



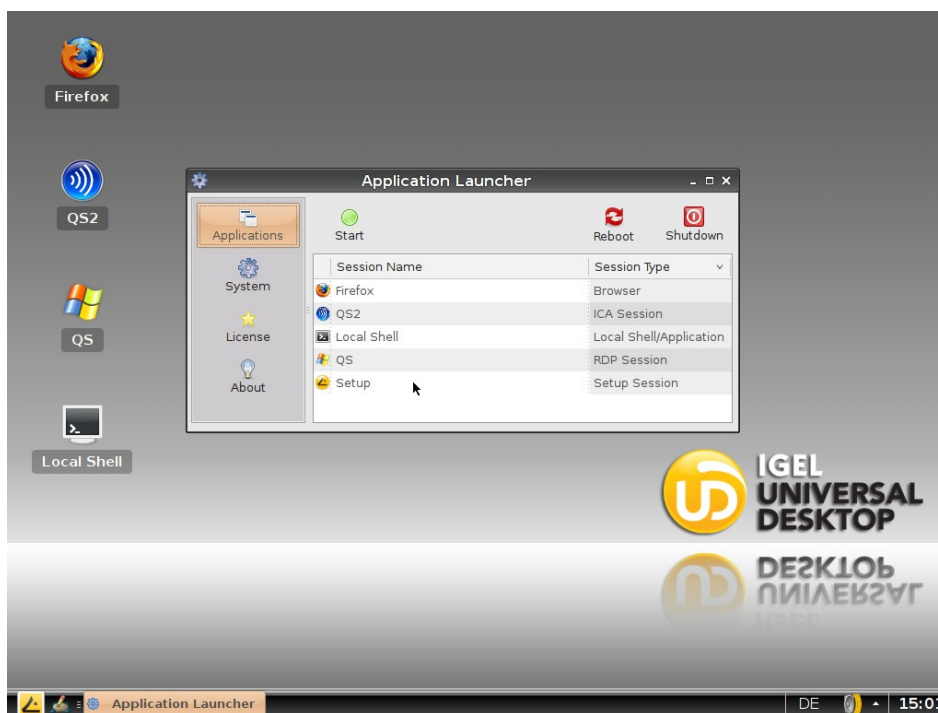
IGEL Thin Clients



IGEL
UNIVERSAL
Firmware

Universal Desktop User Guide

For IGEL Thin Clients with IGEL Flash Linux



Important Information

Copyright

This publication is protected under international copyright laws, with all rights reserved. No part of this manual, including the products and software described in it, may be reproduced, manipulated, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of IGEL Technology GmbH.

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 disclaim 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 Technology GmbH.

Microsoft™ Windows™ is a registered trademark of Microsoft Corporation.

Java™ is a registered trademark of Sun Microsystems, Inc.

VMware™ is a registered trademark of VMware, Inc.

PowerTerm™ WebConnect™ and PowerTerm™ InterConnect™ are registered trademarks of Ericom Software.

CUPS™ and the CUPS logo are trademarks of Apple 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 intended 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. This version is based on firmware 4.02.100.

Copyright © 2009 IGEL Technology GmbH. All Rights Reserved.

Table of Contents

1 INTRODUCTION.....	1
2 QUICK INSTALLATION.....	2
3 BOOT PROCEDURE.....	3
3.1 Boot Menu.....	3
3.1.1 Quiet Boot.....	3
3.1.2 Verbose Boot.....	3
3.1.3 Emergency Boot.....	3
3.1.4 Reset to Default Factory Settings.....	3
3.2 Networking.....	3
3.3 X Server.....	3
4 APPLICATION LAUNCHER.....	4
4.1 General System Information.....	4
4.2 Application List.....	5
4.3 System Update.....	5
4.4 Reboot and Shutdown.....	5
5 SETUP APPLICATION.....	5
5.1 Starting the Setup.....	5
5.2 Leaving the Setup.....	5
5.3 Setup Sections.....	6
5.3.1 Sessions.....	6
5.3.2 Accessories.....	6
5.3.3 User Interface.....	6
5.3.4 Network.....	6
5.3.5 Devices.....	6
5.3.6 Security.....	7
5.3.7 System.....	7
5.4 Search for Setup pages.....	7
6 SYSTEM SETTINGS.....	7
6.1 Tool tips (System Section).....	7
6.2 Language.....	7
6.3 Time and Date.....	7
6.4 Update.....	8
6.4.1 Buddy Update.....	8
6.5 Remote Management.....	8
6.6 Shadowing.....	8
6.7 SSH Remote Access.....	9
6.8 Service Information.....	9
6.9 IGEL System Registry.....	9
7 USER INTERFACE.....	10
7.1 Input.....	10
7.1.1 Keyboard (and Additional Keyboard).....	10
7.1.2 Mouse.....	10
7.1.3 Touch Screen.....	11
7.2 Display.....	12
7.2.1 Global Display Settings.....	12
7.2.2 DPMS.....	12
7.2.3 XDMCP.....	13
7.2.4 Access Control.....	13
7.2.5 Desktop.....	14
7.3 Font Services.....	16
7.3.1 XC Font Service.....	16
7.3.2 NFS Font Service.....	16

7.4	Screen Saver.....	16
7.5	Hotkeys → Commands.....	16
8	NETWORK.....	17
8.1	Main Network Settings.....	17
8.2	Interfaces.....	18
8.2.1	Authentication.....	19
8.2.2	Interface 2.....	20
8.2.3	Wireless.....	21
8.3	Dial Up Connections.....	21
8.3.1	ADSL.....	21
8.3.2	PPTP.....	22
8.4	Routing.....	22
8.5	Hosts.....	22
8.6	Network Drives.....	23
8.7	NFS.....	23
8.7.1	SMB (Windows Drive).....	23
9	SESSIONS.....	24
9.1	ICA (Global ICA Settings).....	24
9.1.1	Window.....	24
9.1.2	Server Location.....	25
9.1.3	Keyboard (Hotkey Mapping).....	25
9.1.4	Drive Mapping.....	26
9.1.5	COM Ports.....	26
9.1.6	Printer.....	27
9.1.7	Firewall.....	27
9.1.8	Logon.....	28
9.1.9	Options.....	28
9.2	ICA Sessions.....	29
9.2.1	Connections.....	29
9.2.2	Logon.....	29
9.2.3	Window.....	29
9.2.4	Firewall.....	30
9.2.5	Options.....	30
9.2.6	Reconnect.....	31
9.3	ICA Program Neighborhood.....	31
9.3.1	Options.....	31
9.3.2	Logon and Logoff.....	31
9.3.3	Appearance.....	32
9.3.4	Password Change.....	32
9.3.5	Reconnect and Refresh.....	32
9.4	RDP (Global RDP Settings).....	32
9.4.1	Window.....	32
9.4.2	Server.....	32
9.4.3	Drive Mapping.....	32
9.4.4	COM Ports.....	33
9.4.5	Printer.....	33
9.4.6	Sound/Keyboard.....	33
9.4.7	Performance.....	33
9.4.8	Options.....	33
9.5	RDP Session.....	33
9.5.1	Server and Logon information.....	33
9.5.2	Display, Keyboard and Mapping settings.....	34
9.5.3	Performance and Options.....	34
9.6	VMware View Client.....	34
9.7	Quest vWorkspace Client.....	34
9.8	Leostream Connection Broker.....	34

9.9 Appliance Mode.....	34
9.10 Nomachine NX.....	34
9.11 SSH Session.....	35
9.12 ThinLinc.....	35
9.13 PowerTerm WebConnect.....	36
9.14 PowerTerm Terminal Emulation.....	36
9.15 X Session.....	36
9.16 Firefox Browser Global.....	37
9.17 Firefox Browser Session.....	37
9.18 SAP Client.....	37
9.19 MPlayer.....	38
9.19.1 License.....	38
9.19.2 Download Codecs.....	38
9.19.3 Video Settings.....	38
9.19.4 Audio.....	38
9.19.5 Options.....	38
9.19.6 Hotkeys.....	38
9.19.7 Browser Plug In.....	38
9.20 Java Web Start Session.....	38
9.21 VoIP Client.....	38
10 ACCESSORIES.....	39
10.1 Xterm.....	39
10.2 Card Reader.....	39
10.3 Setup and Application Launcher.....	39
10.4 Sound Mixer.....	39
10.5 Java Manager.....	39
10.6 USB Storage Restart.....	39
10.7 Kerberos Logout.....	39
10.8 Network Tools.....	40
10.8.1 Device Information.....	40
10.8.2 Ping.....	40
10.8.3 Netstat.....	40
10.8.4 Traceroute.....	40
10.8.5 Lookup.....	40
11 DEVICES.....	41
11.1 Hardware Information.....	41
11.2 Printer.....	41
11.2.1 CUPS (Common UNIX Printing System).....	41
11.2.1.1 IPP Printer Sharing.....	41
11.2.2 LPD (Line Printer Demon).....	41
11.2.3 TCP/IP.....	42
11.2.4 ThinPrint.....	42
11.3 USB Storage Devices	43
11.3.1 Storage Hot plug.....	43
11.3.2 Automount Devices.....	43
11.4 PC/SC.....	44
12 SECURITY.....	44
12.1 Password.....	44
12.2 Kerberos.....	44
13 IGEL SMARTCARD SOLUTION.....	45
14 CUSTOM PARTITION ON COMPACT FLASH.....	47

1 Introduction

Welcome

Congratulations on purchasing an IGEL Thin Client. IGEL Thin Clients with Universal Desktop are composed of state-of-the-art hardware and an operating system either based on the IGEL Flash Linux Technology or Microsoft Windows Embedded Standard®. We have done our best to deliver an excellent product and we promise to provide support and service of the same quality.

The IGEL Universal Desktop

The software, or firmware, embedded in every IGEL Universal Desktop is highly multi-functional and contains the industry's largest collection of server-based protocols or "digital services" for connecting you to all your centralized applications. There is only one version of firmware for each operating system we offer; Linux, Windows Embedded Standard 2009 and Windows Embedded CE. So that you only pay for what you need, the digital services are available in three packs; Entry, Standard and Advanced.

