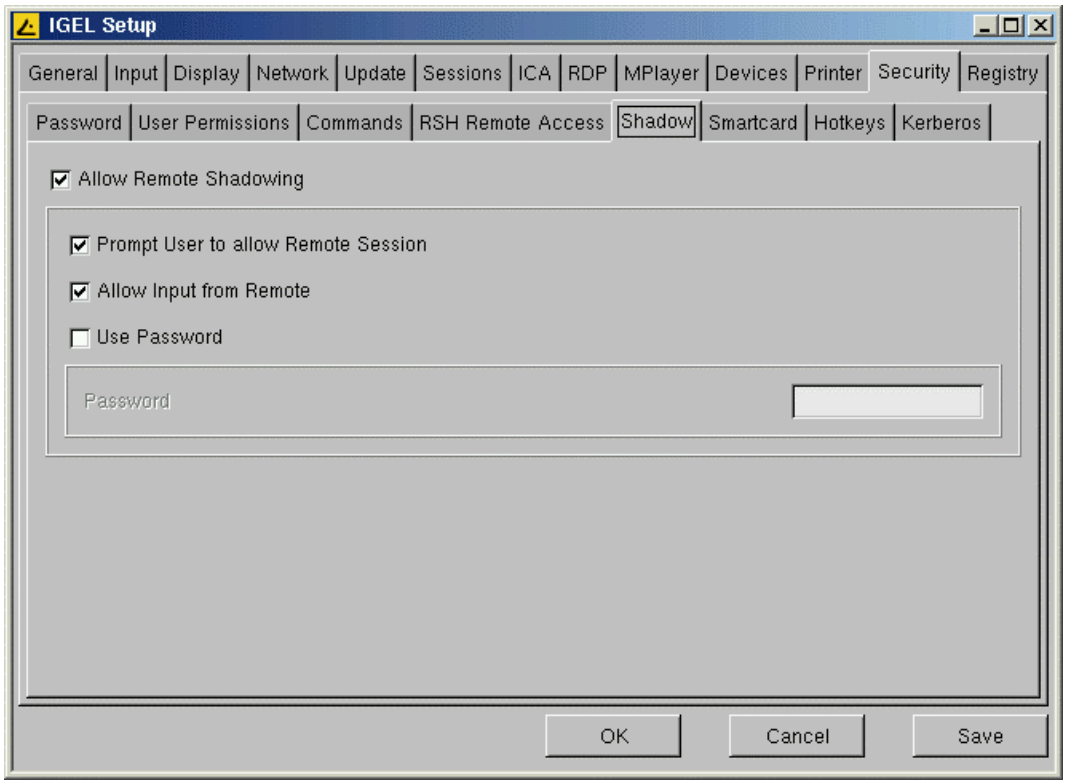


For centralized administration, the Thin Client can be configured to be accessed through your WAN.

By default, the remote access to the local setup is allowed as soon as you have disabled (or properly configured) the “Access Control” (Chapter 5.4.2.4).
But you can restrict the remote access to a specific user from a specific host here. Therefore enable the restriction and enter the host’s full qualified name (e.g. xterm.igel.de) and the admitted user.



5.14.5 Shadow



For helpdesk purposes, you can shadow the client via the IGEL Remote Manager.

- ***Prompt User to Allow Remote Session***

Legal rights in some countries forbid an unannounced shadowing.
(Do not disable this if you are located in such country!)

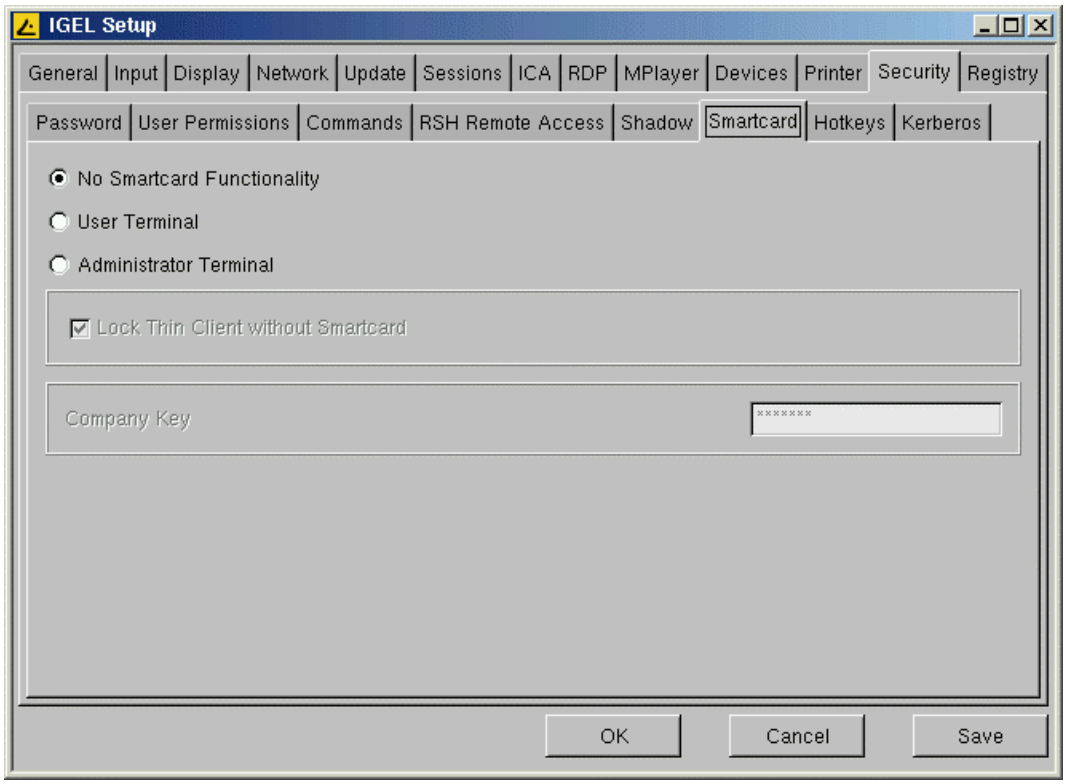
- ***Allow Input from Remote***

As long as this feature is enabled, the remote user is allowed to input keyboard and mouse events as if he were the local user.

- ***Use Password***

Check this box in order to set up a password that the remote user has to enter before being able to shadow.

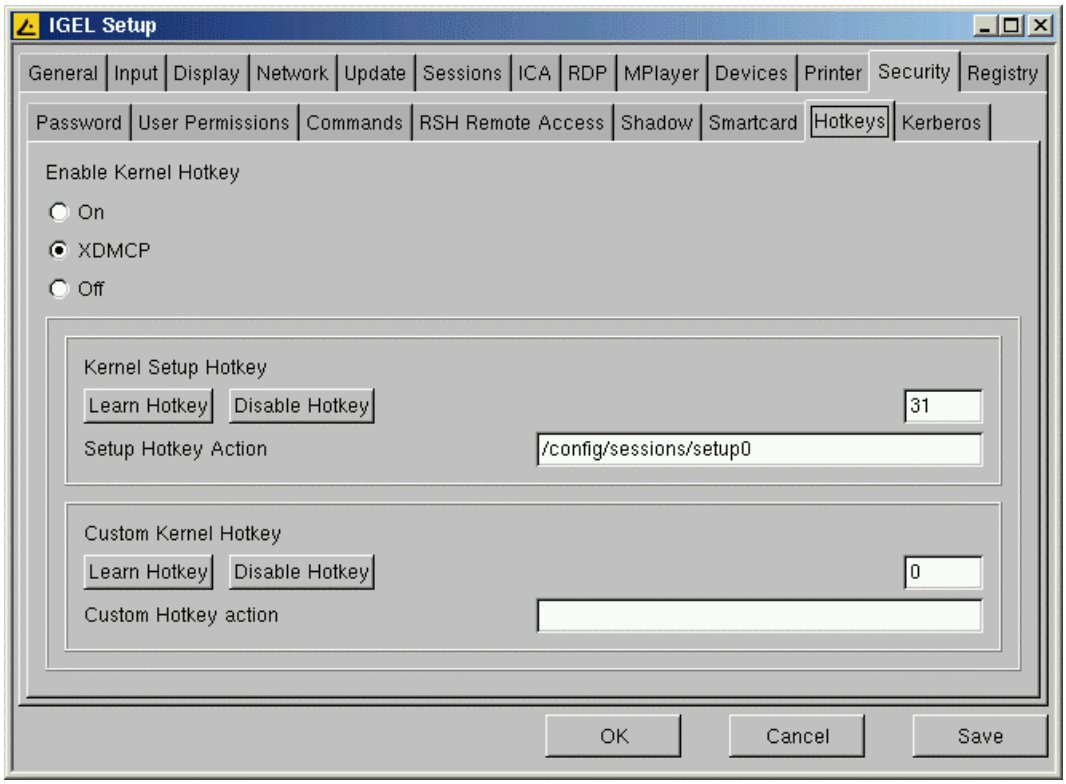
5.14.6 Smartcard



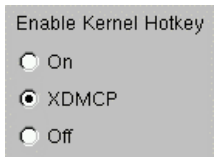
Enable/disable the Smartcard feature or rather choose between user mode and administrator mode (only in administrator mode are you able to create/manipulate smart card).

