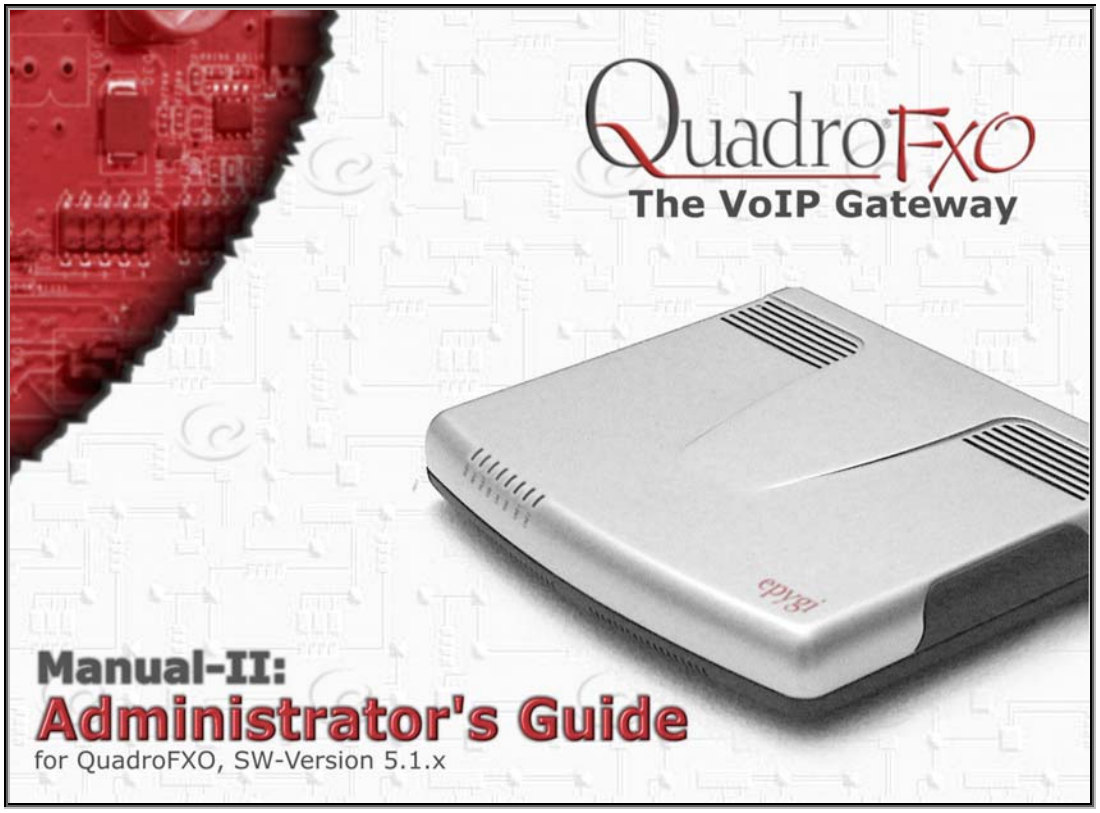


Edition 1
SW Release 5.1.13 and higher, June 2009

Table of Contents

Manual I: see Installation Guide

Step-by-step guide to install and configure Quadro.

Manual II: Administrator's Guide

About this Administrator's Guide

The Quadro Manual is divided into three parts:

- **Manual I: Installation Guide**
  gives step-by-step instructions to provision the QuadroFXO and configure the phone extensions with the Epygi SIP Server. After successfully configuring the QuadroFXO, users will be able to make SIP phone calls to remote Quadro devices, make local calls to the PSTN and access the Internet from devices connected to the LAN.
- **Manual II: Administrator's Guide** explains all Quadro management menus available for extension users. A list of all call codes can be found there, too.

This guide contains many example screen illustrations. Since Quadro IP PBXs offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular Quadro IP PBX as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

Quadro's Graphical Interface describes the Quadro's graphical user interface and explains all recurrent buttons.

Administrator's Menus explains the Administrator's management pages according to the menu structure shown on the main page of the Quadro management.

Extension User's Menus explains some input-options for administrators only that may be selected from the extension user's main page.

Appendix: System Default Values lists all factory defaults.

Appendix: Software License Agreement includes the contract for using Quadro's hardware and software.

Quadro's Graphical Interface

Administrator's Main Page

When the administrator logs in, the **Quadro Management** page is displayed with a table of active calls (including information about call peers, call duration and start time) at the startup. Here the administrator may access the following settings and perform the actions:

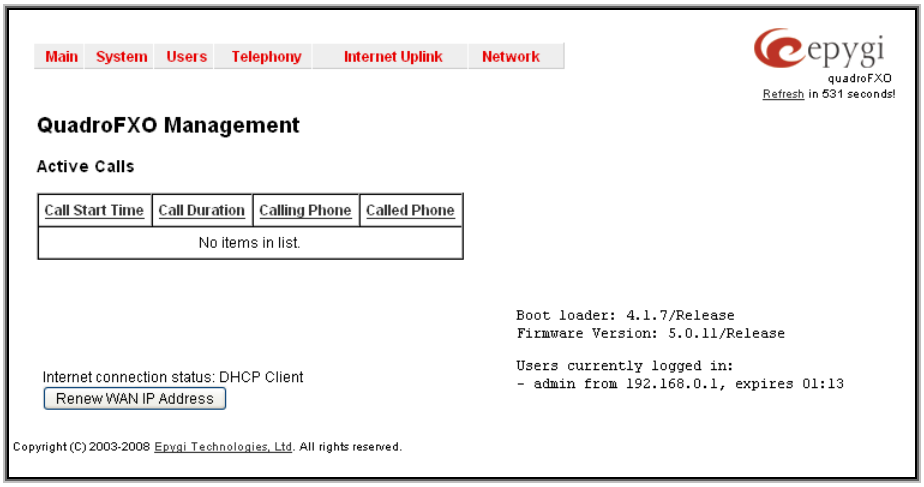


Fig. II-1: QuadroFXO Management

System Menu

- System Configuration Wizard
- Internet Configuration Wizard
- Status
- IP Routing Configuration
- Configuration Management
- Events
- Time/Date Settings
- Mail Settings
- SMS Settings
- Firmware Update
- Networking Tools
- SNMP Settings
- Diagnostics
- Upload Language Pack
- User Rights Management

Telephony Menu

- Call Statistics
- SIP Settings
- RTP Settings
- NAT Traversal Settings
- FXO Settings
- PSTN Lines Sharing
- Gain Control
- SIP Tunnel Settings
- Call Routing
- VoIP Carrier Wizard
- RADIUS Client Settings
- Voice Mail Common Settings
- Dial Plan Settings
- System Hold Music Settings
- RTP Streaming Channels

Internet Uplink Menu

- PPP/ PPTP Settings
- VPN Configuration
- Dynamic DNS Settings
- Firewall and NAT
- Filtering Rules
- IDS Log

Users Menu

- Extensions Management
- Authorized Phones Database

Network Menu

- DNS Settings
- DNS Server Settings
- DHCP Settings for the LAN Interface

Registration Form
(in menu tree only)

Logout

The functional button **Renew Wan IP Address** appears on the administrator's main **Quadro Management** page if the Quadro device acts as a DHCP client. The **Renew WAN IP Address** button is used to obtain a new WAN IP address in case, e.g., the Quadro moves to another network.

The functional button **Establish Your Internet Connection Now** respectively **Terminate Your Internet Connection Now** occurs on the Quadro Management page if PPPoE is used as WAN interface protocol.

The link **Please Check Your Pending Events** will be displayed on the administrator **Main Menu** page if new system events exist. The link leads to the **Events** page that can be also accessed from the System menu.

The list of **Users currently logged into the system** is seen in the lower right corner of the Administrator's Main Menu. Information about IP address user accessed Quadro GUI from, the username user is logged in and the time until the next automatically logout is provided herein. The current version of the Quadro's firmware and of its boot loader is also available here. The idle session timeout is set to 20 minutes. If no action is performed during that time, user will be automatically moved to the Login page and will be requested to login again.

The link **Refresh in** occurs in the upper right corner beside the field displaying the number of seconds until the next refresh and is used to perform a manual reload of the page. If a page with a Refresh counter is left opened, the session time-out counter will be updated periodically and the logout timeout will never expire.

Recurrent Buttons

Throughout this guide, you will see a variety of recurrent buttons. Below is a description of these buttons.

Button	Description
Previous	This button leads back to the previous page of a fixed sequence of pages (used mainly in wizards).
Next	This button leads forward to the next page of a fixed sequence of pages (used mainly in wizards).
Cancel	This button discards the latest not yet confirmed entries.
Finish	This is the last button of a fixed sequence of pages that completes and saves the entries of an entire sequence.
Help	This button opens the help page belonging to the currently active Quadro management page.
IP-Clipboard	This button opens a window where the last inserted IP addresses are listed. It allows the user to make a quick selection of an IP address that has been previously used. This will avoid the user needing type it again. The clipboard can hold up to 10 IP addresses and a new IP address will replace the oldest one from the list.

Button	Description
Back	This button returns you to the page you were previously on.
Ok	This button confirms an operation you started before.
Yes	This button confirms an operation you chose before.
No	This button discards an operation you chose before.
Save	This button saves the settings modified on the currently active management page.
SIP-Clipboard	This button opens a window where the last inserted SIP addresses are listed. It allows the user to make a quick selection of an IP address that has been previously used. This will avoid the user needing type it again. The clipboard can hold up to 10 SIP addresses and a new SIP address will replace the oldest one from the list.

Recurrent Functional Buttons

In connection with the tables, the following are the few buttons you will see:

Functional Button	Description
Add	Allows adding a new record to the displayed table. A new page will be displayed to enter any new settings.
Edit	Allows modifying the settings of the record selected by a checkbox. Normally only one (1) record may be selected. A new page will be displayed to enter the modified settings.
Delete	Deletes the selected entry(s) of a table. A warning message will ask for confirmation before deleting an existing entry.
Select All	Selects all table entry(s) for example for further deletion.
Inverse Selection	Inverses (opposites) an existing selection of table entry(s). If no entries are selected, clicking the button will select all records.
Refresh in...	May be shown in the upper right corner of a page. It displays the number of seconds remaining until the next refresh of the page will occur. It may be used to reload the page manually.

Most of the tables offer the option to sort the entries in ascending or descending order by clicking the headings of the columns. A small arrow next to the column heading indicates the direction of sorting - upward or downward. The entries of the table can be selected by using the corresponding checkboxes in order to edit or delete them.

Entering SIP Addresses Correctly

Calls over IP are implemented based on Session Initiating Protocol (SIP) on the Quadro. When making a call to a destination that is somewhere on the Internet, a SIP address must be provided.

SIP addresses needs to be specified in one of the following formats:

"display name" <username@ipaddress:port>
"display name" <username@ipaddress>
username@ipaddress:port
username@ipaddress
username

For your convenience, the following combinations can be used:

- *@ipaddress - any user from the specified SIP server
- username@* - a specified user from any SIP server
- *@* - any user from any SIP server

The display name and the port number are optional parameters in the SIP address. If a port is not specified, 5060 will be set up as the default one. The range of valid ports is between 1024 and 65536.

A flexible structure of wildcards is allowed. In comparison with a wildcard, the "?" character stands for only one unknown digit and the "*" character stands for any number of any digits.

Please Note: Wildcards are available for caller addresses only. No wildcard characters are allowed for called party addresses. Exceptions are addresses in **Supplementary Addresses** table that are used by **Outgoing Call Blocking** service. To use "*" and "?" themselves (as non wildcard characters), use "*" and "\?" correspondingly.

Administrator's Menus

System Menu

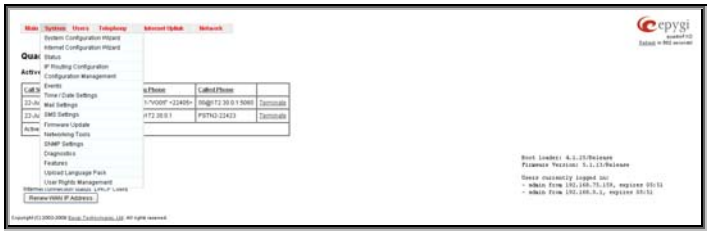


Fig. II-1: System Menu in Dynamo theme

Fig. II-2: System Menu in Plain theme

System Configuration Wizard

The **System Configuration Wizard** allows the administrator to define the Quadro's Local Area Network settings and to specify regional configuration settings to make Quadro operational in its LAN. The **System Configuration Wizard MUST be run upon Quadro's first startup** to make sure that it works properly in its network environment. The Wizard allows navigating through the following basic configuration parameters and settings:

- System Configuration (see below)
- DHCP Settings for the LAN Interface
- Regional Settings and Preferences (see below)

Fig. II-3: System Configuration Wizard - Start page

DHCP Settings for the LAN are described in the chapters below. The LAN configuration and regional settings will be described later in this chapter.

Please Note: It is strongly recommended to leave the factory default settings if their meanings are not fully clear to the administrator.

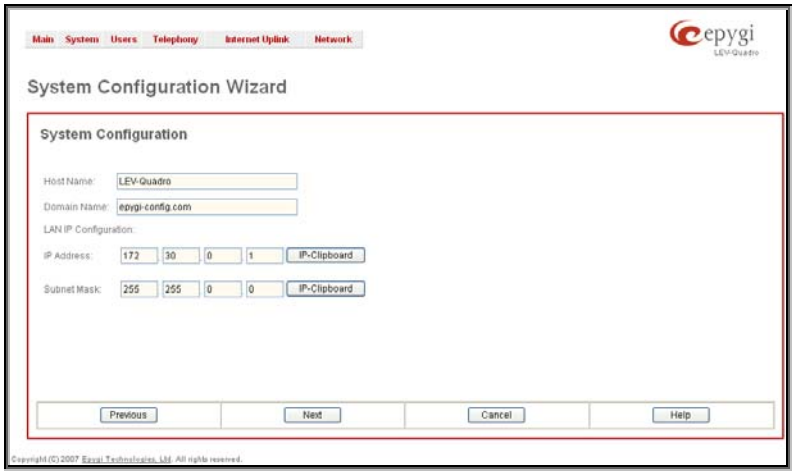


Fig. II-4: System Configuration Wizard - System Configuration page

The **System Configuration** page contains the host name, IP address and Subnet Mask information about the Quadro LAN interface. These settings make Quadro available to the internal network.

The **System Configuration** page offers the following input options:

Host Name requires a host name for the Quadro device.

Domain Name requires the LAN side domain name which the Quadro belongs to.

IP Address requires the Quadro host address for the LAN interface.

Subnet Mask requires the Quadro hosts' Subnet Mask.

The **Regional Settings and Preferences** are used to select settings specific to the location of the Quadro. This is important for the functionality of the voice subsystem.

The **Regional Settings and Preferences** page has two drop down lists to select the **Location** (country) and a corresponding **Timezone**. Quadro will support Daylight Savings (DST) correction if it is available for the selected time zone.

This page also has a manipulation radio button group to choose:

- **System Language** – selection is available only when the custom Language Pack has been uploaded and it is used to enable custom language for system voice messages or returning back to the default language English.
- **GUI Theme** - selection used to select the GUI theme style of the web based configuration pages.