The IGEL Setup application structure now is the same on all devices and the Management Suite; so you will have no problems switching between the local and remote configuration tools, all configuration parameters are to be found in the same tree structure now.

Each Universal Desktop comes with IGEL's Universal Management Suite; an extremely powerful yet easy to use software application that allows you to remotely deploy and manage your Thin Client estate. This keeps TCO to a minimum and ensures maximum desktop productivity and up-time.

How to use this Guide

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

This guide is divided into the following chapters:

- | | |
|------------------------------|--|
| 1. Introduction | Welcome and User Guide Information |
| 2. Quick Installation | Instructions for a Quick Installation |
| 3. Boot Procedure | Information about the Boot Process |
| 4. Setup | Configuration of the Global and Session Settings |

Note: All screen shots and descriptions refer to the *Advanced* firmware status of the IGEL Universal Desktop Series. Some applications may not be available within the *Entry* or *Standard* firmware versions. In case you need further support that your dealer or distributor cannot provide you may use our online support form at www.igel.com (section *Service & Support*).

2 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 or DVI monitor, an AT compatible keyboard with PS/2 or USB connector, a USB mouse, LAN via RJ45 and AC power.
- Boot the terminal and wait until the graphical desktop has started and the window of the Application Launcher appears on the screen and run Setup application.
- Set system language and keyboard layout (User Interface → Language)
- Set display resolution (User Interface → Display).
- Complete the terminal setup program by entering a local IP address in the *Network* section of the setup 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: Nearly 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.

3 Boot Procedure

3.1 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 choose between three 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**

3.1.1 Quiet Boot

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

3.1.2 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.

3.1.3 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 640x480 – 60 Hz and finally starts directly into the setup. This is very useful if you selected a too high screen resolution or configured a wrong mouse type.

3.1.4 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 this. 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.com in the “service” section. Provide the displayed *terminal key* and the stated firmware version and, of course, your contact data. The *terminal key* will be displayed after pressing *Enter* three times. 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.)

3.2 Networking

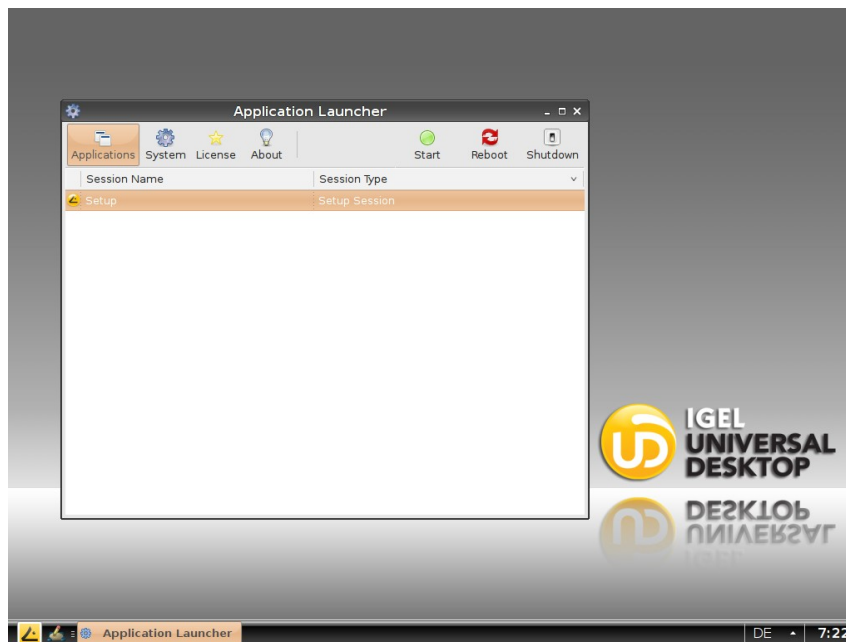
After loading the kernel the network configuration follows. Three different ways can be chosen to include the terminal in the network environment. According to the settings of the terminal, DHCP, BOOTP or manual configured IP address can be used.

3.3 X Server

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

4 Application Launcher

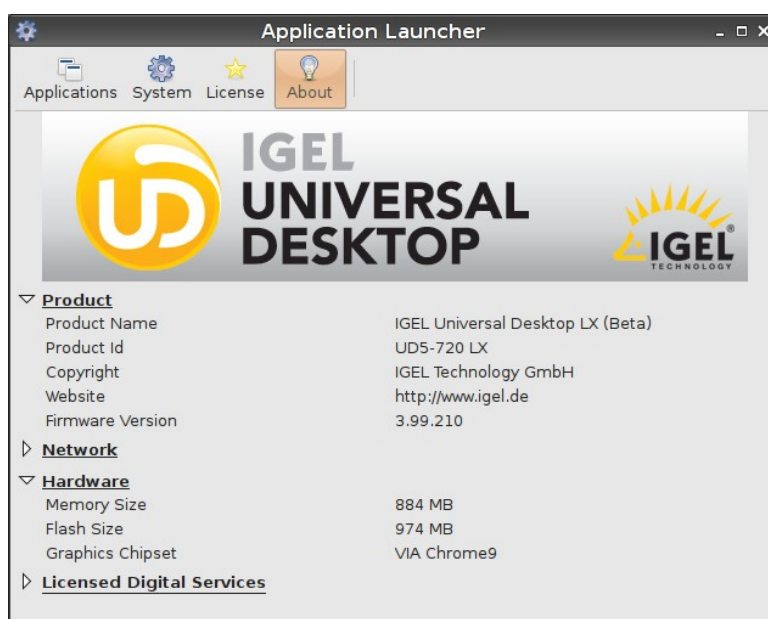
After the boot procedure has completed, a desktop such as the above will be displayed on the screen.



The *Application Launcher* starts automatically because it is set to autostart and 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.

4.1 General System Information

The Application Launcher provides an *About* page to inform about the very basic system data such as firmware version, licensed services and hardware specifications.



4.2 Application List

All sessions defined are listed in the application list (if activated within the session's title page). An application can be started by double click or clicking the *Start* button (upper right corner of the Launcher).

4.3 System Update

The *System* button allows to run the firmware setup as it is defined in the corresponding setup page.

4.4 Reboot and Shutdown

The Application Launcher provides two buttons to reboot or shut down the device. Both actions can be disabled for the user (Setup → User Interface → Hotkeys or Setup → Security → User Permission).

5 Setup Application

5.1 Starting the Setup

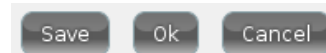
You can reach the Setup in four different ways:

- Select the *Setup* entry in the *Application Launcher* and double click it or press the *Start* button.
- Double click the *Setup* icon on the desktop (if configured).
- 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 the application to be reachable in every combination of these four possibilities within the Setup itself (Section *Accessories*).

5.2 Leaving the Setup

In general, every particular setup page provides the buttons *OK*, *Cancel* and *Save*.



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 a pop up window *Apply Settings*. Decide if you want to let the changes take effect immediately (*Yes*) or save and let the settings become effective on next reboot (*No*).

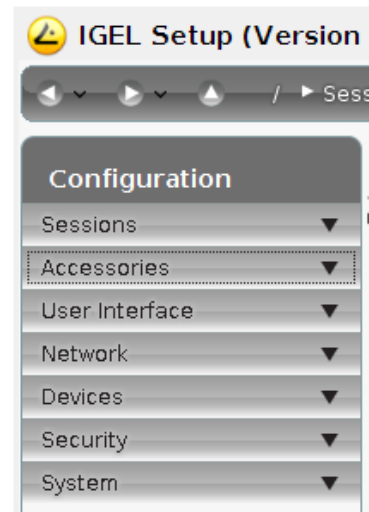
5.3 Setup Sections

The Setup application does provide the following main sections:

- Sessions
- Accessories
- User Interface
- Network
- Devices
- Security
- System

A mouse click on one of the sections will open a subtree. The tree structure allows to navigate through all setup options. Three navigation buttons let you step backwards and forwards within the Setup pages you did visit or get up to the next higher level of the structure.

The Setup options are described more detailed later – this is a short overview:



5.3.1 Sessions

The section *Sessions* allows to create and configure application sessions such as ICA, RDP, Powerterm, Browser and other.

5.3.2 Accessories

Some local tools can be configured within this section. You will find the Setup pages for the local shell (Xterm), Sound Mixer and other as well as the options for the Application Launcher and the Setup application itself.

5.3.3 User Interface

Configure the display settings, input devices, hot key commands and other within this section.

5.3.4 Network

All network settings for your LAN / WLAN interfaces and the configuration of dial up connections and network drives can be set here.

5.3.5 Devices

Set the parameters for your devices attached to the Thin Client such as Printer or USB storage devices. The button *Hardware Info* runs the Device Manager which provides information on the hardware this firmware is running on.



5.3.6 Security

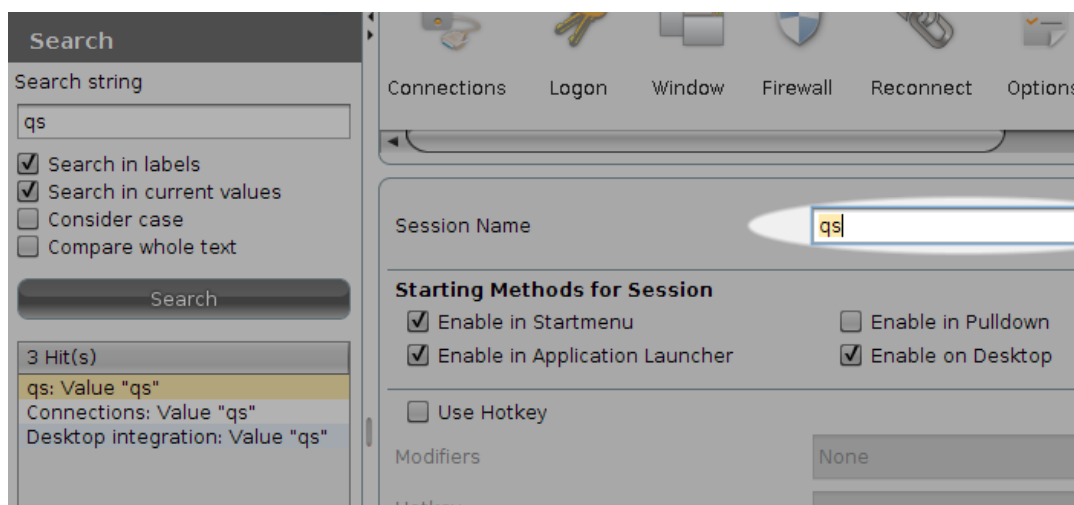
Set passwords for the administrator and user and define the user permissions etc.