Note: For a very detailed description on setting up Smartcard functionality, please refer to the "***Smartcard Quick Setup Guide.pdf***"

5.14.7 Hotkeys



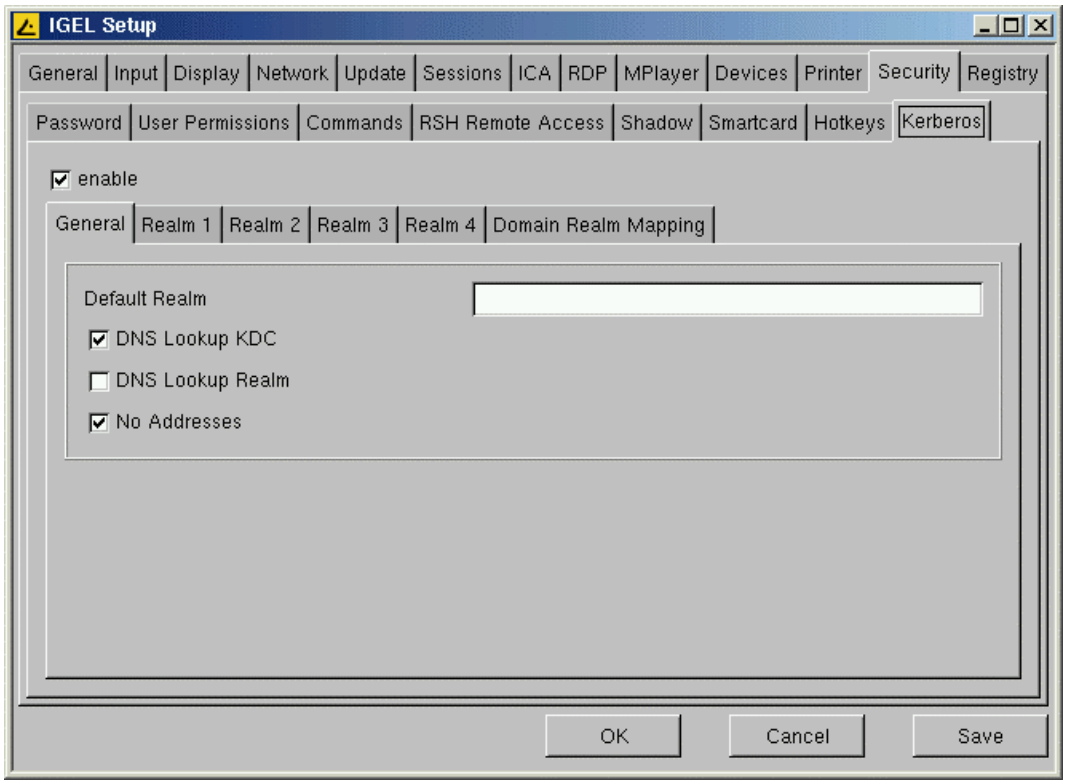
There are certain hotkeys recognizable by the kernel to call the setup.
In some circumstances, this might be the only way to get into setup without using emergency boot.



As you see right, the hotkey is by default only activated for the XDMCP mode. If you want to have it always on or always off, you can set this here.
<CTRL> + <ALT> is the fixed modifier for the setup hotkey. The default associated key is <S>, which means that pressing <CTRL>+<ALT>+<S> calls the setup in XDMCP mode if you do not manipulate the default settings.
To change the associated key, simply click the “Learn Hotkey” button and press the wanted key when prompted.

Another hotkey is available for free configuration. You may, for example, assign an ICA session to it.

5.14.8 Kerberos



- ***Default Realm***

Identifies the default Kerberos realm for the client. Set its value to your Kerberos realm.

- ***DNS Lookup KDC***

Indicate whether DNS SRV records should be used to locate the Key Distribution Centers (KDCs) and other servers for a realm if they are not listed in the information for the realm.

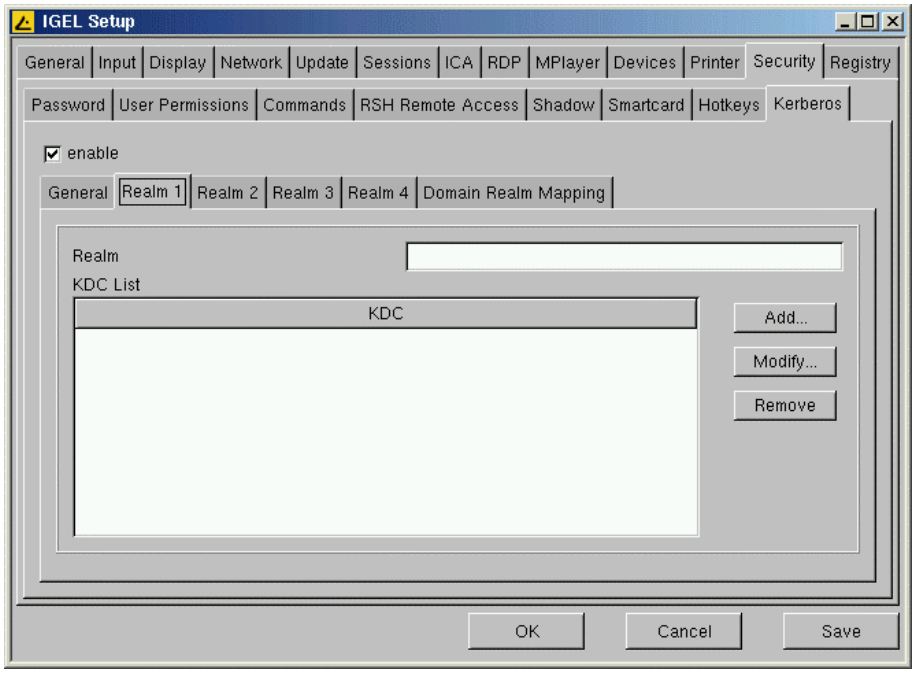
- ***DNS Lookup Realm***

Indicate whether DNS TXT records should be used to determine the Kerberos realm of a host.

- ***No Addresses***

Setting this flag causes the initial Kerberos ticket to be address less. This can be necessary if the client resides behind a Network Address Translation (NAT) device.

Realm 1 – Realm 4

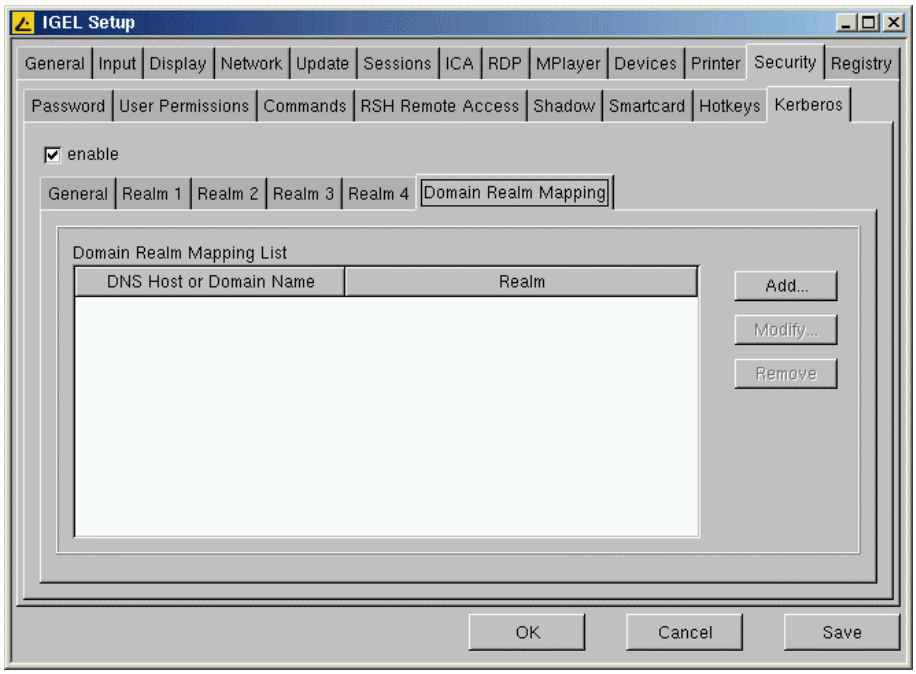


- ***Realm***

The name of the realm you want to authenticate to.

- ***KDC List***

IP or FQDN list of Key Distribution Centers for this realm. An optional port number (preceded by a colon) may be appended to the hostname.



- ***Domain Realm Mapping***

Entries in the Domain Realm Mapping List provide a translation from a hostname to the Kerberos realm name for the services provided by that host.

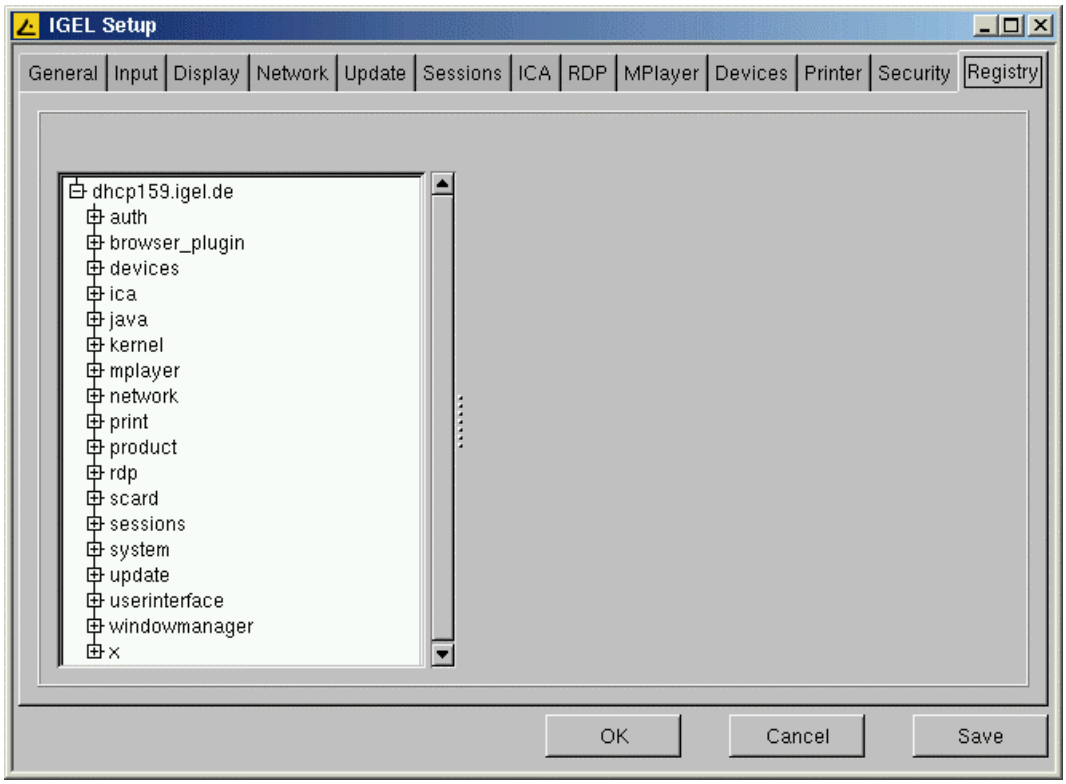
- ***DNS Host or Domain Name***

The entry can be a hostname, or a domain name, where domain names are indicated by the prefix of a period ('.') character.
Host names and domain names should be in lower case.

- ***Realm***

The value is the Kerberos realm name for that particular host or domain.

5.15 Registry



You can manipulate nearly every parameter of the firmware within the registry.
Refer to the tooltips for details on the single items.

Caution: Only very experienced administrators should make modifications to the Thin Client's configuration via the registry!
By setting wrong parameters, you can easily ruin the configuration, ending up with a stalled system.
With such a misconfiguration, the only way to recover your Thin Client is to restore the default factory settings. (Refer to 4.2.4.)