The **Choose Theme on Login** checkbox indicates whether the GUI theme selection radio buttons should be displayed on the Quadro Login page. Selecting the checkbox will allow users to choose the GUI theme before logging into the Quadro. Leaving the checkbox unselected will require the administrator to run the System Configuration Wizard to change the theme.

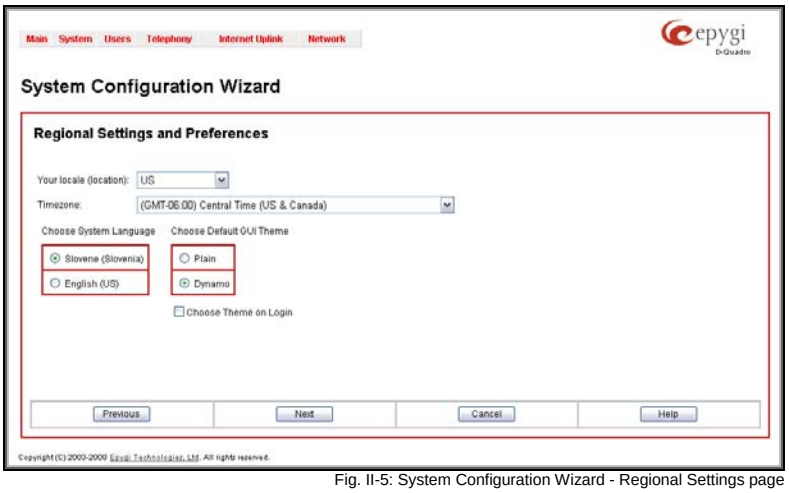


Fig. II-5: System Configuration Wizard - Regional Settings page

Internet Configuration Wizard

The **Internet Configuration Wizard** allows the administrator to configure the WAN interface settings and to adjust Quadro's connectivity with an external network. The **Internet Configuration Wizard MUST be run for Quadro to be connected to the Internet**.

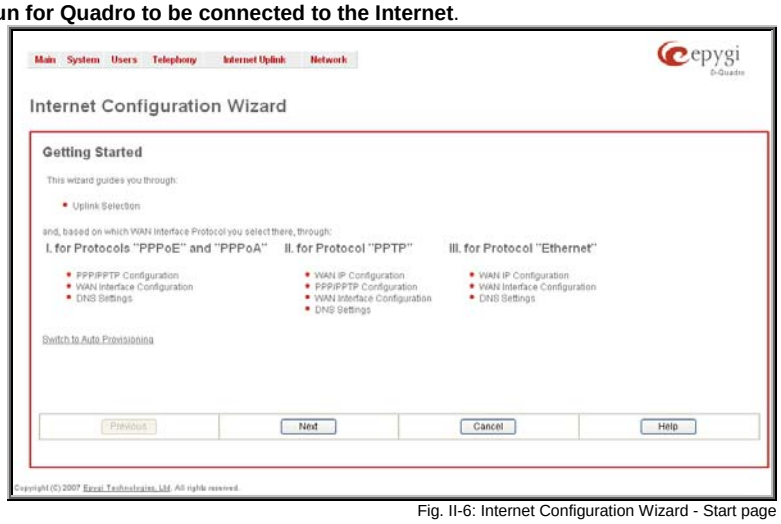


Fig. II-6: Internet Configuration Wizard - Start page

All the settings of the **Internet Configuration Wizard** are described in the chapters below except those for the IP settings, which will be described in this chapter.

Please Note: It is strongly recommended not to change the factory default settings if their meanings are not fully clear to an administrator.

The Wizard allows navigating through the following basic configuration parameters and settings:

- Uplink configuration (see below)

For WAN Interface protocol **PPPoE**, **PPPoA**, **1483B** and **1483R**:

- PPP/ PPTP Settings
- WAN Interface Configuration (see below)
- DNS Settings

For WAN Interface protocol **PPTP**:

- WAN IP Configuration (see below)
- PPP/ PPTP Settings
- WAN Interface Configuration (see below)
- DNS Settings

For WAN Interface protocol **Ethernet**:

- WAN IP Configuration
- WAN Interface Configuration (see below)
- DNS Settings

The **Switch to Auto Provisioning** link moves you to the Automatic Provisioning page where Quadro can be configured automatically.

The **Uplink Configuration** page allows you to select the Quadro's WAN interface connection type and its bandwidth settings. These settings will make Quadro available to the external network.

Depending on the Uplink Interface Protocol selection, the page following the **Uplink Configuration** page is different. Thus if **PPPoE** is selected, the next page will be **PPP Configuration**, while selecting **Ethernet** will bring up the **WAN IP Configuration** page.

The **Uplink Configuration** page offers the following components:

The **WAN Interface Protocol** radio buttons are used to choose the protocol depending on the requirements of the ISP (Internet Service Provider):

PPPoE - turns on the PPP over an Ethernet connection.

PPTP – turns on the Point to Point Tunneling Protocol (**PPTP**) interface used for the connection between Quadro and ADSL modem. A fixed IP address configuration is needed in this case.

Ethernet - turns on the Ethernet connection.

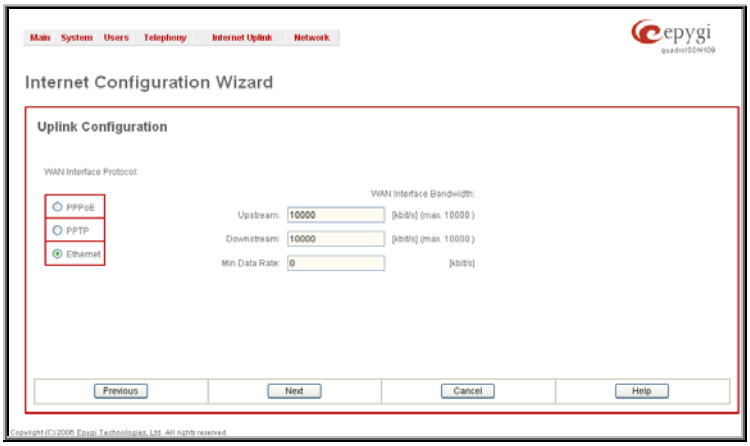


Fig. II-7: Internet Configuration Wizard - Uplink Configuration page

The **WAN Interface Bandwidth** settings allow the specification of the upstream and downstream speeds in kbit/s, helping to assure the quality of IP calls. An IP call looses the voice quality if there is no available bandwidth. When approaching the limits of bandwidth capacity, another IP call will be declined.

The bandwidth provided by the ISP has to be specified in the text fields **Upstream Speed** and **Downstream Speed**. The default entry in both fields is 10000, the maximum bandwidth of a 10 MB Ethernet. In most cases, providers offer a smaller bandwidth than 10000 kbit/s.

The bandwidth required by an IP call depends on the codecs used and these specifications are listed in the table below:

Required Bandwidth for Standard Packets:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:							
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	G.723	iLBC-13.33
10	105	58	66	74	82	50	-	-
20	84	37	45	53	61	29	-	-
30	76	30	38	45	53	22	21	27
40	74	27	34	42	50	19	-	-
50	71	25	32	40	48	17	-	-
60	67	22	30	37	45	15	13	20

Required Bandwidth for Encrypted Packets when a VPN is used:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:							
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	G.723	iLBC-13.33
10	148	98	105	118	124	92	-	-
20	105	59	65	74	81	49	-	-
30	90	43	52	60	66	35	35	41
40	85	38	45	53	61	30	-	-
50	80	34	41	48	56	26	-	-
60	74	29	37	45	52	22	20	26

The **Min Data Rate** text field requires the amount of upstream bandwidth that ought to remain for data applications even if voice applications use the entire available upstream bandwidth. The value selected here needs to be smaller than the upstream bandwidth and is measured in kbit/s.

The **WAN IP Configuration** page is only displayed if **Ethernet** or **PPTP** has been selected to be the uplink protocol. It offers the following components:

The **Assign automatically via DHCP** radio-button selection switches to automatic retrieval of the WAN IP address from a DHCP server at the ISP/uplink.

Please Note: DHCP referred to here is the one that runs on the provider's side and not the Quadro's personal DHCP server.

The **Assign Manually** radio-button switches to the manual adjustment of IP settings. This selection requests the following parameters:

IP Address requires the IP address for the Quadro WAN interface.

Subnet Mask requires the subnet mask for the Quadro device WAN interface.

Default Gateway requires the IP address of the router where all packets are to be sent to, for example, to the router of the provider.

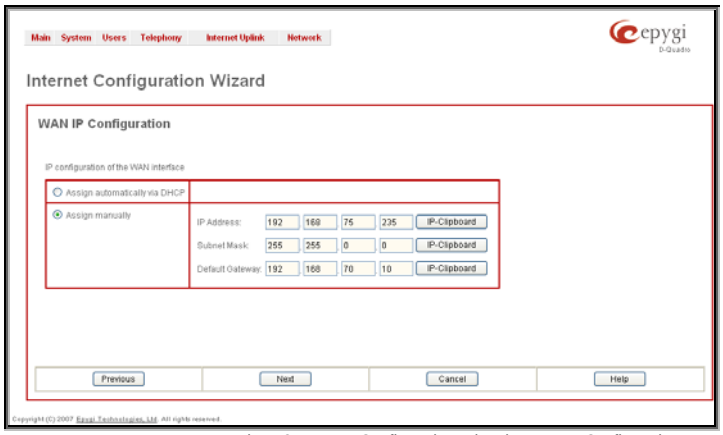


Fig. II-8: Internet Configuration Wizard - WAN IP Configuration page

The **WAN Interface Configuration** page may be used to modify the MAC address of the Quadro. This might be necessary if the ISP (Internet Service Provider) requires a specified MAC address, for example, for authentication. This page offers the following components:

MAC Address Assignment manipulation radio-buttons:

- **This Device** turns to the default MAC address of the Quadro.
- **User Defined** requires user defined MAC Address.

The **MTU** drop down list allows you to select the maximum packet size on the Ethernet (in bytes). MTU is used to fragment the packets before transmitting them to the network. The MTU preferred value is dependent on the Ethernet connection . The default MTU size is 1500 Bytes for Ethernet and 1400 Bytes for PPPoE.

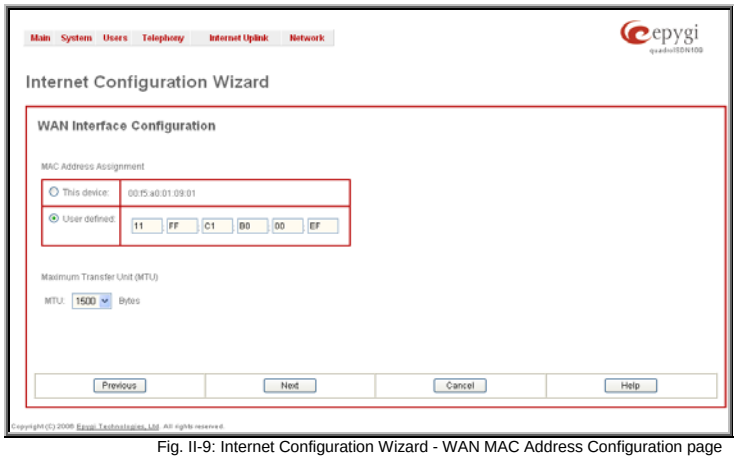


Fig. II-9: Internet Configuration Wizard - WAN MAC Address Configuration page

Status

The system status window displays non-editable tables providing extensive system status information about Quadro: General Information, Network Status, Lines Status, Memory Status, Hardware Status and SIP Registration Status. The links on this page lead to device Transfer Statistics, user mailboxes and supplementary services configuration pages.

The **System Status** page has several tables providing system information.

General Information

The **General Information** page includes the following information:

- **Uptime duration -** Period Quadro is on since last reboot.
- **Device hostname -** Quadro device host name.
- **Quadro Operating System -** Quadro operating system version.
- **Application Software -** Software and file system versions of the Quadro.
- **Boot Loader -** Quadro boot loader version.
- **DSP Software -** Quadro DSP software version and the date of build.
- **Language Pack** – this field is present only when the custom language pack is uploaded and it indicates the version.

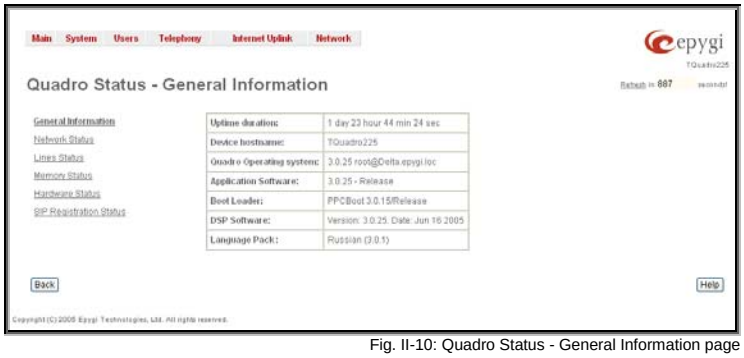


Fig. II-10: Quadro Status - General Information page

Network Status

The **Network Status** page includes the following information about **Interfaces**:

Interface Name lists the Network interfaces available on the Quadro (LAN and WAN).

IP Address lists the IP addresses corresponding to each network interface.

Subnet Mask lists the subnet masks corresponding to each network interface.

Properties will list the MAC address corresponding to each network interface on the Quadro.

Monitor includes links to survey LAN and WAN traffic correspondingly. The selection of these links will open a new window with a table of network traffic statistics on the following selected interfaces:

- Received Bytes
- Received Packets
- Received Errors
- Received Drop Errors
- Received Overrun Errors
- Received MultiCast Packets
- Transmitted Bytes
- Transmitted Packets
- Transmitted Errors
- Transmitted Drop Errors
- Transmitted Carrier Errors
- Transmitted Collisions

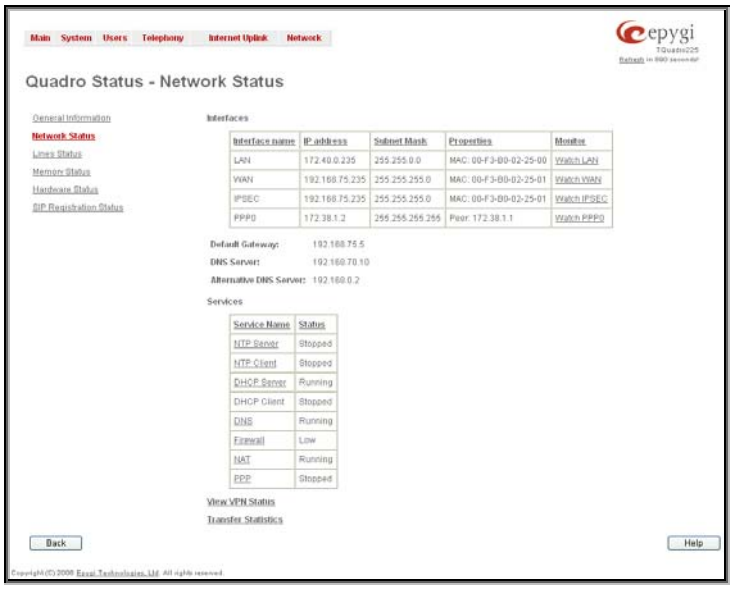


Fig. II-11: Quadro Status Network Status page

When opening the corresponding interface statistics window, no traffic values are displayed at first. After opening the window, the tables will serve as a counter and traffic statistics will be updated every minute.