5.3.7 System

Some basic system parameters are set here such as the system language (English or German), time and date, firmware update information, remote management and other.

5.4 Search for Setup pages

A search functionality allows to find parameter fields or values within the setup. Please select one of the hits and click on *Show Result* to get to the corresponding Setup page. The parameter or value found will be highlighted as shown in the picture below.



6 System Settings

As mentioned above, some basic system settings can be set within the subtree.

6.1 Tool tips (System Section)

These are small pop up windows with a short description of the pointed menu entry. These tool tips open up if you stay on a menu entry with your mouse pointer for the entered amount of *Tool tip Delay* time (in tenth of seconds).

6.2 Language

Select the appropriate system language from the list, keyboard layout and input language can be set here as well.

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

6.3 Time and Date

Click on *Time and Date* to open up this dialog-page. Make your changes and confirm them by pressing the *Set time and date* button. If a Time Server 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.

6.4 Update

The *Update* page shows you a simple dialog for updating the Thin Client's firmware. The common procedure to update your Thin Client(s) is as follows:

- Download the wanted firmware image from our server www.download-igel.com.
- Unpack the *.zip file, as this is the usual way we provide updates.
- Put all files into the designated directory on your local server (FTP or HTTP).
- Enter the necessary settings (see below for details) and press *Update firmware*.

Now the update process will advance automatically.

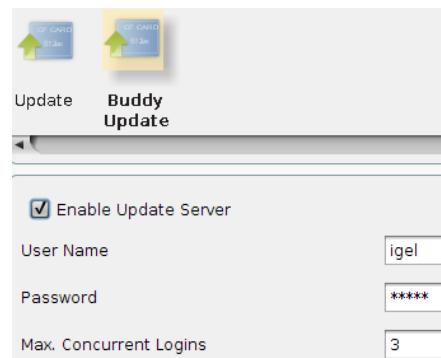
Note: The update procedure cannot be done via PPP /ISDN connections.

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

- **Protocol** – Select the protocol to use from the drop down list (FTP, HTTP, HTTPS etc.).
- **Server Name** – Enter the name or the IP address of the used server.
- **Server Path** – Enter the name of the directory you stored the update files in (relatively from the root directory).
- **User Name** – Enter the User account name.
- **Password** – Enter the corresponding password of that user / account.

6.4.1 Buddy Update

You can define your Thin Client as update server for other IGEL Thin Clients (Buddy Update). When using a Thin Client as update server only the FTP protocol can be used for updating the firmware.



6.5 Remote Management

If the Thin Client is registered by an IGEL Remote Manager Server the server address and port number is displayed here. You can set this data manually as well to let the Client be managed by a particular server. You can disable the Remote Management service by deactivating the checkbox *Enable Remote Management*.

6.6 Shadowing

For help desk purposes, you can shadow the client via the IGEL Remote Manager or any other VNC client (e.g. TightVNC). The options for the VNC features are:

- **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.

6.7 SSH 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. 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.

6.8 Service Information

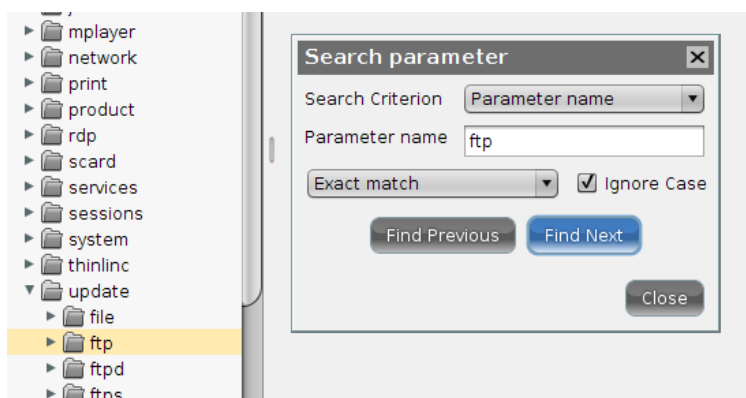
This list of available services allows you to quickly enable or disable firmware services (session types) such as Powerterm, Mplayer and other. If a service has been disabled the corresponding session type is no longer available after reboot – already existing sessions will be hidden (not deleted!). A session type disabled will not be updated during firmware update – so to speed up update procedures you should disable unused services.

6.9 IGEL System Registry

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

Note: 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.

You can search for setup parameters within the IGEL registry by clicking the button *Search parameter*. If you are looking for the FTP settings to update the Linux firmware, you can search for the parameter name *ftp* - the parameter found in the registry structure will be highlighted:



7 User Interface

7.1 Input

Set your keyboard layout and other input options on this Setup pages. The following parameters can be configured:

7.1.1 Keyboard (and Additional 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.
- **Keyboard Type** – Choose your keyboard type from the available from the drop down box.
- **Character Repeat** – In this section you can set the auto repeat behavior for the keyboard:
 - **Repeat Delay** – Sets the delay time (milliseconds) before 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.
- **Start with Numlock on** – Enable this checkbox if you want *Numlock* to be automatically activated during the boot process.
- **Disable XKeyboard extension** – To use *xmodmap* instead of *xkeyboard* extension disable this checkbox.

Define additional keyboard layouts for the user to choose. The layout can be chosen in the task bar.

7.1.2 Mouse

- **Mouse Type and Mouse Port** - Set the type and port of the attached mouse device from the two drop down boxes.
- **Left-hand mode** - Changes the orientation of the mouse to left hand 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 were pressed simultaneously, if 3-button emulation is enabled.
- **Mouse Speed** - 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.

7.1.3 Touch Screen

Note: To get into and navigate within the setup, it is recommended to do the initial configuration with an attached mouse and keyboard. Soft Keyboard setup is described below.

- **Touch Screen Type** - The supported types are currently serial Elographics touch screens and EvTouch USB touch screens.
- **Touch Screen already calibrated** - After enabling the touch screen functionality, you have to calibrate it initially. 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 panels' 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.

Supported USB controller types are:

- eGalax Inc. USB TouchController Vendor "3823" Product "0001"
- eGalax Inc. USB TouchController Vendor "3823" Product "0002"
- eGalax Inc. USB TouchController Vendor "0123" Product "0001"
- eGalax Inc. USB TouchController Vendor "0123" Product "0001"
- eGalax Inc. USB TouchController Vendor "0eef" Product "0001"
- eGalax Inc. USB TouchController Vendor "0eef" Product "0002"
- eGalax Inc. USB TouchController Vendor "1234" Product "0001"
- eGalax Inc. USB TouchController Vendor "1234" Product "0002"
- eTurboTouch Vendor "1234" Product "5678"
- PanJit Touchset Vendor "134C" Product "0001"
- PanJit Touchset Vendor "134C" Product "0002"
- PanJit Touchset Vendor "134C" Product "0003"
- PanJit Touchset Vendor "134C" Product "0004"
- 3M Microtouch EX II Vendor "0596" Product "0001"
- ITM Touchscreens Vendor "0403" Product "F9E9"
- Gunze AHL61 Vendor "0637" Product "0001"
- DMC TSC-10/25 Vendor "0AFA" Product "03E8"
- Elo Touchscreen Vendor "04e7" Product "0020"
- Generic ts-adc touchscreen modules name "ts-adc"
- Lifebook B-Series name "LBPS/2 Fujitsu Lifebook TouchScreen"

Activate the soft keyboard for touch panel usage in setup *Accessories* → *Soft Keyboard*, the layout of the normal keyboard will be used by the soft keyboard as well.

7.2 Display

7.2.1 Global Display Settings

- **Color Depth** - This menu allows you to specify the desktop color depth from these available:
 - 16 bits per pixel (High color / 65k colors)
 - 24 bits per pixel (True color / 16,7million colors).

Note: Make sure all displays connected to the Thin Client support the color setting!

- **DDC** - Enable usage of *Display Data Channel* to exchange information between system and display. In case you have display problems please test with enabled and disabled DDC setting. Default is *DDC disabled*.
- **Screen configuration** - Each screen connected to your IGEL UD device (up to 4 with UD7) can be configured independently. The position of each screen can be set in relation to *Screen 1* – please press button *Identify* to display the screen ID on each device.

7.2.2 DPMS

If your display supports *Display Power Management Signaling* it allows more functions (energy saving) than just a screen saver. There are three different modes called *Standby*, *Suspend* and *Off*, which are activated after their adjustable time loops (in minutes) ran off.

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

7.2.3 XDMCP

Enable the XDMCP functionality for the display by activating the checkbox.

- **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 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.

7.2.4 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*.

7.2.5 Desktop

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 tool tips.

General Settings – Configure the desktop appearance by changing *Theme*, *Fonts* or *Icon size* and set display and delay time for *Tooltips*.

Background / Wallpaper – Configure the background of your desktop with predefined IGEL wallpaper, solid color, color gradient or set your own wallpaper. The background is configurable for each monitor connected to the Thin Client.

Custom Wallpaper – A customized wallpaper can be provided on a download server. Activate custom wallpaper and set wallpaper file name in *Desktop* → *Background* and define your download server in *Desktop* → *Background* → *Custom Wallpaper Server*. In case you did already define a server for your system update files you can use same server settings for downloading the wallpaper.

