



IGEL Remote Manager

User Guide



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, 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 disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, IGEL Technology GmbH reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of IGEL Technology GmbH to notify any person of such revision or changes.

- **Trademark Recognition**

IGEL is a registered trademark of IGEL Technology GmbH.

SAP DB is a trademark of SAP AG.

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

Java is a registered trademark of Sun Microsystems, Inc.

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

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice, and should not be construed as a commitment by IGEL Technology GmbH.

IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including the products and software described in it.

Copyright © 2006 IGEL Technology GmbH. All Rights Reserved.

Table of Contents

1	INTRODUCTION	5
2	PREREQUISITES.....	5
3	THE COMPONENTS	5
4	FIRST STEPS.....	6
4.1	Connecting to an IGEL Remote Management Server	6
4.2	Scanning for Thin Clients	7
4.3	Launching the Remote Manager Console via Java Web Start	9
4.4	Changing the Locale of Remote Manager Console.....	10
5	THE USER INTERFACE.....	10
5.1	Main Screen	10
5.2	Main Menu Bar.....	12
5.3	Thin Client Content Panel	15
5.4	Thin Client Directory Content Panel.....	16
5.5	Profile Content Panel	17
5.6	Profile Directory Content Panel.....	18
5.7	Context Menus.....	20
5.8	Search Menus	21
5.9	Shortcuts	22
6	MANAGING THIN CLIENTS	22
6.1	Modifying Thin Client Configuration.....	22
6.2	Send Configuration	23
6.3	Retrieve Configuration.....	24
6.4	Thin Client Codecs	25
6.5	Registering from the Thin Client	25
6.6	Thin Client Mass – Import.....	25
6.7	Automatic Remote Manager Server Detection	27
6.8	Shadowing	27
7	GROUPING THIN CLIENTS.....	31
7.1	Creating new Directories	31
7.2	Moving Thin Clients	31
7.3	Default Directory Rules	32
8	VIEWS.....	34
9	PROFILES.....	36
9.1	Organizing Profiles.....	36
9.2	Creating Profiles.....	38
9.3	Renaming Profiles	39
9.4	Edit Profile Settings	39
9.5	Assigning Profiles.....	40
9.6	Precedence of Profiles.....	43
9.7	Removing Profiles from Thin Client.....	44
9.8	Deleting Profiles	44
9.9	Examples on how to use Profiles.....	44
9.9.1	Same Display but different Sessions	45
9.9.2	Copy a session from one Thin Client to another	45
9.10	Exporting Profiles.....	46
9.11	Importing Profiles.....	46
9.11.1	Importing profiles with unknown firmware.....	47
10	SCHEDULED JOBS	48
10.1	Job Menu	48
11	MANAGING CERTIFICATES	52
11.1	Server certificates	52
11.2	Installing Server Certificate on Thin Clients.....	53
11.3	Installing Console Certificates	53
12	ACCESS CONTROL.....	53
12.1	Introduction	53
12.1.1	Access rights and their effects:.....	53

12.1.2	Effective Access Rights	54
12.2	Remote Manager Accounts	54
12.3	Defining Access Rights	56
12.4	Mandatory Access Rights for RM-Functions.....	58
12.5	Use Cases	59
13	THE IGEL REMOTE MANAGER ADMINISTRATOR.....	62
13.1	Settings Panel.....	62
13.2	Windows XP Embedded Images.....	63
13.2.1	Creating a Web Resource	63
13.2.2	Assign and manage Web Resources.....	64
13.2.3	Orphaned Web Resource definitions	66
13.3	Database Manager Operations	66
13.4	Backup and Restore Database contents	67
13.5	The Database Panel.....	68
13.6	The database management tool <i>igelsapdbm</i>	69
13.7	Configuring Data sources.....	69
13.7.1	Defining a data source	70
13.7.2	Setting an active Data source	70
13.7.3	Copy Data source	71
14	TROUBLESHOOTING.....	71
14.1	Log files	71
14.2	Known issues	72

1 Introduction

This document contains information about the usage of IGEL Remote Manager. For the installation of the product, please refer to the IGEL Remote Manager Installation Guide. Detailed descriptions of the Thin Client parameters are described in the Thin Client's User Guide.

2 Prerequisites

This document assumes a working installation of the IGEL Remote Manager and at least one IGEL Thin Client that can be administered.

3 The Components

The IGEL Remote Manager consists of the SQL Database SAP DB, the IGEL Remote Manager Server and the IGEL Remote Manager Console. The IGEL Remote Manager Server is actually split up into two parts, the TC Server and the GUI Server. The TC Server provides the configuration data to the Thin Clients while the GUI Server communicates with the IGEL Remote Manager Console; the data transfer between TC Server and Thin Clients or GUI Server and Remote Manager Console is SSL-encrypted.

As you can see in the figure below, the Remote Manager Console may be installed on a different computer to that where the IGEL Remote Manager Server is installed.

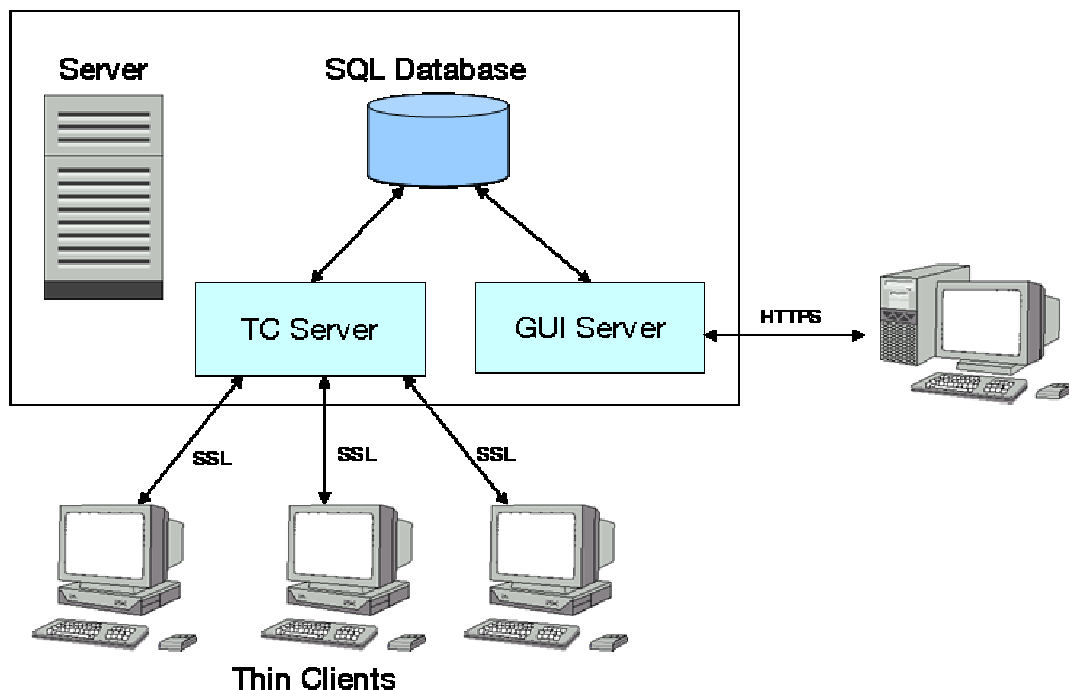


Figure 3-1 IGEL Remote Manager Components

Every configuration of the managed Thin Clients is stored in the database. Configuration changes are made only in the database and transferred to the Thin Client on demand.

The Thin Client can retrieve its information from the database at boot time or you can manually send the new configuration to a set of Thin Clients.

The IGEL Remote Manager Console is the interface to the Remote Management Server. It connects to the GUI, executes all the database accesses and provides data encryption. The following chapters give you detailed information on the usage of the IGEL Remote Manager Console.

4 First steps

4.1 Connecting to an IGEL Remote Management Server

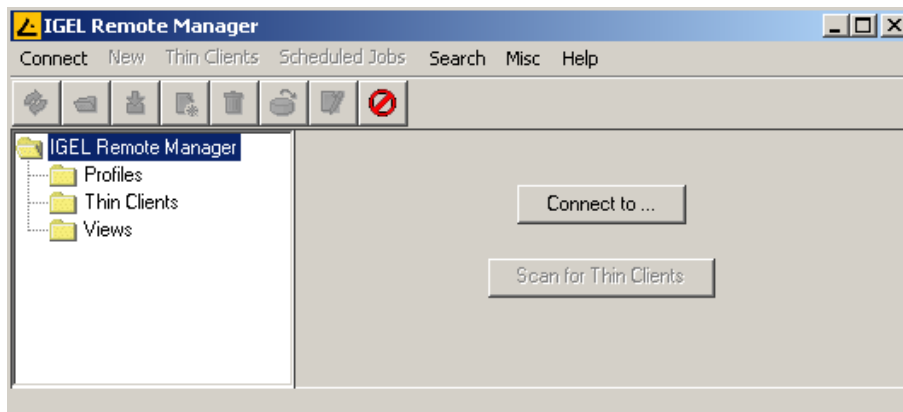


Figure 4-1 First screen after start

After launching IGEL Remote Manager Console, you need to connect to an IGEL Remote Manager server. Click to the **Connect to ...** button in the middle of the screen or choose connect from the menu bar and select **Connect to**

Enter the login data into the popup window as follows:

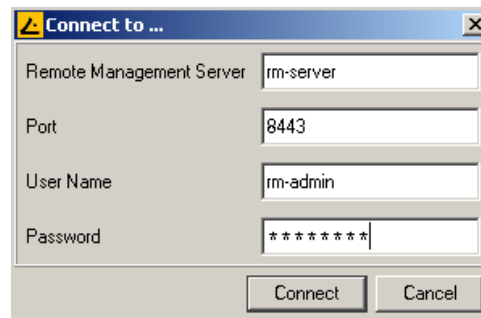


Figure 4-2 Connect window

Remote Management Server: If you have installed the IGEL Remote Manager Console and Server on the same machine, you can use the hostname **localhost**. If you only installed the IGEL Remote Manager Console, enter the hostname of the server you wish to connect to.

Port: This number specifies the port on which the IGEL Remote Manager GUI server accepts connections. This port is by default set to 8443 but may be altered using the IGEL Remote Manager Administration tool.

User name and Password: Specify the user name of the database user account that was created during installation of the IGEL Remote Manager Server. After pressing the Connect button, you will be connected to your IGEL Remote Manager Server.

Note: The server name, the port and the user name that are entered here are stored for future connect procedures. When connecting next time, you just enter the password.

4.2 Scanning for Thin Clients

Click the **Scan for Thin Clients** button or select it from the menu bar via the **Connect to...** dialog. A window pops up - select the network you want to scan.

You can use either your local network or an IP range (depending on your network structure). In order to save time, the use of IP ranges is restricted to class B network ranges. For larger networks and scanning ranges in different networks you can specify a list of network ranges.

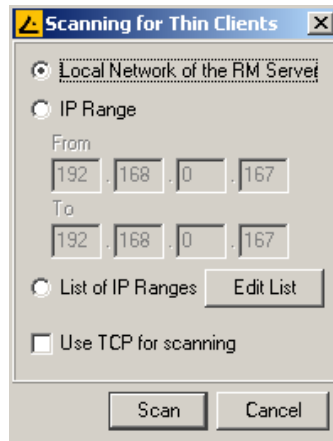


Figure 4-3 Scan window

The scan options are:

- Local Network of the RM Server**
 This sends a broadcast through the network, in which the IGEL Remote Manager Server is located. (Please remember that this might be a different network segment to that of the IGEL Remote Manager Console!)
 If the server on which IGEL Remote Manager Server is installed has multiple network interfaces, only the first is used to send out the broadcast.
- IP Range**
 Every IP in the defined range is contacted by sending a message to it, even if routers prevent broadcast messages.
- List of IP Ranges**
 If multiple network segments need to be scanned, you may set a list of ranges. Use the **Edit List** button and add ranges via the **Add...** button this window:

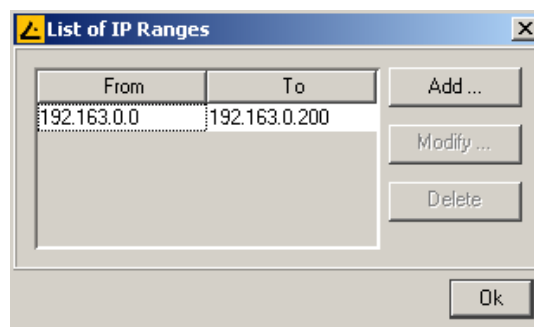


Figure 4-4 IP Range Edit Window

- Use TCP for scanning**
 Choose this option to use TCP instead of UDP for scanning. With TCP scanning works more reliable in some networks, on the other hand it will take a longer time.

Once you have specified the suitable options, click the **Scan** button in the scan window (Figure 4.3).

Note: A Thin Client needs to be up and running in order to scan it. Furthermore, the firmware of the Thin Client needs to support the IGEL Remote Manager software.

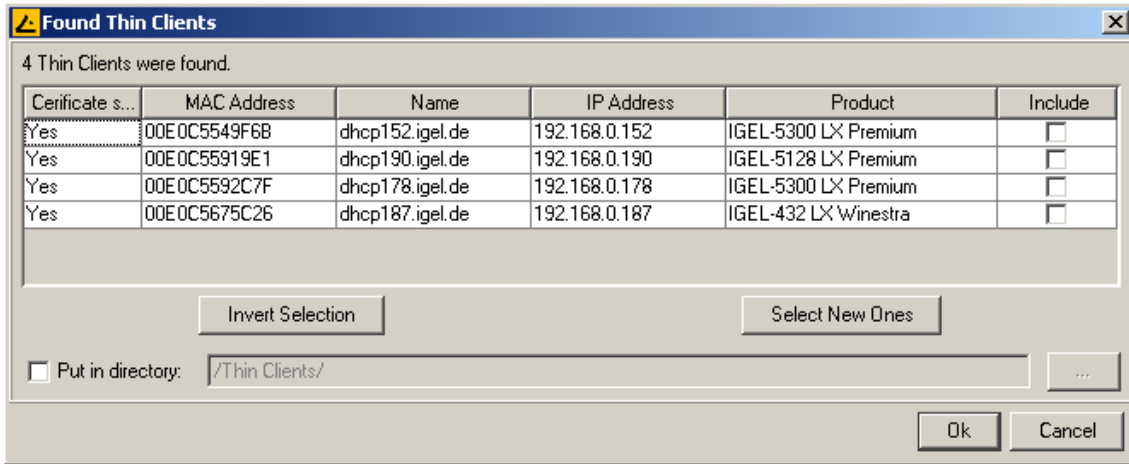


Figure 4-5 Scan result window

After scanning has finished, the detected Thin Clients are displayed in the Scan result window. In the first column, you can see if a Thin Client already has a certificate from an IGEL Remote Manager Server. You need the correct certificate to access this Thin Client (see chapter 9).

When the Thin Client is registered in the IGEL Remote Manager database, the certificate of this server is stored on the Thin Client. Future accesses to this Thin Client will be validated against this certificate. Only the holder of the other private part of the certificate is allowed to control the Thin Client. (For details on certificates, see chapter 9)

Columns 2-5 contain information that allows easier identification of the Thin Clients (MAC address, terminal name, IP address and the product name).

Use the checkboxes in the last column to select which Thin Client(s) you want to register in your IGEL Remote Manager database. After confirming your choice by clicking **OK**, the Thin Client(s) will be registered to your database.

(This may take a while, depending on the performance of the IGEL Remote Manager Server machine.)

After registration, a new window shows the result of the operation and any error messages. Closing this window takes you back to the main screen.

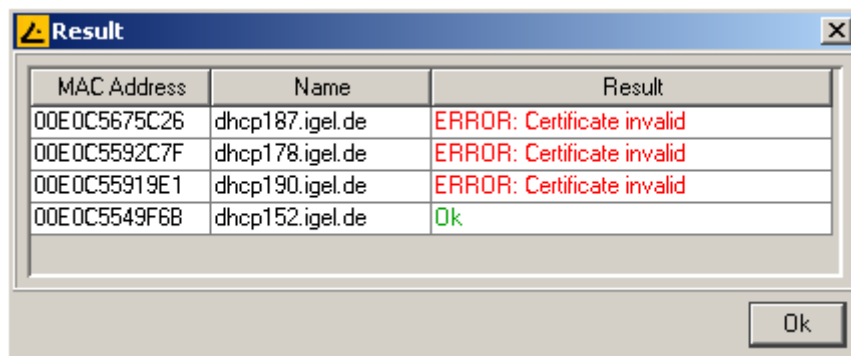


Figure 4-6 Registration result window

Apart from scanning for Thin Clients you can also use the mass import functionality described in Chapter 6.5.

4.3 Launching the Remote Manager Console via Java Web Start

If you have installed J2SE 1.4.2 on your computer, you can launch the IGEL Remote Manager Console without having it installed previously. Just enter the url http://hostname:8080/start_rm.html in your browser or in the Java Web Start manager (*hostname* is name of the computer where you have installed the Remote Manager Server). You can change the port number 8080 with the Remote Manager Administrator tool

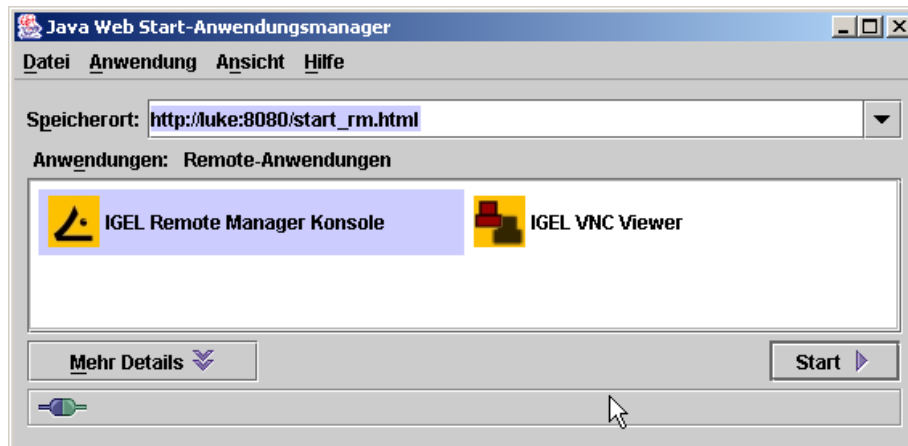


Figure 4-7 Starting from Java Web Start Manager

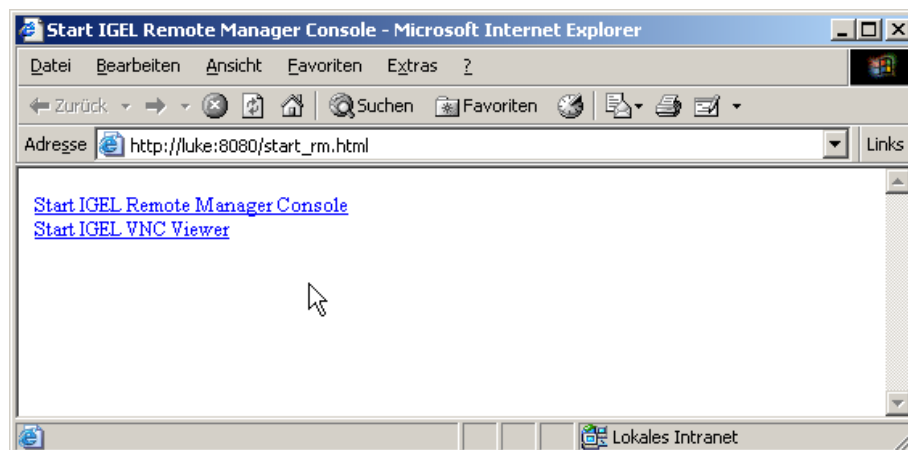


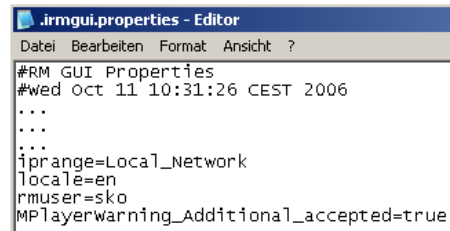
Figure 4-8 Starting from the browser

Two links to applications appear. Click on the link **Start IGEL Remote Manager Console** to launch the Console. The second link launches an application which enables to shadow Thin Clients (or PCs with a VNC server) via VNC (see section 6.8 Shadowing). When you click on the link the application is downloaded to your local PC. Then you get a warning, that the application requires full access to your PC and that you should not start it, but start it nevertheless.

Next you are asked, if you want to integrate the application into your desktop environment, that means if you want to have an icon on the desktop which you can use for launching the application in the future. Now the IGEL Remote Manager Console is started and you can connect to the Remote Manager Server. If you do so, you get again a security warning and you have to confirm again.

4.4 Changing the Locale of Remote Manager Console

By default the IGEL Remote Manager Console uses the locale (the language and other regional settings) of your system. Currently, IGEL Remote Manager only supports the English and the German locales. If the locale of your system is not supported, the English locale is automatically used. However you can switch the locale manually. In order to do this, you must edit the property file `.irmgui.properties` in your home directory (e.g. `C:\Documents and Settings\). This file is created when you use the Console the first time. Add the line locale=en or locale=de for the English or the German locale respectively.`



```
.irmgui.properties - Editor
Datei Bearbeiten Format Ansicht ?
#RM GUI Properties
#wed Oct 11 10:31:26 CEST 2006
...
...
...
iprange=Local_Network
locale=en
rmuser=sko
MPlayerwarning_Additional_accepted=true
```

Figure 4-9 Changing the localization

5 The User Interface

This chapter gives you an overview of the graphical user interface to *IGEL Remote Manager*. The functionality is described in detail in the following chapters.

5.1 Main Screen

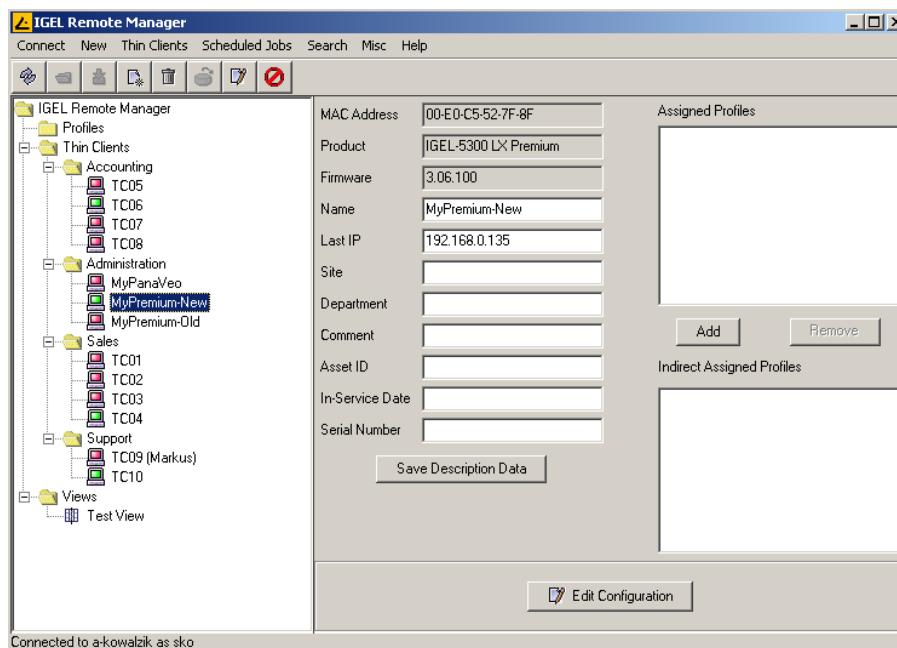


Figure 5-1 Main Screen

The main screen consists of two areas, the *Remote Manager Tree* panel on the left and a content panel on the right. Depending on the selection in the tree, the content panel shows either the content of the directory, information about a single Thin Client, or information on a profile. The *Remote Manager Tree* is divided into three subtrees: *Profiles*, *Thin Clients* and *Views*. All subtrees may contain directories.

The **Thin Clients** subtree contains the Thin Clients registered in the database. If you select a directory, the content panel displays the **Thin Client Directory Content Page**. That page shows information about the content of the directory or assigned profiles. (You can toggle the view by clicking the tabs in the upper left of the screen.)

Every Thin Client (identified by its MAC address) can only appear once in the **Remote Manager Tree**. The name displayed in the tree can be freely modified. It is only used to identify the Thin Client in the Remote Manager and is not necessary identical to the name of the Thin Client in the network, although this internal name is set to the network name when you register the Thin Client the first time. Any name need not be unique and can be used multiple times.

The color of the Thin Client(s) in the **Remote Manager Tree** shows two states: Green if it is online and red if it is currently offline. Detection is performed automatically by frequently sending UDP packets to the Thin Clients which are currently shown in the **Remote Manager Console**.

The **Profiles** subtree allows you to manage your profiles. You can create directories to store profiles and you can add, remove or modify the profiles in this part of the tree.