DNS Server, **Alternative DNS Server** and **Default Gateway** - these display the Quadro settings corresponding to what has been configured with the System Configuration Wizard.

Services (NTP Server and Client, DHCP Server and Client, DNS, Firewall, NAT, PPP) statuses: shows if they have **stopped** or if they are still **running**.

Transfer Statistics - link to the Transfer Statistics page.

The **Transfer Statistics** page shows a user-defined statistics table with the transmit/receive value (criteria), interface type and time period. It contains the following components:

Time range of statistic table - the drop down list includes the period (in days) statistics data that is to be collected and the corresponding diagram charts that are to be built.

Interface - the drop-down list offer the values:

- **WAN** - Wide Area Network (WAN) events only
- **LAN** - Local Area Network (LAN) events only

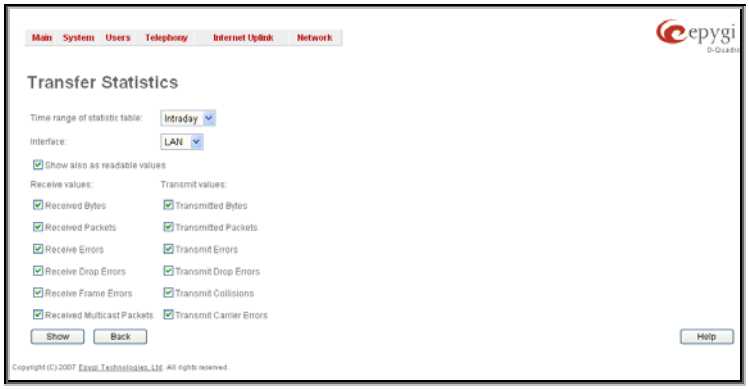


Fig. II-12: Transfer Statistics page

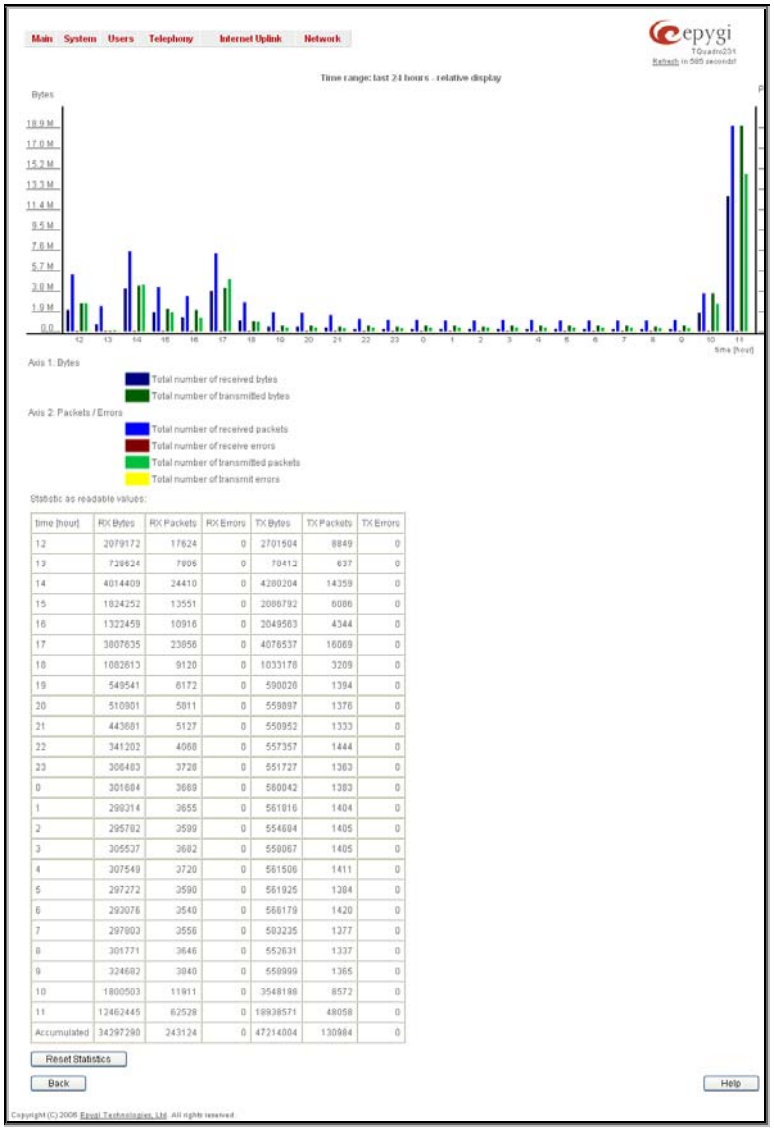


Fig. II-13: Transfer Statistics Diagram Chart

The area **Receive Values** provides the following:

- **Receive Bytes** - number of received bytes.
- **Receive Packets** - number of received Ethernet packets.
- **Receive Errors** - number of received packets containing errors.
- **Receive Drop Errors** - number of received packets that have been discarded.
- **Receive Overrun Errors** - number of received overrun errors that occur when the receive buffer is not large enough to hold all incoming packets. This error usually appears due to a slow receiving system.
- **Receive MultiCast Packets** - number of received broadcast packets.

The area **Transmit Values** provides the following:

- **Transmit Bytes** - number of transmitted bytes
- **Transmit Packets** - number of transmitted Ethernet packets.
- **Transmit Errors** - number of transmitted packets containing errors.
- **Transmit Drop Errors** - number of transmitted packets that have been discarded.
- **Transmit Carrier Errors** - number of transmit carrier errors that occur due to a defective or lost connection on the Ethernet link.
- **Transmit Collisions** - number of transfer errors that occurred during a simultaneous packet transmission from both sides.

To see the **Transfer Statistics Diagram Charts**, select the desired criteria and click **Save** to generate the corresponding chart and the table showing the transfer statistics values (if enabled). The letters **M** (millions) and **K** (thousands) used in the legend of the displayed diagrams show the total number of specified criteria. The **Reset Statistics** button is used to reset the chart and the table (if enabled).

Lines Status

The **Quadro Status** - **Lines Status** page shows the current status of each FXO line with all details of the active calls. Since only one line of information can be displayed at a time, the **FXO#** functional buttons are used to navigate through information regarding other lines.

Fig. II-14: Line Status - FXO Status page

The **Lines Status** table of each **FXO Line** provides information about the **Allowed Call Types**, the extension number (attendant or routing client), to whom the **Incoming Call** is **Routed To** and the **State** of the line (**Free** or **Busy**).

The **FXO Channel Usage Statistics** link is only present for local FXO lines (this option is not available for shared FXO lines) and leads to the page where diagram chart of FXO lines usage can be viewed.

The **FXO Channel Usage Statistics** page consists of following components used to define the chart parameters:

Trunk checkboxes are used to select the FXO line number(s) over which the FXO traffic chart will be built. At least one Trunk checkbox should be selected, otherwise error message appears.

Time range of statistic table drop down list includes the period (in days) statistics data that is to be collected and the corresponding diagram chart that is to be built.

Incoming Calls and **Outgoing Calls** checkboxes are used to select whether the FXO traffic statistics for only incoming or outgoing or for both type of calls should be displayed in the diagram chart.

Maximum Active Calls checkbox is used to have the number of maximum active calls displayed in the diagram chart.

At least one of these checkboxes should be selected, otherwise error message appears.

Fig. II-15: FXO Channel Usage Statistics page

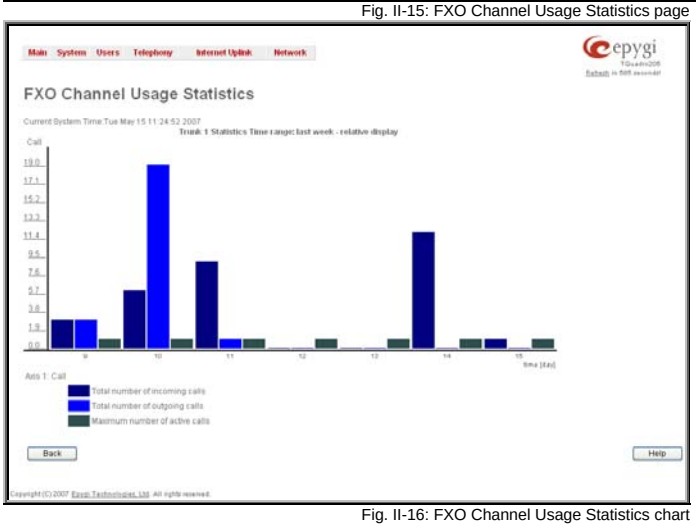


Fig. II-16: FXO Channel Usage Statistics chart

Show button is used to generate an FXO channels usage diagram chart over the parameters selected above.

When this button is pressed, **FXO Channel Usage Statistics** chart appears. It represents dependency between the time frame and the number of calls performed during that period. Additionally it may display the maximum number of calls performed in the selected time frame.

Memory Status

The **Memory Status** page includes tables with the available **User Space** information for each extension. These tables display the space used by the voice mailbox and uploaded/recorded system greetings. It shows the free and total space (counted in minutes/seconds) for every extension. This page includes the following information:

Memory Size shows total memory space (counted in minutes/seconds) available on the Quadro and assigned to all extensions.

The table's links lead the administrator to the extension settings page where **User Space** may be altered.

Call Statistics shows the current number of calls with recorded statistic entries.

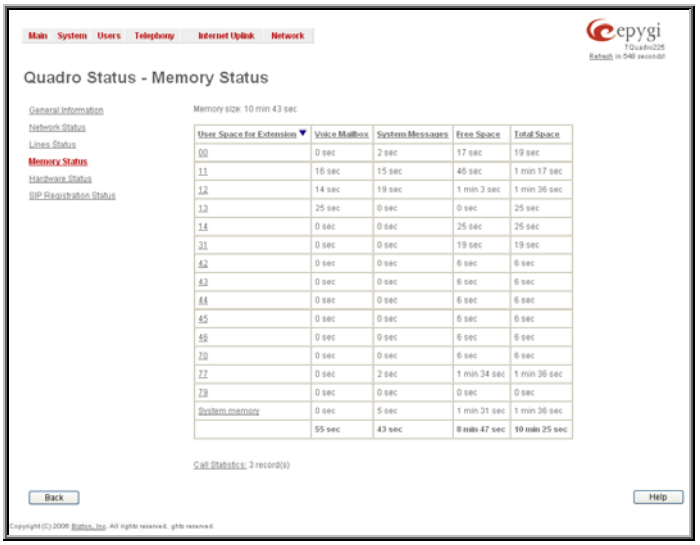


Fig. II-17: Memory Status page

Hardware Status

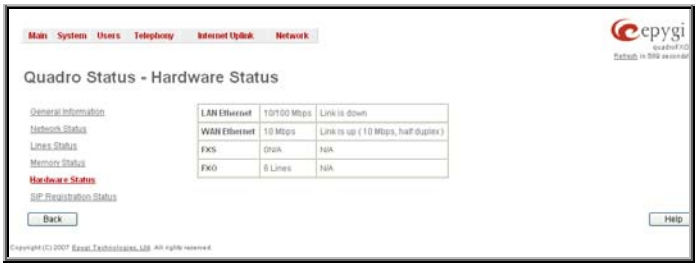


Fig. II-18: Hardware Status page

The **Hardware Status** table displays a list of the hardware devices present and currently available on the Quadro board. The hardware device version number and additional comments about its state are indicated here.

SIP Registration Status

The **SIP Registration Status** is a table displaying the SIP registration information of the Quadro extensions.

The table contains a list of all the registered extensions of Quadro, SIP registration name for each extension, addresses of SIP servers where they are registered (if applicable), whether or not it is registered for each extension, and the registration date and time. By clicking on the row heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The links inside the table will link you to the Extensions Management – Edit Entry page where the SIP registration settings may be altered.

The **Detected Connection Type** field displays the connection type Quadro currently is acting in (direct connection or behind NAT). If Quadro is acting behind NAT, the NAT machine IP address is also displayed.

The **SIP Tunnels to Slave Devices** and **SIP Tunnels to Master Devices** tables list the SIP tunnels between local and the remote Quadros (see SIP Tunnel Settings). The **SIP Tunnels to Slave Devices** table lists those tunnels where local Quadro acts as a master. The **SIP Tunnels to Master Devices** table lists those tunnels where local Quadro acts as a slave.

Fig. II-19: SIP Registration Status page

IP Routing Configuration

Routing is used to relay information across the Internet from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing is different than bridging. The main difference between bridging and routing is that bridging operates at the OSI Data Link Layer (Level Two Media Access Control Layer) and routing operates at OSI Network Layer (Level Three).

Quadro's **IP Routing** service allows you to route IP packets from one destination to another (or to a specified router) through Quadro.

The **IP Routing Configuration** page is used to make IP Static and IP Policy routes for IP packets routing. This page consists of two tables. Entries in the tables are color coded according to the state of the route. For example, yellow indicates disabled routes, green indicates successful routes and red indicates routes with an error.

IP Static Routes are used to forward IP packets from the Network, where the Quadro is connected, to the specified destination.

The **IP Static Routes** table displays all established IP static routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Route To** for the subnet where the incoming packets should be routed to and **Via IP Address** for the router IP address where incoming packets should be routed through.

Add opens the **Add IP Static Route** page where a new static route can be established.

Enable/Disable is used to activate and deactivate a selected route(s). At least one route should be selected in order to use these functions, otherwise the following error message will appear: "No record(s) selected."

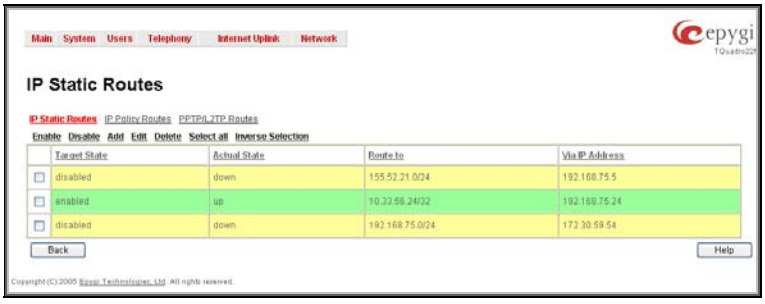


Fig. II-20: IP Static Routing table

The **Add IP Static Route** page offers the following components:

Route To requires the IP address and subnet mask for the destination the IP packet should be forwarded to.

Via IP Address requires the IP address of the subsequent router for IP packet forwarding to the specified destination.

Attention: The rule with the longest subnet (smallest IP range) will take effect when having two or more IP Static routing rules with the coinciding subnets.

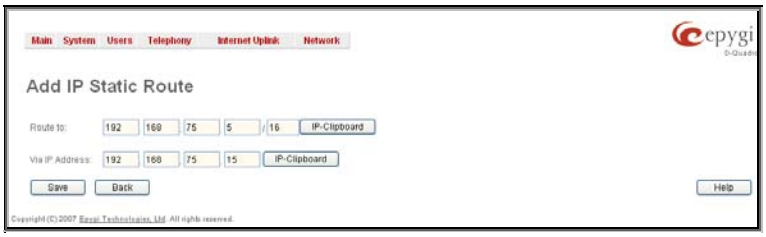


Fig. II-21: Add IP Static Routing page

IP Policy Routes allow IP packets forwarding to the specified router depending on the source IP address as well as defining the priority for the current routing rule.