6 Application Launcher

The “Application Launcher” is the central administration tool for all kinds of available session types (which depend on your Thin Client model; please refer to the Feature Comparison Table on page 2)

The “Application Launcher” consists of two main pages named “***Applications***” and “***Config***”, and the information page “***About***”.

6.1 About

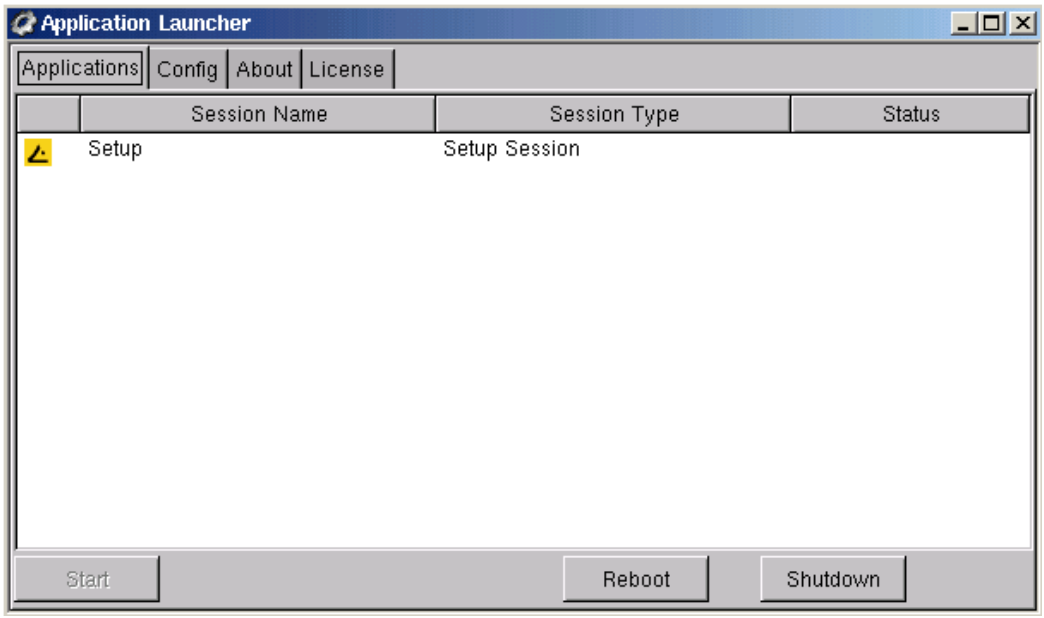
Most of the vital system information is shown on this page.

Before you execute a firmware update, you should consult this page to ensure that you download the appropriate update package (updates are normally stored in ftp.igel.de/pub/firmware/<model>).

In case of a support issue, the firmware version is also most important. The graphics chipset may also be quite helpful.

Note: The value of the display “Memory Size” is the total RAM minus the amount reserved for the VGA.

6.2 "Applications" Page (Starting Sessions)



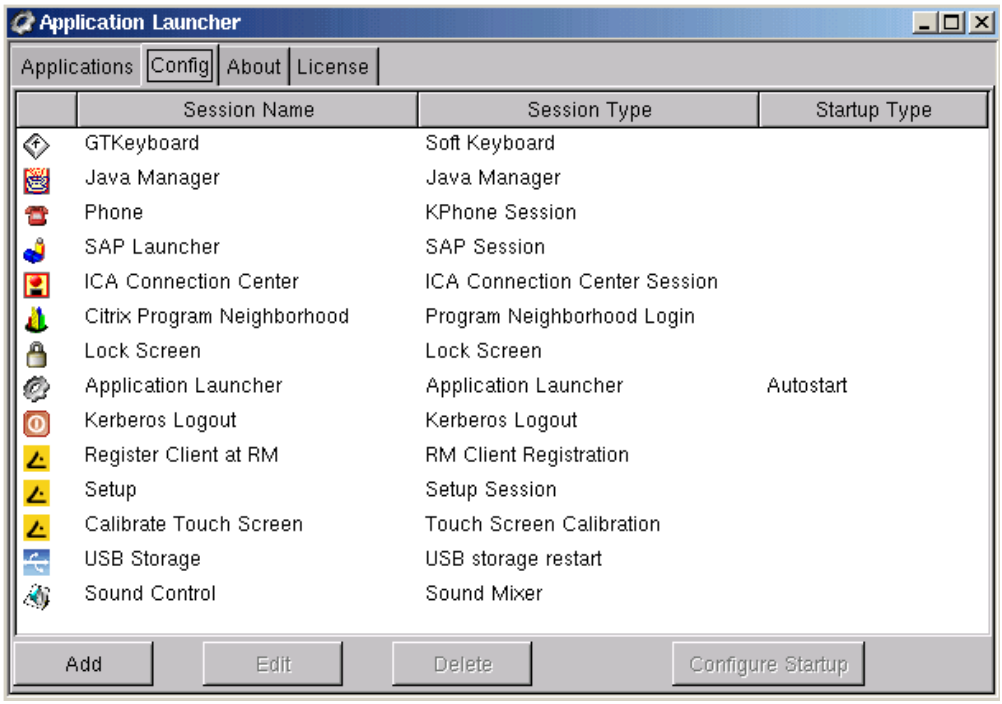
The "***Applications***" page gives you an overview of the configured sessions.
From here, you can launch your sessions by marking the connection to launch and either double clicking it or hitting the "Start" button in the low left corner.
You may also use desktop icons or the start menu to launch your sessions.
The "***Application Launcher***" has the advantage that, in the "***Status***" tab, you also see which sessions are currently running.

6.2.1 "Reboot" or "Shutdown" the Thin Client

In the lower right corner, you find a "***Reboot***" and a "***Shutdown***" button.
(You may reconfigure / eliminate them; see Chapter 5.14.2.)
Use them to execute the corresponding function.
Before doing so, the system will ask for your confirmation or cancellation.

Note: When rebooting or shutting down, your currently running sessions will be disconnected or reset.
This may cause data loss and / or truncated idle sessions on your server.

6.3 "Config" Page (Creating Sessions)



The "***Config***" page allows you to create (and reconfigure) sessions and specify their start methods.
It also gives you a total overview of all configured and configurable sessions and their attributes.

6.3.1 Add, Edit or Delete Sessions

- ***Add*** (a new session)

Pressing the "***Add***" button opens up this "*Session Type*" dialog-box:
Select the session type you want to add and confirm with "ok".
Now the new session will be added to the "Config" page and the appropriate setup program of the selected session type will be started.

Note: The available session types in this menu depend on the Thin Client model! (Refer to the "***Software Feature Comparison Table***")

- ***Edit*** (an already configured session)

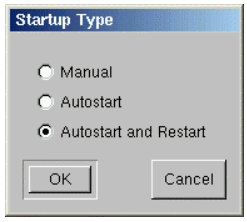
Select the session you want to change and press the "Edit" button. The appropriate session setup appears on the screen and you can start modifying.

- ***Delete***

Select the session you want to delete and hit the "*Delete*" button. The session entry will be removed right away and the "Application Launcher" will be refreshed.

- ***Configure Startup***

With the additional "*Configure Startup*" button you have the possibility of changing the startup type of any configured session without entering its configuration itself. Mark the session from the list, press the "Configure Startup" button and select the wanted startup type in this dialog box:



- The ***autostart*** function enables the session to be started automatically at boot time.

- The ***restart*** function causes a session to be reconnected to the server immediately after logout.

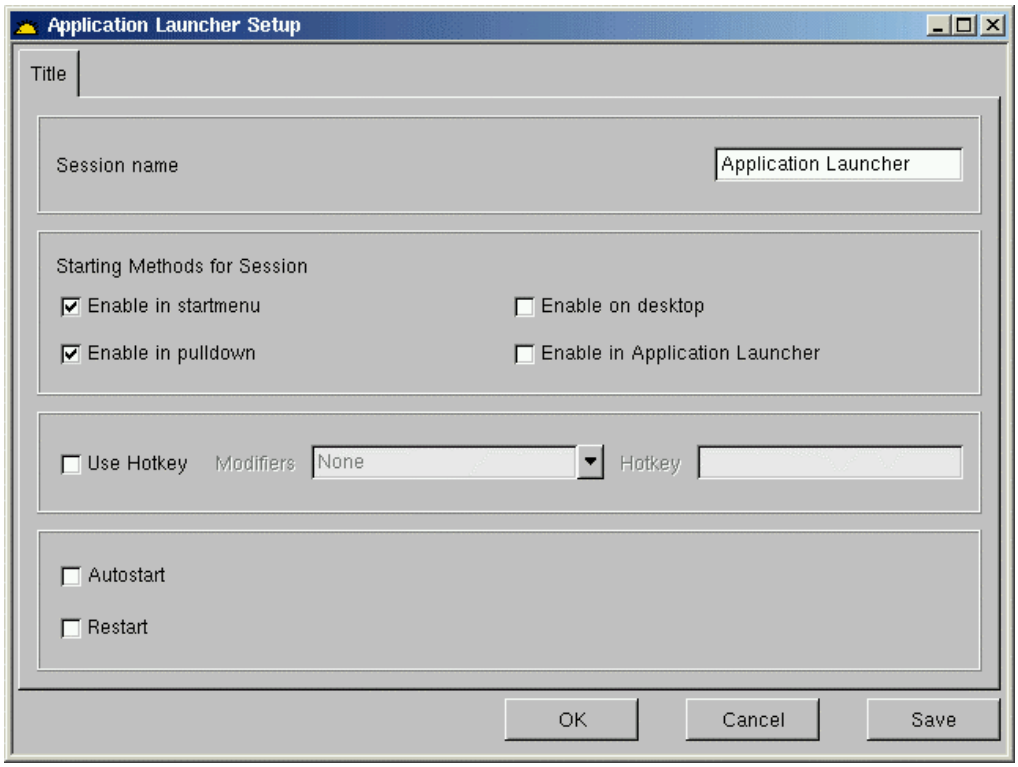
Useful if multiple users use the same thin client and each logs on with his own user and password.

6.4 Session Configuration

This section describes the individual setups of the available session types.
The most common place for all session configurations is the "***Application Launcher***".
As mentioned earlier, you may also do this in the "***Sessions***" tab (Chapter 5.7) within the setup.