In the **Remote Manager Tree** you can use *drag and drop* or equivalently the keyboard shortcuts *Ctrl+X* and *Ctrl+V* to perform the following actions:

- Select a number of **Thin Clients**, drag and drop them on a **Thin Client Directory** (or equivalently select the **Thin Clients** press *Ctrl+X*, select a **Thin Client Directory** and press *Ctrl+V*) to move the Thin Clients to a different directory
- You can do the analogous with **profiles**.
- Select a **directory** drag and drop it on another (of the same type). So the first becomes a subdirectory of the second.
- Select a number of **Thin Clients** and **Thin Client Directories** drag and drop them on a **profile**. This results that the profile is assigned to the selected Thin Clients and Thin Client directories

If you press the **Del** key the last selected item will be deleted.

The **Views** tree lists all defined views of Thin Clients. You can create new views, edit or delete existing views and export the view's result as XML file. This tree can also have sub folders to organize your views.

5.2 Main Menu Bar

The main menu bar contains these menu items:

- **Connect**
 - **Connect to ...:** Allows you to establish a connection to an IGEL Remote Manager Server
 - **Reconnect:** Reconnects you to the previously used Server and refreshes all data.
 - **Disconnect:** Disconnects you from the Server without closing the Console application.
 - **Scan for Thin Clients:** Allows you to scan for Thin Clients in the network.
 - **Exit:** Exit and close **IGEL Remote Manger Console**

- **New**
 - **Directory:** Depending on the selection in the **Remote Manager Tree**, you can create a new directory.
 - **Profile:** Creates a new profile in the profile subtree. If no profile directory is currently selected, the new profile will be placed directly below the profiles node in the **Remote Manager Tree**.
 - **Import Profile:** Import a profile from an external profile – XML file.
 - **Thin Client:** Opens a dialog to create manually a Thin Client. You have to enter the MAC address and select a firmware version of the Thin Client. Then you can configure the Thin Client. If automatic detection of the Remote Manager is set up (see 6.7 Automatic Remote Manager Server Detection), the Thin Client with the entered MAC address fetches its configuration the next time it is started.
 - **Import Thin Clients:** Provides the possibility to import multiple Thin Clients at once from a CSV list
 - **Scheduled Job:** Creates a new job to be executed in the future.

- **Thin Clients**

- **Reboot:** Send reboot command to the selected Thin Client(s).
- **Shutdown:** Send shutdown command to the selected Thin Client(s).
- **Update:** Send an update command to the selected Thin Client(s).
- **Wake up:** Send wakeup packet(s) to the selected Thin Client(s). This does not work well in networks with multiple network segments, because the packet is a broadcast packet that is not routed in other subnets.
- **Reset to Factory Defaults:** The selected Thin Client(s) are reset to factory defaults and removed from the database.
- **Send Message:** Send a message to the selected Thin Client(s) to be displayed on the screen
- **MPlayer → Download Codecs:** Thin Client(s) with MPlayer installed are advised to reboot and download new additional Mplayer codecs.
- **MPLayer → Remove Codecs:** Thin Client(s) with MPlayer installed are advised to remove additional Mplayer codecs and reboot.
- **XPe → Create Firmware Snapshot:** Create a firmware snapshot of Windows XP embedded devices. The target server for the snapshot is defined the thin client's settings.
- **XPe → Download Firmware Snapshot:** Assigns the Windows XPe-thin client to download a firmware snapshot from the server defined in its settings.
- **XPe → Snapshots:** Displays all snapshots stored on your server.
- **Shadow:** The desktop of the selected Thin Clients is shadowed via VNC
- **Settings RM -> TC:** Send all settings from the Remote Manager to selected Thin Client(s). If the configuration has been changed, the values will be merged into the current settings of the Thin Clients into the database.
- **Settings TC -> RM:** Read settings from the selected Thin Client(s) into the Remote Manager database. This operation modifies the database values of the Thin Client(s); profiles are not affected.
- **Store Certificate:** Send the server certificate to the Thin Client(s). This enables authorization of the IGEL Remote Manager Server to those Thin Client(s). Every subsequent access to the Thin Client will be validated against this certificate. This prevents other IGEL Remote Managers from reading or altering the Thin Client configuration. After registration of the Thin Client, the certificate is automatically stored on it locally, so this command makes only sense if you have removed the certificate.
- **Remove Certificate:** Causes the selected Thin Client(s) to erase the server certificate(s). This allows any IGEL Remote Manager to take over control of your Thin Client(s).
- **Remove:** This operation completely removes the selected Thin Client(s) from the database. If a Thin Client is offline, you get an error message at first, but you can remove it nevertheless by clicking on the **Remove offline TCs** button, but be aware that then it still tries to get settings from the Remote Manager at every reboot time and it keeps the certificate
- **Take over settings from ...:** With this function you can copy the settings of a profile (with the same firmware) to the selected Thin Client(s). You can choose, if you want to copy only active settings and if you want to add the sessions to the existing ones or delete the existing ones.

- **Edit Configuration:** Shows the configuration page of the selected Thin Client or profile. Only one client or profile at a time may be configured. If you select multiple profiles or Thin Clients and choose this option, only the element last activated will be configured.
- **Access Control:** Allows the assignment of access rights for objects such as folders, profiles or thin clients to different users of the Remote Manager (NOT users on the thin client!).
- **Scheduled Jobs**
 - **Manage All Jobs:** Takes you to the scheduled job configuration. Status information, modifying and removal of scheduled jobs is available.
 - **Assign Jobs:** Assigns a new job to the currently selected (in the **Remote Manager Tree**) Thin Clients
- **Search**
 - **Thin Clients:** Allows to search for thin clients by data such as name, IP address, MAC address and other.
 - **Profiles:** Allows to search for profiles by data such as name or firmware version.
 - **Views:** Allows to search for views that have been defined before (see chapter *Thin Client Views*).
- **Misc**
 - **Default Directories:** Configure rules to automatically move Thin Clients to certain directories when they get registered.
 - **Online Check:** Configure if and how often it is checked, if the displayed Thin Clients are online
 - **Look and Feel:** Change the look and feel of the application. There are several skins available that can be selected here. The default style is *System*.
 - **Firmware Statistics:** Get an overview how many Thin Clients and profiles have the different firmware versions
 - **Remove Unused Firmwares:** Remove firmware versions currently not used from the database (better performance!)
 - **Change Password:** The currently logged in user can change his own password.
 - **Administrator Accounts:** Create new RM Administrator users and groups.
 - **SQL Console:** Query directly the Remote Manager database (if you are familiar with SQL). NOTE – doing so can damage the Remote Manager database!
- **Help**
 - **Help:** View the online manual (substantially identical to this manual)
 - **Info:** Pops up an information page displaying the exact version of your IGEL Remote Manager and copyright information.

Note: The functions **Reboot**, **Shutdown**, **Update on next Boot**, **Settings RM -> TC** and **Remove** will query the local user, if the command should be executed immediately or during next boot. If the user does not answer the query within a certain time, the command will be carried out anyhow. The default delay is 20 seconds, but may be manipulated via the Client's registry: **userinterface.rmagent.enable_usermessage** allows you to turn off the query and **userinterface.rmagent.message_timeout** is responsible for.

5.3 Thin Client Content Panel

When you select a Thin Client in the **IGEL Remote Manager Tree**, the right side of the main screen displays the **Thin Client Content Panel**. This panel gives you information about the selected Thin Client and allows you to modify the settings.

MAC Address	00-E0-C5-54-9F-6B
Product	IGEL-5300 LX Premium
Firmware	3.05.500
Name	My Own TC
Last IP	192.168.0.152
Site	
Department	
Comment	
Asset ID	
In-Service Date	
Serial Number	

Assigned Profiles

- My IGEL

Buttons: Add, Remove

Indirect Assigned Profiles

Buttons: Save Description Data, Edit Configuration

Figure 5-2 Thin Client Content Panel

- **MAC Address:** This is the hardware address of the Thin Client.
All operations in the database use this string to refer to the Thin Client.
- **Product:** The product name of the Thin Client.
- **Name:** You may enter an arbitrary string to identify the Thin Client. This string is then displayed in the **IGEL Remote Manager Tree** and should be self explanatory. When the Thin Client is registered in the database, the currently set name of the Thin Client will be used. (Further scanning will not overwrite this set name!)
- **Last IP:** The last known IP of the Thin Client.
This address is always updated if the Thin Client gets in contact with the IGEL Remote Manager Server again.
(You may manually edit this value, if for some reason the Thin Client has a different IP address since the last access and thus is not reachable for the IGEL Remote Manager.)

The other strings (**Site**, **Department**, **Comment**, **Asset ID**, **In Service Date** and **Serial Number**) can be freely chosen to ease identification of your clients.

On the right side of the **Thin Client Content Panel** the **Assigned Profiles** and **Indirect Assigned Profiles** are listed. You can assign new profiles or remove profile assignments to the Thin Client by using the **Add** respectively the **Remove** button below the list of **Assigned Profiles**.

The list of **Indirect Assigned Profiles** is for information only. This list shows profiles that are assigned to directories that contain the specific Thin Client in the **IGEL Remote Manager Tree**. If the Thin Client resides in a subdirectory, all the profiles assigned to this subdirectory and the profiles assigned to the parent directory will be listed.

Change the profile assignments of the parent directory or move the Thin Client into another location in order to change the indirect assigned profiles.

Double clicking on an entry in the profile list has selects this profile in the **Remote Manager Tree**. If you point on an entry, a tool tip appears which shows the complete path where the profile is stored and the internal id of the profile.

The profiles are sorted according to there precedence, that means a profile prior in the list overrides settings of subsequent profiles. The precedence of a direct assigned profile is always higher than a indirect assigned profile (see 9.5 Assigning Profiles for details).

On the bottom of the panel is the **Edit Configuration** button. This button leads you to the Thin Client configuration that will pop up in a separate window. This window allows you to configure the Thin Client settings (see 6.1 Modifying Thin Client Configuration).

5.4 Thin Client Directory Content Panel

Select a directory in the in the **Thin Clients Subtree** of the **IGEL Remote Manager Tree** to show the **Thin Client Directory Panel**

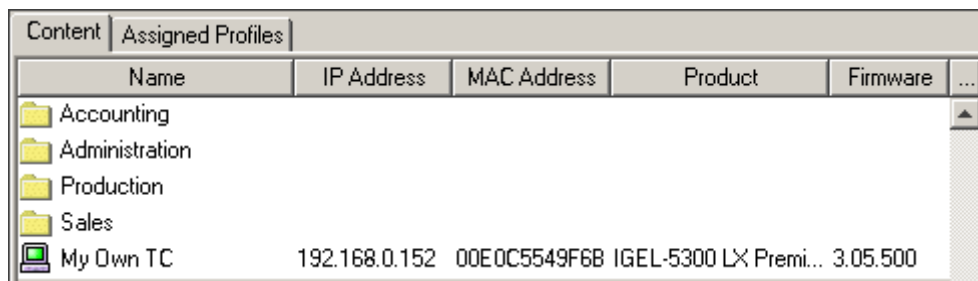


Figure 5-3 Thin Client Directory Content Panel

The panel contains the tabs **Content** and **Assigned Profiles**. Using these tabs you can toggle between the content and the profile view of the directory.

The **Content** view shows all objects located directly below the directory in the **IGEL Remote Manager Tree**. Objects can either be Thin Clients or directories.

You can choose the columns to be displayed by clicking on the ellipsis in the upper right corner. Double clicking an object will make this the active object in the **IGEL Remote Manager Tree** and the content panel will change according to the selection.

You can also right click an object to make the corresponding context menu appear.

If you activate the **Assigned Profiles**, the profiles dedicated to this directory will be listed. Once you activated the profile view, all the directories will show the profile unless you toggle the view back to the context view. Use the **Add** and **Remove** button to alter the profile assignments. Double clicking on the profile has the effect, that this profile is selected in the **Remote Manager Tree**.

Note: Modifying the assignment affects the whole subtree below the current directory!

5.5 Profile Content Panel

Select a profile from the **Profiles** subtree in the **IGEL Remote Manager Tree** to display the **Profile Content Panel**.

This panel allows you to change the profile assignments from the profile view. Here, you add or remove Thin Clients or directories to the list of **Assigned Objects**. This operation has the same effect as if you assign the profile to the object directly.

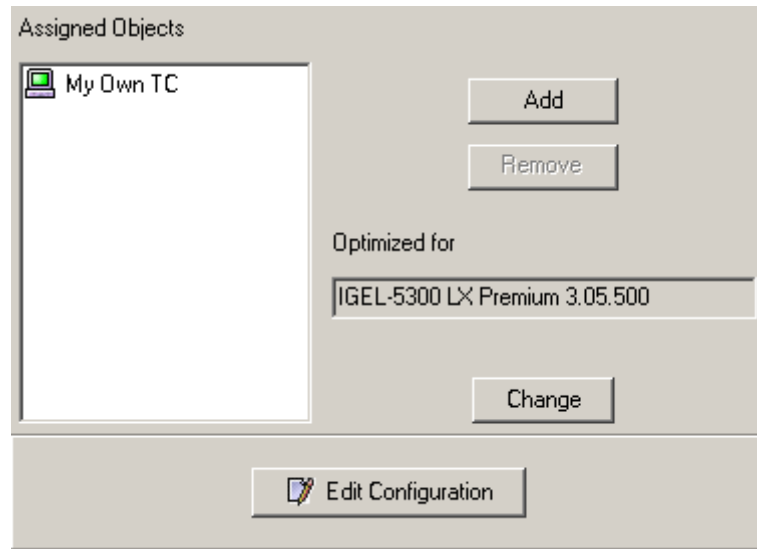


Figure 5-4 Profile Content Panel

When clicking **Add**, you will get a window that allows you to select one or more objects. Keep the **Ctrl** key pressed if you want to select multiple clients. Use the **Shift** key if you want to select a range of objects.

If you double click on an assigned object to it becomes selected in the **Remote Manager Tree**.

The string below **Optimized for** indicates the original firmware version for the profile. If you have different Thin Client models in your environment or your Thin Clients have different firmware versions, they might have different features. For example, if you created a profile based on Winestra, a browser session cannot be configured. The configuration page of the profile will only provide configuration options that the firmware version offers. Anyway, you can assign the profile to every Thin Client regardless its firmware version.

If you want to change the firmware version on which the profile is based, click on the **Change** button. Then you can select from the firmware versions which are available in the database. Note that settings of parameters which are not present in the new firmware version are lost.

Below the firmware version is the button **Edit Configuration**. Pressing this button brings up the configuration page of the profile.

Refer to section 9.4 Edit Profile Settings for more information about modifying profile configurations.

5.6 Profile Directory Content Panel

Directories in the **Profiles** subtree of the **IGEL Remote Manager Tree** are used only for structural reasons. They have the same function as folders on a hard disk. You can have an arbitrary number and levels of directories.

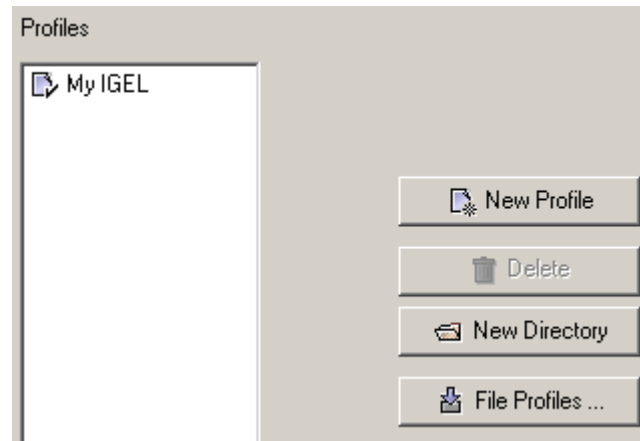


Figure 5-5 Profile Directory Content Panel

If you activate such a directory in the **IGEL Remote Manager Tree**, the **Profile Directory Content Panel** will appear in the content panel. The string in the upper left shows the name of the current directory name.

Below the name is the content list of the selected directory. This list contains directories and profiles that are located directly below the directory in the **IGEL Remote Manager Tree**. If you double click an object, it will become the active object. The content page will change according to the object type. Right clicking an object will give you access to the object's context menu.

On the right side of the content panel are several buttons. The buttons provide the following functions:

- **New Profile:** The new profile page will pop up. This operation creates a new profile in the selected directory. Please refer to section 9.2

Creating Profiles for detailed information about creating profiles.

- **Delete Profile:** This option will only be available, if you have previously selected one or more profiles from the list. When deleting the profile, all profile assignments will be deleted as well.
- **New Sub Directory:** Creates a new directory inside the currently selected directory. Please refer to section 9.1 Organizing Profiles for information about profile directories.
- **Delete Sub Directory:** Deletes the selected directory.
- **File Profiles...:** Allows you to move profiles into the current directory. You will get a selection window to choose a single or multiple profile(s) that should be moved into the current directory.

Note: When deleting a directory, the profiles inside of that directory will not be deleted! They will be moved to the **Profiles** node in the **IGEL Remote Manager Tree**. Profile assignments will not be affected.

5.7 Context Menus

The IGEL Remote Manager Console provides context menus for directories, profiles and Thin Clients (reachable by right mouse click).

The context menu for directories contains these entries:



Figure 5-6 Context menu of a directory

- **Move Thin Clients here:** You can move Thin Clients into the current directory by using this item and selecting a single or a set of Thin Clients afterwards. Depending on what is selected, it may also be **Move profiles here** or **Move objects here**.
- **Rename:** Modify the name of the current directory.
- **New Sub Directory:** Create a new directory inside of the currently selected directory.
- **Delete:** Delete the marked directory.

Note: When deleting a directory, the Thin Clients inside the directory will be moved to the **Thin Clients** node. This automatically means that the Thin Client will lose all settings of profiles that are associated with the deleted directory and possible mother directories! Profiles will be moved to the **Profiles** node, but unchanged. Objects will be treated intuitively as Thin Clients or profiles.

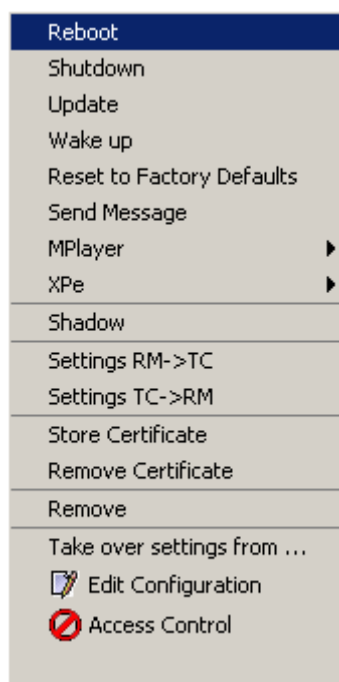


Figure 5-7 Thin Client context menu

The context menu of Thin Clients has the same items as the **Thin Clients** menu of the main menu bar. The difference is that only a single Thin Client can be affected by an operation.

The context menu of profiles offers these options:



Figure 5-8 Profile context menu

- **Edit Configuration:** Opens the configuration page for the selected profile.
- **Rename:** Allows you to modify the name of the profile.
- **Delete:** Removes the profile and all its assignments. The profile will be deleted from the database and all data of the profile will be permanently lost.

5.8 Search Menus

Menu points **Search → Thin Clients** and **Search → Profiles** provide search and filter functionality. Both, the profile search dialog and the thin client search dialog can be configured to search for a certain criterion, if the criterion is case sensitive and the required accuracy the profile's or thin client's attribute must match the criterion.

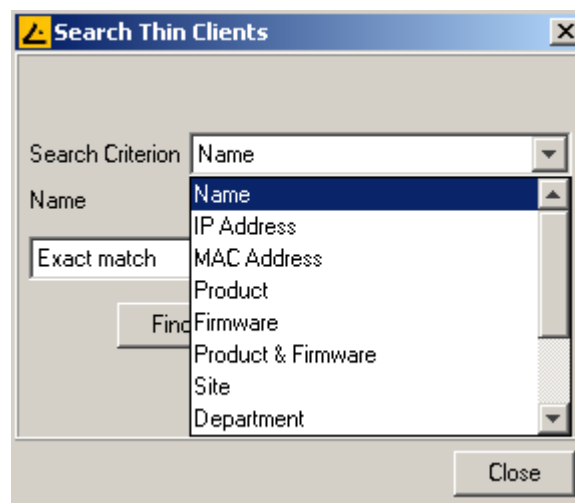


Figure 5-9 Thin Client search criteria

There are three levels for the accuracy:

- **Exact match:** the attribute is equal to the search criterion
- **Contains:** the attribute contains the text provided as search criterion
- **Use Regular Expressions:** the user can define a matching rule based on regular expressions

5.9 Shortcuts

Between the **Main Menu Bar** and the **IGEL Remote Manager Tree** reside some icons that are shortcuts to several operations. Depending on the selection in the **IGEL Remote Manager Tree**, some of them may not be active.



Figure 5-10 Shortcut icons

From left to right they perform the following operations:

- **New Sub Directory:** Create a new directory inside of the currently selected directory.
- **Move Objects here:** Move Thin Client(s) or profile(s) into this directory by selecting Thin Client(s) after clicking this icon.
- **New Profile:** Creates a new profile in the profile subtree. If no profile directory is currently selected, the new profile is situated directly below the **Profiles** node in the **Remote Manager Tree**.
- **Delete:** Deletes the selected object in the **Remote Manger Tree**.
- **Edit Configuration:** Takes you to the profile's or the Thin Client's configuration page.

6 Managing Thin Clients

6.1 Modifying Thin Client Configuration

In order to modify the configuration of a Thin Client, select the desired Thin Client in the **Remote Manager Tree** and click the shortcut symbol or choose **Edit configuration** from the main menu item **Thin Clients**. You can also click on the Thin Client with the right mouse button and choose **Edit configuration** from the context menu.

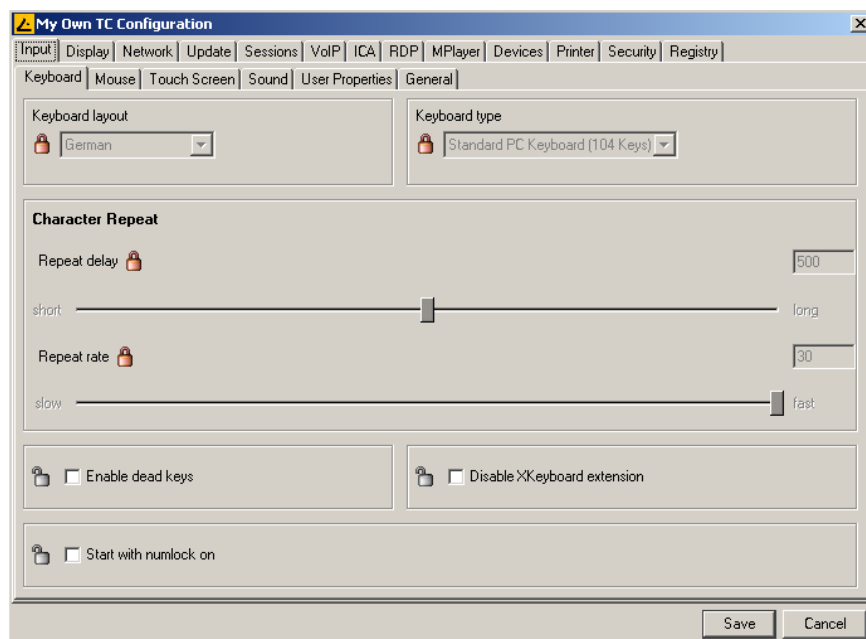




Figure 6-1 Configuration Window

The configuration page of the Thin Client will pop up enabling you to modify the entries. Please refer to the Thin Client's manual for detailed information about the configuration pages.

Each parameter in a configuration page contains either an open or closed lock. The open lock  means that the parameter can be modified here. A closed lock  indicates that this parameter is defined in a profile assigned to the Thin Client itself or a directory that contains the Thin Client. If you point on the lock, you get a tool tip, from which profile the value originates.

Note: Each parameter has two types of values, the values defined by the Thin Client and the values defined by the profiles. They exist in parallel and the rule is that the profile settings always have precedence. If you assign a profile with a value for a parameter and remove the assignment, the value of the parameter changes back to its previous state. The profile value does not get copied into the Thin Client settings!

After you have changed the configuration and pressed the **Save** button, you get asked whether the settings take should take effect after next boot of the Thin Clients or now. In both cases at first the settings are stored in the database. If you choose **Next Reboot** nothing else is done, because at every boot the Thin Client fetches its settings automatically. If you choose **Now** the new settings are transferred to the Thin Client immediately. If the Thin Client is currently offline, this operation fails and the Thin Client gets its setting as recently as it boots again.

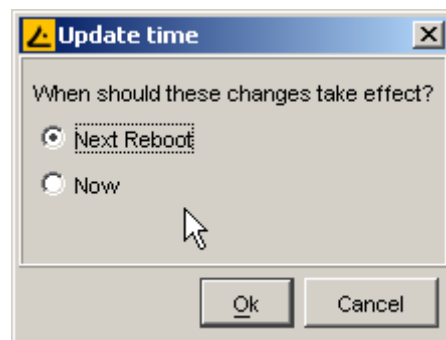


Figure 6-2 Update data popup

Note: If you have chosen **Now**, the user in front of the Thin Client is asked, if the new settings should apply immediately. As in the case with commands sent to the Thin Client (see 5.2 Main Menu Bar), you can change this behavior by means of the registry parameters ***userinterface.rmagent.enable_usermessage*** and ***userinterface.rmagent.message_timeout***.