The **IP Policy Routes** table displays all specified IP policy routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Priority** for the route priority, **Route From** is where the subnet, routed packets come from and **Via IP Address** is where the router IP address incoming packets should be routed through.

Add opens the **Add IP Policy Route** page to establish a new policy route.

Enable and **Disable** are used to activate or to deactivate the selected route(s).

Raise Priority and **Lower Priority** are used to increase or decrease the priority of the selected policy route(s) by one. At least one route should be selected to use these functions, otherwise the error message "No record(s) selected" will appear.

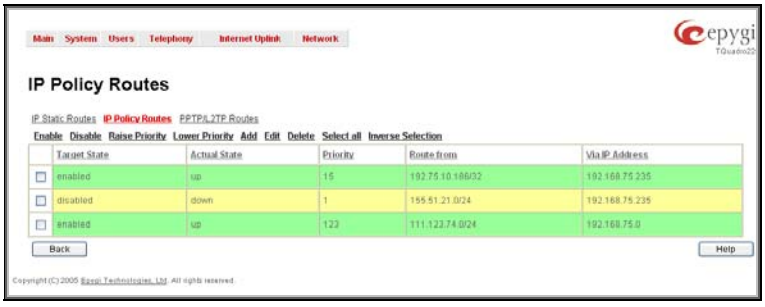


Fig. II-22: IP Policy Routing table

The **Add IP Policy Route** page offers the following input options:

Priority requires a numeric value (from 1 to 252) to define the priority of the routing rule. The lower the number, the sooner the routing rule will take effect (higher priority).

From requires the packet source IP address and subnet mask of the specified destination to match with the rule.

Via IP address requires the IP address of the subsequent router for IP packet forwarding.

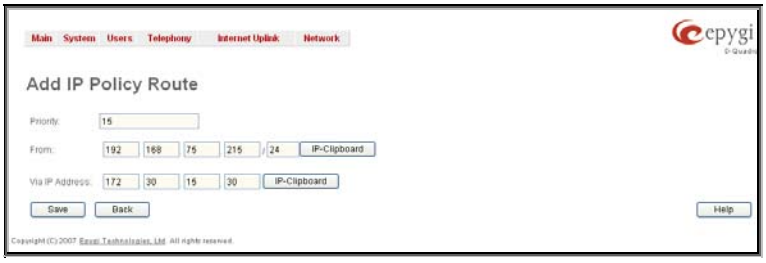


Fig. II-23: Add IP Policy Route page

The **PPTP/L2TP Routes** allow IP packets forwarding through the PPTP and L2TP tunnels of the Quadro. If PPTP/L2TP connections do not exist on Quadro, VPN routes cannot be generated.

The **PPTP/L2TP Routes** table displays all generated VPN routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Route To** for the subnet where the incoming packets should be routed, **Via Tunnel** for the VPN tunnel incoming packets should be routed through and **Tunnel State** for the actual state of the route tunnel (up or down).

The **Add** button opens the **Add VPN Route** page where a new VPN route can be generated.

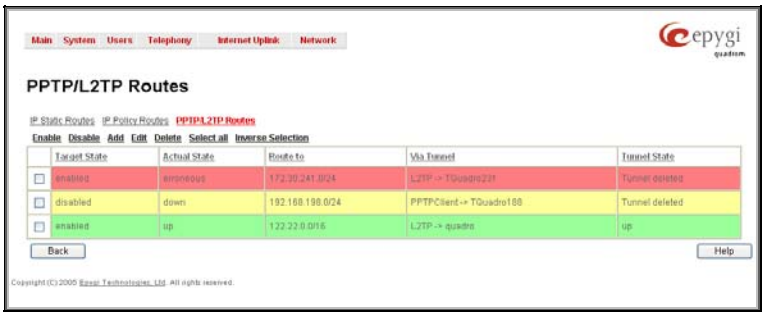


Fig. II-24: VPN Routing table

The **Add VPN Route** page offers the following components:

Route Via contains the available PPTP and L2TP connections on the Quadro. A connection selected from this list will be used to route the IP packet from the Quadro's LAN to the peer behind the PPTP/L2TP tunnel.

Route To requires the IP address range of the possible peers behind the PPTP/L2TP tunnel whereto the IP packets should be routed.

Fig. II-25: Add VPN Route page

The **Enable** and **Disable** functional buttons are used to activate or to deactivate the selected route(s). At least one route should be selected to use these functions, otherwise the error message "No record(s) selected" will appear.

To Add an IP Static Route

1. Select the **IP Static Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Static Routes** page. The **Add Entry** page will appear in the browser window.
3. Enter the destination IP address and subnet mask in the **Route To** text fields. Use the **IP-Clip** button to select a previously entered IP address.
4. Enter the router IP address into the **Via IP Address** text fields.
5. Press the **Save** button to make the static route with these settings.

To Add an IP Policy Route

1. Select the **IP Policy Route**s link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Policy Routes** page. The **Add Entry** page will appear in the browser window.
3. Specify the policy routing rule priority in the **Priority** text field.
4. Enter the packet source IP address and subnet mask in the **From** text fields. Use the **IP-Clip** button to select a previously entered IP address.
5. Enter the router IP address into the **Via IP Address To** text fields.
6. Press the **Save** button to make the policy route with these settings.

To Add a VPN Route

1. Select the **VPN Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **VPN Routes** page. The **Add Entry** page will appear in the browser window.
3. Choose the VPN connection from the **Route Via** drop down list.
4. Enter the destination IP address and the subnet mask into the **Route To** text fields.
5. Press the **Save** button to make the VPN route with these settings.

Configuration Management

The **Configuration Management** page assists the administrator with managing the system configuration settings and voice data. For example, the administrator is able to backup and download the settings to a PC and then upload and restore them back to the Quadro. Additionally, this page provides the possibility of restoring the factory default configuration settings.

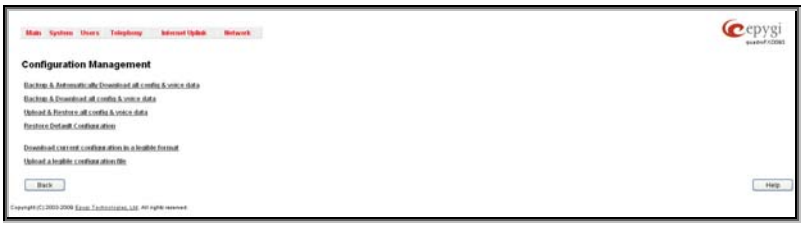


Fig. II-26: Configuration Management page

The **Backup & Automatically Download all config & voice data** link leads to the **Automatically Backup Configuration Settings** page where the automatic backup of the system configuration and the voice data can be configured. The service allows you to setup Quadro so it will automatically backup the system configuration and the voice data and store it in the specified location.

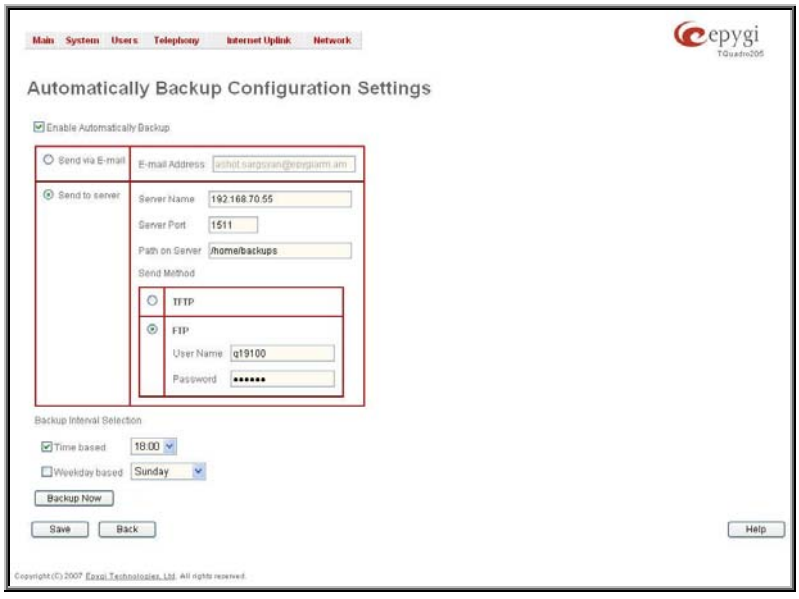


Fig. II-27: Configuration Management page

The **Automatically Backup Configuration** Settings page allows you to enable the automatic backup of the system configuration and the voice data on the Quadro. With this service, Quadro will automatically backup the system configuration and the voice data and store it in the specified location.

This page contains the following components:

The **Enable Automatically Backup** checkbox enables automatic backup mechanism on the Quadro.

The following group of manipulation radio buttons allows you to select whether the backup files will be delivered by email or stored in some location:

- The **Send via Email** radio button is used to send the automatically backed up files via email. The selection enables **Email Address** text field that requires the email address of the administrating person to receive the automatically backup files.
- The **Send to Server** radio button is used to store the automatically backup files on a remote server. This selection enables the following fields to be inserted:

  The **Server Name** requires the IP address or the host name of the remote server.

  The **Server Port** requires the port number of the remote server.

  The **Path on Server** requires the path on the server to store the backup files in.

The **Send Method** manipulation radio buttons allow you to select the remote server type: TFTP or FTP. In case of FTP selection, the authentication username and the password need to be inserted. In case these fields are left empty, anonymous authentication will be used.

The **Backup Interval Selection** checkboxes are used to select the time interval automatically backup the Quardo's configuration and the voice data. The **Time** based checkbox is used to select the hour when the configuration and the voice data will be automatically backed up on the daily basis. The **Weekday** checkbox is used to select the weekday when the configuration and the voice data will be automatically backed up on the weekly basis. At least one of these checkboxes needs to be selected.

Backup Now button is used to perform a manually immediate backup of the system configuration and the voice data.

The **Backup & Download all config & voice data** link generates a backup file with all configuration settings and user uploaded greeting messages. It opens a file chooser window for immediate download to the users PC.

The **Upload & Restore all config & voice data** link opens a page that has a **Browse** button, (which opens a file chooser to select a backed-up file) and a **Configuration to Upload** field requiring the file path to upload and to restore it immediately. Pressing **Save** will restore the selected backup file, and delete all current user defined greetings and replace configuration settings.

The **Restore Default Configuration** functional button resets all configuration settings and restores the board's factory default configuration. By restoring the default configuration you will replace your current configuration, lose all voice mails and reboot the device. You will not be automatically redirected to the GUI start page. After the successful reboot you will need to enter into the management page and login again to access the Quadro's configuration. A warning message will ask you to confirm your selection before restoring the default configuration.

Please Note: Unlike the factory default settings restore procedure initialized from the Reset button on the Quadro board, this link will keep the following data:

- Call Statistics
- Transfer Statistics
- System Events
- Feature Keys
- Device Registration state

The **Download current configuration in a legible format** and **Upload a legible configuration file** links leads you to the Legible Configuration Management page where the legible configuration can be downloaded and uploaded back after the required edits.

Legible Configuration Management

The **Legible Configuration Management** is used to manually manage the configuration on the Quadro. This will allow you to download a piece of configuration from the Quadro in the way of legible file, to make necessary changes in that file and to upload it back to the same or different Quadro(s). With this service, some pieces of configuration (like extension settings, NAT settings, etc.) of one Quadro can be used on another Quadro. This also helps to apply the same group of settings to the several instances (for example, to apply the same SIP settings to multiple extensions on the Quadro) on the same or different Quadros avoiding manual configuration of each of those instances (i.e. extension) from the web management on each of the Quadros. The Quadro reseller, distributor, ISP or carrier usually uses this service.

The **Download current configuration in a legible format** link refers to the **Configuration Summary** page where a partial or complete configuration can be defined and downloaded or viewed.

The **Configuration Summary** page is used to generate a piece of legible configuration and to download it to a PC or to view it directly in the browser. This page consists of the following components:

The manipulation radio buttons are used to select between particular CGI or a named group of CGIs for which the legible configuration file will be generated.

- The **Specific CGI** selection allows you to choose a certain CGI from the list of Quadro's Web management pages for which the legible configuration can be manually managed. For example, selecting "RTP Settings" will generate a legible configuration file with parameters present on the RTP Settings page.
- The **Named Group of CGIs** selection allows you to choose among the four predefined groups: Internet Connection Settings, LAN Configuration Settings, Telephony General Settings and Extension Settings. Each of these groups refer to all CGIs characterized by the selected criteria, e.g. Internet Connection Settings group contains all parameters on the CGIs related to the networking and WAN configuration.

The **Extension** drop down list allows you to limit the settings in the generated legible configuration file to one specific extension. For example, each of the extensions on the Quadro have own SIP settings or Codecs. To download the settings for a particular extension only, you need to choose the corresponding extension from the list. The drop down may also have a blank selection. In that case the legible configuration file will contain the parameter of all available extensions on the Quadro (if the selected parameter applies to the extension and not to the overall system, like RTP settings).

The **Start generate a legible configuration file** button start parsing the configuration structure of the device for the defined parameters. The progress will be displayed in the area below.

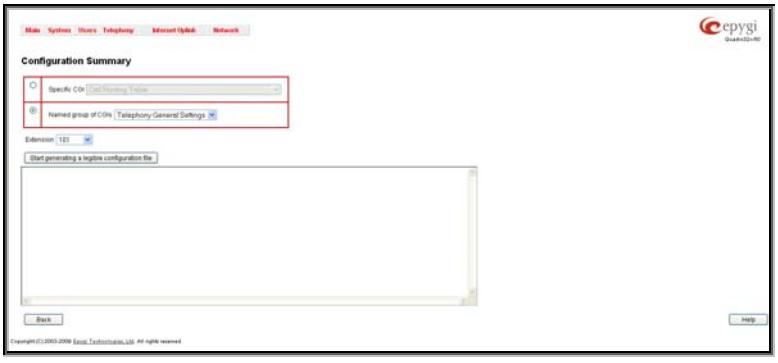


Fig. II-28: Configuration Summary – Parameters page

The **Cancel generation process** button appears when the configuration generation procedure starts and it is used to stop it.

The **Download generated configuration** button becomes available when the legible configuration generation is finished. It is used to download the generated file to the PC in a plain text format. Necessary changes can be made in the downloaded configuration file and then uploaded back to the system. **Attention:** Make sure the changes you have done in the downloaded legible configuration file are valid and will not corrupt the system when being uploaded back to device.

The **View generated configuration** button becomes available when the legible configuration generation is finished. It is used to view the generated file directly in the browser.

The **Restart generation!** button becomes available when the legible configuration generation is finished. It is used to cancel the generated configuration file and to start over.

Fig. II-29: Configuration Summary Preview page

The **Upload Legible Configuration** page is used to upload a configuration file in a text format. The **Browse** button in the opened page is used to browse certain legible configuration file to be uploaded and updated into the system. The configuration files to be uploaded should be in the *.txt format, otherwise a system error occurs. Configuration file upload progress will be displayed in the area below.

Attention: Uploading the legible configuration file will not work if the QuadroFXO is running in the slave mode, i.e. if it is sharing its FXO lines to some Quadro IP PBX (see settings on the PSTN Lines Sharing page).