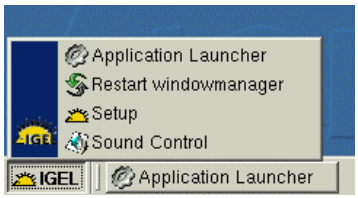
- ***Title***

Every session has a "*Title*" tab like this to set name, reachability and startup. Because this is quite important for the overall handling, it's explained first.



- ***Session Name***

Enter the name you want the session to be called. By default, every session will be named after its type.
It's not necessary to rename it but if you have more than one session of the same kind, it will be quite helpful.

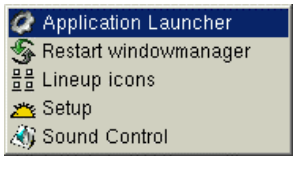


- ***Enable in Startmenu***

The session will appear in the startmenu, which opens up if you press the "IGEL" start button in the lower left corner of the desktop.

- ***Enable in Pulldown Menu***

If you click anywhere on a free space on the desktop with the right mouse button, a menu such as this will come up. By enabling this option, your session will appear here as well.



- ***Enable on Desktop***

The session will appear on the desktop as an icon.

- ***Enable in Application Launcher***

The session will be available in the "***Applications***" tab of the "***Application Launcher***".

- ***Use Hotkey***

Here you may define a hotkey to start the session.

6.4.1 Application Launcher

The “Application Launcher” session is predefined by default.
You may only edit its settings but not delete it.
In case you don’t want it at all, simply disable all starting methods in the “***title***” tab (see above).

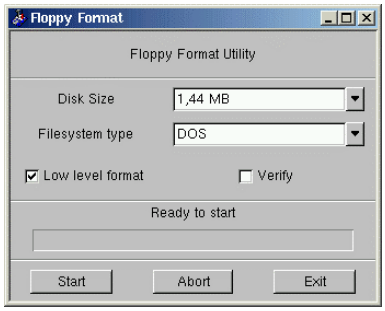
Note: To disable the user to change any session settings, refer to Chapter 5.14.2 “***User Permissions***”.

6.4.2 Setup

The “***Setup***” session is predefined by default as well.
As for the “***Application Launcher***”, it’s not possible to delete this session but to manipulate it.

Note: It may be useful to hide this session in order to prevent misconfiguration by the user. Instead of hiding it, you may also cut down the user setup as shown in 5.14.2 “***User Permissions***”.

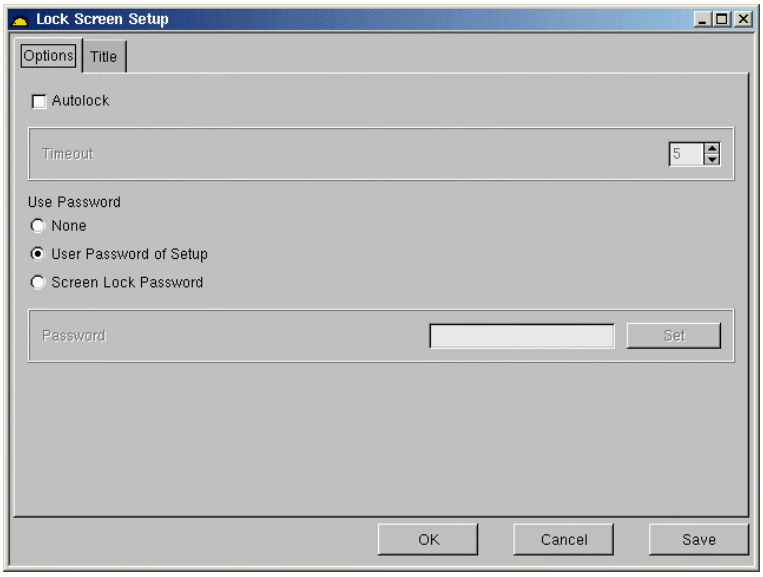
6.4.3 Floppy Format



Use this session if you have locally attached floppy devices and want to format diskettes.
To make this session launchable, edit the predefined one and enable one of the starting methods.

6.4.4 Lock Screen

With this session, you can set up a password-protected screensaver.
Activating “Autolock” will switch from the desktop to the locked screen after the time set in “Timeout”.
You may also start this session from desktop or start menu (if enabled there; see “Title”) to be launched immediately.



6.4.5 Sound Control

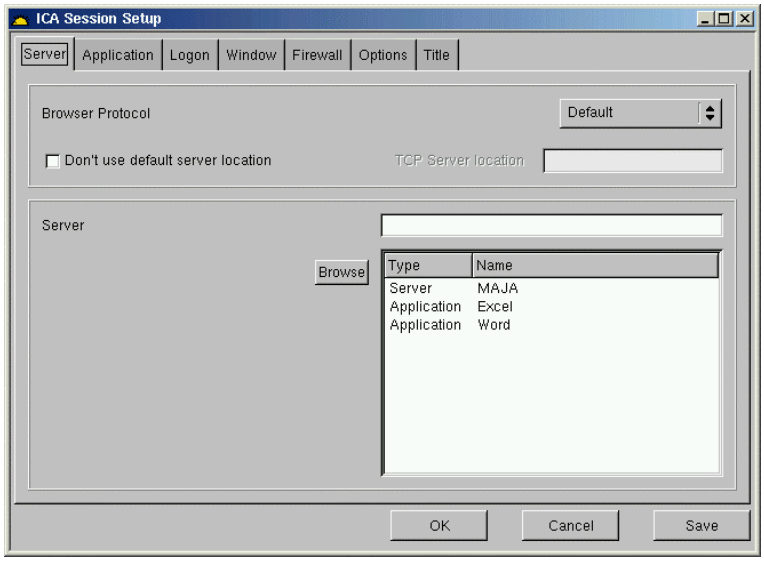
Here you can influence the audio volume and the left-right balance.

6.4.6 ICA

Most of the settings have already been explained in Chapter 5.9 "***ICA (Global ICA Settings)***" across several pages, so we keep a bit briefer here. Many of the settings adjusted in the "***ICA (Global ICA Settings)***" are the defaults for new sessions (called "***global defaults***" below).

Note: The very first source of further details regarding ICA and Metaframe should always be the corresponding documentation from Citrix. This manual only gives some general configuration hints.

Server



- ***Browser Protocol***

Select the needed protocol for broadcast or use the global default set in 5.9.2 ("***Server Location***").
By activating the "***Don't use default server location***" checkbox, you can override the default server for each protocol separately.

- ***Server***

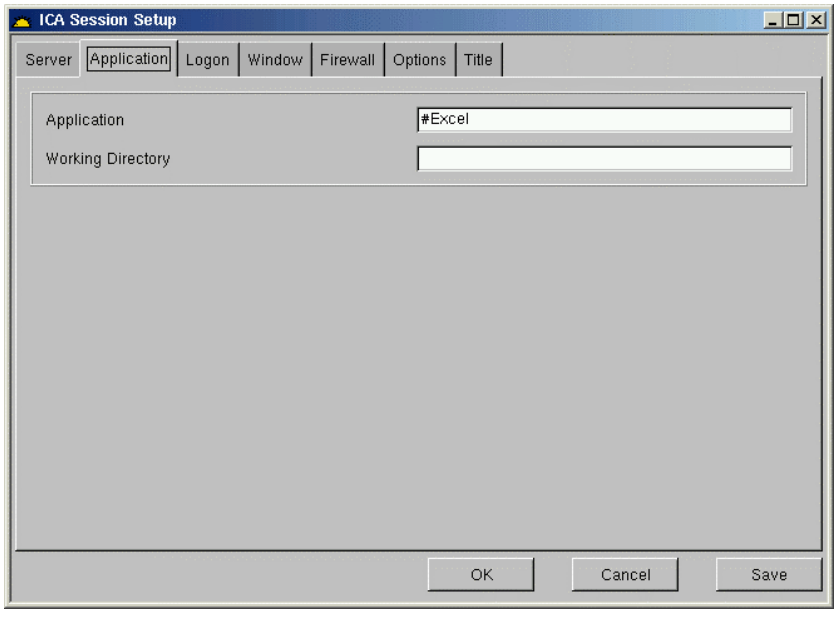
By pressing the "***Browse***" button, you release a broadcast signal asking for all available servers and Published Applications.

In the example above you see one server and two Published Applications:

- Selecting the server will connect the user to the full desktop as if logging in in front of the server itself, providing all applications, rights and settings specified in his user profile (local server profile).
- Choosing one of the Published Applications means that the session will end up in a window containing that one application only and the session will disconnect if you close that application.

You may also enter the IP or the hostname of the server manually into the "***Server***" field.

Application



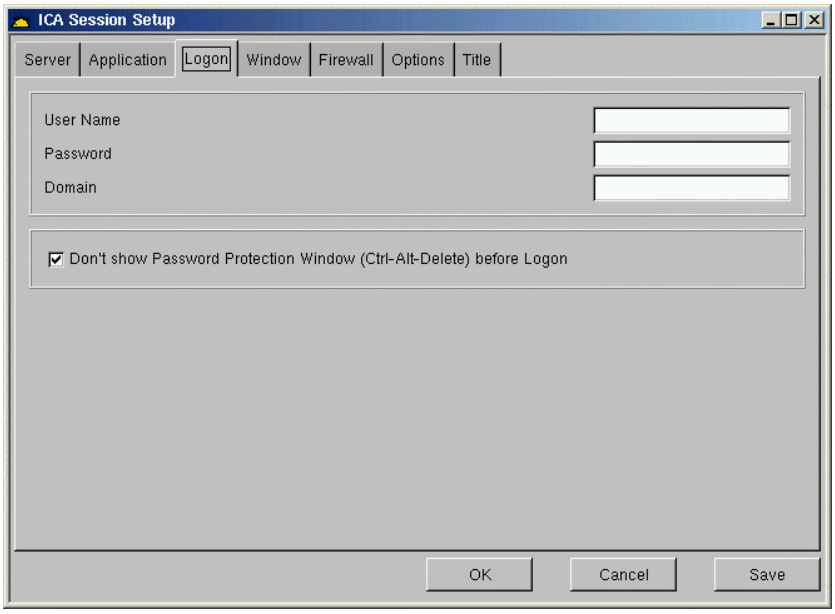
- ***Application***

If you have specified the server manually, you can enter a Published Application here. In case you selected a Published Application from the detected ones, these fields will be filled out automatically.

- ***Working Directory***

In this field you can specify the pathname of the working directory to be used with the application.

Logon



- ***User Name, Password*** and ***Domain*** may be entered here to be used for the ICA session.

They will automatically be handed over to the server so that you don't have to type them into the logon screen.

- ***Don't Show Password Protection Window (Ctr-Alt-Delete) before Logon***

Toggles the "Welcome to Windows" screen on/off.