The custom wallpaper will be downloaded from server location once after activating the functionality and on manual request (*Wallpaper Update*). The download process can be initiated as well within the *IGEL Universal Management Suite* (single command or update job *Update Desktop Customization*).

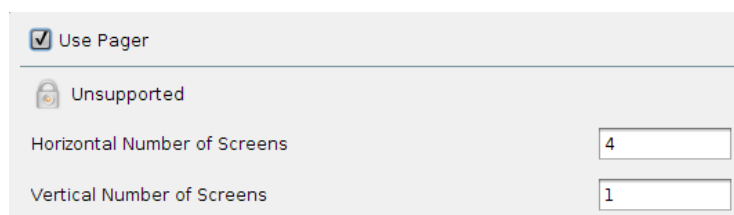
Custom Boot Splash – A customized boot image can be provided on a download server. Activate custom boot splash, define download server and set image file name in *System* → *Firmware Customization* → *Custom Boot Splash*. In case you did already define a server for your system update files you can use same server settings for downloading the boot image.


The custom boot splash will be downloaded from server location once after activating the functionality and on manual request (*Boot Splash Update*). The download process can be initiated as well within the *IGEL Universal Management Suite* (single command or update job *Update Desktop Customization*). The picture will be scaled to 800x600 px. (aspect ratio will be unchanged) and can be positioned vertically and horizontally by changing the *Position* values (between 0 and 100, default is 50 (*centered*)).

Note: Supported file types for *Custom Wallpaper* and *Boot Splash* are BMP, JPG, GIF, TIF, PNG and SVG – and 25 MB in total is reserved for all custom pictures.

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

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



<input checked="" type="checkbox"/> Use Pager	
 Unsupported	
Horizontal Number of Screens	<input type="text" value="4"/>
Vertical Number of Screens	<input type="text" value="1"/>

The Pager is a tool with “Virtual Screens” that you can use to easily move from one open application to another. This window is displayed in the right part of the task bar. 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 four virtual desktops. The first of them is active (dark gray).

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).

Note: All running sessions of all virtual screens will be accessible via the task bar in each of the screens.

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

7.3 Font Services

7.3.1 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.

7.3.2 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.

7.4 Screen Saver

Configure the screen saver to start automatically and choose a password option for the screen saver.

7.5 Hotkeys → 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 four main access areas as there are the *Application Launcher*, the *Start Menu*, the *Desktop* and the *Pull down* 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, a drop down box will be accessible to set modifier and hotkey (every common modifier is available).

8 Network

8.1 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. Changes within this Setup page will be copied into the *Interface* pages as well.

Activate default interface (Ethernet)

Get IP from DHCP Server
 Get IP from BOOTP Server
 Specify an IP Address

IP Address
Network Mask

Unsupported

Default Gateway enable
Terminal Name

Enable DNS Unsupported

Default Domain Unsupported Unsupported
Nameserver Unsupported Unsupported
Nameserver Unsupported

Dynamic DNS registration (via DHCP)

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 not 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 default 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.

8.2 Interfaces

By default the on board network hardware is used (Interface 1) and you have configured the basic network settings in the *Network* page described before.

The screenshot shows a network configuration window with the following elements:

- Top tabs: LAN Interfaces, Analog Modem, ISDN, ADSL, PPTP, Cisco VPN, Routing, Hosts, NFS, SMB.
- Sub-tabs: Interface 1, Interface 2, Tokenring, Wireless.
- Checkbox: Activate default interface (Ethernet)
- General tab selected, Authentication tab also visible.
- Radio buttons for IP configuration:
 - Get IP from DHCP Server
 - Get IP from BOOTP Server
 - Specify an IP Address
- IP Address field: 192.0.0.1
- Network Mask field: 255.255.255.0
- Network Linktype dropdown menu: Auto Sense

There are two additional dialog-boxes to configure the optional LAN Interfaces as there are:

- Interface 2
- Wireless

The configuration masks of *Interface 2* are the same as Interface 1.

8.2.1 Authentication

Enable IEEE 802.1x Authentication (wired 802.1x only)

Enables Network Port Authentication according to 802.1x standard. Currently the following authentication methods are supported:

- EAP-PEAP/MSCHAPv2
- EAP-PEAP/TLS
- EAP-TLS

Note: The Authentication menu changes input options depending on the authentication method chosen.

EAP Type

Choose authentication method:

- PEAP for EAP-PEAP/MSCHAPv2 and EAP-PEAP/TLS
- TLS for EAP-TLS

Validate Server Certificate

If set, the identity of the authentication server is checked.

CA Root Certificate:

Path name to file containing root certificate(s) for server authentication. The file can be in PEM or DER format.

PEAP/Auth Method

Choose phase 2 authentication method

- MSCHAPv2 for EAP-PEAP/MSCHAPv2
- TLS for EAP-PEAP/TLS.

EAP-PEAP/MSCHAPv2/Identity

Maintain user logon name for MSCHAPv2 authentication

EAP-PEAP/MSCHAPv2/Password

Maintain password for MSCHAPv2 authentication

EAP-PEAP/TLS/Client Certificate

Path name to file containing certificate for client authentication in PEM (base64) or DER format; leave blank if Private Key file in PKCS12 format (PFX) is used.

EAP-PEAP/TLS/Private Key

Enter pathname to file containing client private key in PEM (base64), DER or PFX format.

EAP-PEAP/TLS/Identity:

User logon name for TLS authentication.

EAP-PEAP/TLS/Private Key Password

Password to access encrypted private key in private key file.

EAP-TLS/Client Certificate

Path name to file containing certificate for client authentication in PEM (base64) or DER format; leave blank if Private Key file in PKCS12 format (PFX) is used.

EAP-TLS/Private Key

Pathname to file containing client private key in PEM (base64), DER or PFX format.

EAP-TLS/Identity

User logon name for TLS authentication

EAP-TLS/Private Key Password

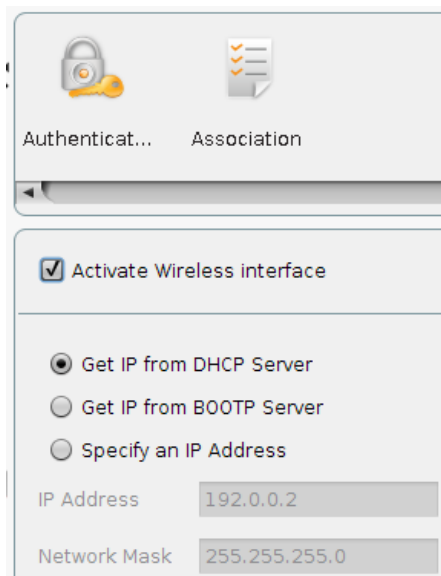
Password to access encrypted private key in private key file.

8.2.2 Interface 2

If you installed an optional Ethernet card in the available PCI slot (only available in some IGEL Thin Client model lines), use this dialog-box to configure the LAN interface called *Interface 2*. The available options are same as for Interface 1.

In case you encounter problems with the auto sense function in your network, you can set a fixed network speed.

8.2.3 Wireless



If you have installed an optional Wireless-LAN card in the available PCI/ISA slots (only available in some IGEL Thin Client model lines), use this dialog-box to configure the LAN interface called *wlan0*.

On the Wireless Security page (*Association* tab) 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 tool tips. Please also refer to the manual of your WLAN equipment.

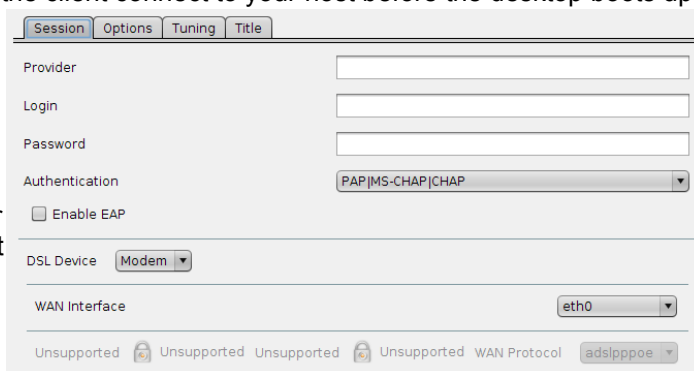
8.3 Dial Up Connections

8.3.1 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).

8.3.2 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.

8.4 Routing

Use this setup page to specify additional network routes if necessary. (The Interface field needs "eth0", "eth1", "tr0" or "wlan0" meaning Interface 1+2 and Wireless Lan.) Altogether you can define up to 5 additional routes.

8.5 Hosts

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

Click *Add* to open the *Host Entry* dialog-box.

- **IP Address** - Enter the IP address of the host you want to add.
- **Full Qualified Host name** - Enter the "Full Qualified Host name" (e.g. <mailserver.igel.de>).
- **Short Host name** - Enter the "Short Host name" (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".

8.6 Network Drives

8.7 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.

Click *Add* to open the *NFS Mount Entry* dialog-box.

- **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.

8.7.1 SMB (Windows Drive)

The SMB protocol is very useful because it is used by Microsoft Windows NT, Windows 95/98, Windows 2000 and Windows 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.

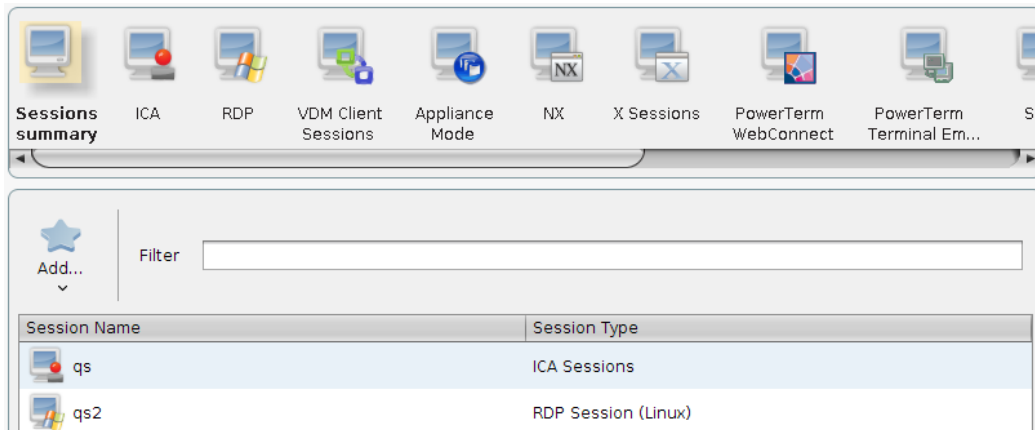
So it is possible on the Thin Client to mount SMB shares from Windows or Unix Samba hosts.