Events

The **Events** page has two tables. All system events that have occurred will be displayed in one table and event settings will be displayed in the other.

The **System Events** page may be accessed through the **Events** link from the main menu. It lists information about system events that have occurred on Quadro. When a new event takes place, a record is added to the System Event table. For failure events (priority 2 and 3, see below), the warning “Please check your pending events!” will appear at the bottom of all management pages.

The system events and the warning message are visible only for the administrator. The warning link, (which leads directly to the **System Events** page) will disappear from the management pages if the administrator has marked all new events as “read”.

Fig. II-30: Event Warning on the Main Menu page

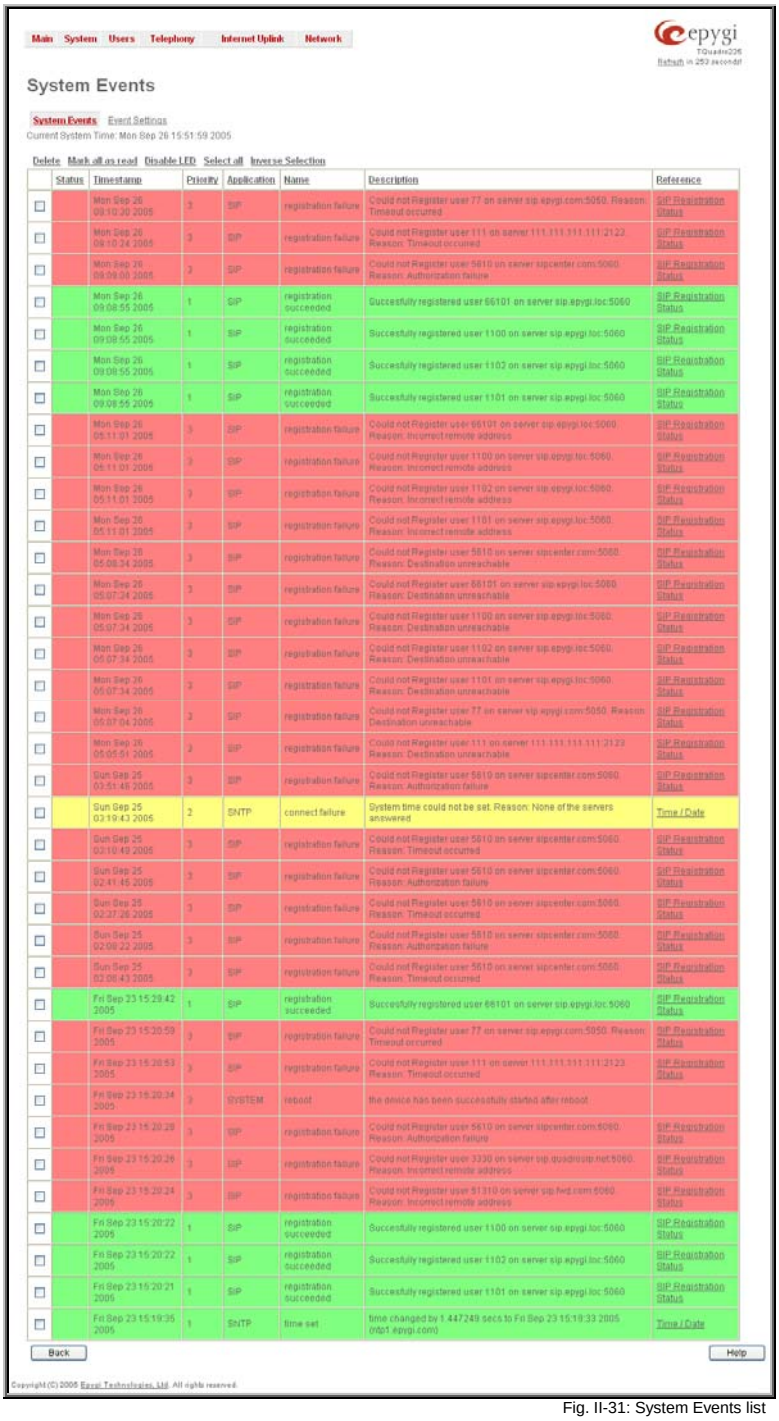


Fig. II-31: System Events list

The **System Events** table is the list of new and read system events. System events have corresponding coloring depending on the nature of the event: success (priority 1, color green), low importance failure (priority 2, color yellow), critical failure (priority 3, color red).

The table shows the **Status** of the event (new or read) as well as the name of the application the event refers to, event description, and the date when the event was received. For example, if the event was caused due to incorrect mail sending or SIP registration, corresponding links will be seen in the Reference column of the table. The administrator can view the detailed log for each event that has occurred.

The **System Events** page offers the following components:

Current System Time displays the local date and time on Quadro.

Mark all as read marks newly occurred events as "read".

Disable LED switches off the flashing LED (if applicable) on the board. An LED notification may appear (depending on the notification type given) in the page Events page when a new event occurs.

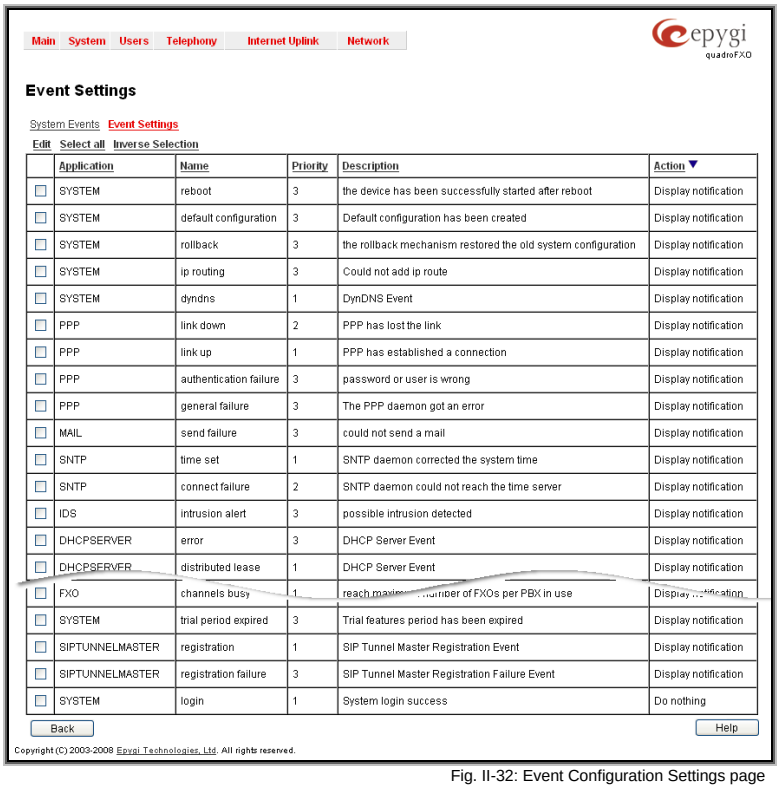


Fig. II-32: Event Configuration Settings page

Numerous circumstances may cause a certain application on Quadro to flag an event.

The **Event Settings** page lists all possible events on the Quadro and allows controlling notification (action) when an event takes place.

Each entry in the events' table has a checkbox assigned to each row. By selecting the corresponding checkboxes, operations such as **Edit** may be done for one or more events.

Edit opens the **Edit Event Settings** page to modify the event action.

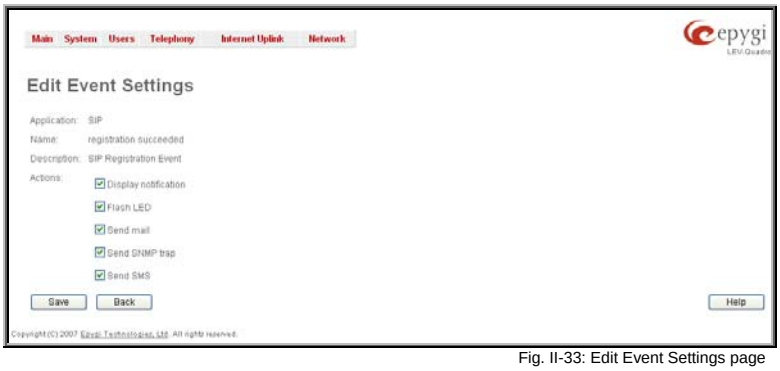


Fig. II-33: Edit Event Settings page

The **Edit Event Settings** page offers the following input options:

Application displays the application the event refers to. **Multiple** is shown here if more than one event has been selected for the action assignment.

Name displays the name of the event. **Multiple** is shown here if more than one event has been selected for the action assignment.

Description displays additional information about the event. **Multiple** is shown here if more than one event has been selected for the action assignment.

Action offers radio buttons to choose one of the actions to notify the Quadro administrator when an event(s) takes place. The following actions can be available:

- **Display Notification** - A notification link will be displayed on the bottom of all pages and a record is added into the Events table. The notification is executed as a link "Please Check you pending events!". The link leads to the System Events page. This action also will take place if Flash LED or Send Mail has been selected, even if not specifically selected.
- **Flash LED** - The second LED (yellow) will blink every second and a notification will be displayed on the bottom of all pages. For some events the LED will start flashing after a delay.
- **Send Mail** – an e-mail notification about the new event on the Quadro will be sent to the e-mail address specified in the Mail Settings page.
- **Send SNMP Trap** – an SNMP notification will be sent to the traphost(s) listed in the SNMP Trap Settings table (see SNMP Settings).
- **Send SMS** – an SMS notification about the new event on the Quadro will be sent to the mobile phone specified in the SMS Settings page.

Actions that are not allowed for the selected event (like mail notification if the PPP link is down or the mail server has been configured improperly) are hidden. For multiple events editing, actions that are not appropriate for least one of the selected events will also be hidden.

Please Note: In case of an IDS (Intrusion Detection System) intrusion alert, only the first possible intrusion in each 10 minute period will initiate an event. This helps to avoid flooding the System Events table, and flooding the user with various intrusion alerts that result from each possible Denial of Service attack. When these events are displayed in the System Events table, the user can receive detailed information about the intrusions through a link to the IDS log list.

If Quadro cannot receive an IP address from the DHCP or PPP servers, or cannot register an extension on the SIP or Routing servers, or cannot reach an NTP server, it raises only one event for the entire period the action has failed, but will continue to try. When the required action is successful Quadro raises an appropriate message.

To Assign an Action to the Event

1. Select the checkbox of one or more events to assign an action to them.
2. Press the **Edit** button. The **Edit Event Settings** page appears.
3. Select an action type from the **Action** radio buttons to notify the administrator about the event.
4. Press the **Save** button to submit the changes or use **Back** to abort the selected action.

Time / Date Settings

The **Time and Date Settings** page provides information about the current system time and date. The settings may be updated through the international time and date servers.

Time is used to set the local time (hour, minute).

Date is used to set the date (month, day, year).

Timezone provides a selection of world time zones and is used to select the local country time zone.

Enable Simple Network Time Protocol Server enables the SNTP (Simple Network Time Protocol) server on Quadro, thus Quadro becomes the timeserver for its LAN.

Enable Simple Network Time Protocol Client enables the SNTP client on the Quadro, thus Quadro becomes a client to an external timeserver. A checkbox disables Date and Time drop down lists and enables the following parameters:

The **SNTP Servers** table lists all defined NTP Servers.

The **Add** functional button opens an **Add NTP Server** page where a new NTP server can be defined. This page offers the **NTP Server** radio buttons that are used to choose between a manual and a predefined NTP server.

> **Manual** requires the NTP server's FQDN (Full Qualified Domain Name) or its IP address.
>
> **Predefined** is used to select the NTP server's host address from the drop down list, where the most common NTP servers are listed.

The **Move Up** and **Move Down** functional buttons are used to sort NTP servers in the order they need to be accessed. If the NTP server in the first position of the **SNTP Servers** table does not answer, NTP server in the next position will try to be reached.

Please Note: You can add another NTP server to the list if the defined NTP servers are not functional (for example, Quadro's date/time is not being updated automatically).

Polling Interval indicates the time interval for the periodical synchronization between the timeserver and Quadro. It counts in hours.

Attention: Time and Date Settings will be reset if Quadro has lost power.

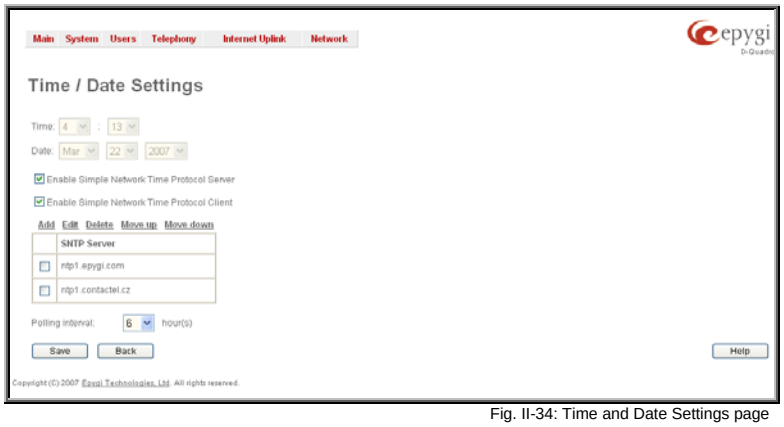


Fig. II-34: Time and Date Settings page

Fig. II-35: Add NTP Server page

Mail Settings

The **System Mail Settings** page allows you to send warnings automatically about the board status or problems to the administrator. System events that require email notification are selected on the Events page. System mail must be enabled and the SMTP server needs to be configured for voice message transmission to the extension user's mailing account.

Enable enables system mail sending and voice messages transmission to the extension user's mailbox.

SMTP Host requires the SMTP host IP address or domain name. The SMTP host needs to be configured to enable voice message transmission.

SMTP Port requires the SMTP host port number.

Mail Sender Address text field requires the source address for the Quadro notification emails. The email address defined here should be an existing valid e-mail address registered on the selected SMTP server or it should have permission to use that particular SMTP server for e-mail transmission.

Mail Recipient Address text field requires an active e-mail address where system emails will be delivered. The e-mail recipient here can be a Quadro administrator or someone responsible for network and system problems.

Mail Recipient Address (CC) text field requires an active email address where a carbon copy (CC) of the system emails will be delivered.

Enable SMTP Authentication must be selected if the specified SMTP server requires authentication. In this case, authentication **User Name** and **Password** configured on the SMTP server should be defined in the corresponding text fields.

Attention: The following symbols are not allowed for the **Password** field: '$', '(', ')','/', `', '&', '\', "'.

Send Test Mail is used to initiate a test e-mail transmission. This button will be enabled if correct values have been submitted and saved on this page.