Note: Please also note the local login module (Chapter 5.9.8) for load balancing!

Window

(Compare Chapter 5.9.1)

- ***Number of Colors***

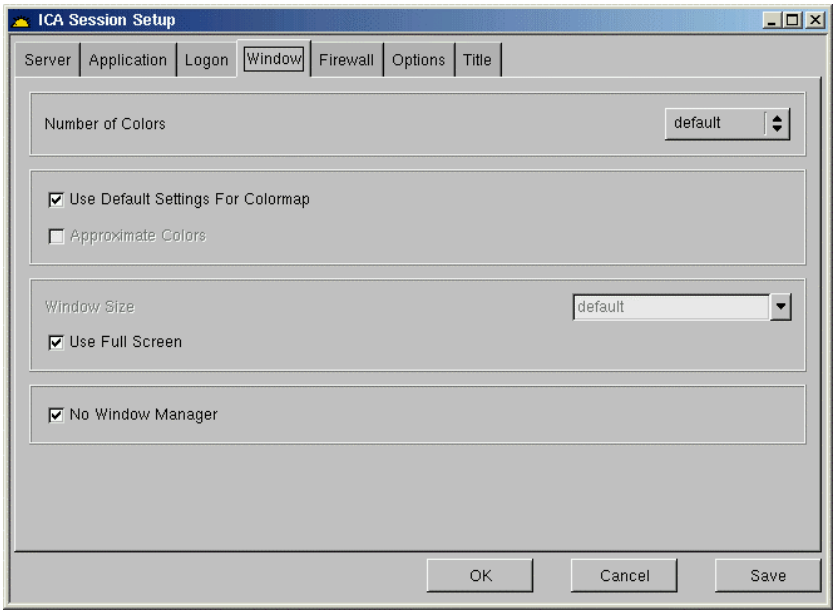
Use the color depth set as global default or alter it for this session.

- ***Use Default Setting for Colormap***

Keep the global default or decide separately if you want to "***Approximate Colors***" for this session.

- ***Window Size***

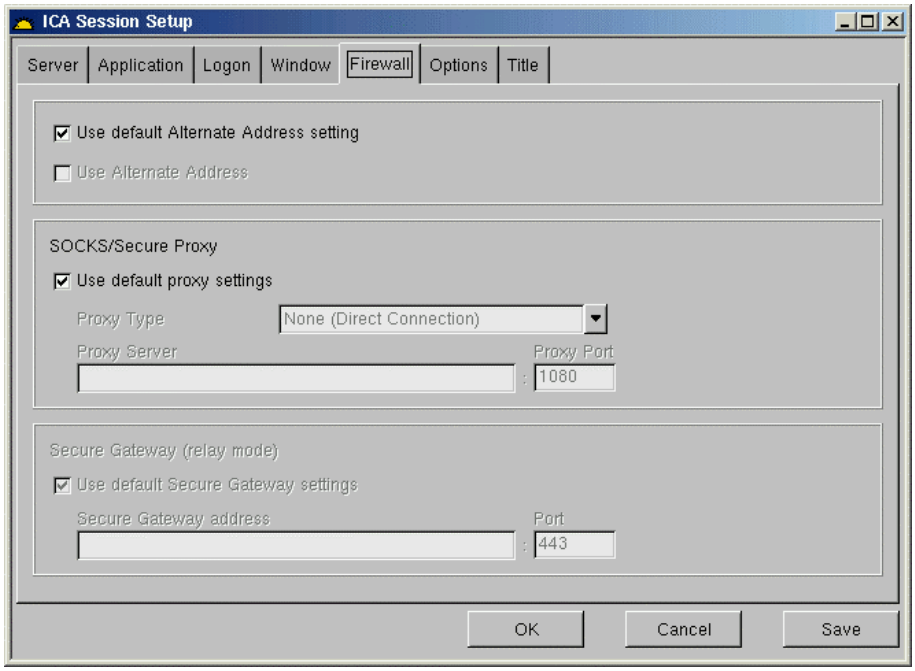
By deactivating "***Use Full Screen***", you may choose between global default and a session-specific one.



- ***No Window Manager***

Press this button to use your configured session without a "Window Manager".
As long as you leave the "Window Manager" enabled, a minimal part of the local desktop will be still visible, whereas when disabled, the session will complete overlay the desktop.

Firewall



- ***Use Default Alternate Address Setting***

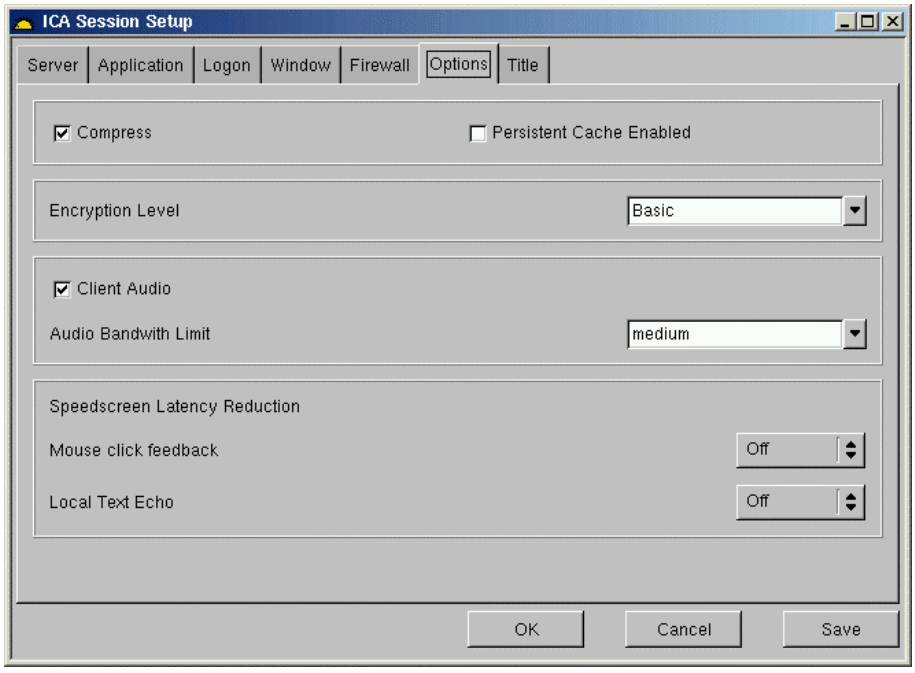
Choose between using the global default or set it for this session separately (compare 5.9.7).

Note: The alternate address itself has to be defined in the "***Address List***" of the "***Server Location***" page of the "***Global ICA Settings"*** (refer to 5.9.2)

- ***SOCKS/Proxy Server***

Same as above; use global defaults or alter for this session. If in doubt, the tooltips are quite helpful.

Options



This is the page to tweak the performance and behavior (see next page for descriptions).

- ***Compress***

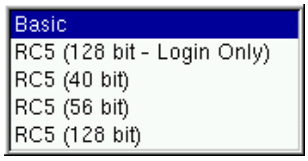
Use data compression to reduce the amount of data transferred across the ICA session.
This lowers the network traffic at the expense of CPU performance.
If you connect your server(s) through WAN, it's recommended to use the compression. If your server is a bit weak and you're in a LAN only, disable this option.

- ***Persistent Cache Enabled***

You have the option to enable the cache (configured in the global ICA settings; see Chapter 5.9.9) for any session. This is useful when using several ICA sessions but only one or two are critical regarding network bandwidth or are heavily used during the day. In that case, you should reserve the cache for those sessions.

- ***Encryption Level***

Encryption increases the security of your ICA connection. By default, basic encryption is enabled, so ensure that the Citrix server supports RC5 encryption before you choose any higher encryption level.



- ***Client Audio***

If enabled, the system sounds and audio from your applications will be transmitted to the Thin Client and emitted out of attached speakers.
The higher the audio quality you choose, the more bandwidth is required to transfer the audio data.

Speedscreen Latency Reduction

"Speedscreen Latency Reduction" improves performance over high latency connections by providing instant feedback to the client in response to keystrokes or mouse clicks.
Both improve the user's sense of sitting in front of a normal PC.

- ***Mouse click Feedback***

This provides visual feedback of a mouse click by immediately changing the mouse pointer into an hourglass indicator.

- ***Local Text Echo***

Accelerates display of the input text, effectively shielding you from experiencing latency on the network.

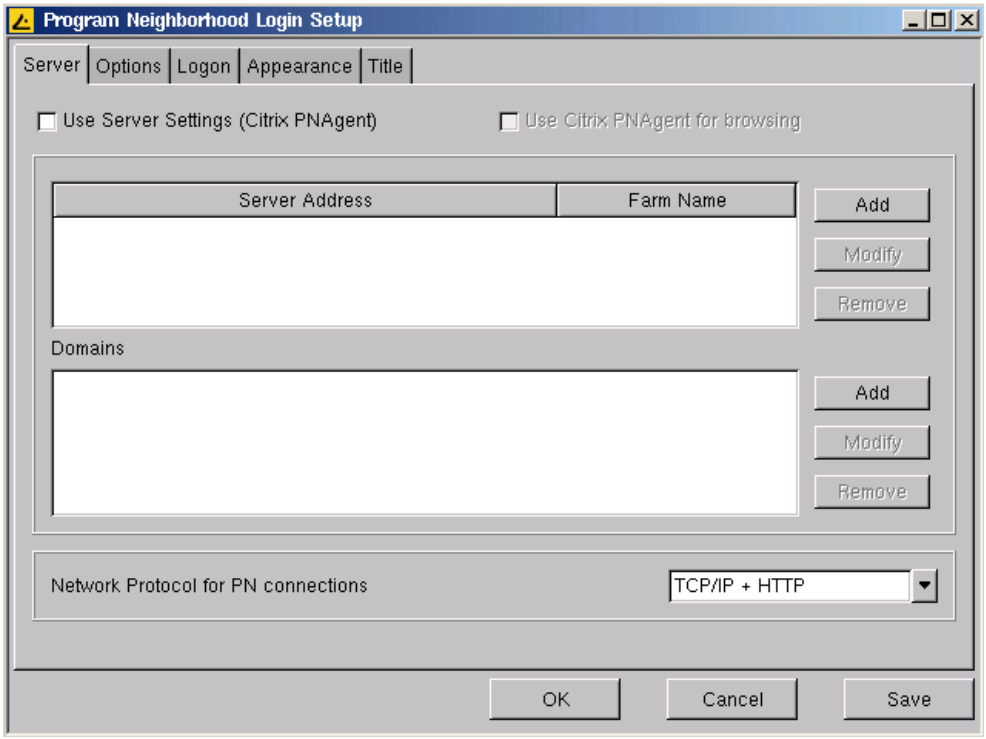
Select a mode from the dropdown list:

- Set the mode to ***"ON"*** for slower connections (connection over a WAN) to decrease the delay between user input and screen display.
- Set the mode to ***"OFF"*** for faster connections (connection over a LAN).
- Set the mode to ***"AUTO"*** if you are not certain of the connection speed.