6.2 Send Configuration

Configuration changes are done in the database and transferred regularly to the Thin Client on system boot. If you want to update the configuration of the Thin Client instantly, you need to initiate the data transfer manually. This can be achieved by selecting a Thin Client, a directory or a group of Thin Clients and choosing **Settings RM -> TC** from the **Thin Client** menu. Keep the **Ctrl** key pressed if you want to select multiple items. Use the **Shift** key if you want to select a range of Thin Clients.

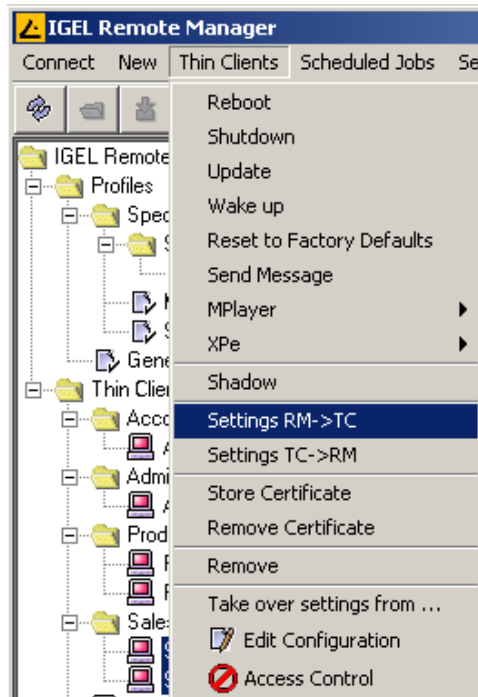


Figure 6-3 Select action **Settings RM -> TC** from **Thin Client** menu

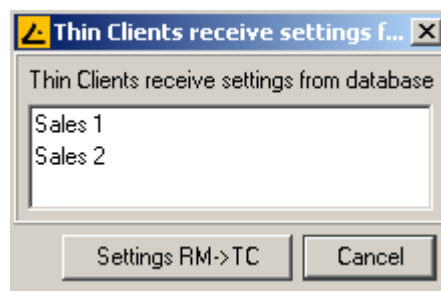


Figure 6-4 **Settings RM -> TC** popup

After choosing the command, the above list of selected Thin Clients will appear. You can now cancel the operation or click on **Settings RM -> TC**. The local settings of the Thin Client will then be updated to the settings from the database. Again, on the Thin Client, a message will pop up which informs the user about the new configuration and asks, if the new configuration should take immediate effect or not. You can change this behavior as described above.

6.3 Retrieve Configuration

When changing the configuration locally by using the Thin Clients built-in setup utility, the configuration changes are usually transferred to the IGEL Remote Managers database. In case of network failures or if the **IGEL Remote Manager** server was down, the configuration changes might not be stored successfully. For such cases, perform the read out of the local settings from the Thin Clients manually here.

Select the Thin Clients that you want to access and choose **Settings TC -> RM** from the **Thin Clients** menu. Click **Settings TC -> RM** in the popup window that shows the selected Thin Clients. Now the local settings will be gathered and the database will be updated accordingly.

Note: This operation is an exception and rarely required.

6.4 Thin Client Codecs

This functionality only affects Thin Client models with Mplayer software installed. By default there is just a basic package of codecs delivered as a component of the Thin Clients firmware. Additional codecs can either be installed locally by the Thin Client's user or remotely by the **RM Administrator**. The codec source file can be configured in a profile or directly for Thin Client.

To advise a Thin Client to download additional Mplayer codecs select menu point **Download Codecs** from the Thin Client menu. Note that a Thin Client must be online to receive this command (eventually first wake them up). Now the selected thin Clients will reboot and start with the download and installation process.

Use menu point **Thin Clients → Remove Codecs** to remove the additional codecs. Codecs integrated in the Thin Clients firmware are not affected by this command.

6.5 Registering from the Thin Client

Besides the way described in section 4.2 Scanning for Thin Clients there is another way to register a Thin Client at the **IGEL Remote Manager**. In order to use this second method you have to be in front of the Thin Client you want to register. If the application **Register Client at RM** is not already present in the **Application Launcher**, select **Register Client at RM** on the **Config** tab of the **Application Launcher**, select **Register Client at RM**, click on **Edit** and check **Enable in Application Launcher**. Now start the **Register Client at RM** application from the **Application Launcher**.

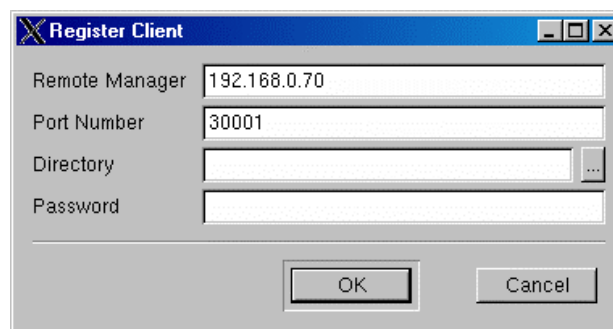


Figure 6-5 Register Client at RM

Enter the Remote Manager Server and the server port (default 30001). Optionally choose a directory of the Remote Manager Tree where the Thin Client is put. Finally enter the password (initially it is the same as the Remote Manager user password, but you can specify a different one with the Remote Manager Admin tool.) and click on **OK**.

6.6 Thin Client Mass – Import

Apart from the functionality described in section 4.2 and 6.2 there is another procedure for RM Administrators to create Thin Client instances, without even having connected any of them. You can create new Thin Clients by importing CSV (Comma Separated Values) files containing all necessary data, in particular MAC-address, the Thin Client's name, and firmware information. These files could be built by any external tool, like spreadsheet editors or simple text editors, that enable you to save tabular data with an “;” as delimiter.

Short Format:

In short format import files, each column is composed of

- MAC-address
- Thin Client name
- Firmware – ID

Administrators can get this firmware id from the information the **Firmware Statistics** dialog provides.

Long Format:

In long format import files there can be provided a target directory where the Thin Client instances are created and some additional Thin Client data as well.

Each column is composed of

- target directory
- MAC-address
- Product
- firmware
- Thin Client name
- site
- department
- comment
- assetid
- inservice date
- serial number

Select menu point **New → Import Thin Clients** from the Remote Manager menu and the Thin Client Import dialog will appear:

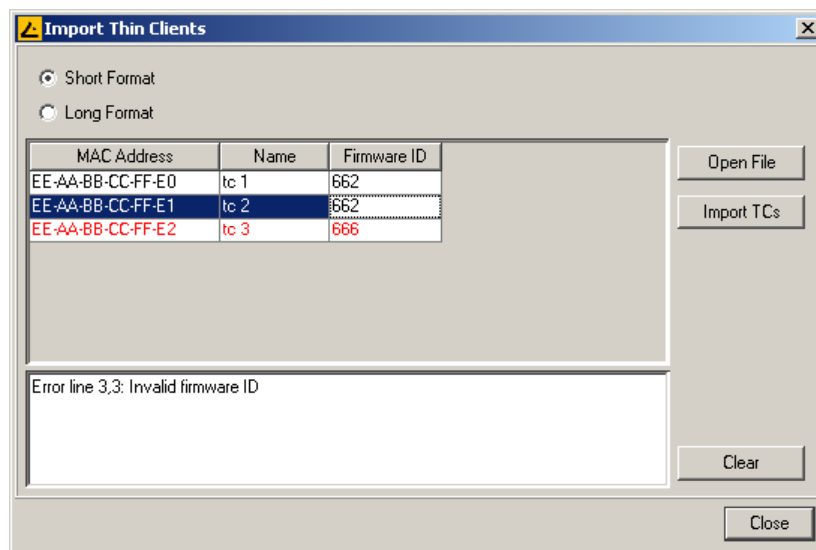


Figure 6-6 Thin Client Import Dialog (Short Format)

You can choose the short column - format for your CSV file or the long, more verbose format containing additional data. In the example above a short format CSV file has already been opened (Open File – button). Its content would have looked like this:

```
EE-AA-BB-CC-FF-E0;tc 1;662  
EE-AA-BB-CC-FF-E1;tc 2;662  
EE-AA-BB-CC-FF-E2;tc 3;666
```

If there is any invalid data like a non existing firmware id (see Figure 6.6), or an error appeared during the import process, an appropriate message is displayed in the message screen in the lower part of the dialog and the line of the affected Thin Client is marked red.

Button Clear removes all messages from the screen.

Button Import TCs starts the import process. Successfully imported Thin Clients are marked green.

When Long Format is selected the Thin Client Import will appear like this:

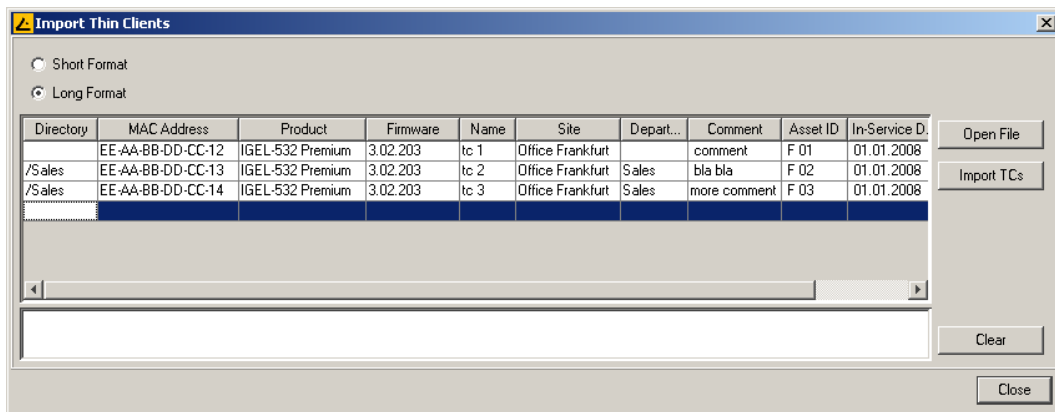


Figure 6-7 Thin Client Import Dialog (Long Format)

The import dialog also provides some basic editor functionality to do some final changes:

- use Ctrl-C to copy a marked line
- use Shift – Insert to insert a line marked for copying
- use Delete to remove a marked line
- press Return / Enter on a field in the last row and a new line will be inserted

6.7 Automatic Remote Manager Server Detection

When you register a Thin Client in the Remote Manager, the IP of the Remote Manager Server is stored on the Thin Client (registry key *system.remotemanager.server0.ip*) and the Thin Client will connect to this IP address to get its settings at every boot time. But there is another way to let the Thin Client know the IP address of the Remote Manager server. First you can specify this IP address with the DHCP option 224. The second way is, to create an alias called **igelrmserver** to the Remote Manager Server in your DNS.

You have to setup one of these possibilities, if you want to insert manually Thin Clients into the Remote Manager database (see 5.2 Main Menu Bar), otherwise the Thin Client cannot connect to the server in this case.

6.8 Shadowing

With the **IGEL Remote Manager Console** you can shadow the desktop of a Thin Client on your local PC using VNC. In order to enable shadowing choose the **Security – Shadow** tab of the configuration dialog.

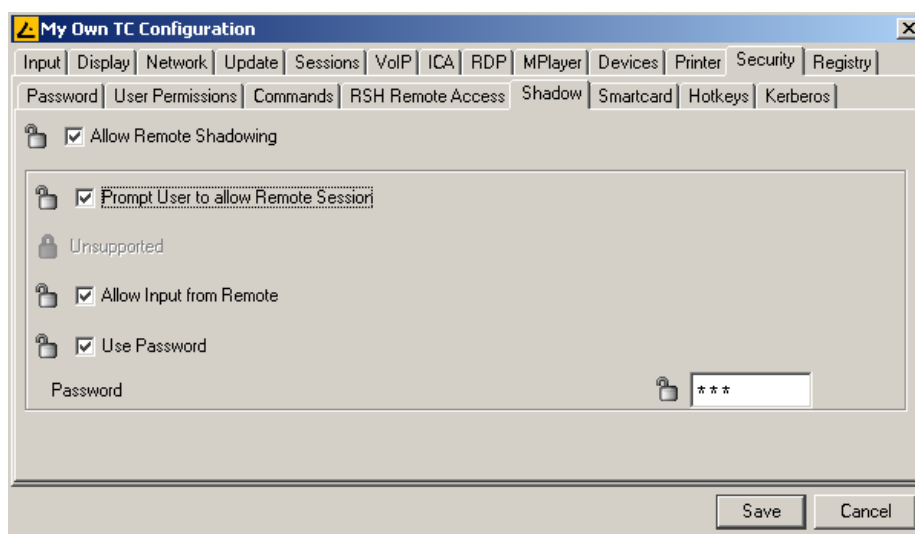


Figure 6-8 Configure shadowing

Now select the Thin Client in the **Remote Manager tree** and select **Thin Client – Shadow** from the main menu. A connection dialog appears where you have to enter the password if you have defined one.

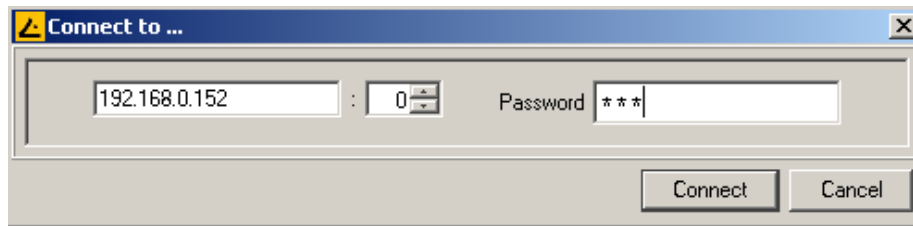


Figure 6-9 Shadowing connect

Furthermore we provide the application **IGEL VNC Viewer** for the purpose of shadowing. Use this application if you do not have the right to use the **Remote Manager Console** or if you want to shadow a device which is not present in the Remote Manager database.

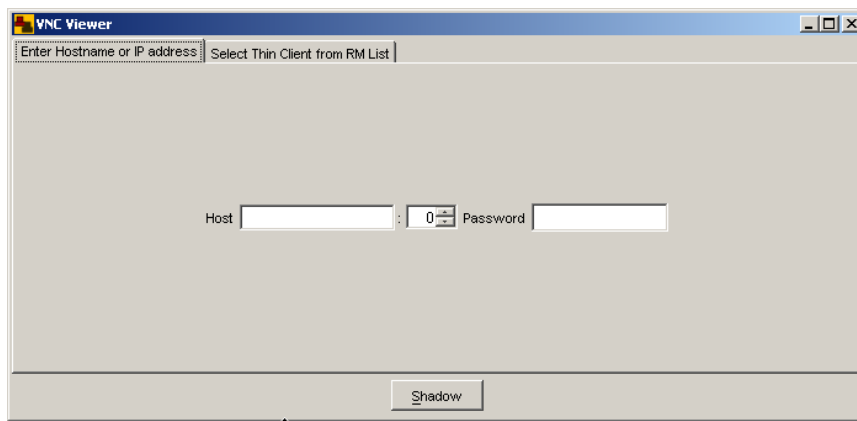


Figure 6-10 IGEL VNC Viewer

You can specify manually a hostname or IP address on the first tab. On the second tab you can select a Thin Client from the Remote Manager tree. If you want to use this second feature you must have a user account to connect to the Remote Manager server.

When the VNC session is established, the remote desktop appears in the following window:

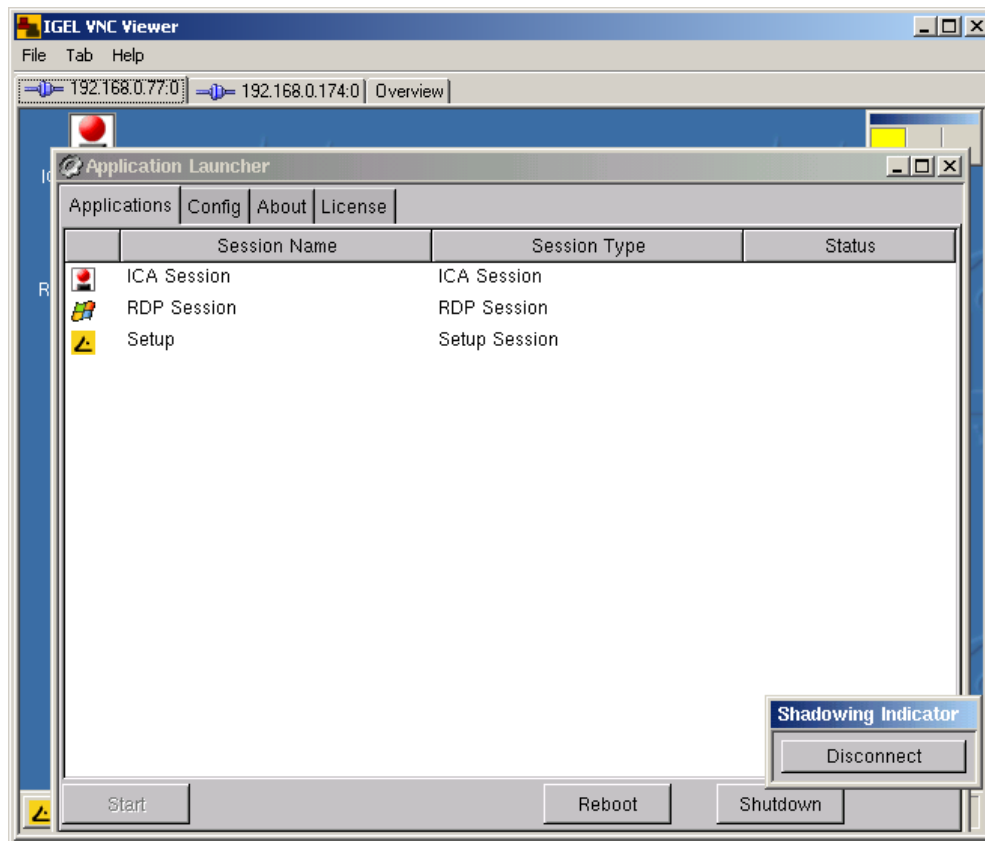


Figure 6-11 Remote Desktop

This window provides its own menu, which contains the following items:

- **File**
 - **Show Overview:** Shows an overview of all currently connected VNC sessions (see Figure 6-12 Overview window). You can double-click on one of the shown remote desktops to see it in full size again.
 - **Quit:** Quits all VNC sessions and closes the window.
- **Tab**
 - **New:** Opens the connection dialog (see Figure 6-9 Shadowing connect) so that you can start an additional VNC session.
 - **Resize:** Adjust the size of the window to the size of the currently shown remote desktop.
 - **Send Ctrl-Alt-Del:** Sends the Ctrl-Alt-Del key combination to the currently shown remote host.
 - **Refresh:** Updates the content of the window.
 - **Screenshot:** Writes a screenshot of the window content to the local disk.
 - **Options:** Opens an dialog where you can specify some options (see below).
 - **Close:** Closes the currently selected tab.
- **Help**
 - **About:** Shows the software version of the IGEL VNC Viewer.

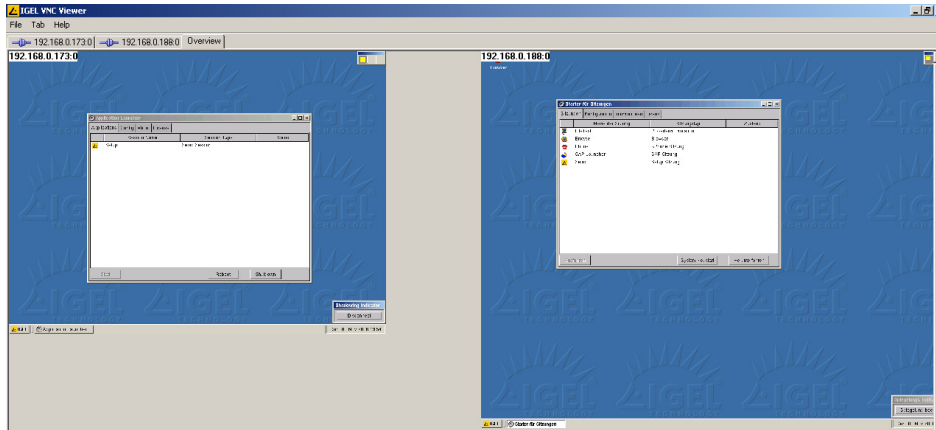


Figure 6-12 Overview Window

In the options dialog (see Figure 6-13 Options dialog) you can specify the following options:

- **Preferred Encoding:** The encoding used for image data send from the Thin Client to your PC. The **Tight** encoding is especially useful on a network with low bandwidth. It has two additional parameters, the **Compression Level** (the higher the compression level the higher is the computing time!) and the **JPEG Quality** (if you choose **Off**, no JPEG data is sent).
- **Use "Draw Rectangle" mode:** This option increases performance (but you may see artifacts).
- **Color Depth:** 8 or 24 bits per pixel
- **Refresh Period:** The VNC Viewer requests an update from the remote host after this period has been elapsed since the last update. A longer time period reduces network traffic but the update is less smooth. Note that if you move the mouse or type a key inside the VNC Viewer (and so this event is sent to the remote host), an update request is sent immediately.
- **Save properties as defaults:** Saves the current settings as defaults for future VNC sessions.

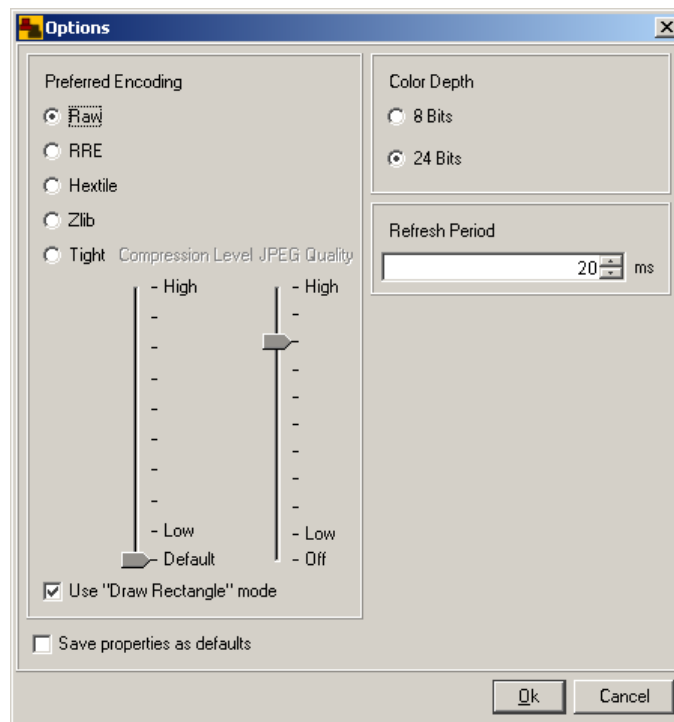


Figure 6-13 Options Dialog

7 Grouping Thin Clients

7.1 Creating new Directories

IGEL Remote Manager allows you to set up groups of Thin Clients. Using this feature enables you to link profiles to any group member without changing the individual configurations. It is also useful to separate Thin Clients from each other and visualize their organizational structure.

Grouping of Thin Clients is done by creating directories and moving Thin Clients that belong to the same group into the same directory. You may create as many directories and subdirectories as needed. If you create subdirectories, the profiles assigned to the top directories will also affect the subdirectories. This means that you can even group groups of Thin Clients.

In order to create a directory or a subdirectory, select either the subtree **Thin Clients** or any directory in this subtree. Now click **New -> Directory** in the main menu bar, use the shortcut for new directory or choose **New Sub Directory** from the context menu of the selected directory.

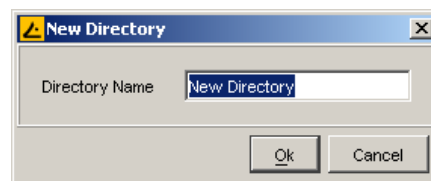


Figure 7-1 New directory popup

Now enter the name for the new directory and click **OK**. The new directory will appear directly below the selected directory or below **Thin Clients**. You can now move Thin Clients into this new directory.

7.2 Moving Thin Clients

The simplest way to move Thin Clients from one directory to another is to use drag and drop on the **Remote Manager Tree**. Keep the **Ctrl** key pressed if you want to select multiple clients. Use the **Shift** key if you want to select a range of Thin Clients.

If your tree has a lot of entries, the second provided method may be more comfortable. Choose the option **Move Thin Clients here** from the context menu of the directory, or click on the **Move Objects here** shortcut. You will get a selection window that allows you to choose which Thin Clients shall be moved to the currently selected directory. After pressing **OK** the selected Thin Clients will be moved to their new location.