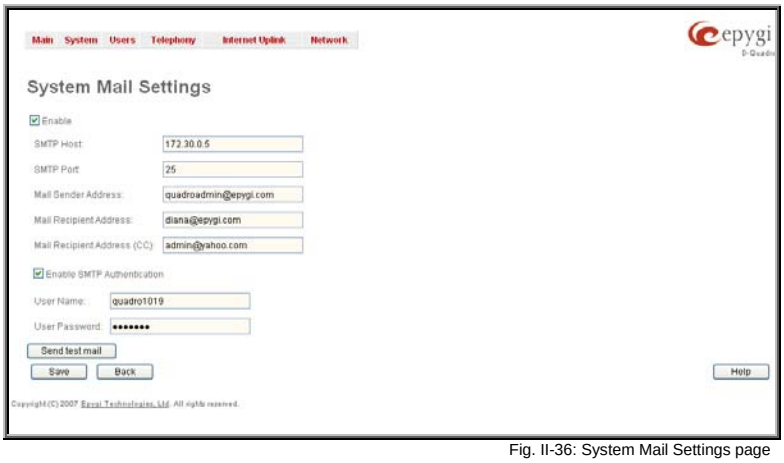


Fig. II-36: System Mail Settings page

To configure the System Mail

1. Enable the system mail sending by the **Enable** checkbox selection.
2. Update or set the SMTP host in the **SMTP Host** text field.
3. Update or set the e-mail sender address in the **Mail Sender Address** text field.
4. Update or set the e-mail address in the **Mail Recipient Address** text field.
5. Enable **SMTP Authentication** if it is required on the server.
6. Insert into the corresponding text fields an authentication **User Name** and **User Password** defined by your SMTP server.
7. Press the **Save** button to submit these settings.
8. Use the **Send Test Mail** button to send a test e-mail with the configured settings.

SMS Settings

The **SMS Settings** are used to configure the SMS parameters that will allow Quadro to send the voice mail notifications or event notifications via SMS to the extension user's mobile phone. Every extension user can enable voice mail notifications when a new voice mail is received and they can to define their own mobile numbers from the Voice Mail Settings or to set the certain Events notification to be delivered per SMS. However, for Quadro to deliver SMS notifications, the SMS service should be enabled and SMS settings should be configured from this page.

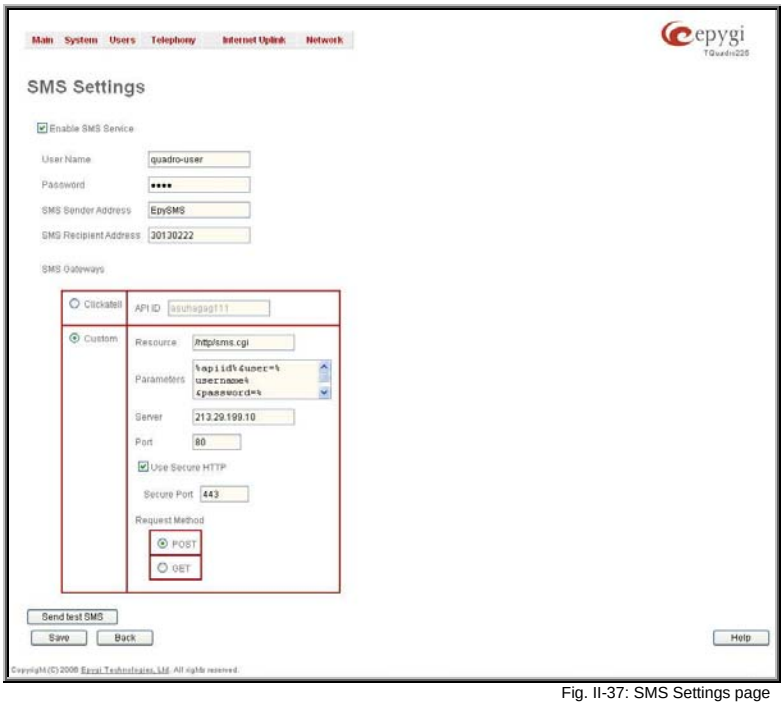


Fig. II-37: SMS Settings page

Enable SMS Service enables the SMS service on the Quadro.

User Name and **Password** text fields require the authentication settings of the SMS server.

SMS Sender Address requires the source address for the Quadro notification SMS. The address defined in this field will be seen in the "From" field of the SMS delivered to the mobile phone.

SMS Recipient Address requires a destination mobile number for a test SMS.

SMS Gateway manipulation radio buttons allow to selected between pre-defined Clickatell SMS gateway and the custom defined SMS gateways.

- **Clickatell** – this selection allows to use a pre-defined SMS gateway. Selection enables the **API ID** text field which indicates a Clicatell specific parameter obtained from the server and should match on both sides.

- **Custom** – this selection allows to use a custom SMS gateway. Selection requires following parameters to be inserted:
  - **Resource** text field requires the HTTP resource name on the SMS gateway, for example: /http/sms.cgi.
  - **Parameters** text field requires the parameters to be submitted to the resource address. The value of this field represents a string with tokens (separated by percent (%) symbols) inside. Each token indicates a value of the certain field on this page. The value is dependent on the SMS gateway requirements. For example:

    user=%username%&password=%password%&to=%to%&from=%from%&text=%text%

    The tokens are the strings that have the following dependencies from the field in this page:

    %username% – indicates the username defined in the field **Username**
    %password% – indicates the password defined in the field **Password**
    %to% - indicates the password defined in the field **SMS Recipient Address**
    %from% - indicates the password defined in the field **SMS Sender Address**
    %text% - indicates the SMS text generated by Quadro (voice mail notification, event notification, etc.)

  - **Server** text field requires the IP address or the host name of the SMS gateway.
  - **Port** text field requires the port number of the SMS gateway.
  - **Use Secure HTTP** checkbox enables access to SMS server via HTTPS. Checkbox selection enables a Secure Port text field that requires the port number for HTTPS traffic.
  - **Request Method** manipulation radio buttons allow to select the HTTP request method used by Quadro the access the SMS gateway: POST or GET.

Send Test SMS is used to send a test SMS to the defined SMS Recipient Address. This button will be enabled if correct values have been submitted and saved on this page.

Firmware Update

This window allows updating the software of Quadro by installing new firmware (image). Users registered at Epygi will receive a notice when new firmware is available and will be able to download it from the Epygi Technical Support WEB page.

Updating new firmware requires a working power supply. Quadro is provided with a battery (accumulator). If the battery is low or simply absent the "There is no battery or voltage is low" warning is displayed.

The Automatic Firmware Update link leads you to the page where the automatic update of the Quadro's firmware (software image) can be configured.

Please Note: Installing new firmware will take about 15 minutes. During this time, QuadroFXO, telephony and Internet access will be disabled.
The firmware update will cause the loss of the following data:

- All voice mails

Please Note: If you do not wish to lose your voice data, have it downloaded from Configuration Management page prior to starting the Firmware Update.

- DHCP leases
- Transfer statistics
- Call statistics

Please Note: If you consider the Call Statistics entries in the displayed tables to be important, it is recommended to download them from the corresponding page prior to starting the Firmware Update.

- All pending events
- User specific GUI states

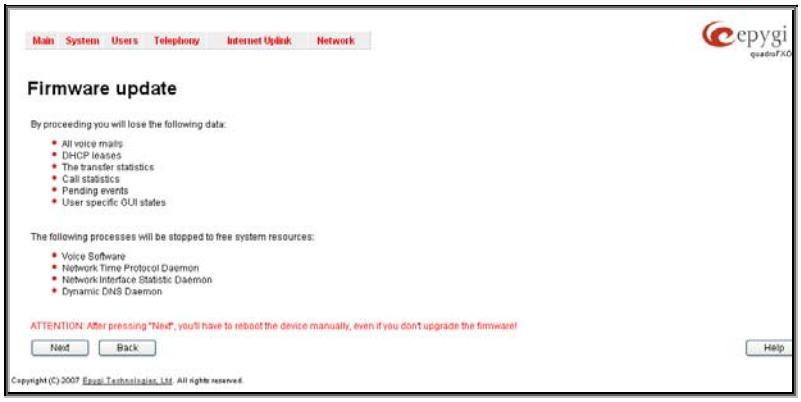


Fig. II-38: Firmware Update page 1

The following main processes will be stopped during the firmware update and will be restarted after the installation is completed:

- Voice Software
- Network Time Protocol Daemon
- Network Interface Statistic Daemon
- Dynamic DNS Daemon

Next will move you to the second page of Firmware Update where the image file should be selected.

Attention: Pressing the **Next** button will stop some vital processes on the Quadro, therefore you will need to reboot your device manually even if you have cancelled the firmware update procedure on the following steps.

The second page of **Firmware update** has a **Browse** button used to browse the image file, and the **Specify Image** text field that will display the selected image filename.

Pressing **Save** will start uploading the image file to the board and the next page will display results and verification of the image being burned.

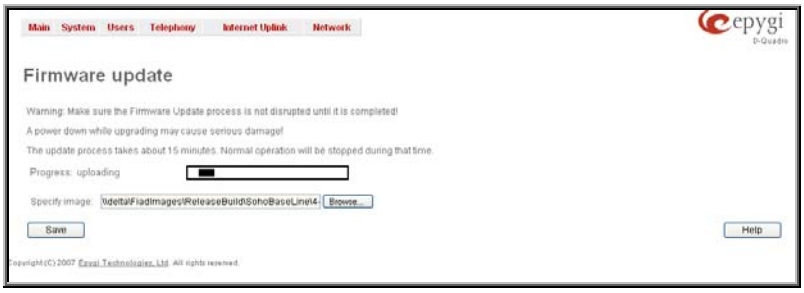


Fig. II-39: Firmware Update page 2

This page displays non-editable information about the image validity. The **Image Check** field will display "invalid" if the image does not correspond to the hardware version.

The **Current Software Version** field shows the old software version. The **New Software Version** field shows the new version of the software image.

This page needs to be confirmed in order to continue image updating. If you are sure that the image version is appropriate for your device press **Save**.

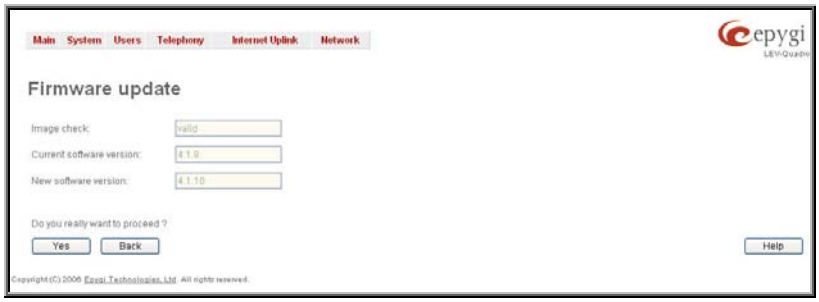


Fig. II-40: Firmware Check page

If you have confirmed the firmware version, a new page with firmware update progress will be displayed next. There are no functions available on this page, just information about the firmware update procedure. At some point the connection with the device is being lost and you need to wait until the firmware will be burned on the Quadro.

You will not be automatically redirected to the Login page. To access the Quadro's Web GUI, you need to connect Quadro again and login.

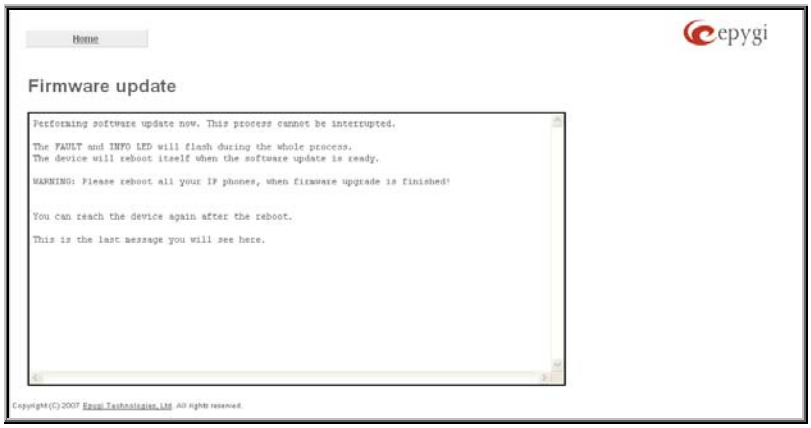


Fig. II-41: Firmware Update page

Automatic Firmware Update

The **Automatic Firmware Update** page allows you to configure an automatic update of the Quadro's firmware (software image) as it becomes available on the server. When this service is enabled, on the configured day and time Quadro will automatically check for a new available firmware on the server and will either notify the administrator or update the firmware right away, depending on the configured settings.

The server configuration can be done manually or through the DHCP server. In case of DHCP server replying configuration, the corresponding adjustments should be done on the DHCP server to automatically point the Quadro to the destination where the firmware is stored.

Please Note: Independent on the selected server type, there should be an "**auto-update**" folder in the root directory of the server. Quadro will check for any new firmware in that specific folder only. Besides the firmware *.bin file, the "**auto-update**" folder should contain supplementary file(s) to point to the correct firmware file.

The detailed instructions on the functionality of automatic firmware update as well as server configuration are described in the "**Automatic Firmware Update"** document which you can find at the Epygi Web support portal.

This page consists of the following components:

The **Enable Automatically Firmware Update** checkbox selection enables the automatic firmware update service on the Quadro.

Attention: When the older firmware is installed on the Quadro, the system configuration will be lost and the device will be factory reset.

The first manipulation buttons group on this page allows you to choose between the manually configured firmware server and the server defined by the DHCP server.

- **Assign manually** – this selection is used to manually configure the firmware server settings. The **Server Name** (the IP address or hostname), the **Server Port** and the **Update Method** should be defined. The **Update Method** drop down list provides a possibility to choose among TFTP, FTP, HTTP or HTTPS methods. For some of these selections, authentication **Username** and **Password** can be entered.
- **Assign automatically via DHCP** - choose this selection if the Quadro acts as a DHCP client in its WAN interface. In this case the firmware server's configuration will be automatically obtained from the DHCP server. This selection requires previous configuration on the firmware server and will work only if the "**auto-update**" directory is created on the TFTP server. The DHCP server should also be configured to provide the "TFTP server name" parameter (option 66) to the Quadro.

The second manipulation buttons group on this page allows you to select the frequency of checking for a new update.

- **Check and notify** – choose this selection if you only wish to be notified about the new available firmware on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the Quadro will check for a new firmware available on the server. The way of notification is configured from the Events page.

Check and update – choose this selection to check and automatically install the new firmware on the Quadro as it becomes available on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the Quadro will check for a new firmware available on the server, will automatically download and install it on the Quadro.

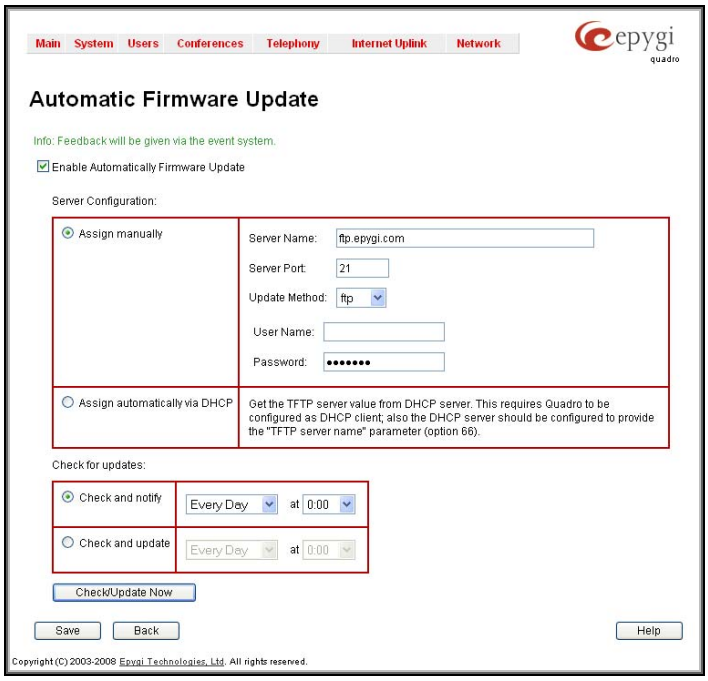


Fig. II-42: Upload Configuration page

The **Check/Update Now** button is used to manually initiate **Check and notify** or **Check and update** actions. The action to be executed depends on the radio button selected above

Networking Tools

The **Networking Tools** page provides the possibility to check the Internet connection.