Note: Speedscreen has to be enabled and configured on the Citrix server first in order to work.

6.4.7 ICA Program Neighborhood

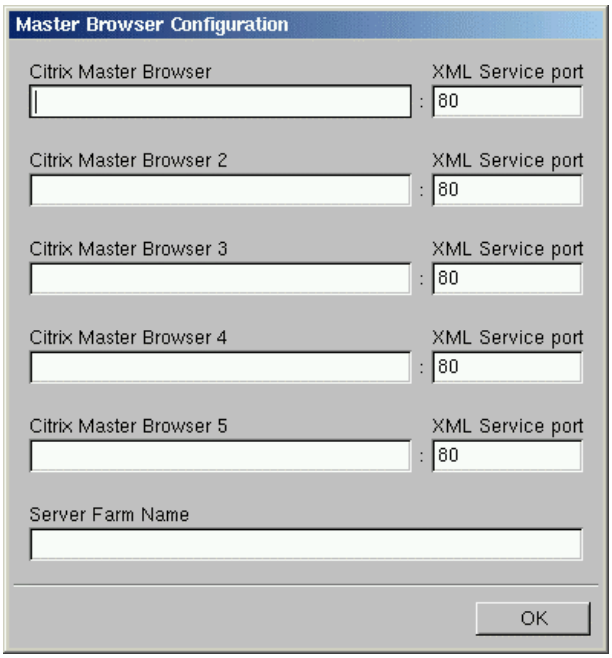
Most of the settings have already been dealt with in "***Global ICA Settings***" (Chapter 5.9) as well as in the ICA session setup (Chapter 6.4.6).



Define the Master Browsers to be browsed for published applications.

You can set up to 5 Master Browsers per domain (see right). In case the first one is not reachable, the second one will be consulted and so forth.

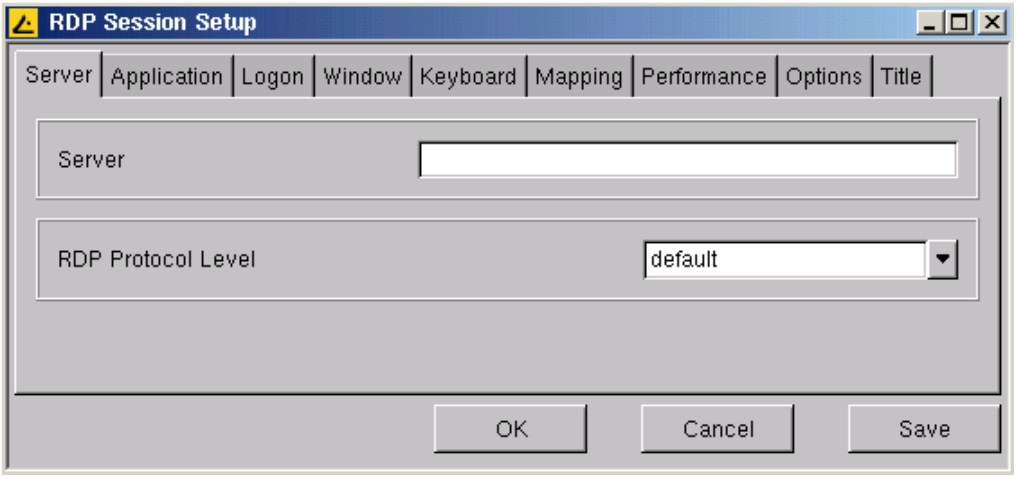
Please note that multi-farm browsing is supported! So you can define Master Browsers for several server farms.



6.4.8 RDP

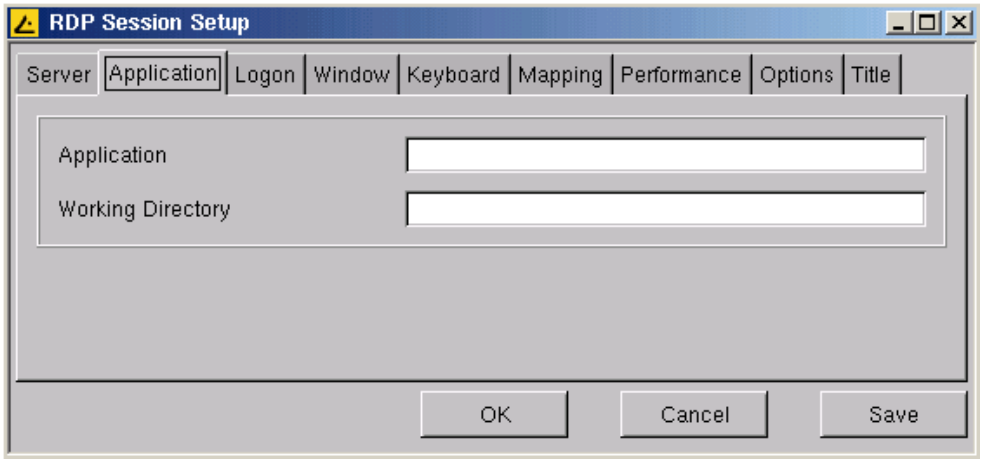
RDP (Remote Desktop Protocol) is used to connect to Microsoft servers without using Citrix Metaframe. It is already built in in most of the Microsoft server products.

Server



Enter the IP or the hostname of the server you want to connect to.
In case you want to use the name, ensure that the terminal has a nameserver reachable for the name resolution.

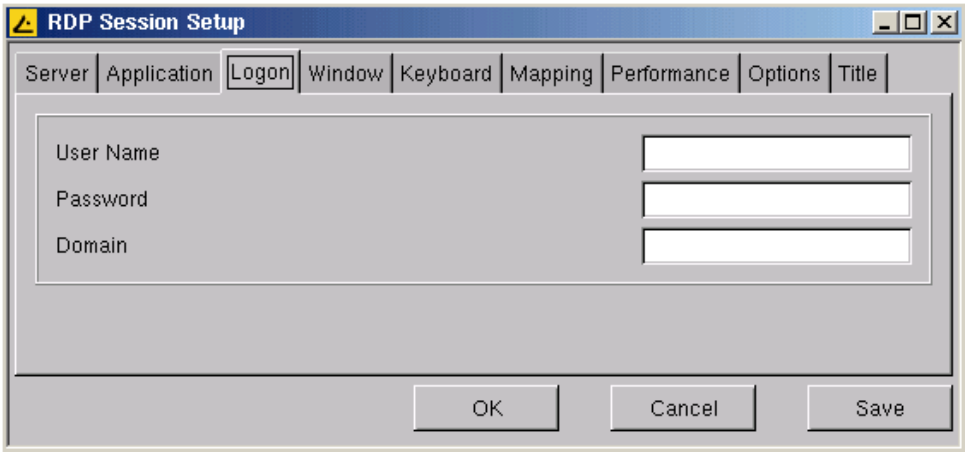
Application



Application
Specify the application you want to be launched on connect.
Enter the application name (e.g. iexplore.exe).

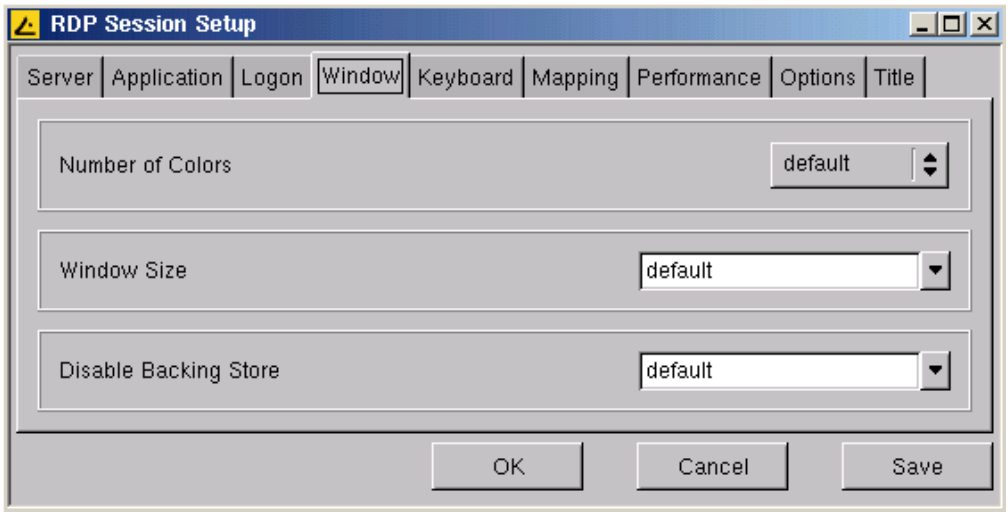
Working Directory
In this field you then have to specify the working directory (e.g. C:\Program Files\Internet Explorer)
If the requested application is not launchable from the “Run…” dialog on the server start menu, this is also the directory where the requested file has to be located.

Logon



In this mask, you can enter static ***User Name, Password*** and the ***Domain*** for the session.
This is useful if you don't want to enter this over and over again.
If no login information is provided here, the normal login prompt will come up.

Window

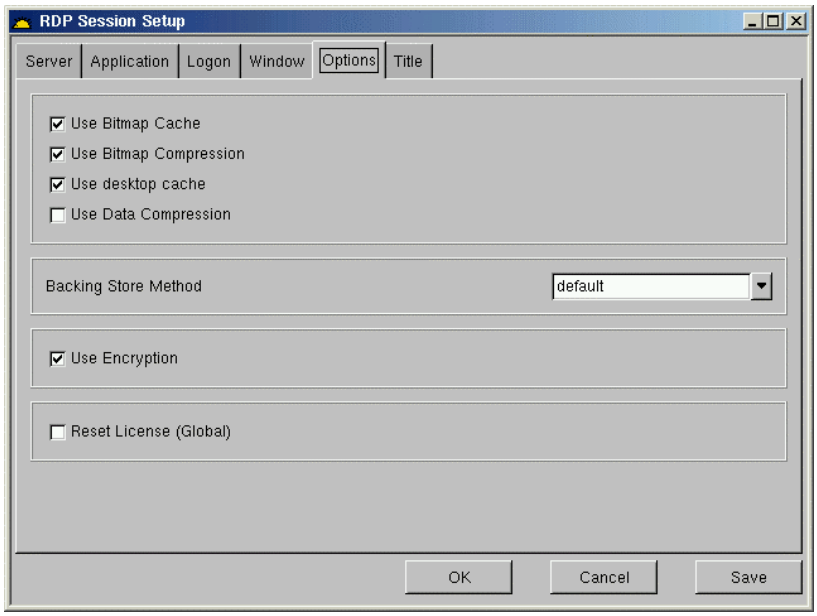


Window Size
Leave the full screen mode active or choose one of the available resolutions to manually define the window size for this RDP session.