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!

- **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 Net BIOS 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 writable** - Activating this also enables the desktop user to write data (otherwise, only "root" is).

9 Sessions

Sessions can be created and configured within the *Sessions* subtree of the IGEL Setup application. The *Session Summary* gives an overview on all session types provided and existing sessions.



Pressing the button *Add* lets you create a new session (disabled system services will not be displayed in the drop down list).

Every session has a configuration page *Desktop Integration* (previously known as *Title* page) where the appearance of the session on the local desktop is defined. Here you can set the name of the session as well as the session start options (Autostart, Restart) and Hotkey usage.

9.1 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.

9.1.1 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**".

9.1.2 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 server 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.

9.1.3 Keyboard (Hotkey Mapping)

Use the “Keyboard” 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. 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 “Hotkey Modifier” and/or “Hotkey Character” of the particular combination.

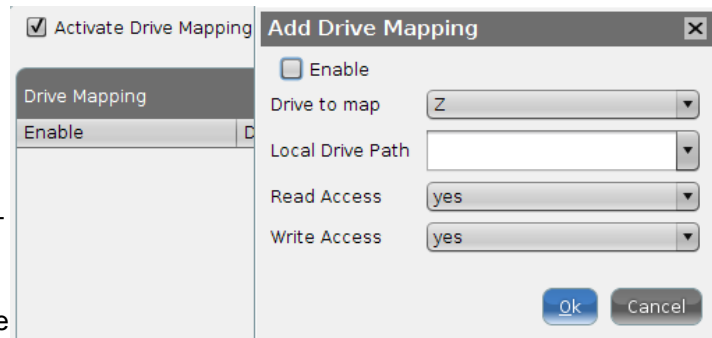
- Possible keys are: F1 – F12 , Plus, Minus, Tab
- Possible modifiers are: Shift, Ctrl, Alt, Alt+Ctrl, Alt+Shift, Ctrl+Shift

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>.

9.1.4 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 (USB) devices that are to be used for drive mapping first have to be configured as device!

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

- Click the button *Add* to bring up the Drive Mapping Window and enable the mapping.
- Then select a “**Drive to map**“ from the list and 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.

9.1.5 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
- Your selection will be mapped to the virtual COM1, a second one will become virtual COM2 and so on.

9.1.6 Printer

Configure the printer for ICA sessions on this page.

- **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 Auto creation** - 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 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.

9.1.7 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 administration manual.)

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

- **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 has to be set to "**SSL/TLS + HTTPS**".

9.1.8 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.)

- **Use Local Logon Window** - 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 Client Name 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.

9.1.9 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.
- **Enable Auto Reconnect** – Define the parameters for the session reconnect.
- **Deferred Screen Update Mode** – Enables batched updates from the local video buffer to the screen. The local video buffer is used when seamless windows or Speedscreen Latency Reduction are in use.
- **Multi Monitor** – Configure the appearance of the session in a Multi Monitor environment.

9.2 ICA Sessions

The ICA Session Setting (as far as they differ from the Global Settings) can be changed when creating or editing a session.

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.

9.2.1 Connections

- **Browser Protocol** - Select the needed protocol for broadcast or use the global default set.
- **Don't use default server location** - 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.
 - 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** - 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.

9.2.2 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 (Ctrl-Alt-Delete) before Logon toggles the "Welcome to Windows" screen on/off.

9.2.3 Window

Number of Colors - Use the color depth set as global default or alter it for this session.

Use Default Setting for Color map - 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. The *Seamless Window Mode* can only be used with Published Applications or with a defined initial program for the server connection.

Start Monitor (Dual view) – Define which screen in a Multi Monitor environment should be used for the session.

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 completely overlay the desktop.

9.2.4 Firewall

- *Use Default Alternate Address Setting* - Choose between using the global default or set it for this session separately.

Note: The alternate address itself has to be defined in the “Address List” of the “Server Location” page of the “Global ICA Settings”.

- *SOCKS/Proxy Server* - Same as above; use global defaults or alter for this session. If in doubt, the tool tips are quite helpful.

9.2.5 Options

This is the page to tweak the performance and behavior (see below 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) 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.
- **Speed screen Latency Reduction** - “Speed screen 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 drop down 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.

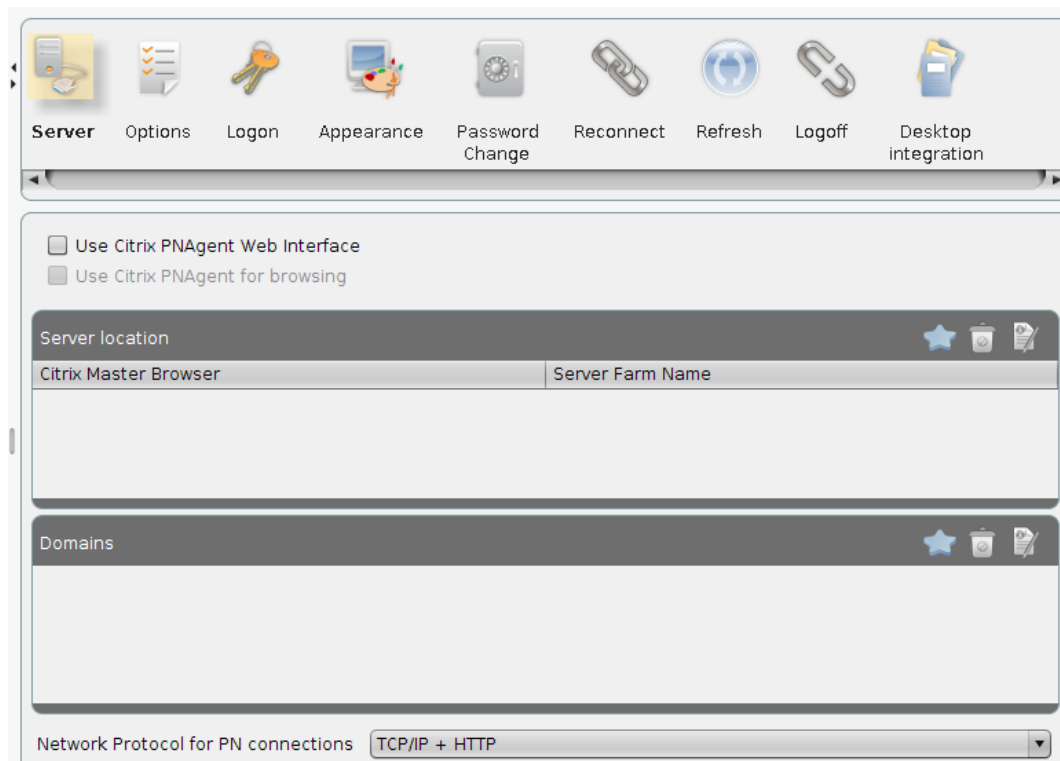
Note: **Speed screen** has to be enabled and configured on the Citrix server first in order to work.

9.2.6 Reconnect

You can edit the Global ICA Settings for this session for the Reconnect Option.

9.3 ICA Program Neighborhood

Most of the settings have already been dealt with in “**Global ICA Settings**” as well as in the ICA session setup.



Define the Master Browsers to be browsed for published applications. You can set up to 5 Master Browsers per domain. 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.

- **Use Citrix PNAgent Web Interface** – Use the PNA Web Interface connection instead of the direct connection to the Presentation Server.
- **Use Citrix PNAgent for browsing** – When using the Web Interface connection this parameter should be set as well. Otherwise the application browsing will happen via the Presentation Server connection while the PN connection itself runs via Web Interface.

9.3.1 Options

Set Audio and Color options etc. as far as they differ from the Global Settings.

9.3.2 Logon and Logoff

Define an Auto Logon option so no typing of user name and password will be necessary when connecting to the server. You can synchronize the password for the Lock Screen application (xlock) with the PN password.

The Logoff option will create a PN Logoff Button and allows to log out from PN with a hotkey as well.

9.3.3 Appearance

You can configure the PN applications to be shown within different parts of the local system – e.g. the local desktop or the start menu. The size of the application icon can be adjusted automatically (*Resize Icon* option).

9.3.4 Password Change

Define the method to establish a connection for password change.

- **Generic Session** – Browses for servers and applications and tries to connect until success.
- **Predefined ICA Session** – Choose a predefined ICA connection by session name.

9.3.5 Reconnect and Refresh

Set the required option to reconnect to sessions. You can reconnect during the login process and by using a *Reconnect Session* (e.g. on desktop). The reconnect procedure can start active and disconnected sessions or disconnected sessions only, a third option is *Ask User*.

A Refresh Session will reload the PN session without disconnecting them.

9.4 RDP (Global RDP Settings)

This section describes how to configure the *Global RDP Settings* that will be valid for all RDP sessions.

9.4.1 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.

9.4.2 Server

- **RDP Protocol Level** - Set the protocol level according to the server you are going to connect to. Default is automatic detection.

9.4.3 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.

9.4.4 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 multi port PCI card, you may have more than 2 ports.

9.4.5 Printer

Set up the printer to be used within RDP session here. Click the button *Add*, choose the printer queue (*lp+lp_lp*, *lp_com1*, *lp_com2* or *lp_usb*) and set the printer's name. 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.

9.4.6 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 and clipboard content.