Ping sends four ICMP (Internet Control Message Protocol) requests with a default size of 64 bytes to the destination (IP address or host name) specified in the text field **Ping Target**. The response times are logged, and the round trip time (the time required from being sent until being received again) is measured. The minimum and maximum round trip time and its average as well as the percentage of lost and of received frames results are displayed in the lower area of the page.

Traceroute checks the Internet connection by triggering the routers (hops) that are passed to reach the destination specified in the **Traceroute Target** text field. Trace routing gives feedback on the routers passed by packets on the way toward the destination and the round trip delay of packets to these routers.

Attention: No **Traceroute** is possible if a high priority Firewall has been enabled (see chapter Firewall and NAT).

For the purpose of tracerouting, several IP packets are sent out. UDP (User Datagram Protocol) is used to send packets and ICMP (Internet Control Message Protocol) is used to receive information about the routers. In their headers, the TTL (Time To Live) value increases from 1 to 30. When the first IP frame is received by the first router, its IP address will be returned in its acknowledgement

The second frame delivers the IP address of the second router and so on and so forth. The results of **Traceroute** are displayed on the lower area of the page.

Ping Target requires the destination (IP address or host name) for the ICMP request.

The **Ping** button starts pinging the specified ping target.

Traceroute Target is used to enter the IP address or host name of the destination to be trace routed.

The **Traceroute** button is used to process the router triggering to check the Internet connection.

In the field below these, the output of the Ping or Traceroute procedure is shown.

Fig. II-43: Networking Tools page

To Check the Internet connection

1. Specify the destination address for the ICMP request in the **Ping Target** text field.
2. Press the **Ping** button to process the ICMP request.
3. Specify the destination address to trace the route.
4. Press the **Traceroute** button to process the router triggering.

SNMP Settings

The **Simple Network Management Protocol** (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices and is used by network administrators to manage network performance, find and solve network problems, and plan for network growth.

On Quadro, SNMP agent is running to allow administrators to remotely manage Quadro's network and the device's configuration. Remote administration is being performed by means of special SNMP monitoring programs (SNMP Manager), which can automatically feedback by the certainly configured actions on some events on the Quadro or remotely modify Quadro's settings.

SNMP Settings page is divided into two pages: **Global SNMP Settings** and **SNMP Trap Settings**.

Global SNMP Settings are used to enable the SNMP agent on the Quadro, to select the SNMP protocol version for communication with the administrating application and to define the community for administrating application to connect the Quadro.

Enable SNMP checkbox is used to enable SNMP agent on the Quadro.

System Location text field requires optional information to describe the network where SNMP management is performed.

System Contact text field requires optional information about the contact person responsible for the SNMP management in the defined network. Field may indicate the point person's name, email address, phone number or other contact information.

Enable SNMP v1 / 2c checkbox is used to enable SNMP v1/2c protocol version for the messaging between Quadro's SNMP agent and the administrating application. If this checkbox is not selected, **SNMP v1** will be implied.

SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about Quadro's). Field may contain some kind of password which should be matching both on Quadro and on the administrating application for successful SNMP management.

Enable SNMP v1 / 2c Read-Write Access checkbox additionally enables a read-write access on the Quadro for the SNMP monitoring application. With this checkbox enabled, administrator will be able to remotely configure the Quadro via SNMP administrating program.

SNMP v1 / v2c Read-Write Community text field is used to insert the community description (public, private, etc.) for the read-write management (like gathering information (events, statistics, etc.) about Quadro's and remotely changing Quadro's configuration). Field may contain some kind of password which should be matching both on Quadro and on the administrating application for successful SNMP management.

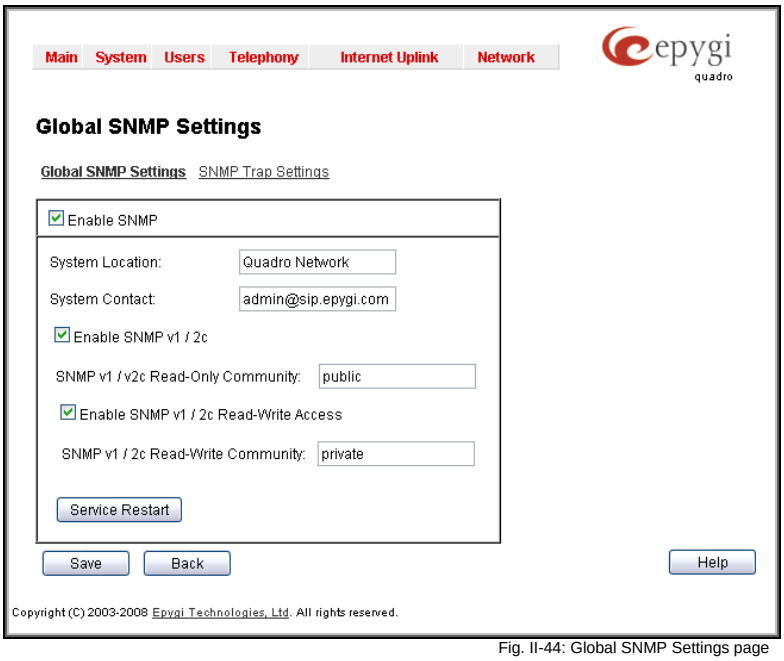


Fig. II-44: Global SNMP Settings page

The **Service Restart** button restarts the SNMP sub-system on the Quadro. Restarting the SNMP sub-system is recommended if it does not respond to a SNMP manager's requests.

SNMP Trap Settings are used to define the traphosts that should be informed when certain events occur on the Quadro. For the listed traphosts to be informed about the events on the Quadro, **Send SNMP Trap** action should be configured for the corresponding event(s) from the Events page.

SNMP Trap Settings page contains a list of all configured traphosts with the referring information.

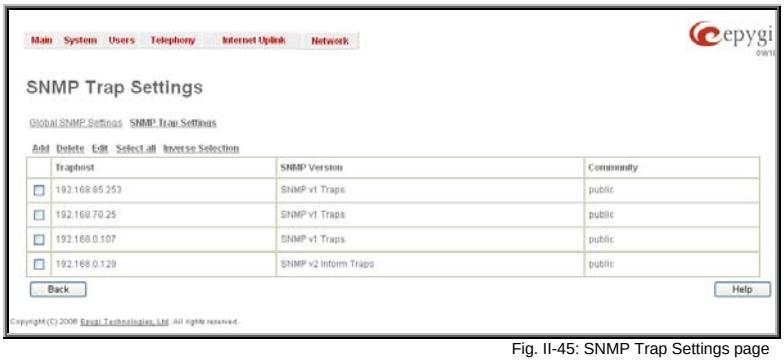


Fig. II-45: SNMP Trap Settings page

Add functional button is used to add a new traphost to the table and opens **Add SNMP Traphost** page where the new traphost might be defined. Page consists of the following components:

Traphost text field requires an IP address or the host name of the traphost. Administrating application's host address should be inserted here.

Community text field requires community description (public, private, etc.) for the administrating application to accept the notifications about the certain events on the Quadro. Field may contain some kind of password which should be the same both on Quadro and on the administrating application for successful SNMP management.

A group of radio buttons is used to select the SNMP protocol version used for events notifications delivered by the Quadro to the administrating application.

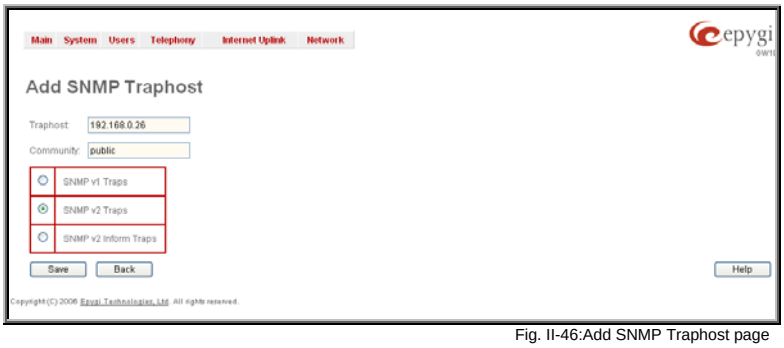


Fig. II-46:Add SNMP Traphost page

Diagnostics

The **System Diagnostic** page gives a possibility of running Network and WAN protocol diagnostics to verify Quadro's connectivity and to download all system logs for possible problems recovery.

The **Start Detecting WAN Protocol** button is used to initiate WAN diagnostics that will detect the WAN IP configurations: static or through DHCP and PPP servers. For static WAN IP configuration, gateway availability is checked. When acting as a client, DHCP and PPP servers' accessibilities are being verified.

The **Start Network Diagnostics** button is used to initiate network diagnostics, i.e., to check the WAN link and IP configuration, to verify gateway, DNS primary and secondary (if configured) servers' accessibilities.

The field below will display the diagnostics results and the connectivity conditions. The system should be reconfigured if problems occur during the diagnostics.

The **Download system logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your Quadro.

The **Reboot this Device** button is used to reboot the Quadro. Please note that the session with the Quadro will be closed, i.e., the Quadro GUI should be newly opened and a new login will be required afterwards.

The **Start FXO Diagnostics** button runs FXO diagnostic tests to determine the optimal value for the FXO country specific regional setting (CSRS) appropriate to your PSTN provider. Once the FXO diagnostic is complete, the recommended value should be set manually on the fxocfg.cgi. Setting this value may resolve echo or poor audio quality issues on FXO lines.

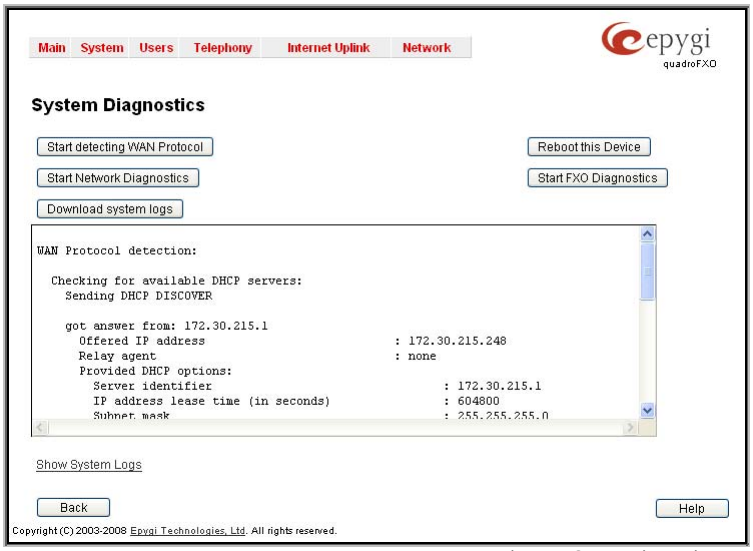


Fig. II-47: System Diagnostic page

Show Call Bandwidth Usage link leads to the **Call Bandwidth Statistics** page where a chart with call traffic bandwidth usage per day/hour basis can be built.

Show System Logs link leads to the page where Quadro's logs might be viewed, downloaded and the logging setting may be adjusted.

Call Bandwidth Statistics

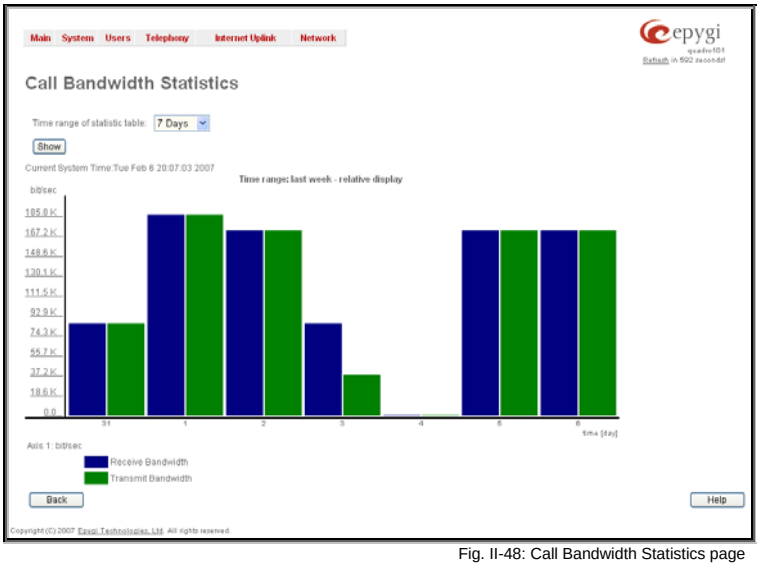


Fig. II-48: Call Bandwidth Statistics page

Call Bandwidth Statistics page allows you to see the bandwidth used at the moment of maximum incoming and outgoing call traffic for the certain time frame. It will give you an idea whether the upload and download bandwidth configured from Internet Configuration Wizard is enough or some calls will be denied in a high load periods.

Initially, this page consists of the following components:

Traffic range of statistic table drop down list is used to select the time interval (from 1 to 90 days) to display the corresponding statistics for.

Show button is used to generate a call bandwidth statistics chart. When this button is pressed, a colored chart appears on this page indicating how much bandwidth has been used at the peak of receive and transmit call traffic on the Quadro. The **K** letter used for the bandwidth indicates the thousand.

System Logs

The **System Logs** page is accessible by pressing the **Show System Logs** link on the **Diagnostics** page. This page is used to adjust where system logging settings, view system logs directly in your browser or download them locally to your PC.

The **System Logs** page consists of three sub-pages.

The **System Logs Settings** page is used to adjust the system logging settings and contains the following components.

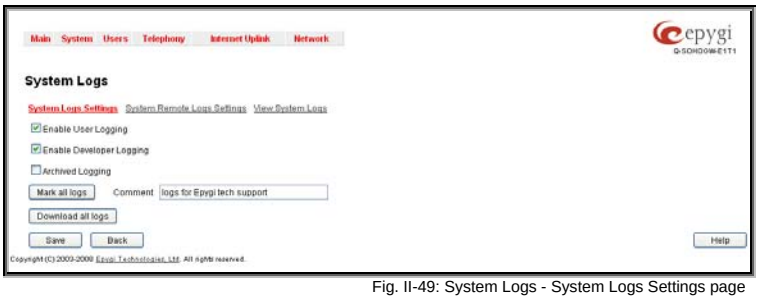


Fig. II-49: System Logs - System Logs Settings page

The **Enable User Logging** checkbox is used to enable user level logging. This logging contains brief information about events on the Quadro.

The **Enable Developer Logging** checkbox is used to enable developer high level logging. This logging contains detailed information about events on the Quadro.

The **Archived Logging** checkbox is used to keep more logs on the Quadro. This option allows to collect more system information in the log files and to keep them longer.

Attention: This option requires quite sufficient resources on the Quadro. It is recommended to use this option in urgent cases only.