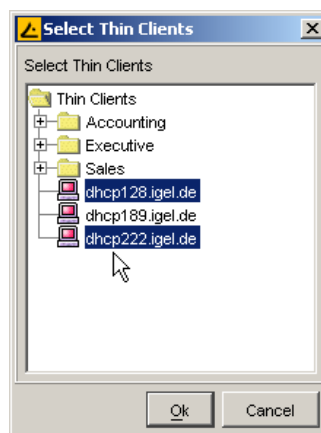


Figure 7-2 Selection window

Note: This operation does not send anything to the Thin Clients. The Thin Client does not get information about profiles that might be already assigned to the directory. The Thin Clients will get the new profile assignments on next boot or if the new settings are sent manually.

7.3 Default Directory Rules

You may define default directory rules so that Thin Clients are moved automatically to certain directories (according to those rules), when they are registered. If you have assigned profiles to those directories, the Thin Clients get their appropriate settings then, so the only thing you have to do, is to register the Thin Clients.

To define such rules, select **Default Directories** from the **Misc** menu. The following dialog appears:

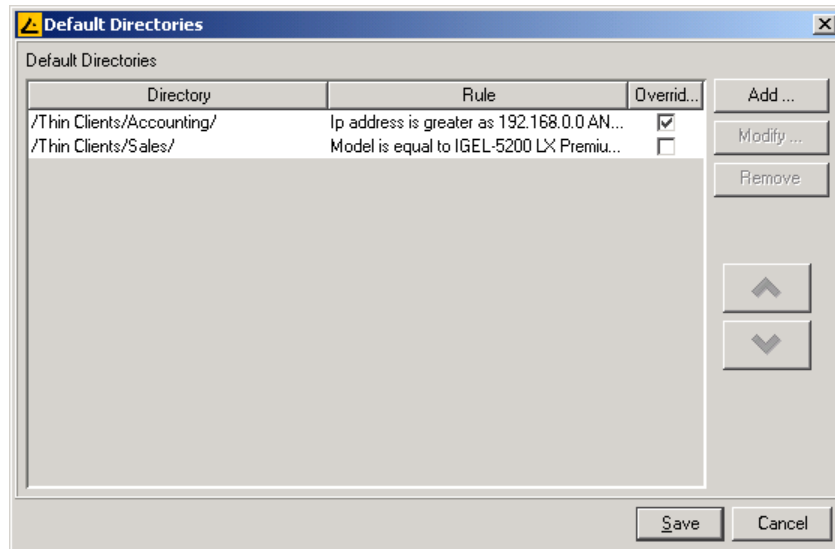


Figure 7-4 Default Directory dialog

In this dialog you see the list of the already defined rules. With the **Add**, **Modify** and **Remove** buttons you can add a new rule or modify or remove an existing rule respectively. You also can change the order of the rules by using the **Up** and **Down** buttons. The order of the rules is important, because the *first* rule which is fulfilled by a Thin Client defines the directory where the Thin Client is put.

If you click on the **Add** button to create a new rule, the following dialog appears:

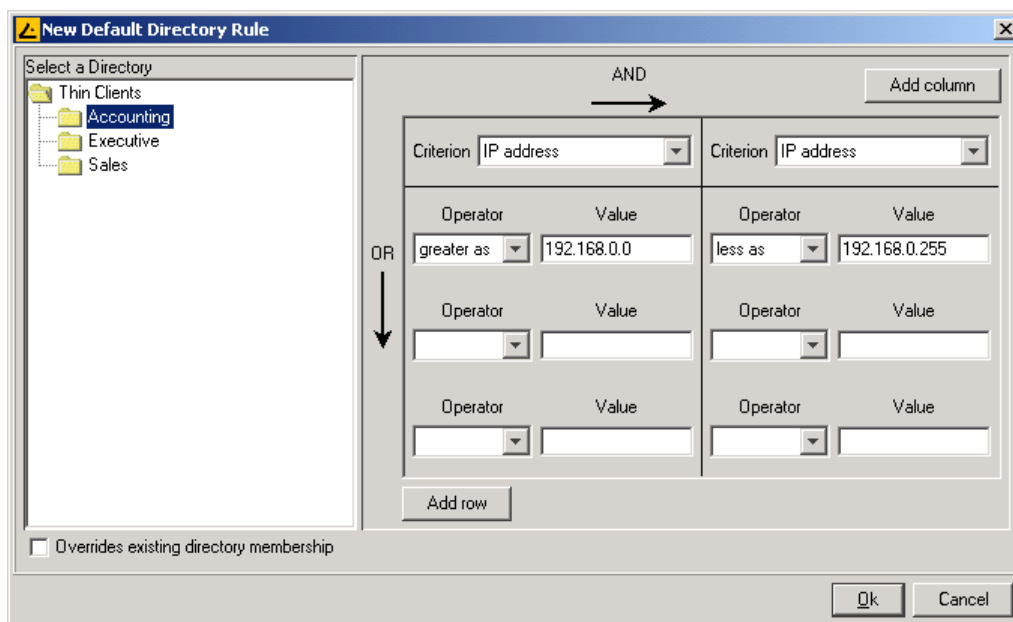


Figure 7-5 Rule dialog

First you have to choose the directory (in the tree on the left side of the dialog) where the Thin Clients are to be put, if they comply with this rule. Then you may check the option **Overrides existing directory membership**. If you check this option, a Thin Client that has been registered already and is now registered again, is moved to the target directory of the rule, although it resides already in another directory.

Next you have to define the conditions which must be fulfilled, so that this rule is applied. The conditions are defined in the table on right side of the dialog. In the first row you have to choose a criterion, available criterions are **IP address**, **Name** (of the Thin Client), **Product name** and **Firmware version**. The criterion refers to the column below. In this column you define constraints of the chosen criterion, e.g. the IP address is greater as 192.168.0.0. If you choose the **like** operator, you have to specify a regular expression (see <http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/Pattern.html>) as value.

A Thin Client fulfils a rule, if all constraints in the first row are met or all constraints in the second row are met or all constraints in the second row are met or all in the third row are met ... Consider the following example:

AND			Add column
Criterion	Product name	Criterion	Firmware Version
Operator	Value	Operator	Value
equal to	IGEL-5200 LX Premium	greater as	3.4.300
Operator	Value	Operator	Value
		like	sales.*
Operator	Value	Operator	Value
Add row			

OR

Figure 7-6 Rule example

A Thin Client fulfils this rule, if it is IGEL-5200 LX Premium with firmware version higher as 3.4.300 or its name starts with "sales".

8 Views

A Thin Client view is a list of Thin Clients defined by a rule. All Thin Clients which fulfill this rule appear in the view. For instance you may want to watch the list of Thin Clients whose IP address is in a certain range. To achieve this you can define a view whose rule is defined by the IP address range. The views are visible in the Remote Manager tree structure and you may configure access rights to them.

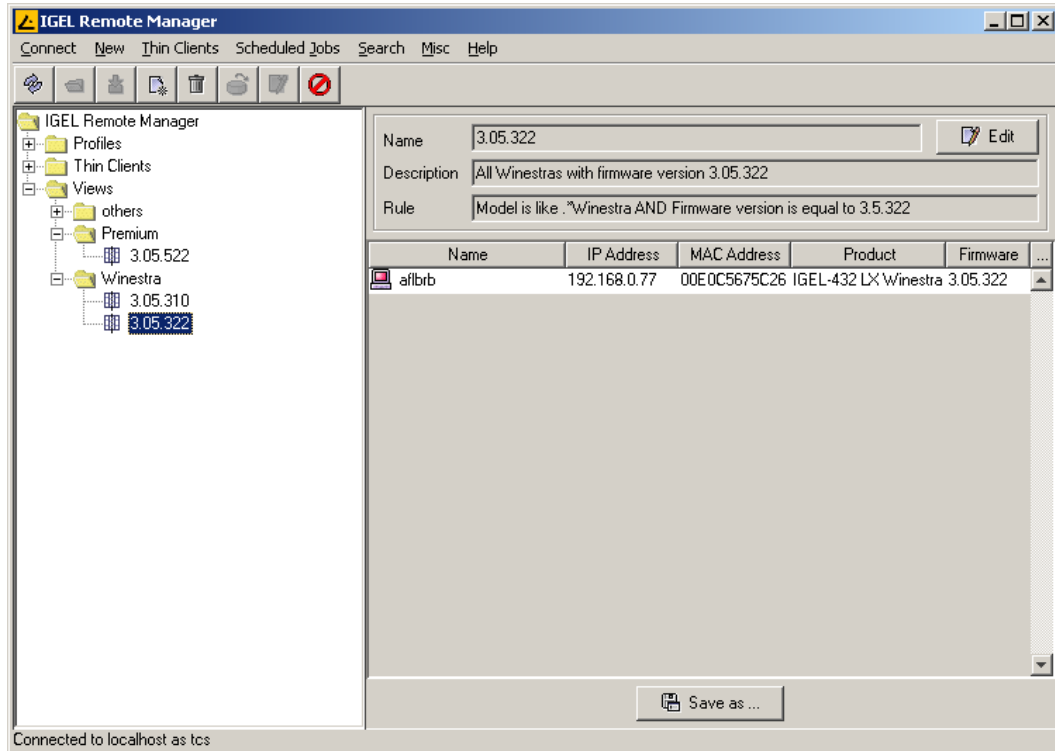


Figure 8-1 The View Panel

To illustrate this definition we show how to create a new view. Select **New -> View** from the menu. Then the following dialog appears:

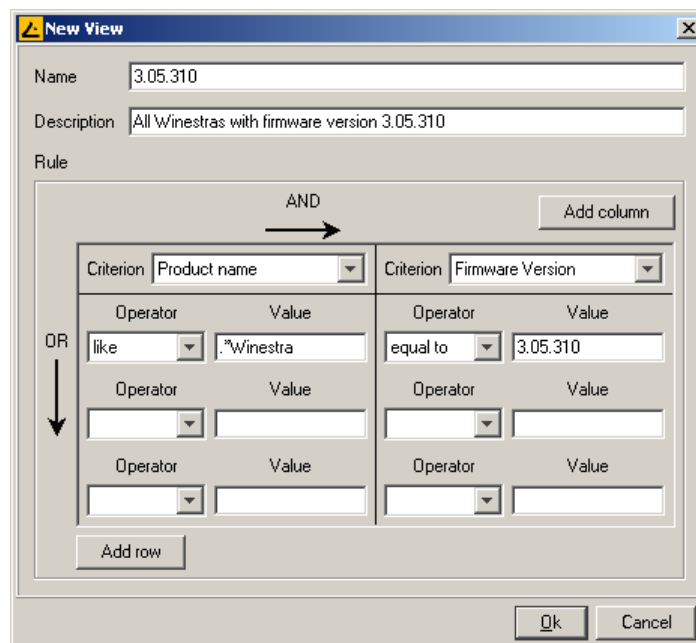


Figure 8-2 New View Dialog

First you have to enter a name for the view and optionally a description. Then you have to create the rule which defines the list of Thin Clients to be listed in the view. A rule consists of one or more criteria and each criterion has one or more constraints (the constitution of such a rule is similar as described in section *Default Rules*).

You have to choose the criterion type from the **Criterion** dropdown box. The following criterion types are available:

- IP address
- Name
- Product name
- Firmware version
- Online
- Directory
- Asset Id
- Comment
- Department
- In service date
- Mac address
- Serial number
- Site

In the example shown in the figure above there are two criterions, **Product Name** and **Firmware Version**. If you need more than two criterions to define your rule you can click on the **Add Column** button. Then an additional criterion column is added to the panel.

Now you may define the constraints. The constraints refer to the criterion on top of the column. Each constraint consists of an operator and a value. The list of available operators depends on the chosen criterion type. Most criterions provide the following operators:

- Like
- Greater than
- Less than
- Equal to

If you choose the like operator the value must be a regular expression. A Thin Client fulfills this constraint if its appropriate property matches this regular expression (in the example shown in Figure 7-2 all Thin Clients which product name ends with *Winestra* match the regular expression `.*Winestra` (‘.’ means any character and ‘*’ means the repetition).

Some simple examples for regular expressions:

- `.*abc` - string ends with *abc*
- `abc.*` - string begins with *abc*
- `.*abc.*` - string contains *abc*

A special type is the *Directory* criterion. It has the two operators *in* and *beneath* and needs as value the id of a directory (if you point on a directory you will get a tool tip including its id). The **in** operator means the Thin Client must reside directly in the specified directory, the **beneath** operator means the Thin Client must reside in the directory or one of its sub directories.

If the specified value does not fit to the criterion type (e.g. it is no IP address) or the operator (e.g. it is no regular expression) this value is tagged with a red symbol:

The image shows a user interface for defining a rule. It has three rows. The first row is for the criterion type, with a dropdown menu set to 'IP address'. The second row is for the operator, with a dropdown menu set to 'greater as'. The third row is for the value, with a text input field containing 'ip'. To the right of the 'Value' label in the second row, there is a red circle with a white exclamation mark, indicating that the value 'ip' is not a valid IP address.

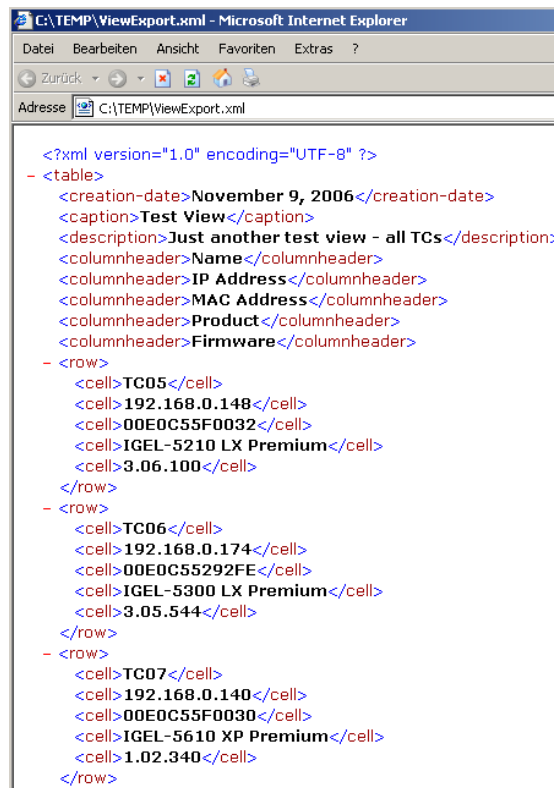
Figure 8-3 Illegal value

A Thin Client fulfills a rule if all constraints in the first row are met **or** all constraints in the second row are met **or** all constraints in the third row are met ...

You can modify an existing view by clicking on the **Edit** button on the **View panel**.

There is also the **Save as** button. This button is used to store the current content of a view in a file including all data which is shown in the table on the **View panel**. Note that you can modify the table by adding additional columns (click on ... to the right of the column headers) or changing the order of the columns (by dragging the column headers). Three file formats are available for the data: XML, HTML, and XSL-FO.

Here is one example for an XML file:



```
<?xml version="1.0" encoding="UTF-8" ?>
- <table>
  <creation-date>November 9, 2006</creation-date>
  <caption>Test View</caption>
  <description>Just another test view - all TCs</description>
  <columnheader>Name</columnheader>
  <columnheader>IP Address</columnheader>
  <columnheader>MAC Address</columnheader>
  <columnheader>Product</columnheader>
  <columnheader>Firmware</columnheader>
- <row>
  <cell>TC05</cell>
  <cell>192.168.0.148</cell>
  <cell>00E0C55F0032</cell>
  <cell>IGEL-5210 LX Premium</cell>
  <cell>3.06.100</cell>
</row>
- <row>
  <cell>TC06</cell>
  <cell>192.168.0.174</cell>
  <cell>00E0C55292FE</cell>
  <cell>IGEL-5300 LX Premium</cell>
  <cell>3.05.544</cell>
</row>
- <row>
  <cell>TC07</cell>
  <cell>192.168.0.140</cell>
  <cell>00E0C55F0030</cell>
  <cell>IGEL-5610 XP Premium</cell>
  <cell>1.02.340</cell>
</row>
```

Note: A view does not make any changes to the Thin Client settings or to the directory structure of the Remote Manager tree – it only provides a special sight onto the Thin Client devices registered at the Remote Manager.

9 Profiles

9.1 Organizing Profiles

The profiles reside under the **Profiles** node in the **Remote Manager Tree**. You can create a hierarchy of subdirectories to organize your profiles.

If you select the **Profiles** node or a subdirectory of it in the **Remote Manager Tree**, the **Profile Directory Panel** is shown on the right side (see Figure 9-1).

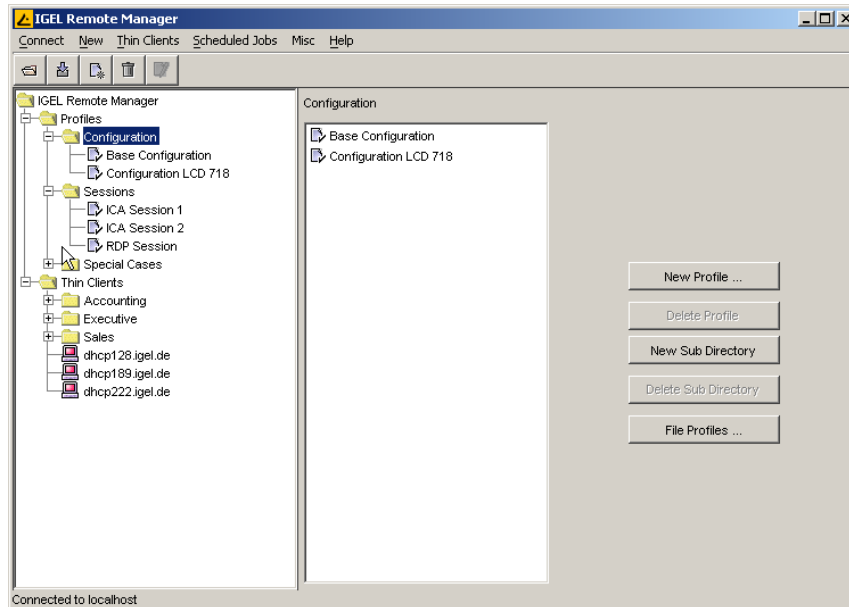


Figure 9-1 The Profile Directory Panel

There are the following possibilities to create a profile sub directory:

- Select the **Profiles** node or a sub directory of it in the **Remote Manager Tree** and press the **New Sub Directory** of the toolbar or the **New Sub Directory** button on the **Profile Directory Panel** (see Figure 9-1)
- Right click the **Profiles** node or a subdirectory of it in the **Remote Manager Tree** or in the list on **Profile Directory Panel** and choose **New Sub Directory**

You can rename the directory by right clicking it and selecting **Rename**.

Moving profiles from one directory to another can be done by

- Drag and drop in the **Remote Manager Tree**,
- With the hotkey combinations **Ctrl X**, **Ctrl V** (cut & paste) in the **Remote Manager Tree**
- Right clicking a profile directory and choosing **Move Profiles here**
- Pressing the **File Profiles ...** button on the **Profile Directory Panel** or the **Move Objects here** button on the tool bar

In the latter two cases a dialog pops up (see Figure 9-2 below) where you select the profiles you want to move.

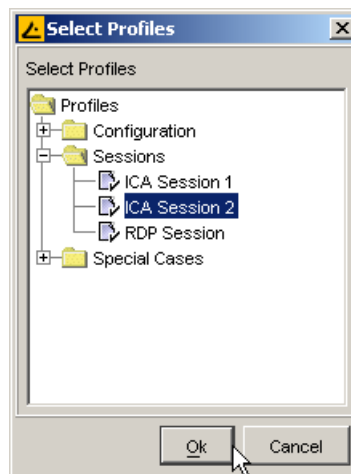


Figure 9-2 The Profile Selection Dialog

9.2 Creating Profiles

In order to create a new profile you have the following possibilities:

- Choose from the menu **New -> Profile**
- Press the **New Profile** button on the tool bar or on the **Profile Directory Panel**

If a profile directory has been selected, the new profile will be deposited in that directory, otherwise directly in the **Profiles** directory. In all cases the **New Profile Dialog** pops up (see Figure 9-3).

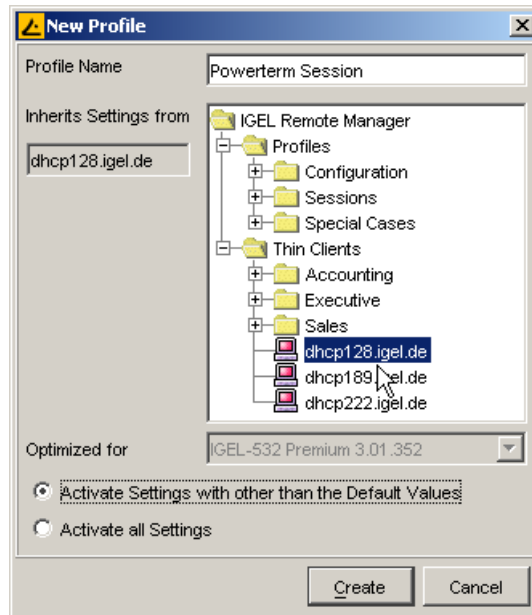


Figure 9-3 The New Profile Dialog

The first thing to do here is to enter a name for the profile, so that you can identify it. Next you have to choose, if the new profile should inherit settings from an existing profile or a Thin Client.

If you want to have an “empty profile” which should not inherit any settings, do not select an object from the tree. In this case you must select a firmware version for this profile (this means, that that this profile has the same set of configurable parameters and sessions as a Thin Client with this firmware version, nevertheless you can assign any profile to any Thin Client). Now choose one option provided by the radio buttons. The first option means here, that initially no setting is active and you have to activate the desired settings when editing the configuration of the profile. The second option means, that initially all settings are active. This option makes only sense, if you want that all settings of a Thin Client are controlled by this profile.

The second possibility is, that you want, that the profile inherits settings. In this case the profile inherits the firmware version too. Inheritance of settings means, that the settings of the profile have the same values as the setting from the object it inherits the settings. In this case you can choose, if settings whose values differ from the default value (every parameter has a default value, e.g. **Reset to Factory Defaults** sets parameters to its default value) should be activated or if all settings should be activated. Usually you will choose the first option (for instance you have configured a ICA session on a Thin Client and you want to have this session in the profile too).

Every value of the set of active settings that also exists in the firmware of the Thin Client will override the appropriate value. Parameters which do not exist on the Thin Client will be ignored. If the parameter exists on the Thin Client, but the value set in the profile is not permitted, the value on the Thin Client is set to its default value.

In order to finish, click on *Create* and the new profile is completed.

Note: If no Thin Client is registered, profiles cannot be created as information about the settings to be assigned to the profile is required. You can only create profiles with a firmware version which is registered in **the Remote Manager** database yet.

9.3 Renaming Profiles

If you want to rename a profile, just right click on it in the **Remote Manager Tree** or in the **Profile Directory Panel** and select **Rename** and enter the desired name.

9.4 Edit Profile Settings

If you select a profile node in the **Remote Manager Tree**, the **Profile Panel** is shown on the right side of the screen.

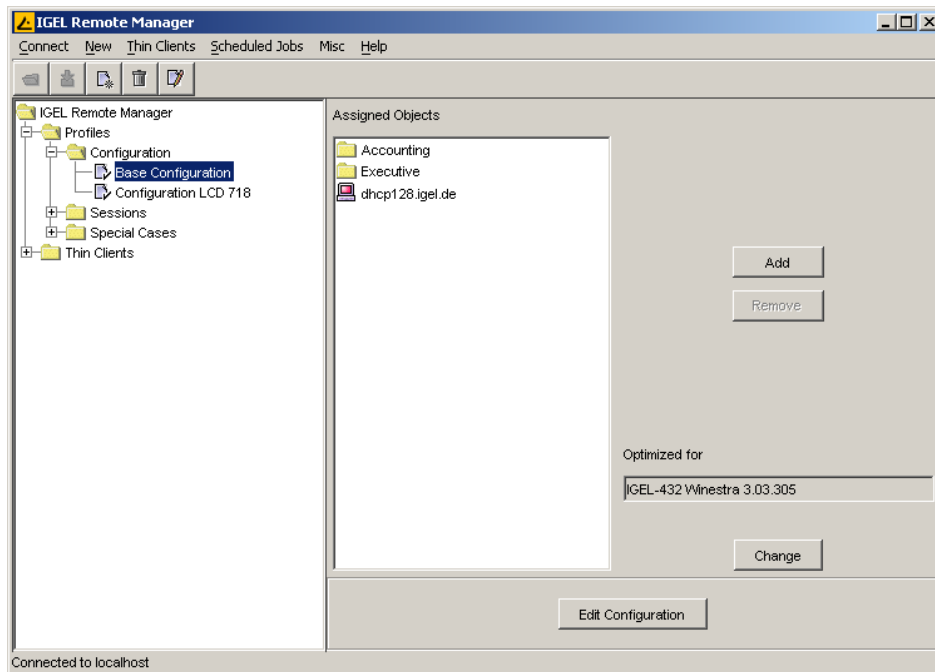




Figure 9-4 The Profile Panel


On this panel you can add or remove object from the list of **Assigned Objects** by clicking on the **Add** or **Remove** button respectively.