Private Color Map
If the color depth of the X-Server is set to 256 Colors, possibly too few colors will be left available for the RDP session, causing graphics malfunction.
Having the "***Private Color Map***" enabled eliminates this behavior by forcing RDP to use its own separate color map.

Enable Window Manager Key Bindings
If enabled, the local X-Server hotkeys (like CTRL+ESC or CTRL+ALT+TAB) are valid.
In case you want to use the Windows server hotkeys instead, disable this option.

Options



The options "***Use Bitmap Cache", "Use Bitmap Compression***

- ***Use Desktop Cache***

and

- ***Use Data Compression***

are currently not supported by the new Rdesktop client 1.2.

- ***Backing Store Method***

This option allows you to choose the Backing Store Method for session-windows that are hidden.

- ***Use Encryption***

Encryption increases the security of your RDP sessions. This option may only be disabled for connections to NT4 servers. Since Win2000, encryption is necessary to be allowed to connect.

- ***Reset License (Global)***

Since Rdesktop 1.2 (since firmware 3.01.310), the so-called "token" for the Microsoft CAL (client access license) is stored locally on the IGEL Thin Client.
In case you had to reinstall your license server or have any other reason to clear the client's token, enable this checkbox. After the next reboot, it will automatically be disabled again.

6.4.9 Browser

Depending on the model of your IGEL Thin Client, the version and or kind of implemented browser differs. By default, Firefox is installed

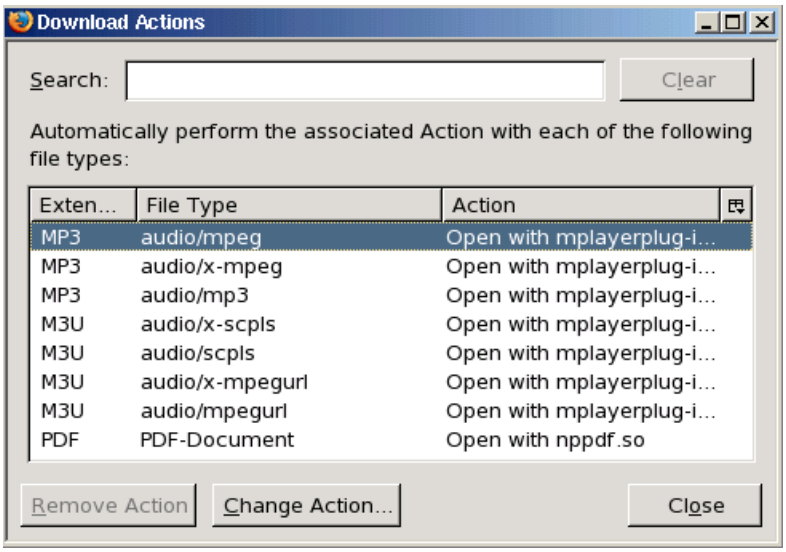
We made browsers most configurable via the session setup, so that you can virtually manipulate everything you are accustomed to on a PC.

Firefox

Firefox is currently the first choice in Linux browsers when it comes to performance and compatibility. It already comes along with the most needed plug-ins pre-installed (depends on model):

- Acrobat PDF-Reader
- Flash Player

To get further information about the installed plug-ins and their exact versions, use the menu path Edit -> Preferences -> Downloads -> View Actions.

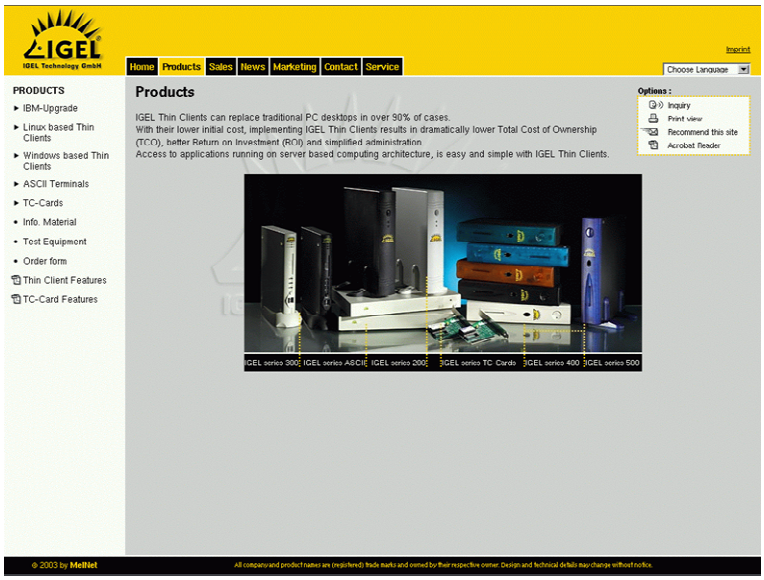


For more information on browser settings please refer to the online help of Firefox browser.

Kiosk Mode

You can strip down the browser as shown right. You can also disable every configurability (like the URL bar) so that users may only surf by clicking links on the displayed web pages. In this way you can limit Internet access to specific sites, as long as they have no links to outside pages.

There is another setting, telling the system not to keep any setting changes. This means during the next reboot, your defined settings will be loaded again.

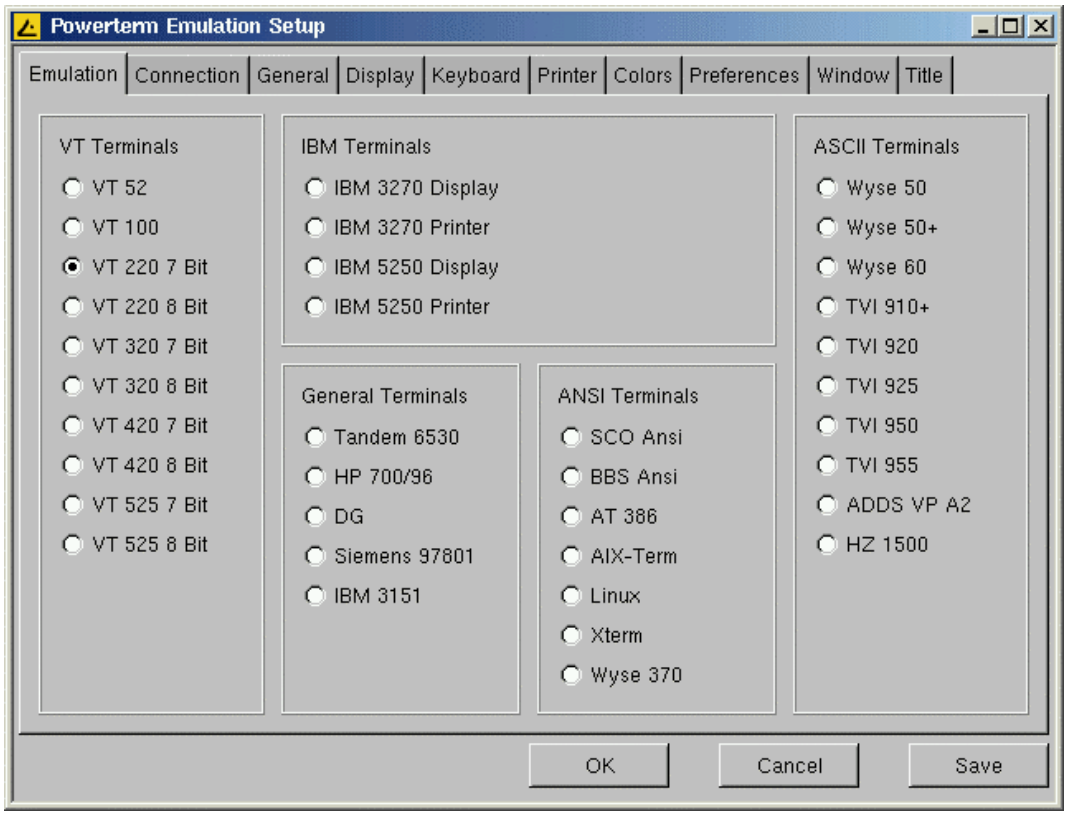


6.4.10 PowerTerm (Terminal Emulation)

The PowerTerm Interconnect/32 software we use in flash Linux is the official Linux version from ERICOM Software Ltd.

- **PowerTerm Emulation Setup**

After you have chosen the “PowerTerm” session type in the “Add a New Session” procedure described in section 6.3.1, the following “PowerTerm Emulation Setup” appears on the screen: (This is also a good overview of what emulation types are supported.)



We have tried to make the appearance of the setup pages used here as similar as possible to the appearance of the setup pages described in the original “PowerTerm Manual” of ERICOM Software Ltd.
So for detailed information about configuring the PowerTerm Software please refer to the “PowerTerm Manual” available on the IGEL FTP-server at ftp://ftp.igel.de/pub/manual/Partner-Documentation

6.4.11 XTERM (Local Application)

With an XTERM session, you can execute local commands via shell.
(this is a kind of DOS prompt, if you have to compare it to Windows.)

6.4.12 Application via RSH

This section describes how to configure an “RSH Session” that can be used to start a remote application via RSH (Remote Shell) on a host and display it on the terminal.

After you have chosen the “Application via RSH” session type in the “Add a New Session” procedure described in section 6.3.1, the following “Application via RSH Setup” appears on the screen.

Command

Use this “Command” page to provide all necessary entries to create an executable command to start an application remote via RSH.

- ***Remote Username***

In this field you have to enter the name of the remote user. Be sure the chosen user has a user account on your remote host.

- ***Remote Host***

In this field you have to enter the name or the IP address of the remote host from which the remote application will be started.

- ***Commandline***

In this field you can specify the name of the application program you want to start.

- ***Display***

This dropdown list allows you to choose between different forms of syntax for the “display” option that depends on the application type you want to start.

The display number (in this example 192.168.0.179:0.0) will be added to the command line automatically.