9.4.7 Performance

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

9.4.8 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.
- **Multi Monitor** – Configure the appearance of the session in a Multi Monitor environment.

9.5 RDP Session

9.5.1 Server and Logon information

The RDP Session Setting (as far as they differ from the Global Settings) can be changed when creating or editing a session.

Define a server and initial application for the Terminal Server session and configure the necessary logon information (otherwise the TS logon window will be displayed to enter the user and password).

9.5.2 Display, Keyboard and Mapping settings

Set Display Colors, Window Size and Multi Screen behavior and configure the keyboard mapping and system shortcuts. Enable/Disable the Audio and Clipboard mapping for the Client.

9.5.3 Performance and Options

Define performance settings for the session if different from the global configuration.

9.6 VMware View Client

By default the View Client session settings are taken from the RDP Global Setup pages, you can change the configuration on the corresponding setup pages for View Client sessions.

9.7 Quest vWorkspace Client

By default the vWorkspace Client session settings are taken from the RDP Global Setup pages, you can change the configuration on the corresponding setup pages for vWorkspace Client sessions. Additionally you can configure Multimedia and USB Redirection for the session.

9.8 Leostream Connection Broker

Define Server, User and Domain for login with Leostream Connection Broker.

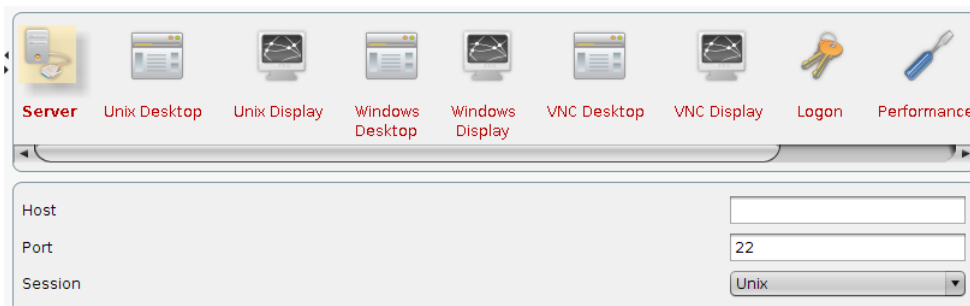
9.9 Appliance Mode

The Appliance Mode session can be enabled for View Client or XEN Desktop connections. When running an Appliance Mode session no other application access is possible. Only the server session to the defined View or XEN Delivery server will be visible.

Note: The default system hotkey Ctrl+Alt+s to bring up the IGEL Setup application does not work within the Appliance Mode, please use Ctrl+Alt+F2.

9.10 Nomachine NX

To configure an NX session maintain the NX server data and choose the session type (Unix, Windows, VNC). Depending on your choice either the Unix Desktop, Windows Desktop or VNC Desktop setup pages will be activated to complete the configuration.



The IGEL Setup pages for NX sessions basically represent an adjusted GUI for the Nomachine NX Client. Further information on configuration details (Performance, Services etc.) can be found in the original documentation provided by Nomachine.

9.11 SSH Session

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.

- **Command** - Use this page to provide all necessary entries to create an executable command to start an application remote via SSH.
- **Remote User name** - 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.
- **Command line** - In this field you can specify the name of the application program you want to start.
- **Display** - This pull down 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 command line automatically
- **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.

9.12 ThinLinc

ThinLinc is a Linux Terminal Server solution which is used to virtualize desktops and applications by the use of Server Based Computing. In addition to the ThinLinc framework itself, the package contains a VNC client to transfer the graphical information of the remote (virtual) desktop or application as well as OpenSSH to secure the connection by encryption.

The session configuration allows to set display parameters such as the screen size, resolution or full screen mode; you can optimize the compression to save bandwidth as well. The SSH port can be adjusted to meet your requirements, default is standard port 22.

You can map several local resources into a ThinLinc session such as printer, serial port, local files (NFS with read and/or write permission) and audio devices (audio output on your local speaker). It is possible to allow the remote shadowing of a ThinLinc session, default is *disabled*.

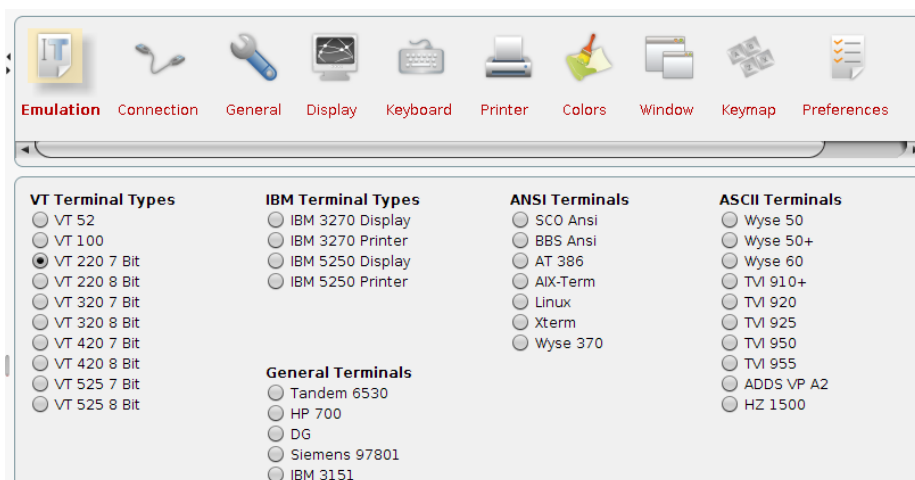
9.13 PowerTerm WebConnect

PowerTerm WebConnect is a solution that provides local and remote access to applications running on Windows Terminal Servers, Virtual Desktops (on top of hypervisors such as VMWare, Microsoft, Xen, and Virtual Iron), Blade PCs, and legacy hosts.

Enter the host name of the WebConnect server you want to connect to. The server configuration itself is described in the WebConnect documentation by Ericom (<http://www.ericom.com/doc/QRG/WebConnectGettingStarted.pdf>).

9.14 PowerTerm Terminal Emulation

The PowerTerm InterConnect 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, the above “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 documentation of ERICOM Software Ltd. So for detailed information about configuring the PowerTerm Software please refer to the “PowerTerm Manual” available on the IGEL download server <http://www.myigel.com> → Partner Documentation or on the Ericom Documentation web page (<http://www.ericom.com/help.asp>).

9.15 X Session

To start an X session configure the basic connection data (type, server, command) on the Server page and set the required hotkey and window parameters.

9.16 Firefox Browser Global

The original Firefox Browser configuration parameters are mapped into the IGEL Setup to allow the centralized configuration via the IGEL Remote Manager. These global settings can be changed for each browser session.

9.17 Firefox Browser Session

The *Settings* pages again provide the original Firefox parameters and the default settings are taken from the *Browser Global* setup. Additionally the following settings can be configured for the browser session:

- **Window** – Set the full screen mode and multi monitor options as well as the Firefox language and secure the browser against changes by the user. You can hide the configuration page (about:config) and the printer dialog.
- **Tool bars** – Show or hide tool bar items or complete tool bars within the session. You can configure a Kiosk mode (Browser in full screen mode, restricted access to tool bars and autostart/restart configuration).
- **Hotkeys** – Enable or disable hotkeys used within the Firefox browser.
- **Context Menu** – Enable or disable items of the browser's context menu.

9.18 SAP Client

You can access your SAP system using the SAP GUI for Java Client. If a configuration file is provided, the corresponding settings will be used by the Client. There are no further configuration parameters within the IGEL Setup.

9.19 MPlayer

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.)

9.19.1 License

Note: Before using the local Mplayer application, please make yourself familiar with the codec license disclaimer! Without proper licensing, it's illegal to use the MPlayer application!

9.19.2 Download 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.

9.19.3 Video Settings

Set up the look of the Mplayer window (Fullscreen Video, Scaling and Ratio) on the *Window* page and adjust the most basic video settings (Brightness, Contrast etc.) on the *Video* page. Some more detailed settings can be done within the *Video Filter* – such as Deinterlacing, Noise Reduction etc.

9.19.4 Audio

Choose the video language. Available are: English, German, French, Italian, and Spanish. You can adjust the A/V Synchronization on this setup page as well.

9.19.5 Options

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

9.19.6 Hotkeys

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

9.19.7 Browser Plug In

If you want to use the MPlayer as browser plug in, you can set configuration values differing from the previous ones which affect manually configured Mplayer sessions.

9.20 Java Web Start Session

To get access to Java Web Applications you have to enter the address of the required JNLP file.

9.21 VoIP Client

This section describes how to configure Voice over IP telephony (VoIP). The IGEL Universal Desktop Linux firmware provides the Ekiga Voice over IP client (<http://ekiga.org>). The client allows you to use the Session Initiation Protocol (SIP) as well as H.323 . In addition to a local contact list the phone book can also browse LDAP address books.

A detailed description of all Ekiga options can be found at <http://wiki.ekiga.org/index.php/Documentation> .

10 Accessories

The setup pages in Accessories provide configuration options for some system tools such as the Setup and Application Launcher programs themselves, Sound Mixer, local shell (Xterm) etc.

10.1 Xterm

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.)

10.2 Card Reader

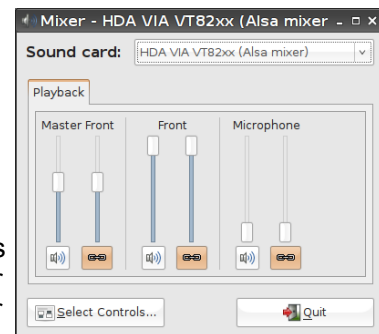
The Smartcard Reader (e.g. to use a KVK Krankenversichertenkarte (*Health Insurance Card*)) can be configured on this page – the required parameter data depends on the card and reader used (e.g. Cherry G80 keyboard with reader). This functionality will change in the future for support of the new *Elektronische Gesundheitskarte (Electronic Health Insurance Card)*. A separate documentation on the usage of a KVK is available on the IGEL download page.