The next feature is to change the firmware version of the profile. For example if you have updated your Thin Clients you may want to update your profile too. Just click on **Change** button and select a new firmware. Note that settings which are not supported in the new firmware are lost.

In order to edit the settings of the profile

- Right click on a profile in the **Remote Manager Tree** or in the **Profile Directory Panel** and select **Edit Configuration**
- Select a profile in the **Remote Manager Tree** and press the **Edit Configuration** button in the toolbar or in **Profile** panel on the right side

Now the **Profile Configuration Dialog** is displayed (see Figure 9-5). This dialog mimics the dialog where you can edit the configuration of a Thin Client. The main difference is that there is an icon in front of each setting. The  symbol indicates that a setting is not active. However the  symbol indicates that the setting is active. Click on the symbol to change the state of a setting.

Only an active setting () of the assigned profile overwrites the value of a setting on a Thin Client. You cannot edit inactive settings; the associated GUI component is disabled. In order to get an overview about all active settings, click on the **Registry** tab and toggle the button **Show only enabled Parameters**.

Note: In case you have configured a session, you cannot deactivate single settings of it. Sessions can only be added as a whole.

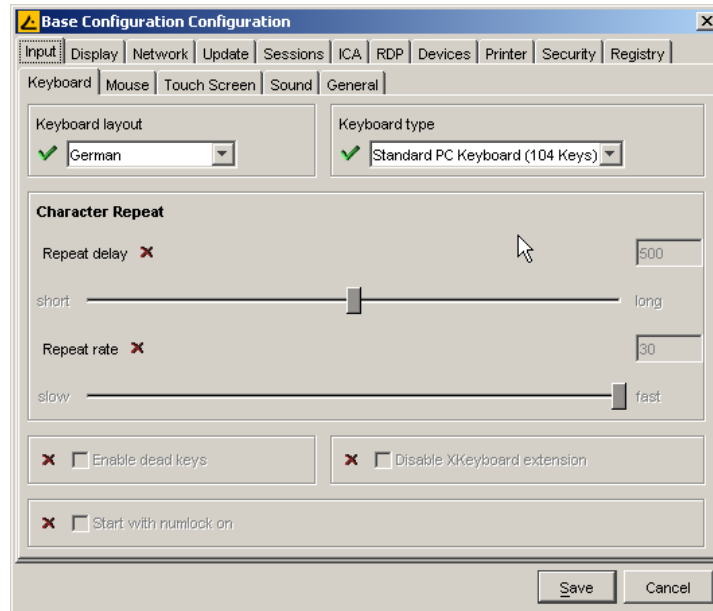


Figure 9-5 The Profile Configuration Dialog

When finished, click on the **Save** button. You will be asked when the new settings should take effect. Choose between **Next Reboot** and **Now**.

In both cases, the new settings are stored in the database.

- With **Next Reboot**, the Thin Clients to which the profile is assigned will apply the new settings at their next reboot.
- With **Now**, the settings are sent immediately to all Thin Clients affected by the profile. If they are currently not powered on, the settings will be applied at their next reboot.

Note: This feature is not available for **Windows CE devices**. You always have to apply the settings while they are running.

9.5 Assigning Profiles

After creating a profile and adjusting its settings, you now can assign it to some Thin Clients. (You can assign an arbitrary number of profiles to each Thin Client.)

Basically there are two modes to do this, *direct* or *indirect*. *Indirect* means, that you do not assign the profile to a single Thin Client but to a Thin Client directory.

If you assign a profile to a directory, it is *indirectly* assigned to every Thin Client in this directory (including its subdirectories).

If you move a Thin Client into this directory afterwards, this Thin Client is also affected by the directory profile. If you move a Thin Client out of this directory, the profile no longer affects it.

There are several possibilities to assign a profile or a Thin Client to a Thin Client directory:

- Select the profile you want to assign and click the button **Add** on the **Profile** panel (see Figure 9-4). The following dialog is shown:

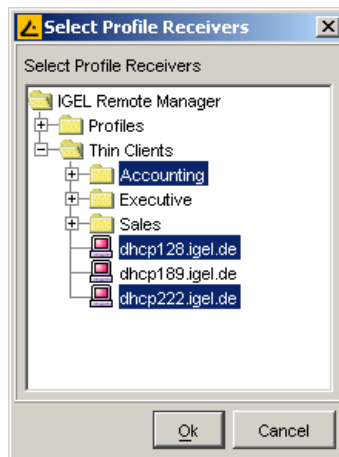


Figure 9-6 The Profile Receiver Selection Dialog

Now select the Thin Clients and Thin Client directories to assign the profile to.

- Select Thin Clients and Thin Clients Directories in the **Remote Manager Tree** and either drag & drop the selection on a profile or use **Ctrl X** and **Ctrl V** to cut & paste them.
- Select a Thin Client in the **Remote Manager Tree** and click the **Add** button on the **Thin Client Panel** (see Figure 9-7). Within the upcoming **Profile Selection Dialog**, select the profile to assign and press **Ok**.

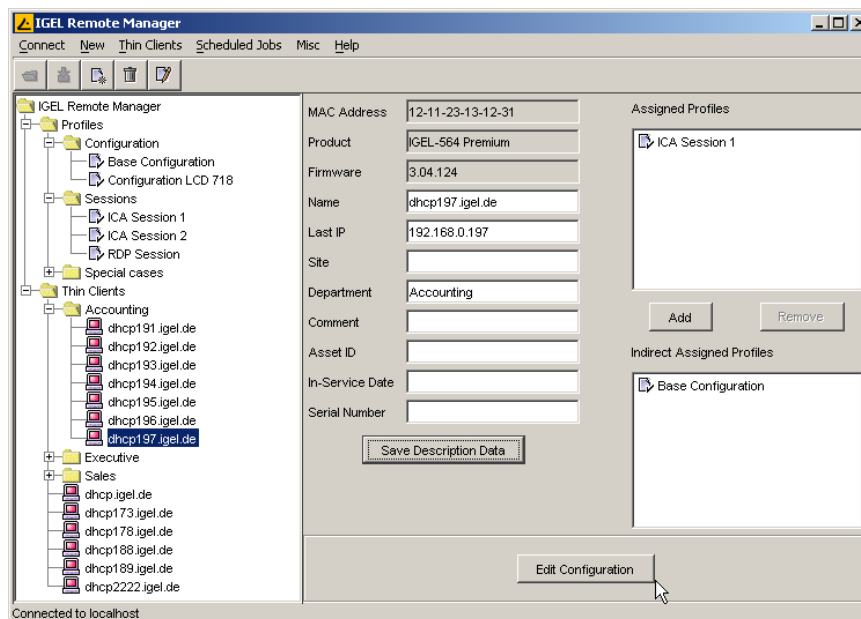


Figure 9-7 The Thin Client Panel

- Select a Thin Client directory in the **Remote Manager Tree** and click on the **Assigned Profiles** tab in the **Thin Client Directory Panel** (see Figure 9-8). Press the **Add** button. Again the **Profile Selection Dialog** is shown (see Figure 9-2).

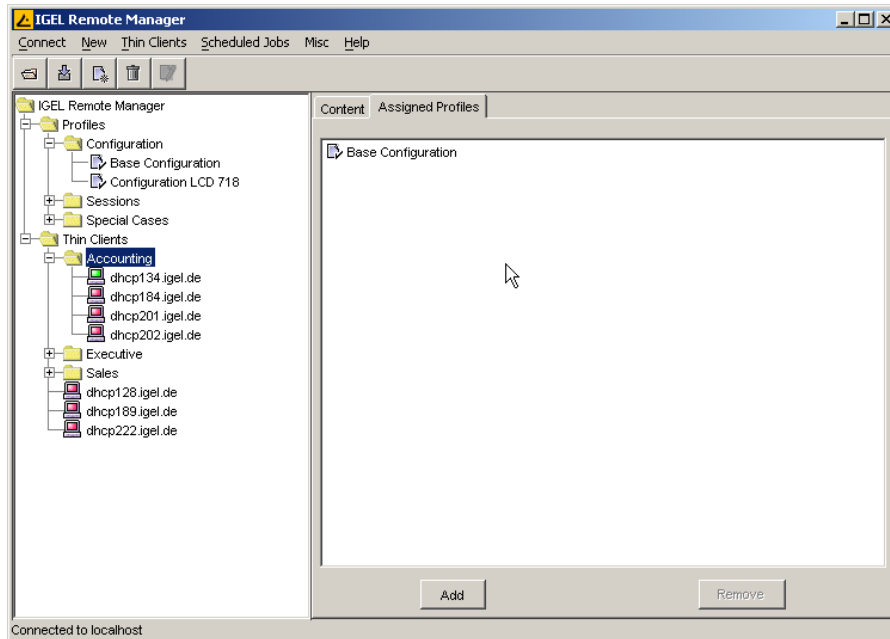


Figure 9-8 The Assigned Profiles Tab of the Thin Client Directory Panel

After you have assigned a profile (directly or indirectly) to a Thin Client, check the results: Select the Thin Client and choose **Edit Configuration** (from the **Thin Client Panel**, from the tool bar, from the **Thin Client** menu or the context menu of the **Remote Manager Tree**).

The **Thin Client Configuration Dialog** is shown (see Figure 9-9) and will display a red closed lock (🔒) in front of each overwritten setting, i.e. an active setting of an assigned profile. The value you have set in the profile is shown and you cannot edit the setting here. If you point on the lock icon, a tool tip will show you which profile overwrites that setting. This is useful if you have assigned more than one profile to the Thin Client. If there is a setting that is active in more than one assigned profile, the value from the most recent profile is valid.

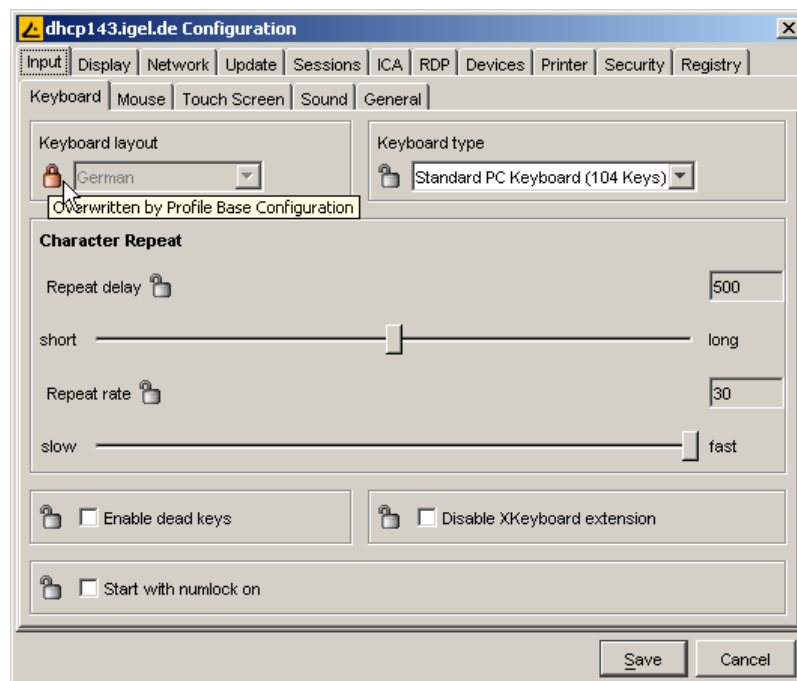


Figure 9-9 The Thin Client Configuration Dialog

Clicking on the **Sessions** tab of the **Thin Client Configuration Dialog** (see Figure 9-10) shows the sessions assigned to the Thin Client by profiles. These sessions are also locked. You cannot remove these sessions or edit settings in this dialog. You may only edit these locked settings in the configuration of the overwriting profile itself. (Remember that this will affect all Thin Clients to which the profile has been assigned!)

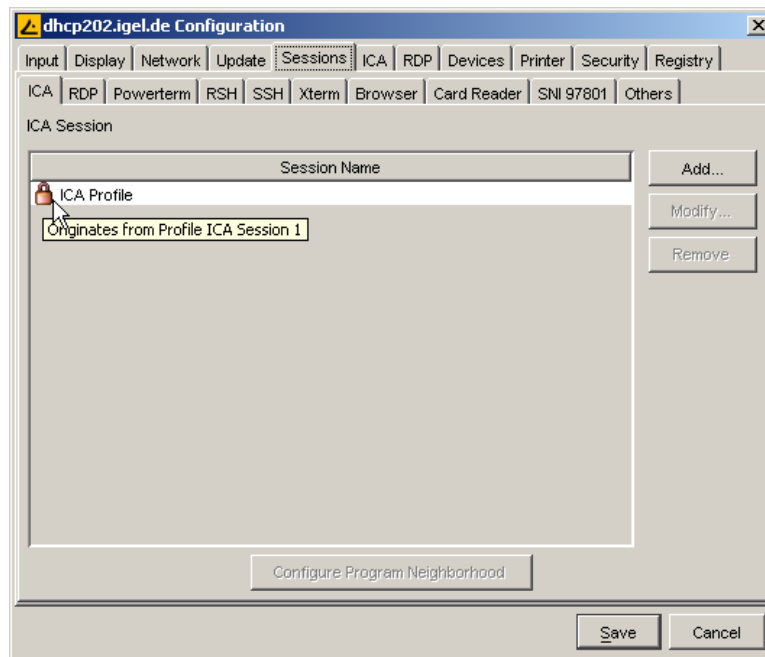


Figure 9-10 The Sessions tab of the configuration dialog

9.6 Precedence of Profiles

If you have assigned more than one profile to a Thin Client and you have activated a certain setting in all these profiles you might want to know, which profile provides the effective value for this setting or in other words, which profile overrides the others.

First of all, in general you should avoid this situation by defining disjoint sets of active parameters for the different profiles.

If you cannot avoid this situation, there is the following figurative rule:

"The nearer by the object, to which the profile is assigned, is to the Thin Client, the higher is its precedence".

In exact words the rule is the following:

A profile assigned to a subdirectory overrides settings of a profile which is assigned to the parent directory. A profile which is assigned directly overrides the settings of an indirectly assigned profile. If more than one profile is assigned to a single directory or is assigned directly respectively the newer profile (with a higher profile id) overrides the settings.

You get a tool tip with the profile id if you point on a profile in the list of assigned profiles.

To clarify this rule have a look at Figure 9-11.

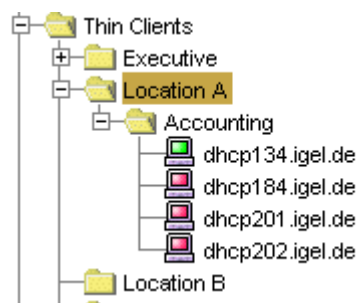


Figure 9-11 Profile Precedence

Profiles assigned to the directory *Accounting* override settings of profiles assigned to directory *Location A*. If two profiles are assigned to *Accounting* the newer one overrides the settings of the older one. Profiles assigned directly to *dhcp145.igel.de* override settings of profiles assigned to directory *Location* and directory *Accounting*. If two profiles are assigned to *dhcp145.igel.de* the newer one overrides the settings of the older one.

Note: The lists of assigned profiles and indirectly assigned profiles is sorted according the precedence, the first one has the highest precedence.

9.7 Removing Profiles from Thin Client

You can remove assigned profiles from a Thin Client or a Thin Client directory:

- In the *Profile* panel (see Figure 9-4) select a Thin Client or a Thin Client directory and click on **Remove**
- On the **Assigned Profiles** tab on the **Thin Client Directory Panel** (see Figure 9-8) or on the **Thin Client Panel** (see Figure 9-7): Select an assigned profile from the list and press the **Remove** button.

Now the single Thin Client or the Thin Clients under the Thin Client directory respectively are no longer affected by this profile. The value of the settings which had been overwritten is set back to the value before the profile had been assigned.

9.8 Deleting Profiles

When you wish to remove a profile, it can be removed in one of the following options:

- Select the profile in the **Remote Manager Tree** and press the **Delete** button on tool bar or the **Del** key
- Right click on the profile and select **Delete**
- Select the profile in the **Profile Directory Panel** and press the **Delete Profile** button

If you delete a profile it is removed from every Thin Client or Thin Client directory it had been assigned to and the values of the affected settings are set back to their previous state. Furthermore all settings of the profile are erased from the database.

9.9 Examples on how to use Profiles

For both examples, we assume that the Thin Clients are already registered in the IGEL Remote Manager database.

9.9.1 Same Display but different Sessions

Situation:

You want all Thin Clients in your company to have the same display settings (same *Color Depth*, *Physical Desktop Size and Frequency* and *Virtual Desktop Size*). On some of them, you want to have an ICA session and on the others an RDP session.

Solution:

Create two Thin Client directories (select the **Thin Clients** node in the **Remote Manager Tree** and press the **New Sub Directory** button on the tool bar), name one *ICA Dir* and the other *RDP Dir*.

Select the Thin Clients you want for an ICA session in the **Remote Manager Tree** and drag & drop them into the *ICA Dir* subdirectory

Select the rest put them into the *RDP Dir* subdirectory.

Next, create a new profile (press the **New Profile** button on the tool bar), name it *ICA Profile* and configure the ICA session in this profile (press the **Edit Configuration** button on the **Profile Panel**, select the **Sessions** tab, and add a new session).

Do the corresponding for the RDP Session.

Create a third profile named *Display Profile* and allocate the desired values to the display settings in this profile.

Finally, assign the *ICA Profile* to the *ICA Dir*, the *RDP Profile* to the *RDP Dir* and the *Display Profile* to both (drag & drop the directories on the appropriate profiles).

9.9.2 Copy a session from one Thin Client to another

Situation:


You have already configured an ICA session on a Thin Client (locally) and want to have exactly the same session on other Thin Clients.

Solution:

While creating a new profile in the **New Profile Dialog** (see Figure 9-3), select the preconfigured Thin Client. After confirming the creation of the new profile, it inherits those Thin Clients settings.

Make sure, that the profile does not contain any other active settings. In order to do this, right click on the profile and select **Edit Configuration**.

Select the **Registry** tab (see Figure 9-5) and toggle the click **Show only enabled Parameters**.

If necessary, deactivate the additional active settings by clicking on the  symbol.

Now assign this profile either indirectly, by moving the designated Thin Clients in a common directory and assigning the profile to this directory, or directly to each of those Thin Clients.

9.10 Exporting Profiles

IGEL Remote Manager enables you to export profile configurations from the database to the file system. This can be helpful for backup purposes or to import the profile data from one Remote Manager installation to another.

The profiles are converted into human readable XML format, so be careful not to publish these files if the source – profiles contain any passwords or other confidential data !

To export a single profiles right click on one and select the **Export Profile** menu point. In order to export several profiles into one file, mark them and select the Export Profile button in the toolbar:

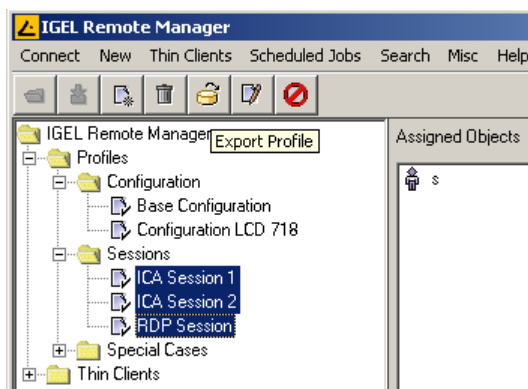


Figure 9-12 Select some profiles for export

Next, a file dialog will pop up where you can select your target file. Note that existing files will be overwritten with the new profile data (you will be requested if overwriting is ok).

9.11 Importing Profiles

Once you have any XML – files containing profile data, you can import them into your **Remote Manager** installation or also into another than the originating installation. Choose menu point **New → Import Profile** and select a profile – XML file. This will open the Profile Import Dialog:

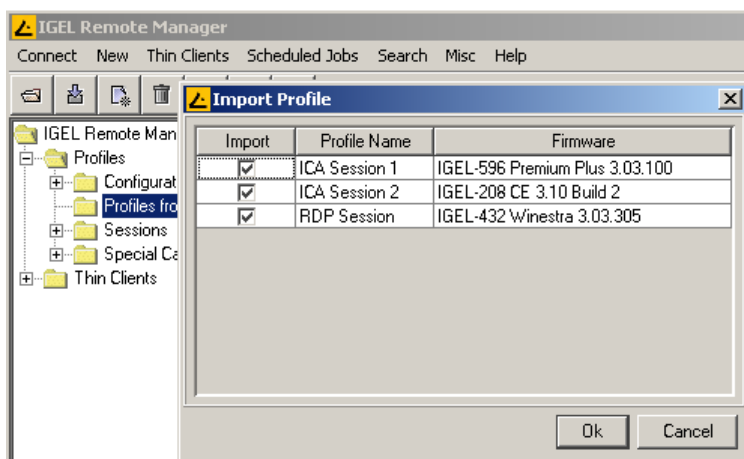


Figure 9-13 Profile Import Dialog

The import dialog displays name and firmware version of each profile configuration that is contained in the file you selected. Deselect one of the checkboxes in left row of the table, and the associated profile will be left out when the import process begins. Finally a dialog will display if all selected profiles have been successfully imported.

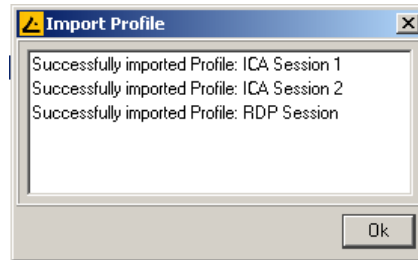


Figure 9-14 Import Status Dialog

9.11.1 Importing profiles with unknown firmware

There are some indications if you try to import any profiles that are optimized for a firmware version that has not been registered yet to your Remote Manager database. When you open a profile – XML file, the Profile Import Dialog shows an error message. The red marked profile can not be selected for import:

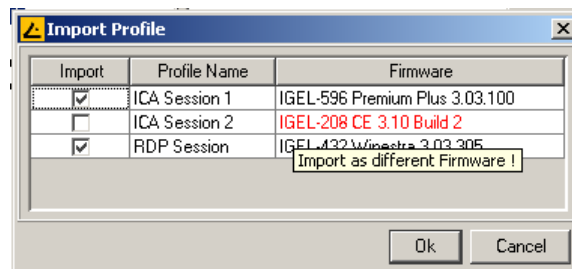


Figure 9-15 Import Profile with unknown Firmware

These profiles can contain settings that do not exist in any of the registered firmware version. Click on the red marked firmware field and choose any of the firmware versions that are known to the system:

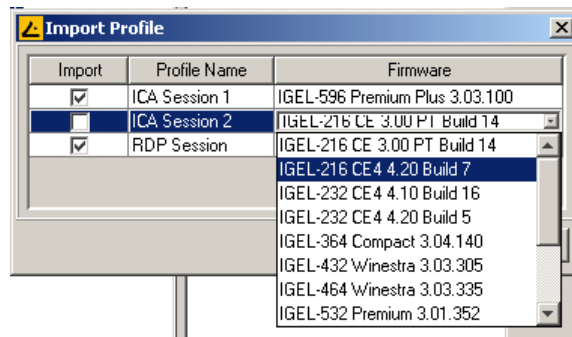


Figure 9-16 Choose other Firmware for import

Now you are able to import the profile. The impact of choosing a known firmware is an implicit conversion of the firmware version. This usually has little effects on the profile settings if you choose a similar firmware or a newer version of the same model. Unknown firmware settings will get lost.

10 Scheduled Jobs

The purpose of the Job Scheduler is to determine the execution time of certain Thin Client commands. These Jobs can be repeated in intervals or at fixed weekdays.