Important Note:

Because of the strict access restrictions on all UNIX systems, you have to make sure that all the necessary configurations (e.g. editing the files /etc/hosts.equiv and/or .rhosts) on the Unix host are made to allow rsh access from the terminal.

Also the terminal display has an access control that is activated by default. If you disable this “Access Control” it would be possible for everybody from any UNIX host to have access to your terminals display.

To allow a host to have access to the terminals display, its name (not the IP address) must be added into a “***List of Trusted X Hosts***”. (Please refer to section 5.4.2.4).

Note: For detailed information about RSH and its authentication methods, please refer to the corresponding “man-pages” of your server operating system.

6.4.13 Application via SSH

This section describes how to configure a “SSH Session” that can be used to start a remote application via SSH (Secure Shell) on a host and display it on the terminal.

SSH provides secure encrypted communications between two hosts (or host and terminal) over an insecure network. X11 connections can also be forwarded over this secure channel.

- **Application via SSH Setup**

After you have chosen the “Application via SSH” session type in the “Add a New Session” procedure described in earlier section 6.3.1, the following “Application via SSH Setup” appears on the screen.

Command

Use this “Command” page to provide all necessary entries to create an executable command to start an application remote via SSH.

- ***Remote Username***

In this field you have to enter the name of the remote user. Be sure the chosen user has a user account on your remote host.

- ***Remote Host***

In this field you have to enter the name or the IP address of the remote host from which the remote application will be started.

- ***Commandline***

In this field you can specify the name of the application program you want to start.

- ***Display***

This pulldown menu allows you to choose between different forms of syntax for the “display” option that depends on the application type you want to start.
The display number (in this example 192.168.0.179:0.0) will be added to the commandline automatically

Options

- ***Enable X11 Connection Forwarding***

X11 connections will be automatically forwarded to the remote side in such a way that any X11 program started from the shell (or command) will go through the encrypted ssh channel. The authentication data will also be set automatically. This option is enabled by default.

- ***Enable compression***

Use compression to reduce the amount of data transferred across the data channel. Default disabled

- ***Force Protocol Version***

You must prove your identity to the remote host using one of several identification methods that depend on the protocol version used. This section allows you to force the protocol version after you have decided what method of identification will be used.

Note: For detailed information about SSH and its different authentication methods please refer to the corresponding “man pages” of your server operating system.

7 Appendix: Hardware Configuration

	IGEL Series Name	Smart	Compact	Winestra	Premium	
	IGEL Models Name	2100 LX	3200 LX	4200 LX	5200 LX	5300 LX
	Embedded Operating System	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux
HARDWARE BASIS	Flash Disk Size	128 MB	128 MB	128 MB	128 MB	256 MB
	RAM Size	128 MB	128 MB	128 MB	128 MB	256 MB
	RAM expandable up to	1024 MB	1024 MB	1024 MB	1024 MB	1024 MB
	CPU Speed	400 MHz	533 MHz	800 MHz	1 GHz	1 GHz
	CPU Type	VIA Eden	VIA Eden	VIA C3 LP	VIA C3 LP	VIA C3 LP
	Video RAM	8 MB UMA	8 MB UMA	8 MB UMA	8 MB UMA	8 MB UMA
	VGA Chipset	VIA CLE266	VIA CLE266	VIA CLE266	VIA CLE266	VIA CLE266
	Max. VGA Resolution at 16 Bit	1600 x 1200	1600 x 1200	1600 x 1200	1600 x 1200	1600 x 1200
	Max. VGA Resolution at 24 Bit	1600 x 1200	1600 x 1200	1600 x 1200	1600 x 1200	1600 x 1200
	AC'97 compliant Audio Chipset	✓	✓	✓	✓	✓
ENVIRONMENTAL	Fanless Construction (convection)	✓	✓	✓	✓	✓
	Steel Housing	✓	✓	✓	✓	✓
	Power Supply	external	internal	external	external	external
	Power (max. consumption)	20 Watt	30 Watt	48 Watt	48 Watt	48 Watt
	Power Frequency (single phase)	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz
	Operating Temperature	0to35℃ 32to95℉	0to35℃ 32to95℉	0to35℃ 32to95℉	0to35℃ 32to95℉	0to35℃ 32to95℉
	Storage Temperature	-20to60℃ -4to140℉	-20to60℃ -4to140℉	-20to60℃ -4to140℉	-20to60℃ -4to140℉	-20to60℃ -4to140℉
	Relative Humidity (non-condensing)	5% to 95%	5% to 95%	5% to 95%	5% to 95%	5% to 95%
	Line Voltage (autosensing)	100 - 240 V AC	100 - 240 V AC	100 - 240 V AC	100 - 240 V AC	100 - 240 V AC
	Dimensions of Unit (H x W x D in mm)	215 x 35 x 215	240 x 43 x 225	290 x 53 x 230	290 x 53 x 230	290 x 53 x 230
	Dimensions of Unit (H x W x D in inch)	8.46 x 1.38 x 8.46	9.45 x 1.69 x 8.86	11.42 x 2.09 x 9.06	11.42 x 2.09 x 9.06	11.42 x 2.09 x 9.06
	Weight of Unit	1,8 Kg - 4 Lbs	2,5 Kg - 5.5 Lbs	3,3 Kg - 7.26 Lbs	3,4 Kg - 7.48 Lbs	3,4 Kg - 7.48 Lbs
PHYSICAL CONNECTIVITY	2 * PS/2 Port (mouse and keyboard)	✓	✓	✓	✓	✓
	Number of DB9 Pin Serial Ports	1	2	2	2	2
	DB 25 Pin Parallel Port	✓	✓	✓	✓	✓
	Number of USB 2.0 Ports (front / back)	2 - 0	1 - 2	2 - 2	2 - 2	2 - 2
	RJ 45 10/100BaseT Port (autosensing)	✓	✓	✓	✓	✓
	DB 15 Pin VESA Monitor Port	✓	✓	✓	✓	✓
	Digital Video Interface (DVI-I)	-	-	-	✓ *	✓ *
	16 Bit Stereo Sound Ports	✓	✓	✓	✓	✓
	Built-In Speaker	✓	✓	✓	✓	✓
	PCMCIA Socket Onboard	-	-	-	✓	✓
	Free PCI Slot	-	-	✓	✓	✓
SUPPORTED HARDWARE	Wireless LAN supported via	USB	USB	USB + PCI	USB+PCI+PCMCIA	USB+PCI+PCMCIA
	AVM Fritz PCI (ISDN,ISDN/DSL,DSL)	-	-	✓	✓	✓
	Touchscreen (Elo- + Microtouch)	✓	✓	✓	✓	✓
	IBM122 + Trimodal + SUN Keyboards	✓	✓	✓	✓	✓
	Analog Modem	external	external	ex- + internal	ex- + internal	ex- + internal
	Token Ring Card PCI	-	-	✓	✓	✓
	Fiber Optics Card	-	-	✓	✓	✓
	Smartcard Reader (internal)	-	built-in	optional	built-in	built-in
	USB Mass Storage Support	✓	✓	✓	✓	✓

* max. Resolution DVI is 1280 x 1024
- Changes and errors excepted -

	IGEL Series Name	Legacy Terminals		Netvista Upgrades	TC Cards
	IGEL Models Name	1100 Legacy	5100 X-Term	2210 / 2810	TC5200-CF LX
	Embedded Operating System	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux	IGEL Flash Linux
HARDWARE BASIS	Flash Disk Size	128 MB	128 MB	128 MB	128 MB
	RAM Size	128 MB	128 MB	Depends on Hardware of target System	
	RAM expandable up to	1024 MB	1024 MB		
	CPU Speed	400 MHz	1 GHz		
	CPU Type	VIA Eden	VIA C3 LP		
	Video RAM	8 MB UMA	8 MB UMA		
	VGA Chipset	VIA CLE266	VIA CLE266		
	Max. VGA Resolution at 16 Bit	1600 x 1200	1600 x 1200		
	Max. VGA Resolution at 24 Bit	1600 x 1200	1600 x 1200		
	AC'97 compliant Audio Chipset	✓	✓		
ENVIRONMENTAL	Fanless Construction (convection)	✓	✓		
	Steel Housing	✓	✓		
	Power Supply	external	external		
	Power (max. consumption)	20 Watt	48 Watt		
	Power Frequency (single phase)	50 - 60 Hz	50 - 60 Hz		
	Operating Temperature	0to35℃ 32to95℉	0to35℃ 32to95℉		
	Storage Temperature	-20to60℃ -4to140℉	-20to60℃ -4to140℉		
	Relative Humidity (non-condensing)	5% to 95%	5% to 95%		
	Line Voltage (autosensing)	100 - 240 V AC	100 - 240 V AC		
	Dimensions of Unit (H x W x D in mm)	215 x 35 x 215	290 x 53 x 230		
	Dimensions of Unit (H x W x D in inch)	8.46 x 1.38 x 8.46	11.42 x 2.09 x 9.06		
	Weight of Unit	1,8 Kg - 4 Lbs	3,4 Kg - 7.48 Lbs		
PHYSICAL CONNECTIVITY	2 * PS/2 Port (mouse and keyboard)	✓	✓		
	Number of DB9 Pin Serial Ports	1	2		
	DB 25 Pin Parallel Port	✓	✓		
	Number of USB 2.0 Ports (front / back)	2 - 0	2 - 2		
	RJ 45 10/100BaseT Port (autosensing)	✓	✓		
	DB 15 Pin VESA Monitor Port	✓	✓		
	Digital Video Interface (DVI-I)	-	✓ *		
	16 Bit Stereo Sound Ports	✓	✓		
	Built-In Speaker	✓	✓		
	PCMCIA Socket Onboard	-	✓		
	Free PCI Slot	-	✓		
SUPPORTED HARDWARE	Wireless LAN supported via	USB	USB+PCI+PCMCIA	USB/USB+PCI	USB + PCI
	AVM Fritz PCI (ISDN,ISDN/DSL,DSL)	-	✓	-	✓
	Touchscreen (Elo- + Microtouch)	✓	✓	✓	✓
	IBM122 + Trimodal + SUN Keyboards	✓	✓	✓	✓
	Analog Modem	external	ex- + internal	external	external
	Token Ring Card PCI	-	✓	- / ✓	✓
	Fiber Optics Card	-	✓	-	-
	Smartcard Reader (internal)	-	-	-	optional
	USB Mass Storage Support	✓	-	- / ✓	✓

* max. Resolution DVI is 1280 x 1024
- Changes and errors excepted -