10.3 Setup and Application Launcher

Let the Setup and Application Launcher be displayed on the local Desktop or Start menu, define hotkeys and autostart option. You can hide some elements from the user such as the buttons for shutdown or reboot the device.

10.4 Sound Mixer

The Sound Mixer allows to adjust the output volume and input level as well as the balance for input and output.



10.5 Java Manager

The Java Control Panel is a multipurpose control panel. It allows you to view and set a wide range of parameters controlling how Java runs on your computer. It lets you view and delete temporary files used for Java Plug-in, which allows Sun Java to be used by your web browser to run applets, and Java Web Start, which allows you to run Java applications over the network. It allows you to control certificates, making it safe to run applets and applications over the network. It allows you to set runtime parameters for applets run with Java Plug-in and applications run with Java Web Start. For more information on this please have a look at <http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>.

10.6 USB Storage Restart

If you encounter problems while using a USB storage device you can use the Restart session to logically disconnect and reconnect the attached USB device without having to remove it from the Thin Client physically.

10.7 Kerberos Logout

This session allows to empty the credentials cache of Kerberos secured connections (Single Sign On). After running this Logout session you have to sign on via Kerberos server again.

10.8 Network Tools

The IGEL Universal Desktop Linux Firmware provides some tools for network analytics such as

- Device Information
- Ping
- Netstat
- Traceroute
- Lookup

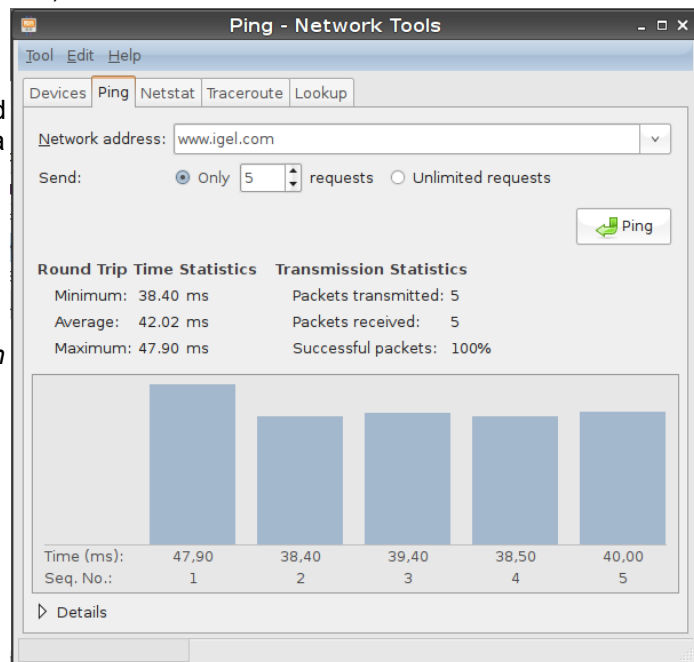
10.8.1 Device Information

Provides information on the status of your network device such as MAC and IP, Link speed and some interface statistic (Bytes transferred, Errors etc.).

10.8.2 Ping

Allows to send a fixed number (or unlimited until stopped by user) of network pings to a network address. The ping result is shown below and the ping time of the last five pings is visualized in a bar graph.

The Thin Client can be configured to beep on every ping sent out. This option can be activated in the menu bar (*Tool* → *Beep on ping*).



10.8.3 Netstat

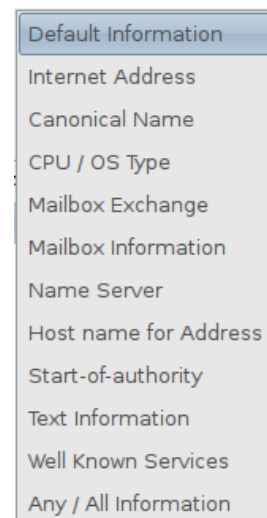
Provides information on active network services with protocol and port information as well as routing table and multicast information for your network devices.

10.8.4 Traceroute

Trace the route to a network address.

10.8.5 Lookup

Displays information of different type on a network address. Information Types available are shown on this screen shot:



11 Devices

11.1 Hardware Information

Press the Hardware Info button to get an overview of your IGEL Thin Client device.

11.2 Printer

Several printing systems can be used with the Thin Client:

11.2.1 CUPS (Common UNIX Printing System)

The Common UNIX Printing System™, or CUPS, is the software you use to print from applications like the web browser you are using to read this page. It converts the *page descriptions* produced by your application (put a paragraph here, draw a line there, and so forth) into something your printer can understand and then sends the information to the printer for printing.

The CUPS can be configured to use printing devices using the following ports:

- Parallel (LPT 1, LPT 2)
- Serial (COM1, COM2, USB COM1, USB COM2 – with USB-to-Serial adapter)
- USB (1st and 2nd USB Printer)
- Network (TCP/IP, LPD, IPP)

When adding a printer device you can define the printer's manufacturer and model data, the configuration data depends on the printer port chosen.

11.2.1.1 IPP Printer Sharing

The IPP (Internet Printing Protocol) provides the following configuration options:

- Network / Host for sharing of local printers – Allow printing on the local device from local or global network.
- Enable IPP Printer Browsing – Browse for shared printers on the local or global network and advertise your shared printer to the network. A shared printer is visible to the network but printing from the network might be impossible because of missing authorization!

11.2.2 LPD (Line Printer Daemon)

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.

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 the pop up 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.

11.2.3 TCP/IP

You can map printers attached to your device to a TCP/IP port. Activated by default is the LPT1 port (TCP/IP port 3003). The printer can be attached to one of the following ports (if available on your device):

- Serial port (COM 1 or COM 2)
- Parallel port (LPT 1)
- USB (USBLP 1)

11.2.4 ThinPrint

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.

The Parameters on the Thinprint setup page are:

- **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.
- **Open Printer Interval** - Maximum waiting period in case of blocked printer (in seconds).
- **Open Printer Tries** - Number of attempts to contact a printer to start a print job.

The page Printer will display the list of ThinPrint printers and allows to add, edit or delete a printer configuration. It 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:

- **Class** - Enter the printer class name (optional).
- **Active** - Enable / disable network visibility for this printer.
- **Default** – Set this device as the default printer.

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

11.3 USB Storage Devices

11.3.1 Storage Hot plug

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.

11.3.2 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 drop down 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 below)!

- **File System Type** - Set the file system that will be used here. In general, you should choose “auto”, but if you use “ext2” or encounter any other trouble, set the file system 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 min.).

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

11.4 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 (if available in your device). Some models already have one built-in as well as the reader being available separately. You may also use an external reader attached to the USB port.

12 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.

12.1 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 IGEL Setup, the shell access in an "**Xterm**" and on the console to the administrator! The *Reset to factory defaults* will only be possible with this password.

- Remote User Password – Set a password for the remote session user (SSH).

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...

12.2 Kerberos

To use a Kerberos Server to secure your network connection please activate and configure the Kerberos Service on this Setup pages.

- **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 1-4** - 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.

13 IGEL Smartcard Solution

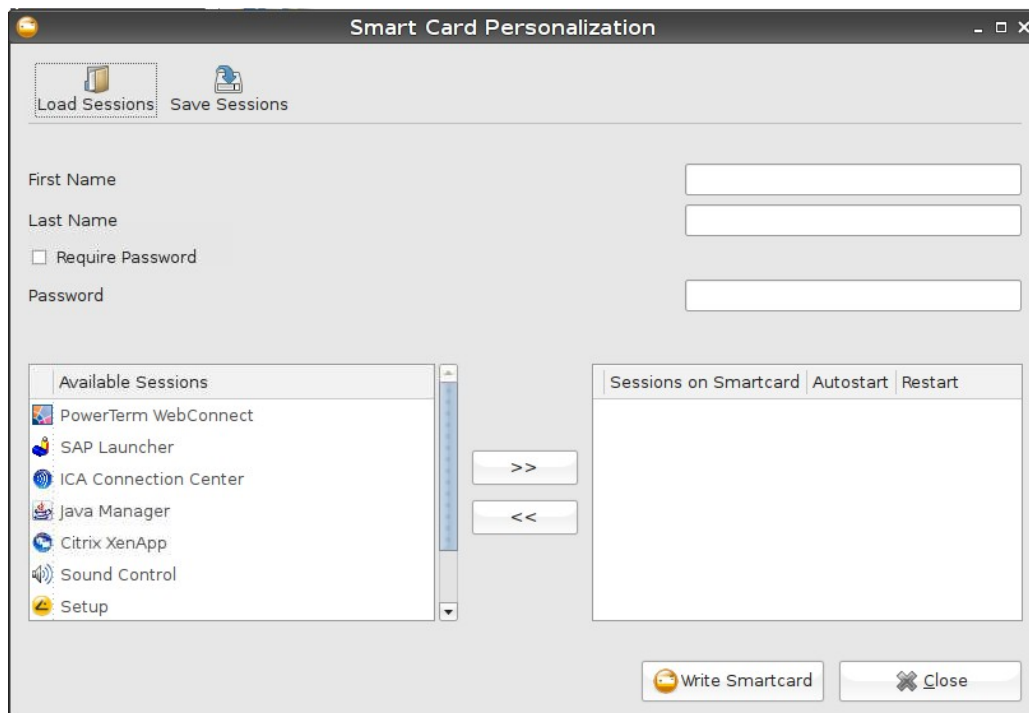
You can use the optional IGEL Smartcard for local authentication and personalized session configuration ("Flying Doctor Scenario").



The IGEL Smartcard can be used with the internal reader (UD3 / UD5) or external reader (USB).

Activate IGEL Smartcard Solution in setup application → *User Interface* → *Logon* → *Smartcard*. Enter a company key to write your IGEL Smartcards and save the setting before starting the personalization of the card.

The Personalization window allows you to set a login password and to add sessions to the card. Session configurations will be stored on the card's IC and the session can be used on any IGEL Thin Client reading the card.