In order to get an overview of all Scheduled Job that have been defined so far, choose menu topic Scheduled Jobs → Manage all Jobs and the Manage Jobs Dialog opens:

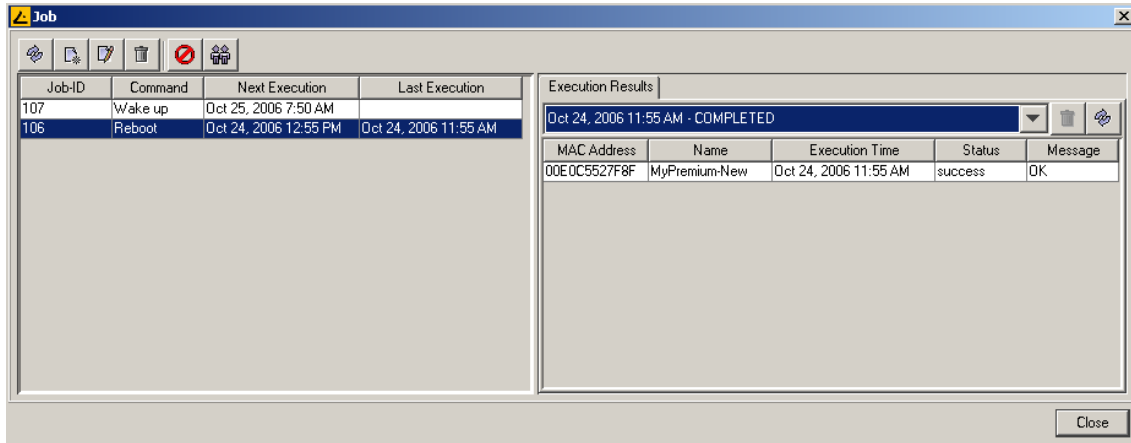
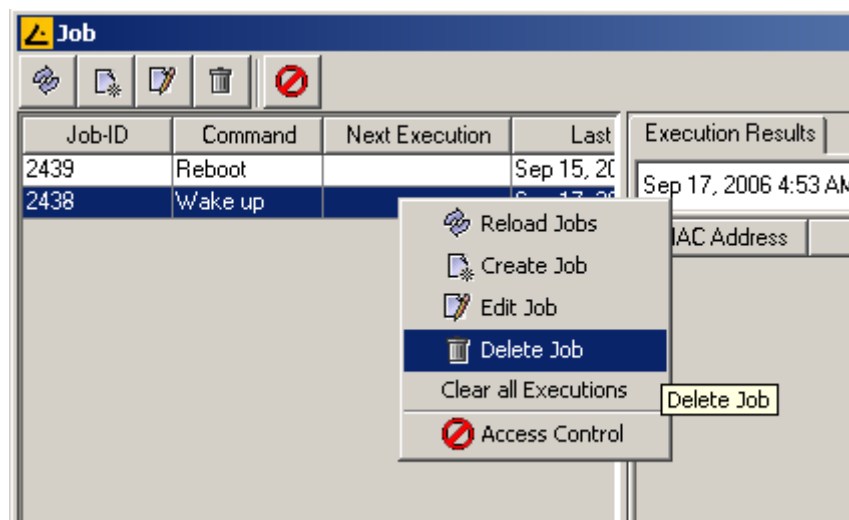


Figure 10-1 Scheduled Jobs overview

The table on the left contains the list of jobs and shows the internal job-ID, the command to be executed, the time of the next schedule as well as the time of the last execution – provided that there is one. The part right displays the Result Panel, here the currently selected job's last execution results are displayed.

10.1 Job Menu

On top of the Scheduled Jobs list, a menu bar with operations for managing jobs is located. The same menu pops up if you right click somewhere in the job list.



- *Reload Jobs*: All data is reloaded from the Remote Manager database
- *Create Job*: Opens the Create Job dialog for scheduling a new job. The Remote Manager user who created a job by default has full access rights on his job.
- *Edit Job*: Opens the Edit Job dialog for modifying the selected job. (user needs write permission)

- *Delete Job*: Deletes the selected job as well as eventually scheduled future executions and all results associated with this job. (user needs write permission)
 - *Clear outdated results*: Deletes all outdated (i.e. all past) job executions apart from the last or the next one scheduled and all related results. (user needs write permission for the corresponding job)
 - *Access Control*: Opens the Access Control dialog for assigning or displaying the permissions for the selected job. (user needs access control permission to edit rights)
 - *Default Permissions*: Opens the Access Control Dialog for assigning or displaying the default permissions **for all defined** jobs. (user needs access control permission to edit rights)
- Create Job

To create a new job either select menu point Create Job in the Manage Jobs dialog or menu point *New* → *Scheduled Job* from the RM main menu. You can also use Assign Jobs from the Scheduled Jobs menu and the currently selected thin clients are already assigned to the new job when the Create Job dialog opens:

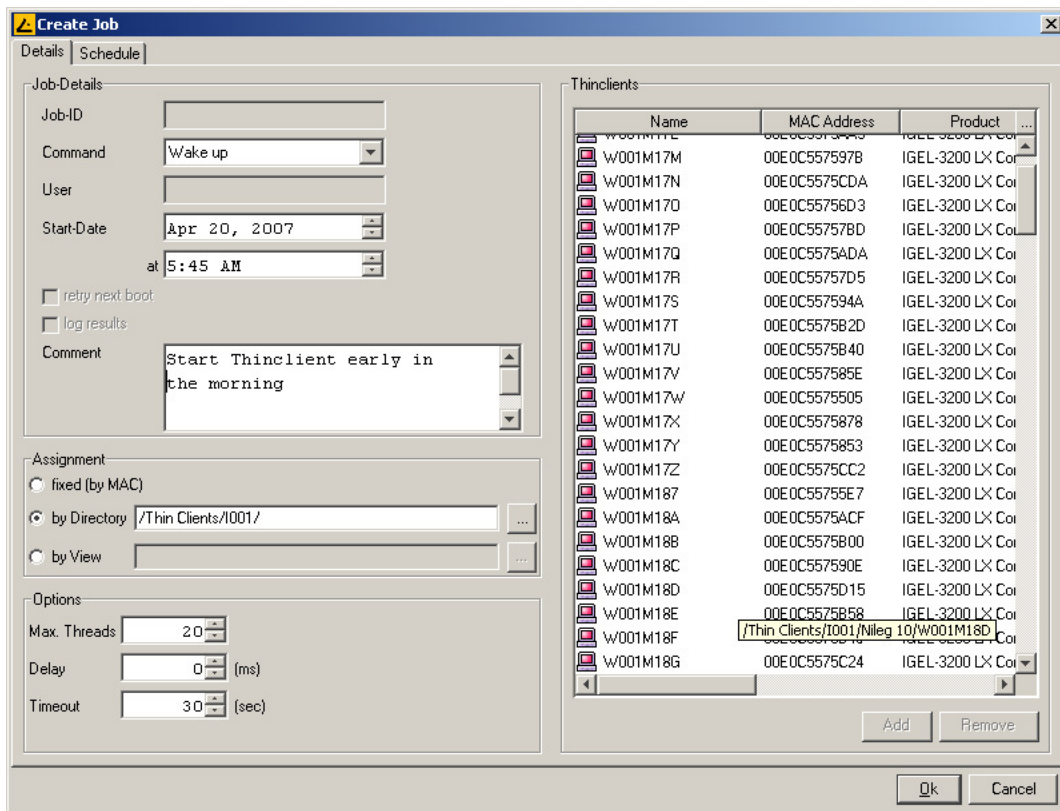


Figure 10-2 Create a new job

Below all options for new jobs are described in detail:

- *Job-ID*: For a new job this field is empty, it displays the internal job ID, not editable.
- *Command*: The Command which is executed on all assigned Thin Clients.
- *User*: Name of the RM User who executes the command.
- *Start date*: Date when the Scheduled Job gets active, the first execution date.
- *Retry next boot*: At the moment only supported for command Firmware Update. If the command execution fails for a Thin Client - for example because the device is switched off - the RM tries to start an update next time the Thin Client is powered on.

- *Log results*: Configures if the results of a command are logged to the database. Not for command wakeup - this command does have no result to be logged.
- *Comment*: Description or comment for this job.
- *Assignment*: There are three options for assigning Thin Clients to a job:
 - o Fixed assignment by MAC address of the device - use the buttons Add and Remove to assign or remove the Thin Clients selected from the list.
 - o Dynamic assignment by directory - all Thin Clients located in the chosen directory **at runtime of the job** will be affected.
 - o Dynamic assignment by view – all Thin Clients meeting the conditions of the view **at runtime of the job** will be affected.
- *Max. threads*: Maximum number commands executed in parallel.
- *Delay*: Time span which is left between the posting of a command to any Thin Client and the posting to the next one.
- *Timeout*: Maximum time for RM waiting for a reply of the Thin Client until it continues with the next device.

The options *Max.Threads*, *Delay* and *Timeout* make sense for all commands whose execution take a longer time or cause high network traffic e.g. downloading a firmware update, codecs or a snapshot. To avoid a high number of Thin Clients which concurrently are downloading data from a file server it is recommended to reduce the number of parallel threads (e.g. 10) and to configure a delay (e.g. 1 minute).

To create a static Thin Client assignment by MAC or a dynamic assignment by directory or by view read permission on the according objects is sufficient. At the time of execution the job's user (the one who created the job) needs write permission on the affected thin client. This has to be regarded if other users than the creator have write permission on a job, in particular if the database user created a job.

For performance reasons and for keeping the arising amount of data as small as possible the option *log results* should be deactivated for commands where the result has a secondary role.

- Job Schedule

The Job Schedule panel offers some options to create a schedule for the job's execution(s).

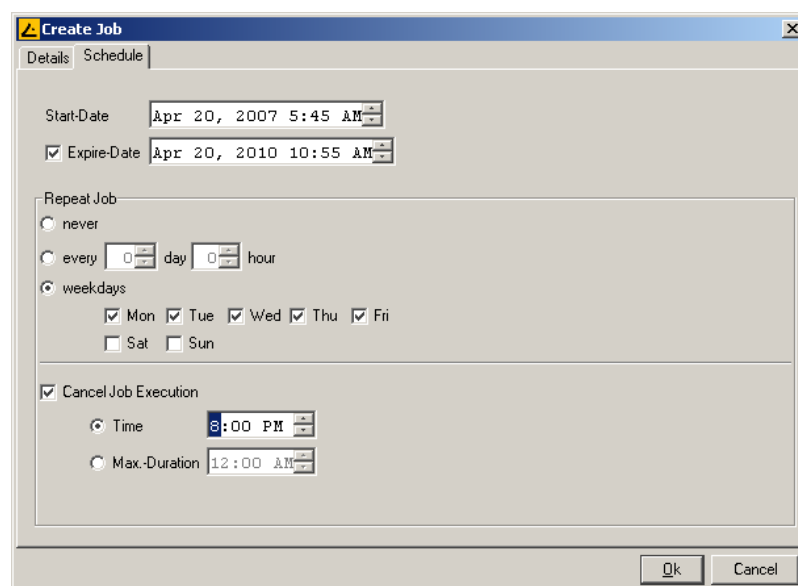


Figure 10-3 Job Schedule

- *Expiration date:* If this option is activated the job expires at the given date and time. No further commands will be executed after this time.
- *Repeat Job:* A job can be executed repeatedly either in fix intervals (days and/or hours) or on certain weekdays. If the latter option is chosen the job is running on all selected weekdays at the same time of day as specified by the job's start time.
- *Cancel Job Execution:* (repeated execution only) Here you can optionally specify a time or a maximum duration when no more commands should be posted to Thin Clients and not finished jobs will be canceled.

- Job Results

If option log results is activated for a job, the results for each single command that is sent to a Thin Client is stored to database. These results can be checked in the Manage Jobs dialog:

Execution Results				
Sep 19, 2006 1:13 PM - EXECUTING				
00E0C5572E04	W0390366	Sep 19, 2006 1:14 PM	in progress	
00E0C5572E33	W0390946	Sep 19, 2006 1:14 PM	in progress	
00E0C5572E37	W0390947	Sep 19, 2006 1:14 PM	in progress	
00E0C5572E39	W0390944	Sep 19, 2006 1:14 PM	in progress	
00E0C5572E3A	W0390943	Sep 19, 2006 1:14 PM	in progress	
00E0C5572E44	W0390945	Sep 19, 2006 1:14 PM	in progress	
00E0C5575234	W001M198	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C5575265	W001M19A	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C55752A8	W001M18w	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C55752AA	W001M19Y	Sep 19, 2006 1:14 PM	in progress	
00E0C5575355	W001M192	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C557535C	W001M19K	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C557535D	W001M193	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C557535E	W001M199	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C5575365	W001M195	Sep 19, 2006 1:14 PM	failed	Error: Could not send TC command or go...
00E0C557536A	W001M18N	Sep 19, 2006 1:14 PM	in progress	
00E0C55753CD	W001M19V	Sep 19, 2006 1:14 PM	in progress	
00E0C55753E0	W001M197	Sep 19, 2006 1:14 PM	in progress	
00E0C557540A	W001M18P	Sep 19, 2006 1:14 PM	in progress	
00E0C5575419	W001M19T	Sep 19, 2006 1:14 PM	in progress	
00E0C557541C	W001M19M	Sep 19, 2006 1:14 PM	in progress	
00E0C5575421	W001M18K	Sep 19, 2006 1:14 PM	in progress	
00E0C557545D	W001M19Z	Sep 19, 2006 1:14 PM	in progress	
00E0C5575486	W001M19w	Sep 19, 2006 1:14 PM	queued	
00E0C55754A3	W001M18D	Sep 19, 2006 1:14 PM	queued	

Figure 10-4 Results list

You can use the drop down box on top of the list to choose the execution date you are interested in (by default the results of the last execution are displayed).

Next to the execution date the state of the job execution is displayed:

- **executing:** Job is running right now.
- **completed:** Job is finished, all assigned Thin Clients have been processed.
- **canceled:** Job has been aborted before all assigned Thin Clients have been processed because cancel time or max. duration was reached.
- **terminated:** Job was stopped because of unknown reasons (e.g. server down).

The results list displays all Thin Clients which have been processed as well as the individual state of the command and eventually an (error-) message.

Below the different command states:

- aborted: Aborted due to internal error or unknown reason.
- failed: Command failed, reason is displayed in the message-column.
- in progress: Command is currently running. Server is waiting for a reply.
- run next boot: Command will run the next time the device boots up.
- not processed: Command has not been executed as the job's timeout was reached.
- queued: Job is running, command will be executed the next time a process is available.
- success: Command has been successfully executed.

- Editing a Job

Same dialog as for creating a job. The command can not be changed anymore once the job has been running.

11 Managing certificates

11.1 Server certificates

During installation of the IGEL Remote Manager, some private/public key pairs are generated. These keys are used to prevent unauthorized installations of the IGEL Remote Manager from accessing the IGEL Remote Manager Server and the Thin Clients that are under its control. The certificates are:

- **<INSTALLDIR>\rmguiserver\irm_keystore**: Contains the private/public key pair that controls connections to the IGEL Remote Manager Console. The console needs to have the corresponding cacerts file.
- **<INSTALLDIR>\rmclient\cacerts**: Contains the public key that matching to irm_keystore. If you want to deploy consoles on several computers that will access the IGEL Remote Manager Server, you need to hold this file in readiness during the installation process of the consoles.
- **<INSTALLDIR>\rmtcserver\server.pem**: This is the private key that the IGEL Remote Manager Server uses for the communicating with the Thin Client.
Backup this file and keep it secret! If the file gets lost, you will not be able to communicate with previously registered Thin Clients, unless you manually remove the corresponding public key certificate from the Thin Client.
- **<INSTALLDIR>\rmtcserver\server.crt**: The certificate contains the public key of the IGEL Remote Manager Server belonging to private key **server.pem**. It is stored on the Thin Client during the registration process.
Ensures that only IGEL Remote Manager Servers with the corresponding private key are allowed to configure the Thin Client.

Note: The certificates will not be deleted when uninstalling the IGEL Remote Manager. If you reinstall the software, it will use the keys that are already installed. If you install the software on a different machine, you need to copy the certificates into the corresponding directories of the new installation. If you remove the certificate server.pem, be sure to remove the public part from any client device as well. Otherwise you will be unable to discover that client(s).

11.2 Installing Server Certificate on Thin Clients

The IGEL Remote Manager can store a certificate on each Thin Client that is under its control. This certificate prevents unauthorized access to the Thin Client's configuration. During installation, a unique public/private key pair is generated for each IGEL Remote Manager Server. The public part can be stored on a Thin Client and every future access is checked against the private key of the server. If other IGEL Remote Manager installations try to access the Thin Client, access will be denied. If a Thin Client is registered in the IGEL Remote Managers database, the public key certificate gets stored automatically on the Thin Client. In order to remove this certificate you can use the **Remove Certificate** entry from the command menu. After this operation, every IGEL Remote Manager Server can access the Thin Client configuration until one of them registers the client. You can also store the certificate on a Thin Client that is already registered in the database. This might be particularly useful if the certificate was deleted manually from the Thin Client. Storing the certificate on the Thin Client can be achieved by selecting a group or a single Thin Client and executing **Store Certificate** from the command menu. The alternate way is to reregister the Thin Client.

11.3 Installing Console Certificates

When installing the IGEL Remote Manager Console on a different computer, you need to import the certificate `<INSTALLDIR>\rmclient\cacerts`. Copy this file to a floppy or just put it into a shared folder that is accessible from the target computer.

12 Access Control

12.1 Introduction

The Igel Remote Manager provides functionality to assign access rules to any object in the **Igel Remote Manager Tree** for individual **RM user accounts** or **groups of RM users**. Each access right can be explicitly set (allowed) and also withdrawn (denied).

12.1.1 Access rights and their effects:

Access Right	Effect
Display	User can see the object
Browse (for Directories only)	User can browse the directory, directory itself is visible
Read	User can view settings and information about the object
Write	User can edit settings or rename the object
Access Control	User can change an objects access rights
Shadow	User can perform remote maintenance operations on a Thin Client

The **Browse** permission is a special case that just affects directories. It makes the directory visible to the user (even if **Display** is not set) and enables the user to navigate into the directory and all sub-directories with this permission set. Leaf objects like **Profiles** and **Thin Clients** are invisible to the **RM user** as long as no **Display** permission is granted for these objects. These permission can be used to create partial views of the **Igel Remote Manager Tree**. The **Shadow** permission enables the **RM user** to perform maintenance operations on Thin Clients such as wake up, reboot, update or reset the firmware.

12.1.2 Effective Access Rights

The privileges that result for an individual user for each Remote Manager object are evaluated from previously defined access control entries by following rules:

Group-Membership:

The individual user's permissions are affected by all positive or negative access control entries defined directly for the user itself or by all entries for groups which the user is a member of. If these rules are conflicting (one denies a right, another allows the same) the following rule takes effect:

Denied overrides allowed:

A withdrawn / prohibited right always overrides an access control entry that sets a permission. If for a user or group a certain permission is set for a specific object and for the same object the permission is denied for another group the logged in **RM user** is a member of, the denying/revoking rule is the valid one.

Inheritance:

A container object propagates the permission entries that are defined for itself to all its child objects. If for an object a permissions is neither explicitly allowed nor denied for the user (or one of his groups), this right is inherited from the parent (container) object of this object. A rule that is directly defined for an object overrides any rules the object inherits from its parent object.

12.2 Remote Manager Accounts

During the installation process a **database user** for the **Remote Manager** application has been created. This user account is intended to be used for administration purposes such as creating **RM User accounts** and assigning users to groups. The **database user** always has full access rights on all Remote Manager objects and all Remote Manager functionality. There is always one unique database user for a Remote Manager installation.

To create a new user account or change group assignments log in as the database user. The database user is the only one who is able to create new accounts, groups or change group assignments. The database user account itself will never appear within access control dialogs. Its access is controlled directly within the RM database system.

Select menu **Misc** → **Administrator Accounts** and the **Remote Manager Users and Groups Dialog** will pop up:

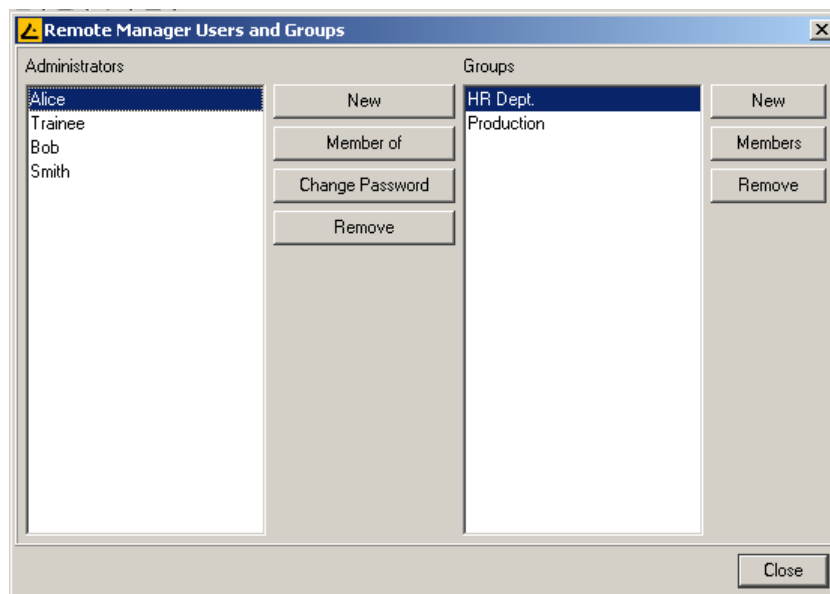


Figure 12-1 Remote Manager Users and Groups

The left half of the dialog shows already defined **RM Administrator** users. For creating or deleting an account use the left hand **New / Remove** – buttons. When creating a new Admin-account, you will be asked to assign an initial password:



Figure 12-2 Create a new RM User

This password can either be changed later in this dialog by the database user (“Change Password”), or by the individual **RM Administrator** himself when he selects the menu item **Misc → Change Password**. If the **database user** selects **Misc → Change Password**, this will change the password for the underlying SAP-DBMS!

Administrator Groups are created or deleted in the same manner by using the **New / Remove** buttons on the right half of the **Users and Groups** dialog. Group accounts are not protected by a password and can not be used to log in. They are intended to simplify rights management by assigning several users to a group and then provide identical access rights to all the users with one single definition for their group.

In order to view or to change the users within a group press button **Members** and the **Members** dialog for the selected group will pop up:

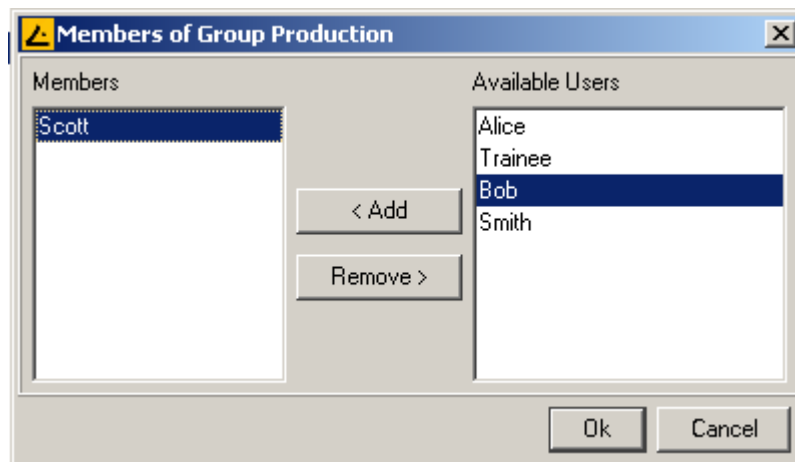


Figure 12-3 Group – User Assignment

With the **Add** and **Remove** buttons or simply by using “Drag and Drop” you can assign or remove the selected user(s) to this group. Similarly you can change an individual group assignment when you select the **Member of** button in the **Users and Groups** main dialog.

Note: Initially there are no access rights defined for a newly created user or group. So without explicitly setting access rights, the new user - when logged in - will not have any permission on a Remote Manager object or even be able to view any object. Best assign the new user to a group with some default rights.

12.3 Defining Access Rights

To define new access rights for Remote Manager objects, such as Thin Client-Settings, Profiles or Directories, the **RM Administrator** user needs “Access Control” permission.

Selecting menu item **Access Control** (in the **Remote Manager Tree's** pop-up menu or in the toolbar) will let pop up the **Security Dialog** that enables the user to edit the object's access rights (See figure 11-4).

The upper part of the dialog shows a list of users and groups for which access control entries are defined for the object itself or one of its parent objects. With the **Add** and **Remove** buttons new entries can be created or deleted.

With the checkboxes beneath, each individual permission for the selected user / group can be set (allowed) or revoked (denied). User-permissions that are inherited from a parent object are displayed by disabled (greyed out) checkboxes. To save your changes press the **OK** - or **Apply** button. The **Remove** button is active only if there exists a directly defined access rule for the selected user / group. If all rights are inherited from parent objects, you can not delete the entries (Open **Security Dialog** for the object the rights are inherited from).

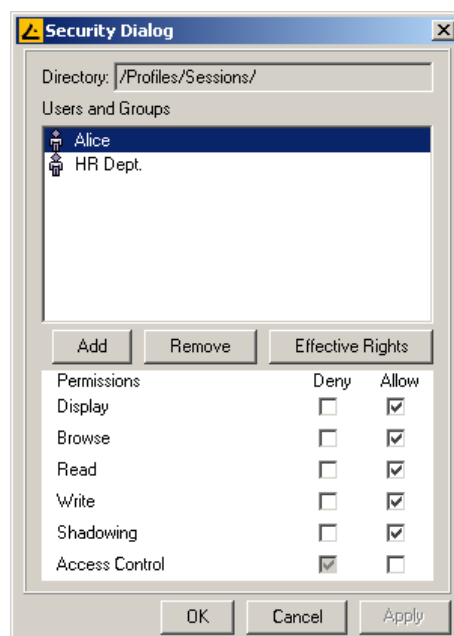


Figure 12-4 Defining Access Rights

The **Effective Rights** button opens a dialog that shows the resulting permissions for each user or group, considering the rules described above. If a user does not effectively have the **Access Control** permission for an object, menu item **Access Control** directly opens the **Effective Rights** dialog instead of the access rights editor:

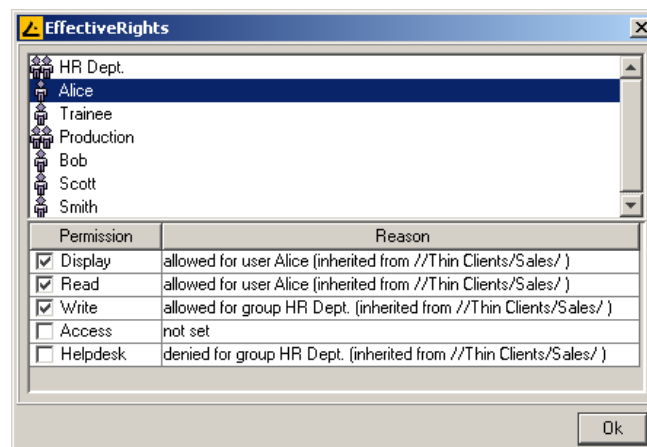


Figure 12-5 Effective Rights Dialog

This dialog can be helpful to determine why your user can not perform a certain operation, e.g. delete/edit a Profile or Thin Client configuration. It displays permissions set or not set and gives a reason for each.

Note: You can always only edit or view access rights for a single object, as there may be different sets of entries defined for each of them.

Access Rights Best Practices:

- Prefer defining access rules for groups instead for individual users. It is easier to assign or remove a user to one or more groups than to create new access control entries for the whole **Remote Manager Tree**.
- Avoid denying access rights, better do not assign them in first place. Do not forget that a denied one overrides a permission that is set. This can be confusing with a user's membership in multiple groups. Start with a limited set of permissions for root-objects and widen it in deeper levels of the tree.
- Prefer defining access rights on directories than on each single object contained in it. Note that in this case moving an object can result in different access right. In case this is undesired behavior you have to explicitly define access control entries on the object.
- The "chain of rights" has to begin with the root nodes of the tree. If a user has no browsing access down to a node he will also be unable to display or change objects within this node.

Special Case: Root-Nodes

Note that the root nodes for profiles, thin clients and the **Remote Manager** node itself cannot be made invisible for a user (see section 11.5), as they are an integral component of the **RM Client** user interface (they are displayed even if your client is not connected to the server). Anyway, you can define access control entries on these root objects and the resulting permissions are propagated to subcomponents. All other permissions except the ones that affect the root nodes' visibility (**Display** and **Browse**) are handled without difference to other objects.

12.4 Mandatory Access Rights for RM-Functions

The following table lists all Remote Manger operations a user who is logged in can perform, and what the minimum access rights are for thereby affected objects.

Action	affected Objects:	Display	Show Content	Read	Write	Access	Shadow
View an Object	Thin Client, Profile Directory	X	X				
Delete Object	Object to be deleted Source Directory				X		
Move Object	Object to move Source Directory Target Directory				X		
Assign Profile	Object which Profile is assigned to Profile				X		
Detach Profile	Object from which Profile is detached Profile				X		
Edit Settings	Profile, Thin Client				X		
Show Settings	Profile, Thin Client			X			
Create Object	Target Directory Profile -Template (for new Profile only)				X		
Import	Target Directory				X		
Export Profile	Profile			X			
Rename/Update	Object to be renamed				X		
Change Profile-FW	Profile				X		
Scheduled Jobs	Thin Client						X
Change Access Rights	any Object					X	
View effective Rights	any Object	X					
Take over Settings	Thin Client Profile				X		
Reboot	Thin Client						X
Shutdown	Thin Client						X
Update	Thin Client						X
Wake up	Thin Client						X
Reset to Factory defaults	Thin Client				X		X
Send Message	Thin Client						X
Download Codec	Thin Client						X
Shadow	Thin Client						X
Save Settings to Thin Client	Thin Client				X		X
Get Settings from Thin Client	Thin Client						X
Store / Remove Certificate	Thin Client				X		X
Remove Thin Client	Thin Client				X		X

12.5 Use Cases

Create restricted views and hide objects access rights Display and Browse):

One of your RM Administrators, let us call her Alice, is responsible for configuring all Thin Clients, but she ought better let the well tested and configured profiles untouched. She has to assign profiles to the Thin Clients, but she is not allowed to change the profiles. You also created some profiles for testing purpose, directly in the profiles base folder. These should not be assigned to any Thin Clients, unless you are not sure they work properly. There is also a folder for special cases. Alice may only use the "Network" profile, the others are hidden for her. Let us compare the **Remote Manager Tree** as it does show to the database user and the view Alice gets to it:

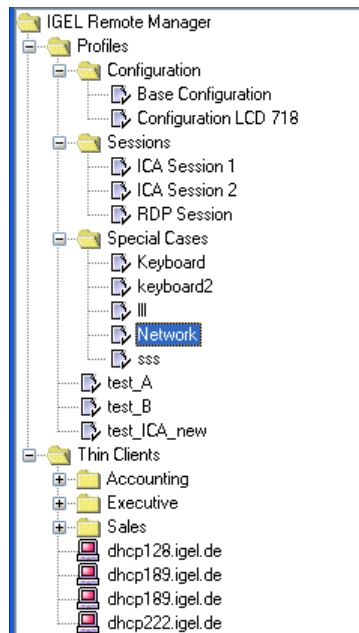


Figure 12-6 Full View

Steps:

- Directory /Profiles: allow Browse
 - Alice can browse the profile directory and its subdirectories, profiles itself are not visible (except Display is explicitly set)
- Directory /Profiles/Configuration and /Profiles/Sessions: allow Read
 - Alice can view the profiles contained, read the settings and assign them to any Thin Clients
- Profile /Profiles/Special Cases/Network: allow Read (implicitly Display)
 - Alice can view read the settings and assign it to any Thin Clients

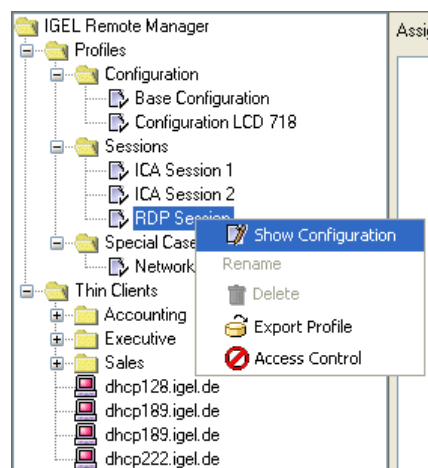


Figure 12-7 Restricted view

As you can see, the profiles for testing purpose as well as all special cases except “Network” are hidden from Alice. When she does a right click on a profile she can view the settings (**Show Configuration**), but she is not allowed to edit the configuration, rename or delete the profile.

Menu point **Access Control** from the context menu will pop up the **Effective Rights** dialog for the currently selected object (Alice has no **Access Control** permission set):

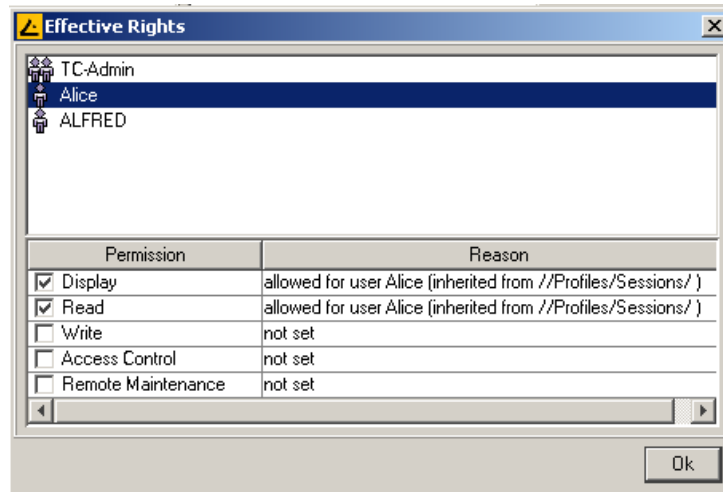


Figure 12-8 Effective Rights

Assign Responsibilities to a Department :

One of your RM Administrators, Mr. Miller is responsible for all Thin Clients of the sales department. He needs full access on the sales Thin Clients and should be able to delegate Jobs to his trainee “Trainee Bob”. It is probably useful that he knows about all other Thin Clients (e.g. where they are located, their IP-addresses etc.).

Prerequisites:

- there is a group TC-Admin which has Read permission on the full Thin Client subtree
- there is a group Sales which has Browse permission on the full Thin Client subtree and Read permission on the “Thin Client/Sales” directory

Steps:

- assign Miller to group TC-Admin and group Sales Dept.
- assign Trainee Bob to group Sales Dept.
- set full access rights for user Miller on directory “Thin Client/Sales”

Result:

- Miller has full access on directory “Thin Client/Sales” and Read permission on all other Thin Clients
- Miller can delegate access rights within his department

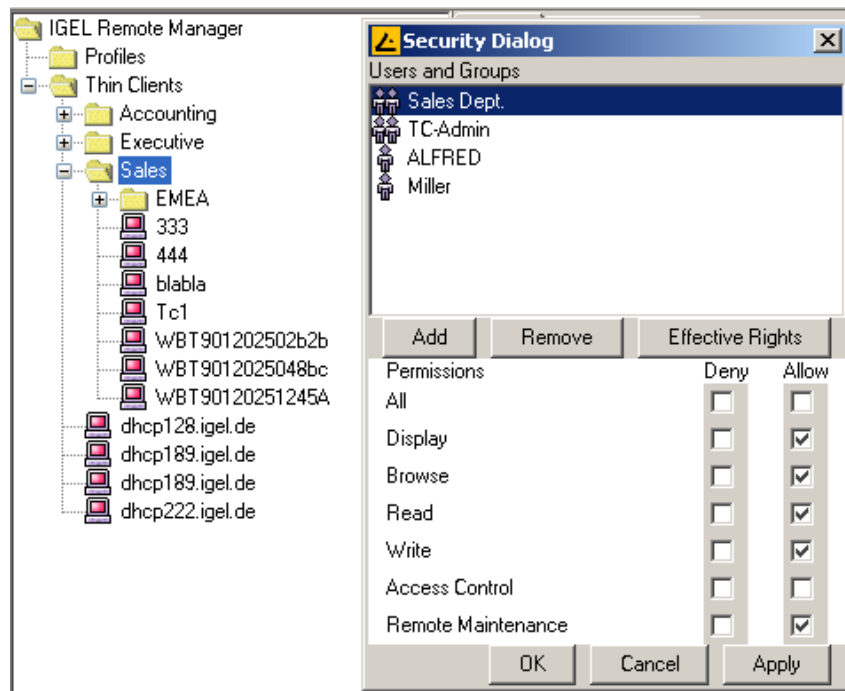


Figure 12-9 Miller can change access rights

If user Miller logs in he decides to widen the access rights for all other members of group Sales Dept. for the Sales directory and allows Write and Shadow. As Trainee Bob is a member of this group, Miller decides to deny everything for Bob on the /Sales/EMEA subfolder as long as Bob still is a trainee.

When Bob logs in, this is the view he gets:

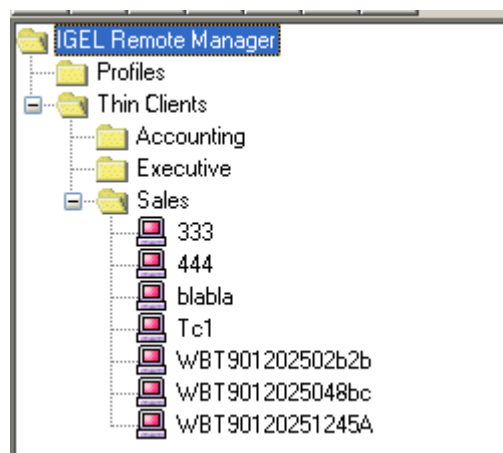


Figure 12-10 the trainee's view

Bob has all rights the Sales Dept. group needs to maintain their Thin Clients, but the EMEA subfolder is not visible to him. He cannot change any access rights or get information about other departments' Thin Clients.

Note: In this example, Miller himself is a member of group Sales Dept. If he decides to explicitly deny the Access Control permission to the members of this group, he would effectively revoke this permission from himself !

13 The IGEL Remote Manager Administrator

The IGEL Remote Manager Administrator tool enables you to

- manage basic parameters of the IGEL Remote Manager such as ports and passwords
- create and restore backups of the SAP – DB
- manage data and log files of the SAP – DB
- configure database connections for SAP – DB and Oracle (9i/10g) databases

The IGEL Remote Manager Administrator is only available in the start menu of a Remote Manager Server installation.

You need to have access to the IGEL Remote Manager files. The access rights to the IGEL Remote Manager files are restrictive. Permission to change settings depends on the permission to change these files on the server system. So you should use the same user account in order to start IGEL Remote Manager Administrator as used during the installation of the Remote Manager.

13.1 Settings Panel

At startup, the Remote Manager Administrator's Settings Panel is displayed. Here you can configure ports in use by the Remote Manager and other related settings like timeout etc.:

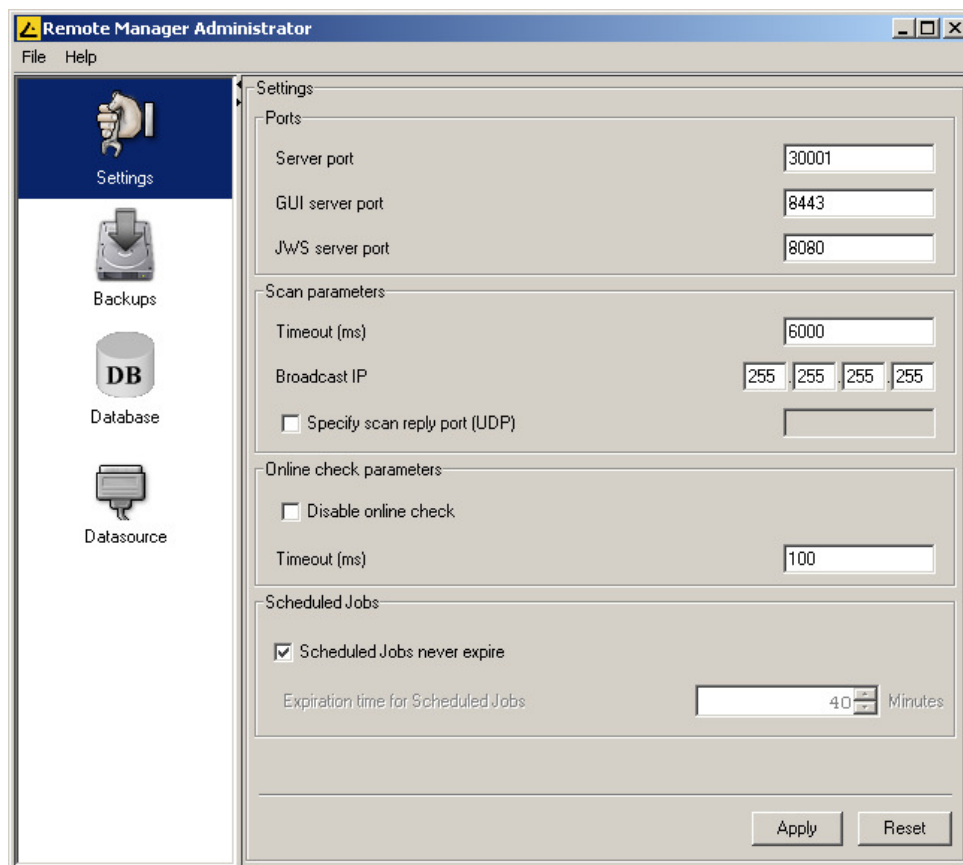


Figure 13-1 Ports and Timeout Configuration

The IGEL Remote Manager Server is using three open ports for incoming requests: The first port is the **Server port** which the TC server is using. The Thin Clients connect to this port. It is by default 30001 and can be changed here. The **GUI server port** is used by the IGEL Remote Manager Console to connect to the server. You need to enter this port number in the connect dialog of the IGEL Remote Manager Console. It defaults to 8443.

The third port is used by the Java Web Start interface. If you want to use Java Web Start as described in 4.3 Launching the Remote Manager Console via Java Web Start, you have to specify this port in the connection URL, e.g. http://hostname:8080/start_rm.html.

In the **Scan Parameters** section, three values are configurable.

The first one, **Timeout**, specifies how long the IGEL Remote Manager should wait for the answer on scan packets that were sent to the network. The value is in milliseconds and is by default set to 6000.

The second parameter **Broadcast IP** determines the broadcast address to use for scan packets. This is only used to scan the local network. When using IP ranges, the UDP packets are sent out to each client within the IP range. The default here is 255.255.255.255 and usually there is no need to change it.

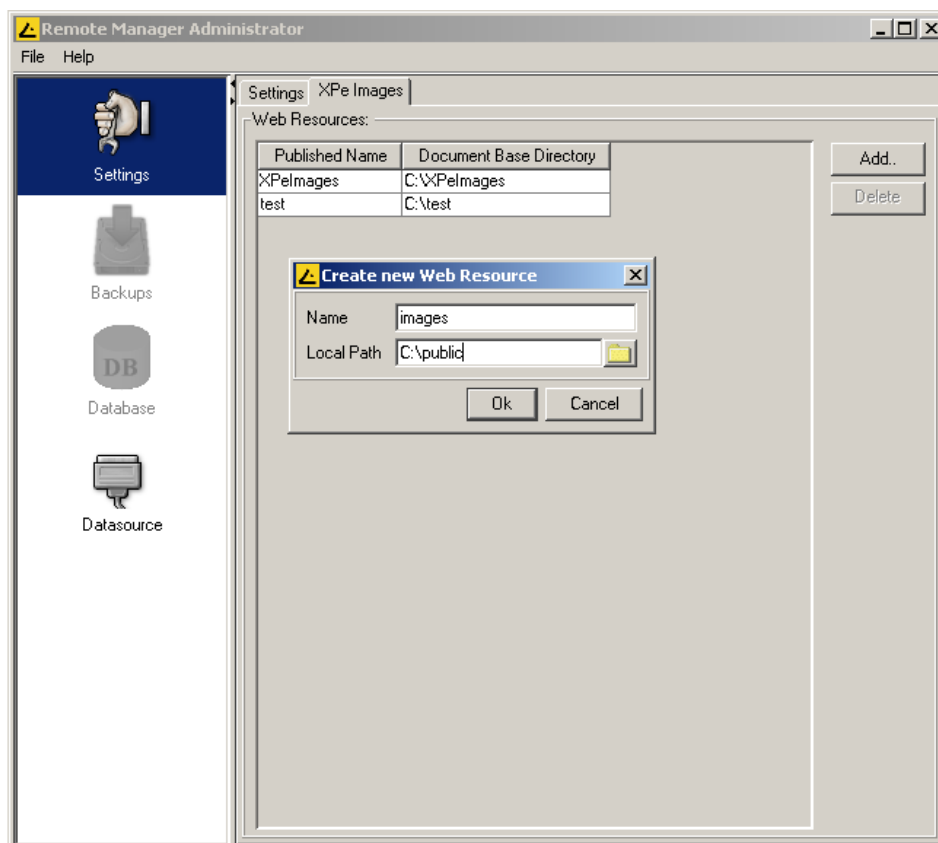
Finally the third parameter **Specify scan reply port (UDP)** is used to define a fixed port on which the Thin Clients reply when you are scanning using UPD (with TCP the reply occurs on the established socket, so this port is not needed). If you specify no port (the default) the application chooses an arbitrary free port.

The **Timeout** value in the **Online Check Parameters** section specifies how long to wait for the answer of an online status query message. The IGEL Remote Manager Console tries to contact all Thin Clients that are in the visible screen range. Every Thin Client in this range needs to respond in the given time to the status query or it gets labeled as offline. (The default is 100). You can disable the online check at all by choosing **Disable online check**. Note that you can disable the online check on the Remote Manager Console, the difference is that in the latter case this feature is only disabled for this particular Remote Manager Console.

13.2 Windows XP Embedded Images

13.2.1 Creating a Web Resource

IGEL Windows XP Embedded Thin Clients offer an option to create snapshots of the entire CF card memory and to store and restore these images onto or from a server supporting the WebDAV protocol. Web Resources to store the images on the IGEL Remote Manager Server can be created in the IGEL Remote Manager Administrator. Select the "XPe images" tab in the settings menu of the RM Administrator and name the Web Resource in the popup dialog and add the corresponding path on your file system.



This generates a URL mapping which enables the Thin Clients to store their images to the path given with "File System Path" or restore them from this directory. The URL consists of the Web Resources' name relative to the Remote Manager URL. For the example given above the URL would be:

<http://localhost:8080/images/>

A new directory "WEB-INF" will be created within the corresponding directory (e.g. C:\public) and will contain the "Deployment Descriptor" for the Remote Manager Server. This Descriptor contains necessary information to publish the Web Resource to the network and must not be removed! Otherwise the URL mentioned above will not be accessible any more.

Access to URLs relative to the given URL of the Web Resource correspond to a file system access relative to the "Document Base Path".

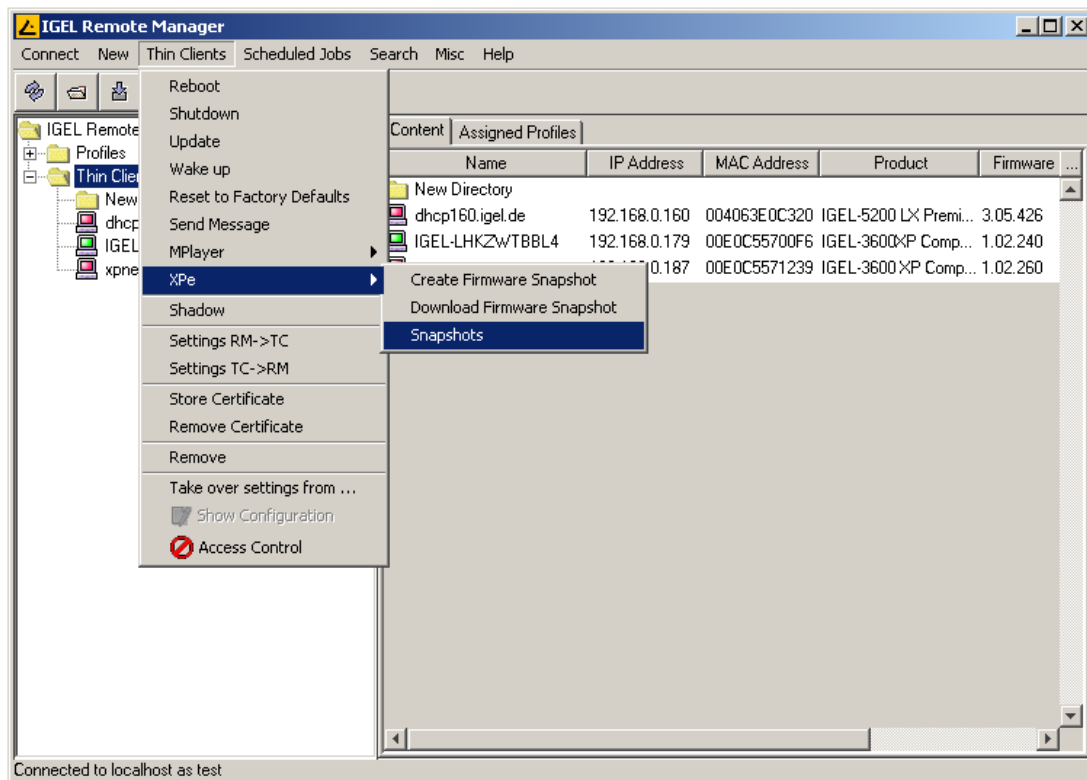
Example:

If the image download address <http://localhost:8080/images/downloads/premium5600.xpe> is assigned to the Thin Client this corresponds to file access to

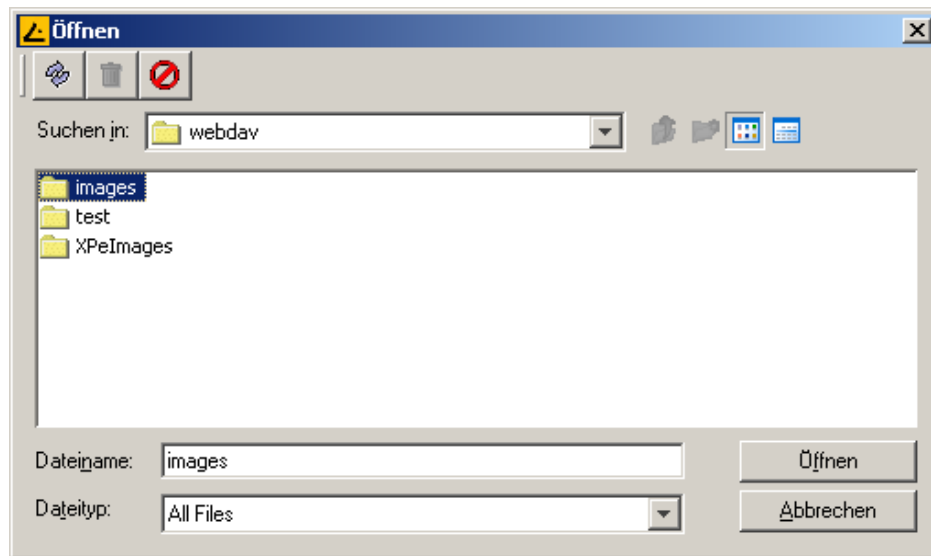
C:\public\downloads\premium5600.xpe.