Company Key

The IGEL Smartcard Solution also includes a “Company Key” which is an additional code written to the smartcard that must match the code in the terminal being used. If the two codes don’t match, the smartcard can not be used on that terminal. This is an additional security measure to ensure someone from outside the company cannot access your terminals. It could also be used within a company to restrict employees to certain terminals.

Setting User and Password for authentication

You can enter the user’s first and last name – they will then be prompted by this name when the smartcard password is requested. Checking the “Require Password” box will pop-up a password box anytime the smartcard is inserted. Failing to enter the PIN correctly will deny access to the terminal.

If the smartcard is just being used to control access to the terminal you can now insert a suitable smartcard and write the data clicking the “Write Smartcard” bar. When the write completes successfully you can remove the smartcard and program the next.

Saving Sessions on the Smartcard

In a scenario where an employee may use several different terminals or where terminals are used by many different employees it may be preferable to store the sessions the employee uses on his smartcard rather than on the terminal. In this way the employee only needs to see the applications he needs to perform his duties.

As soon as the employee inserts his smartcard into the terminal, their customized set of applications will be shown on the terminal. Create the sessions that you wish to add to the smartcard on the terminal, including autostart option and any personalization of logon credentials.

Besides adding the first and last name of the card user, plus an optional password, you can add any of the sessions shown in the “Available Sessions” pane to the smartcard. Once all the desired sessions have been added press the “Write Smartcard” button to store the data on the smartcard.

Testing the Created Smartcard

After the warm boot you should be able to insert the smartcard and immediately see the sessions show up on the desktop. Any session that you designated to automatically start with the insertion of the smartcard should start running.

Note: If you test the smartcard on the terminal you used to create the smartcard you will see a duplicate set of the sessions on your desktop. This is because the sessions are saved in the terminal and another set is saved in the smartcard. When you insert the smartcard into a terminal with no “local” sessions you will just see the sessions on the smartcard.

14 Custom Partition on Compact Flash

General Information

Version 4.01.500 of the *IGEL Universal Desktop LX* firmware provides users with a partition on the storage medium (CF card). A download/update function can be set up for this custom storage area to load and, if necessary, update data from a server.

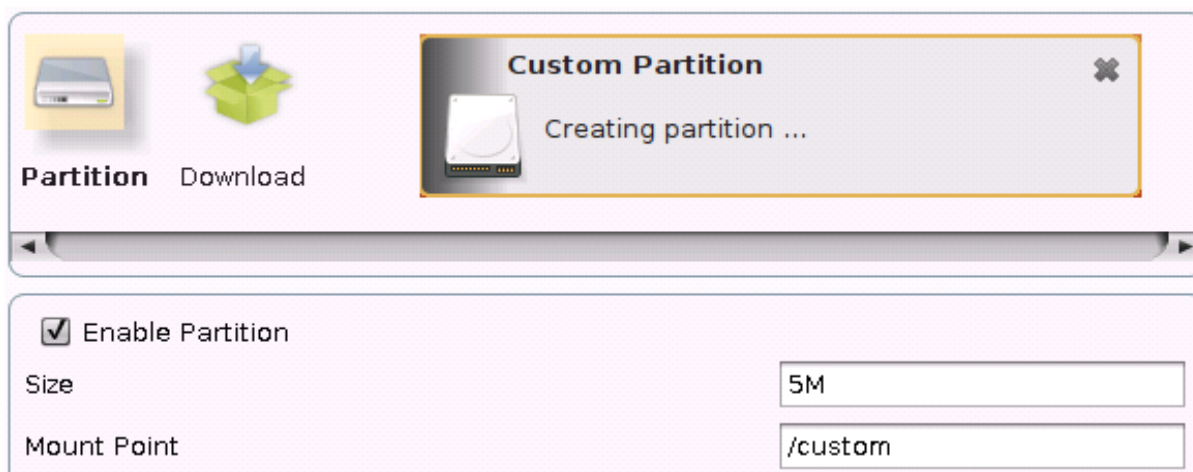
Activating Custom Partition

The custom partition is not active as standard but can be activated in the IGEL Thin Client setup (or using the *IGEL Universal Management Suite*) via the

System → *Customize* → *Custom partition* → *Partition*

setup path. The size of the partition is determined by a numerical value (byte) together with a multiplicative suffix. Recommended sizes would be 100K (for 100 KiB = 100 * 1024 bytes) or 100M (for 100 MiB = 100 * 1024 * 1024 bytes).

A minimum of 100 KiB should be selected for the size of the partition and not more than 300 MiB should be reserved by the custom partition (in relation to the 1 GB standard CF of the IGEL Linux Thin Clients) as subsequent firmware updates may require more storage space than the current version.



After confirming the settings with *Accept* or *OK*, the partition is created and mounted at the designated mount point. A status window charts the process and displays any errors that may occur during partition creation. If there is not enough free space on the storage medium, for example, the partition can not be created.

Changing the size of a pre-existing custom partition can also be hampered by a process that still accesses this partition, e.g. whilst its content is displayed in the terminal window.

Defining download (source)

To upload data to the custom partition, at least one source for partition data must be created in the *Download* area. Click on *Add* to do this.

The same protocols that are used in the firmware update, i.e. HTTP, HTTPS and FTP, are available for this transfer also. An INF file must be specified as the destination, which in turn references a *tar archive* packed using *bzip2*.

The structure of the INF file is as follows:

[INFO]	<i>Header-</i>
[PART]	<i>information</i>
file="test.tar.bz2"	<i>Packed tar archive</i>
version="1"	<i>File version</i>

The files to be transferred must be packed initially in a *tar archive*, which is then compressed using *bzip2*. This file is referenced in the INF file that represents the destination of the URL.

With Windows, the *tar archive* can be generated using the open source software 7-Zip (www.7-zip.org); this program also permits compression as *bzip2*. Under Linux, *tar* and *bz2* files can often be generated using standard tools.

This procedure allows the file(s) on the server to be replaced with a current version so that the thin client reloads this data during the next boot process. To this end, the parameter *version* must be increased in the INF file.

Executing actions

After mounting and/or unmounting the custom partition, commands (shell scripts) can be executed automatically. For example, a program downloaded to the partition can be launched or terminated during shutdown (whereupon the partition is unmounted).

Sample scenario: A custom background image is to be used. The image file is *igel.jpg*, packed using 7-Zip in the referenced file *test.tar.bz2* (see INF file above).

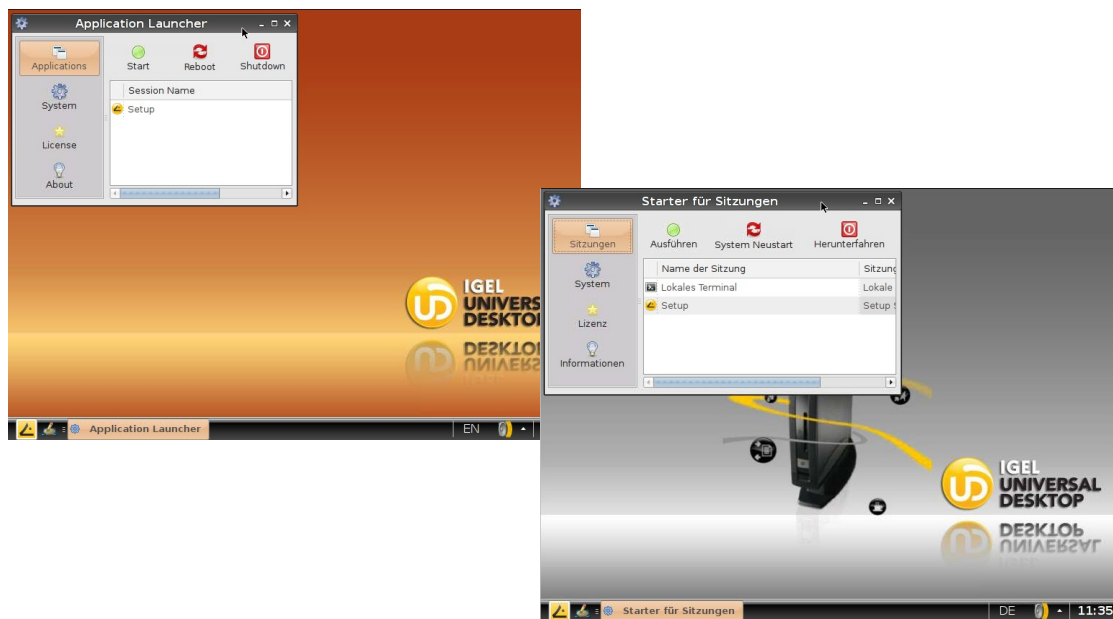
The INF file and the packed archive are stored in a web resource of the IGEL UMS that can be accessed from the thin client via HTTP.

The following settings are defined in the thin client configuration of the UMS:

1. Activate custom partition (size e.g. 1M) and mount at */custom*.
2. A new URL is created under *Download* that has the file *test.inf* as destination on the UMS server: <http://ums-server:9080/web-ressource/test.inf>
3. Enter the access data for the web server and activate the check-box *Automatic update* (if the image is to be replaced at a later date).
4. Enter the following copy command as the initialization action to copy the unpacked image to the right place:

```
cp /custom/igel.jpg /usr/share/pixmaps/IGEL_UD_4x3_blue.jpg
```
5. Under User interface → Screen → Desktop select as background image the entry *Igel blue (4x3)* – the associated file is then replaced by the custom file.

Save the changes in the IGEL setup and reboot the thin client so that it retrieves the changed settings from the UMS server. The custom partition is created and mounted and the packed file is transferred, unpacked and copied to the destination directory. The changed background image is loaded and displayed:



If this image is now to be replaced by a new one, change the JPG in the file *test.tar.bz2* and increase the version in the file *test.inf*. When the client is next rebooted, the changed version is downloaded and applied.

It is of course also possible to load executable files to the custom partition and call them up once mounted.

NOTE: If the Thin Client is reset to factory defaults, the custom partition is deleted along with all data stored on it.