13.2.2 Assign and manage Web Resources

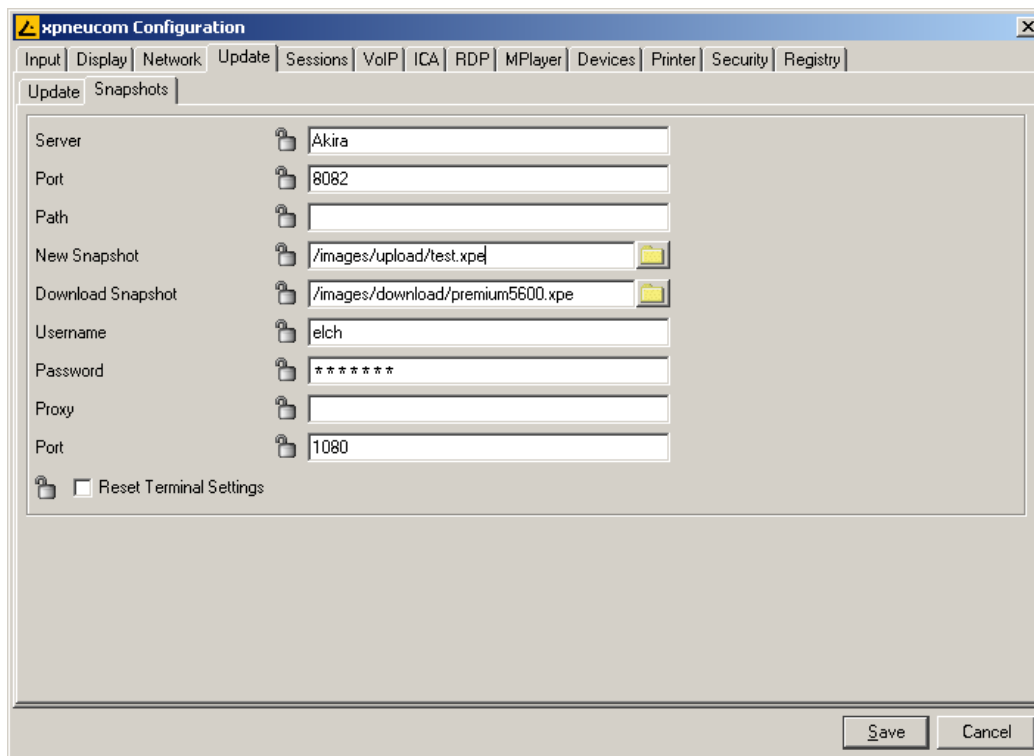
Web Resources created with the IGEL Remote Manager Administrator can be assigned to devices easily within the Remote Manager Client. They are fully integrated in the Remote Manager's authorization concept.



Choose from the Remote Manager Console's menu Thin Clients → XPe → Snapshots or select the directory symbol in the settings of a Windows XPe device (Update → Snapshots) and the following dialog will open to manage Web Resources defined before.



You can delete files, create new (sub)directories or assign access rights. Make sure the values for server, server port and path are set correctly when a file is selected.

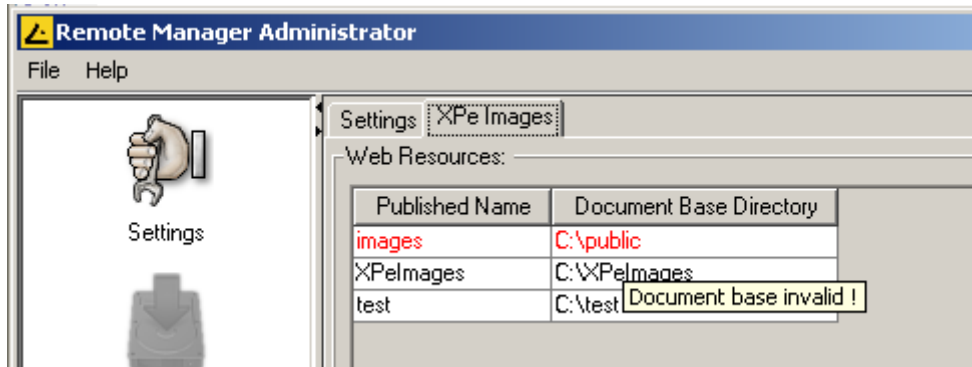


If a setting is locked by a profile the selection is not possible from this dialog and the value has to be maintained manually.

13.2.3 Orphaned Web Resource definitions

Possible problems when restoring a DB backup:

The definition of Web Resources created with the Remote Manager Administrator as well as assigned authorizations are stored in the database system. After restoring a backup it might happen that records lead to files or directories not existing in the file system. In this case definitions of Web Resources are marked and can be deleted.



13.3 Database Manager Operations

Selecting the Backups or Database icon on the left hand menu panel enables you to perform some database administration operations for the local SAP-DB. These features are not supported for Oracle databases or remote databases. How to set up your current database system see section 12.6 → Configuring Data sources.

For both options, Backups and Database, you have to enter the DBM password (database manager password) when you choose one of these menu points for the first the time.

DBM Password:

The password of the database manager (set during installation of the IGEL Remote Manager !). This password is needed for operations like start, stop and uninstall of the SAP database. Note that this is in general not the password you use to connect to the IGEL Remote Manager Server !

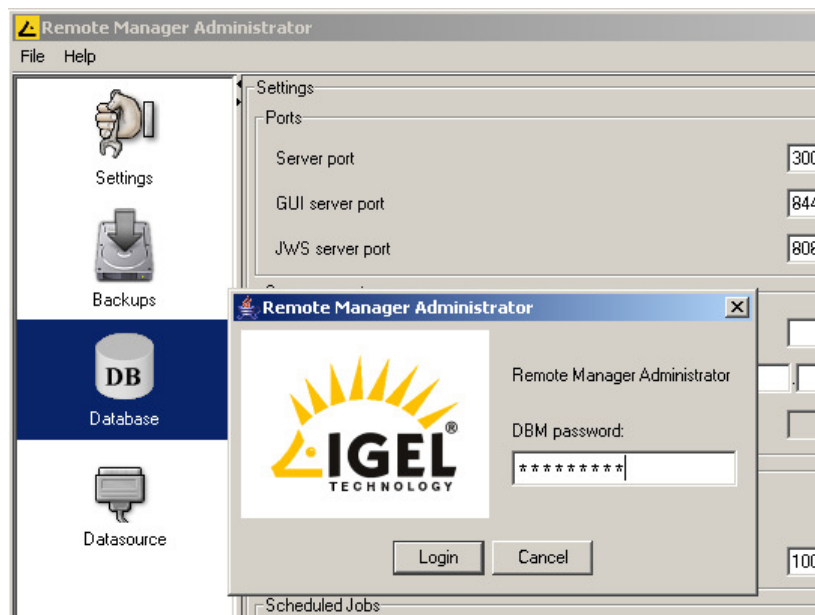


Figure 13-2 Login with DBM password

13.4 Backup and Restore Database contents

The backup panel allows you to save the database contents in a different location, restore data or remove old backup data. If you need to update IGEL Remote Manager, use this utility to restore the data into the new database and convert it in case the format has been changed.

There are two different backup methods (switch by selecting the other tab):

Legacy Backup:

This is the backup functionality of older releases of the Remote Manager. You are not able to create backups using this process any longer, but you can restore your backup from older RM – releases, i.e. prior to 2.0.

New Backup:

The new backup process is safer and more efficient than the legacy backup process. It directly uses the database's backup functionality and forbears from exporting all data to XML – files. This significantly increases performance.

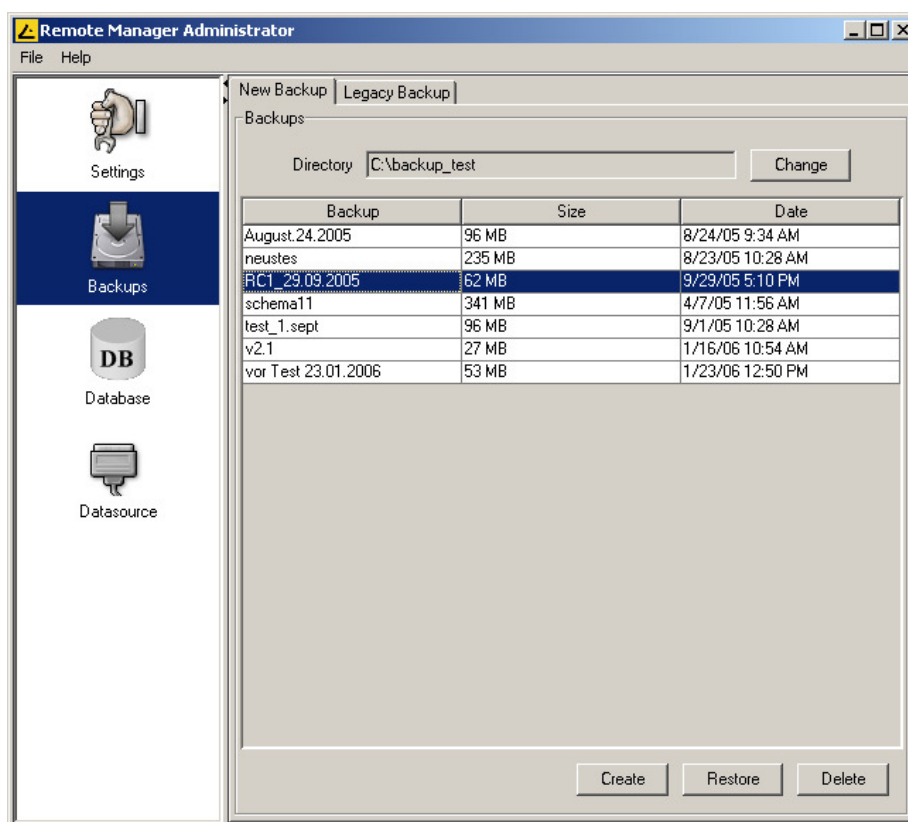


Figure 13-3 Database Restore/Backup

For both, legacy and new backup the handling of the according tab is equivalent:

In order to create a data backup click on the **Create** button and enter a name for this backup in the popup window. The data will be saved into the directory you select.

The certificate files server.pem and server.crt are also included in the backup.

In order to change the target directory, click the **Change** button next to the directory on the top of the screen. A file selection box comes up allowing you to specify the location of your backups.

If you want to restore a saved backup, select the backup in question in the backup list and click **Restore**.

Note: Your current database state will be overwritten! It is strongly recommended you create a backup of the current data before restoring another!

The **Delete** button can be used to delete superfluous backups. This operation deletes the corresponding directories from your hard disk.

Furthermore we provide a command line tool for creating a backup which you can use in time controlled scripts. It is called **rmbbackup** and you find it in the installation directory. You can start it with the following options:

```
rmbbackup ((-d directory -b name) | (-r backup_path)) -u username
          -p password [-s]
```

The meaning of the parameters is:

- **-d directory:** a backup is created and is put in the specified directory
- **-b name:** the name of backup which is created
- **-r backup_path:** the backup with the specified path is restored
- **-u username:** Remote Manager username
- **-p password:** password of the Remote Manager user
- **-s:** no output is generated

13.5 The Database Panel

This panel is used to manage the data and log volumes of the database. It provides information about the total space in use, the used and the free space. Check these values from time to time, full log volumes can decrease performance.

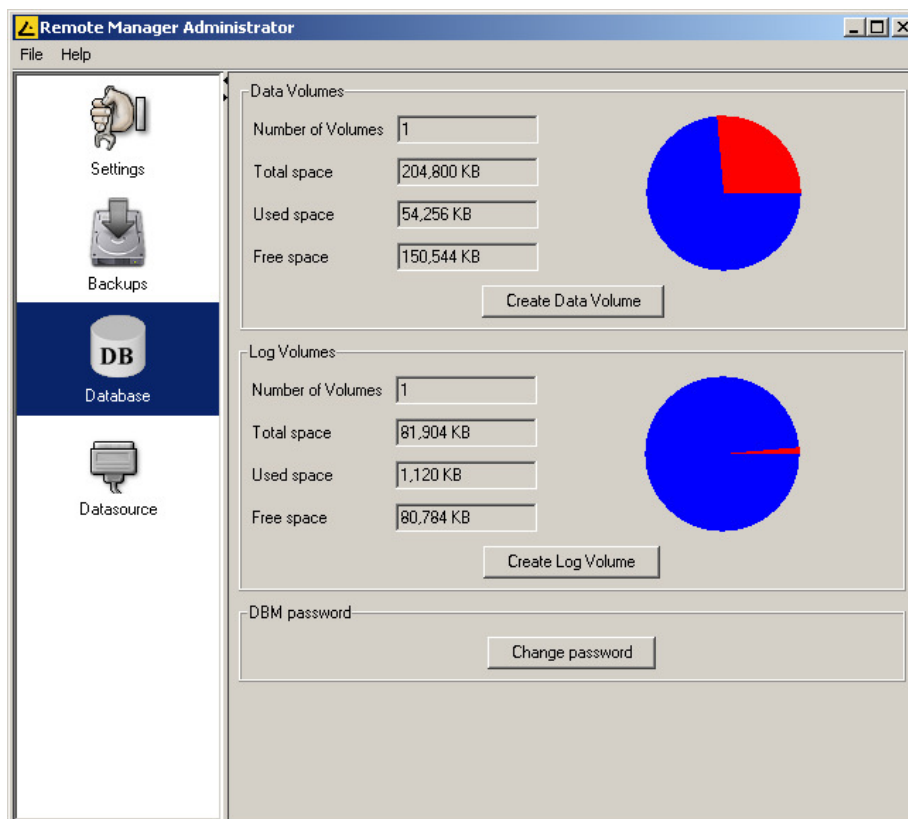


Figure 13-4 Database Panel

Select button **Create Data Volume** to add an additional data volume or **Create Log Volume** respectively. A little dialog where you can set the size of the new volume appears.

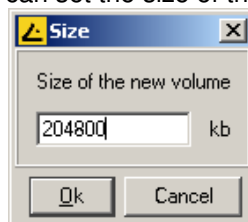


Figure 13-5 Set Volume Size

13.6 The database management tool *igelsapdbm*

In the sub directory *rmadmin* of the installation directory you find the utility *igelsapdbm*. This tool is used to manage the data and log volumes of the database. If you have a lot of content in your database (e.g. several hundreds of Thin Clients and profiles, dozens of firmware versions) the data and log volumes may become full. An indication of this state is that the database slows down heavily. In this case you should use *igelsapdbm* to detect if the volumes are full and create if necessary additional ones. You can start the tool with the following arguments:

```
igelsapdbm <dbm_password> <options>
```

where <dbm_password> is the database manager password and <options> are:

- **-d:** show DATA volumes
- **-l:** show LOG volumes
- **-D size:** add a DATA volume; size in KB
- **-L size :** add a LOG volume; size in KB

13.7 Configuring Data sources

Starting with version 2.02 IGEL Remote Manager adds support for Oracle databases. During the installation process the user can choose the standard installation that includes a default setup for the SAP-DB, or to install the application without database setup. In the latter case, the configuration of a data source that is described in this section is needed to complete the RM-Server installation.

The Data sources Configuration Tool is used to define remote or local SAP-DB or Oracle database-connections and prepare them for use by Remote Manager. This means a database-scheme containing all necessary tables for RM-data is created or an existing one is mounted and eventually updated to the current version.

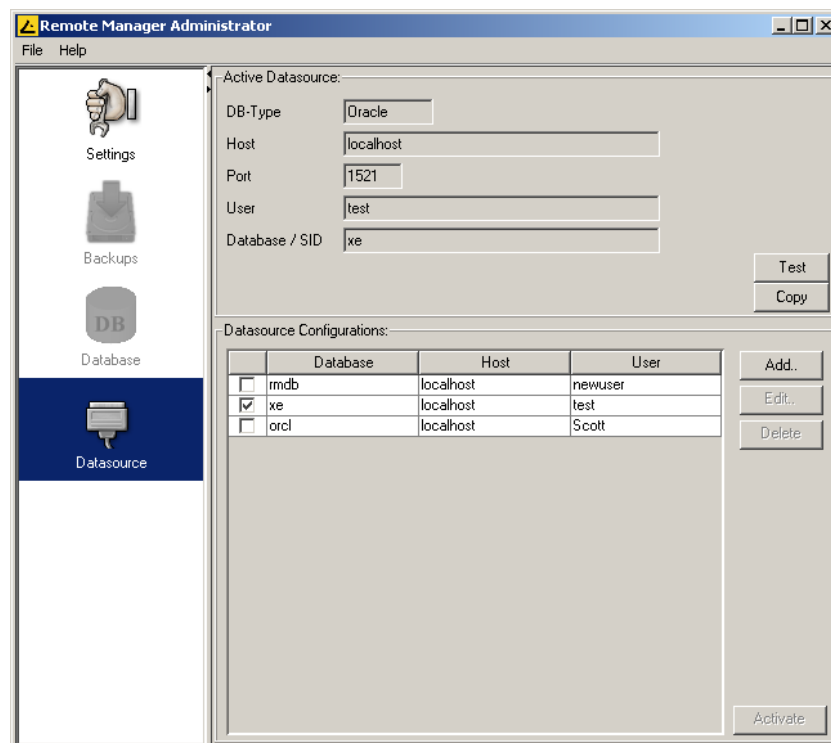


Figure 13-6 Data source Configuration

The upper part of the Data source Configuration Panel displays the Remote Manager's currently active database connection. This database and user/scheme is used to manage data. There is always just one data source set active. The list below displays predefined data sources, the active one is marked with a hooked checkbox.

13.7.1 Defining a data source

To add a new data source configuration press the Add – button on the right side of the data sources list and fill out the configuration data:

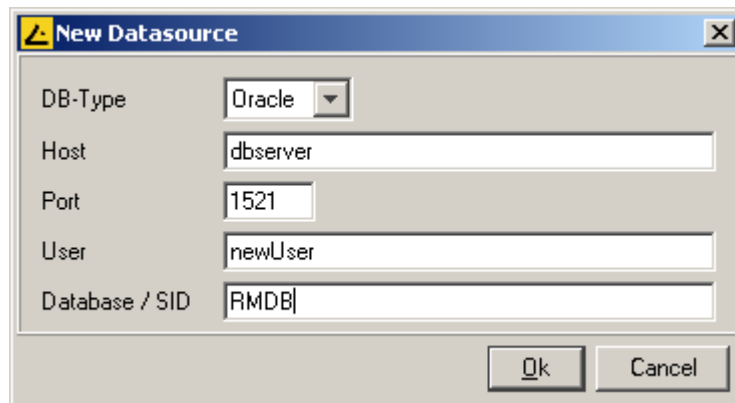


Figure 13-7 Define a new data source

These connection options can be configured:

- DB-Type: the database type, i.e. either a Oracle or a SAP-DB database system.
- Host: the hostname where the DBS is running.
- Port: the port the DBS uses for incoming requests.
- User: The user / schema –name the RM connects to.
- Database: Name of the database, the SID for Oracle systems.

Options Port and Database can not be configured for SAP-DB.

Note: For the database user the role *resource* must be granted to enable the user to create the scheme objects.

Use buttons Edit and Delete preconfigured data sources.
Button Test checks if the active data source is still valid.

13.7.2 Setting an active Data source

To activate a predefined data source press the Activate button. Next the user will be asked to enter the password for the selected data source:

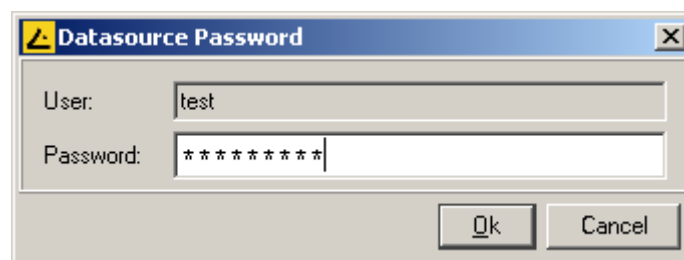


Figure 13-8 Enter Data source – PW

Within the Data source activation process the application checks if a valid database scheme is found. If no scheme is found a new one is created, an outdated one is updated, and if the scheme contains unknown data, this data is overwritten. For each action the user is asked for confirmation:

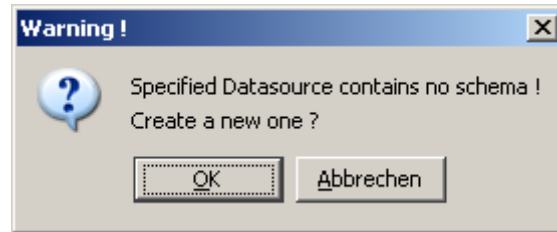


Figure 13-9 Confirm creating new DB-scheme

Note: Overwriting existing data means to clear the entire db-scheme, not only outdated tables used by IGEL Remote Manger !

13.7.3 Copy Data source

RM Administrator provides a powerful functionality to mirror or migrate the Remote Manager application data from one database system to another. If you select Copy Button in the Active Data source panel, the data is transferred from the active data source to any other predefined Data source:

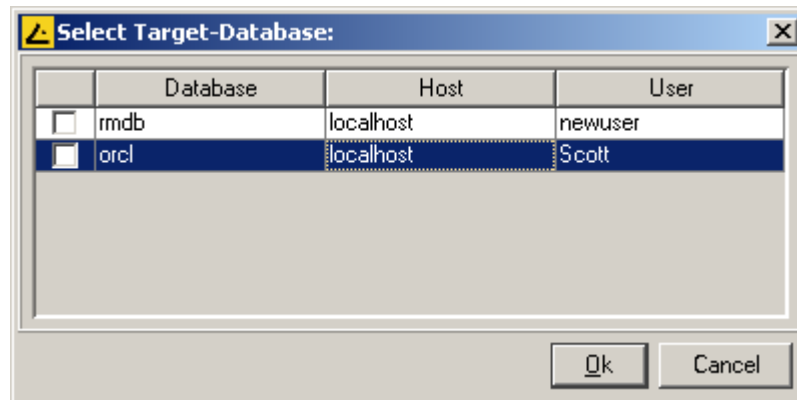


Figure 13-10 Select a target data source

Once the copy process been has successfully completed (this can take a while, approximately 30 minutes for a database with thousand of thin clients), the user is asked if the target data source is the new active data source.

14 Troubleshooting

14.1 Log files

Whenever you experience problems with the software, you should have a look at the log files of the IGEL Remote Manager. Since the IGEL Remote Manager exists of different modules programmed in different languages, there are different locations where you can find log messages.

The **SAP DB** and the **IGEL TC Server** write their messages into the Event Log system. If you want to send the message from the Event Log to your supporter, right click on the application protocol and select **Save Log File As** and in the **Save As** dialog box choose **Text** as type from the drop down list.

The **IGEL GUI Server** writes log messages in files in the directory `<installation_directory>\rmguiserver\logs`. There you find the files `stderr.out`, `stdout.out`, `catalina.xxxx.log` where `xxxx` stands for a date.

If the Remote Manager Console or the Remote Manager Administrator tool seems to make trouble, you can start these applications from the command shell in the following manner so that they write additional information in a log file:

IGEL Remote Manager Console
(Windows) RMClient.exe -is:log <filename>
(Linux) ./RMClient.bin -is:log <filename>

IGEL Remote Manager Administrator:

(Windows) RMAAdmin.exe -is:log <filename>
(Linux) ./RMAAdmin.bin -is:log <filename>

When running the application until the error occurs, the file contains logging information that usually helps to track down the problem.

14.2 Known issues

Issue:

After the installation or an update you cannot connect from the Remote Manager Console to the server.

Possible reasons and solutions:

- Have a look at the <installation_directory>\rmguiserver\logs\stderr.log file. If you find a message *java.net.BindException: Address already in use* there is another application which listens on the *GUI Server Port* or *JWS Port*.
Solution: Use the Remote Manager Administrator utility to change the port(s).
- The *cacerts* file does not match to the Remote Manager Server installation or is missing
Solution: If you are connecting from remote to the Remote Manager Server, copy the file <installation_directory>\rmclient\cacerts from the server installation to the remote PC. If the file on the server does not exist or does not match, you can create a matching *cacerts* file with the following two commands (after removing the wrong file where applicable):

```
<installation_directory>\_jvm\bin\keytool -export -alias igelkey -file <
installation_directory>\key.tmp -keystore
<installation_directory>\rmguiserver\irm_keystore -storepass igelkey (one
line)
<installation_directory>\_jvm\bin\keytool -import -alias igelkey -file
<installation_directory>\key.tmp -keystore
<installation_directory>\rmclient\cacerts -storepass igelkey -noprompt
(again one line)
```

Issue:

You can connect from the Remote Manager Console to the server, but when you try to register a Thin Client after scanning, an error occurs:

Possible reasons and solutions:

- Look in the Event Viewer for additional information. If it is a database problem, have a check if the ODBC settings are correctly.
- In some cases security and firewall software (e.g. the Windows XP Internet Connection Firewall) prevents the IGEL Remote Manager from working.
Solution: Uninstall the Internet Connection Firewall or install the IGEL Remote Manager on a computer without security software