The **Mark all Logs** button is used to set a line marker in the logs. If you need to follow a certain piece of log, push this button to set a starting mark in all logs and then perform the needed actions over the Quadro. When the actions are done, push this button again to set an ending mark in all logs. This way you shall clearly see a piece of log between the staring and ending marks generated during the certain actions taken over the Quadro. The **Comment** text field is used to insert some text information which will be displayed next to the marks inserted in the logs. This comment may describe the problem captured in the following logs and may be useful for the Technical Support.

The **Download all Logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your Quadro.

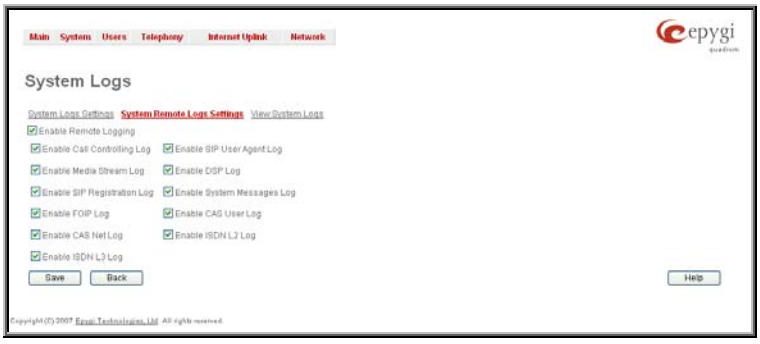


Fig. II-50: System Logs - System Remote Logs Settings page

The **System Remote Logs Settings** page is used to adjust the system logging settings and contains the following components.

The **Enable Remote Logging** checkbox is used to enable remote monitoring of Quadro's logs. When this option is selected, remote administrators may connect Quadro with Telnet protocol (port number 645) and access the logs selected on this page. This is done for remote Quadro's diagnostics and is mainly used by Epygi's Technical Support Office. To make the Quadro's logs open for remote access, appropriate Firewall level or Filtering Rules must be created.

Checkboxes below on this page are used to select those log types that should be accessible remotely. Select only those logs that you wish to have monitored remotely.

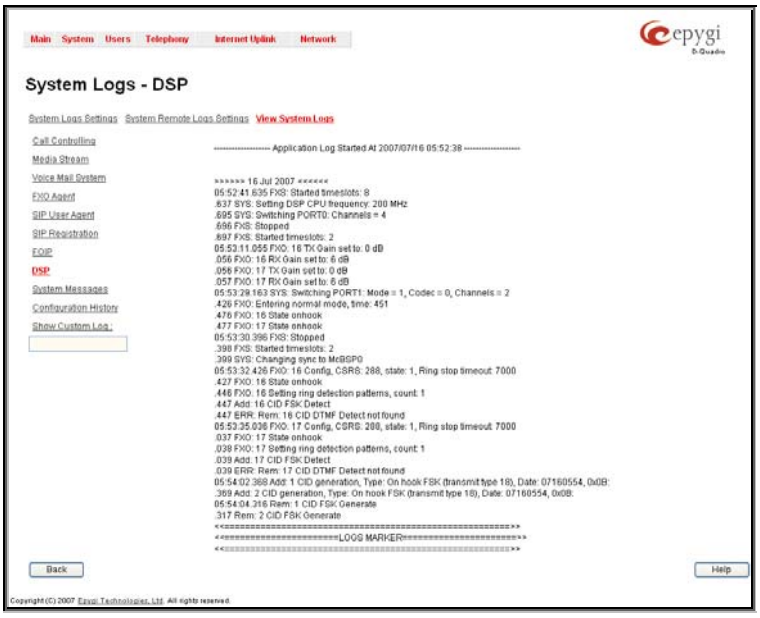


Fig. II-51: System Logs – View System Logs page

In the **View System Logs** page you may view the generated logs on the Quadro. System logs are useful to determine any king of problems on the Quadro as well as to monitor the user's access and the usage of it.

On the left side of the page, a list of main logs is displayed. Clicking on the needed link will display the log on the right side of the page.

The text field on the left side is dedicated for support personnel only and is used to search a custom log not listed on this page. To do so, insert a required log name to the text field and press **Show Custom Log** functional button.

Automatic Provisioning

Automatic Provisioning provides the possibility to automatically configure the WAN network settings of Quadro. This is very useful when the administrator is not actually aware about the Quadro's network settings. **Automatic Provisioning** automatically detects the matching network configuration settings, applies them on the Quadro, thus connecting the device to the internet through the available ISP connection.

Please Note: **Automatic Provisioning** can only be run from the LAN side of the Quadro, i.e. from the PC connected to the Quadro's LAN.

Automatic Provisioning automatically detects and configures the following settings on the Quadro:

- WAN interface type (PPPoE or Ethernet)
- WAN IP settings
- PPP settings
- ISP settings
- DHCP settings
- DNS settings
- NAT Traversal settings

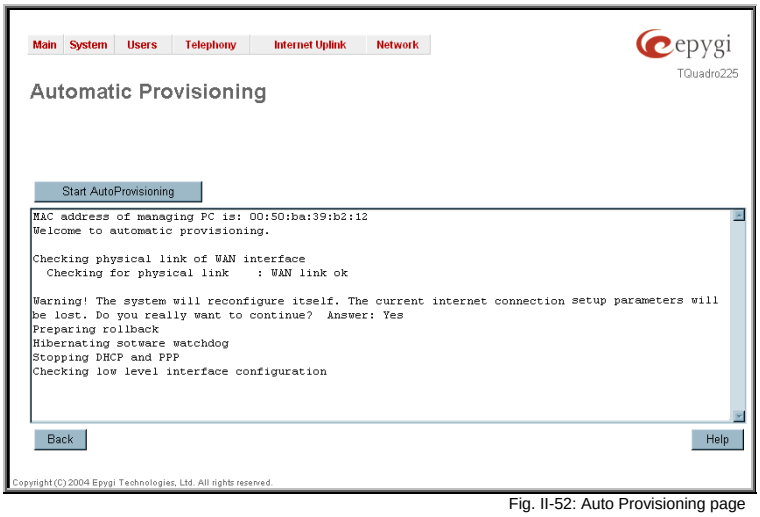


Fig. II-52: Auto Provisioning page

Upload Language Pack

Upload Language Pack page allows to upload a custom language for GUI and Voice Messages of the Quadro. The language of voice messages can be switched to the custom Language Pack language from GUI setting page at the System Configuration Wizard. The language of GUI session can be changed to the custom Language Pack language from the radio buttons on the login page.

Uploading a Language Pack will cause the loss of the following data:

- All voice mail and custom voice messages
- Call statistics
- Pending events
- Transfer statistics

Please Note: Only one custom Language Pack can be uploaded at the time. Uploading a Language Pack will remove the existing one (if existing) and will reboot the Quadro.

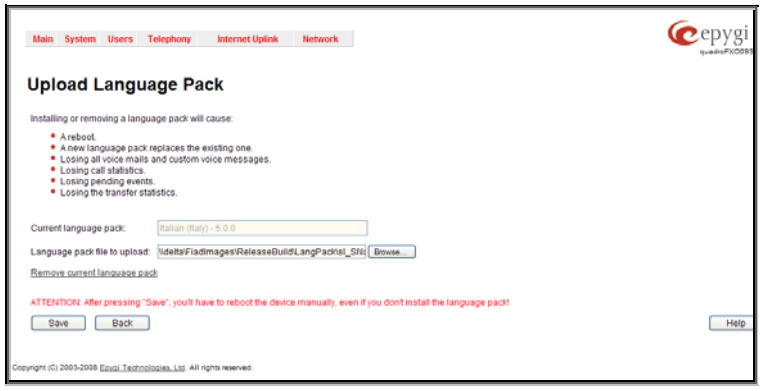


Fig. II-53: Upload Language Pack page

Current Language Pack field displays read-only information about the custom language pack uploaded. When no custom language pack is uploaded, field indicates “unknown”.

Below, there is a **Language Pack File to Upload** text field which displays the selected image filename. **Browse** button is used to browse the custom language pack to be uploaded.

Remove Current Language Pack link is seen only when custom language pack is uploaded and is used to remove it from the system.

Attention: Pressing **Save** will start uploading the custom language pack to the board. The next page will be displayed, showing the result of a verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if any).

After final confirmation, system will upload the selected custom Language Pack and will reboot.

User Rights Management

The **User Rights Management** service sets restrictions on the GUI access for various users, permits or denies the access to certain Web GUI configuration pages and creates multilevel user management of the Quadro. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the Quadro’s configuration.

Two levels of Quadro GUI administration are available:

- **Administrator** – this is the main administrator’s account. The administrator can configure to have the factory reset safe the default password or choose not to. The administrator has access to all Web GUI pages and no one else has configuration permission to adjust this account. The administrator is responsible for granting access to all other user groups.
- **Local Administrator** – this is a common (sub-) administrator’s account. The password is not factory reset safe. Local Administrator can have permission to adjust each GUI page.
- **Extension** – this account refers to all extensions created on the Quadro. The password for default extensions is not factory reset safe but is contained in the backed up configuration. Permissions for an extension to access each GUI page can be adjusted here.

The **User Rights Management** page consists of two pages. The **Users** page is used to manage the available users on the Quadro. The **Roles** page is used to assign the corresponding permissions to the users.

The **Users** page contains a table where the Administrator and Local Administrator users are listed. This page allows them to modify the passwords of available users in the table and to manage the Local Administrator’s account. The following functional buttons are available on this page:

The **Change Password** functional button is used to change the password of the Administrator and Local Administrator user’s account. Select one of the available users in the table by toggling the corresponding checkbox and press **Change Password** to open the corresponding page.

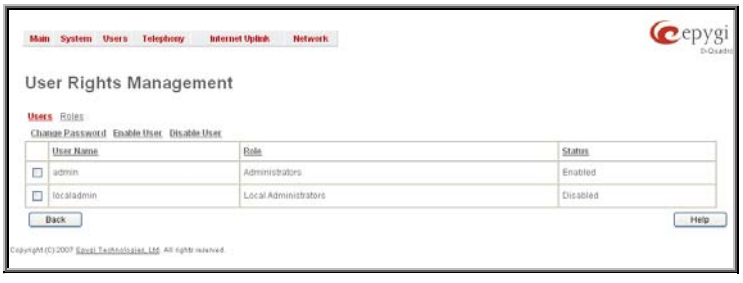


Fig. II-54: Users page at User Rights Management

The **Change Password** page is used to change the user's password. It offers the following components:

The **Old Password** text field is only present when modifying the Administrator account password and requires the current password of the Administrator. An error message prevents entering the wrong password.

The **New Password** text field requires a new password for the Administrator or Local Administrator. Reentering the new password in the **Confirm New Password** text field will confirm the new password.

The password can consist of numerical values only. Up to 20 digits are allowed. A corresponding warning appears if any other symbols are inserted.

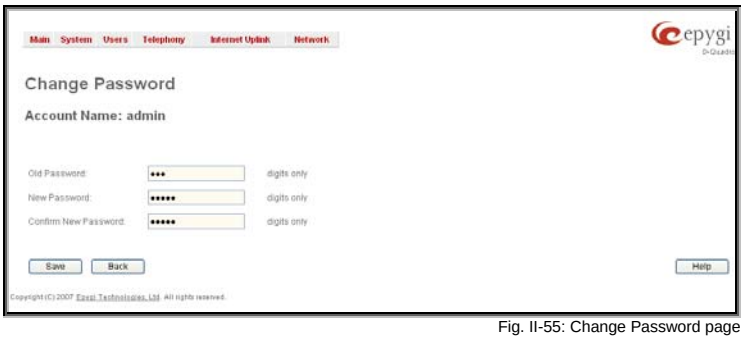


Fig. II-55: Change Password page

The **Enable User** and **Disabled User** functional buttons are used to enable or disable the Local Administrator's account.

Please Note: The Administrator's account cannot be disabled.

The **Roles** page contains a table where the Local Administrator and Extensions users are listed. This page allows you to set the permissions to the GUI pages for each user in the table.

The **Edit** functional button leads to the **Change Access Rights** page where a list of user specific GUI pages is displayed. Select the user in the table and press **Edit** to manage the permission for the corresponding user.

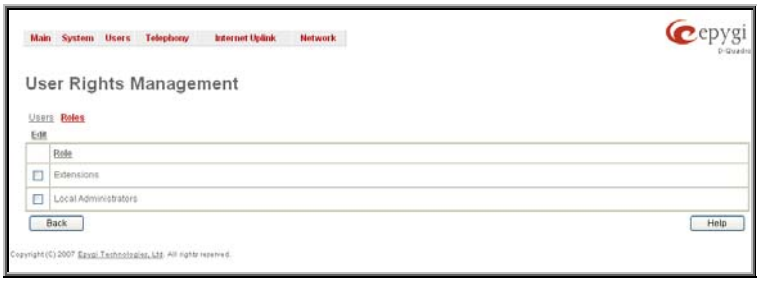


Fig. II-56: Roles page at User Rights Management

On the **Change Access Rights** page, **Grant Access/Deny Access** functional buttons are used to grant or deny access to certain GUI page(s) for the selected user.

When access to a certain GUI page is denied for a user, the "You are not authorized to access this page!" warning message will be displayed.

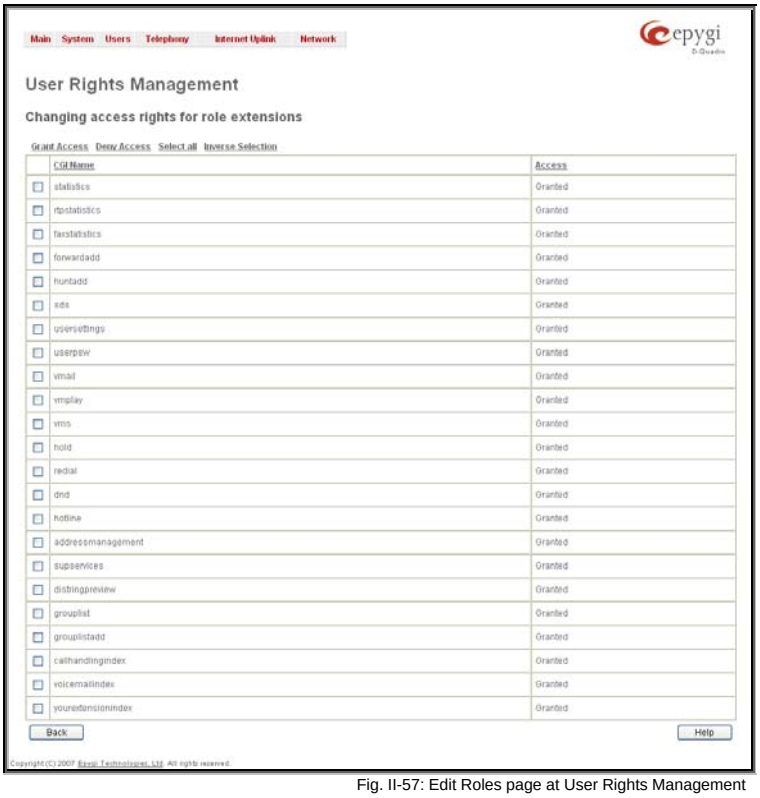


Fig. II-57: Edit Roles page at User Rights Management

Users Menu

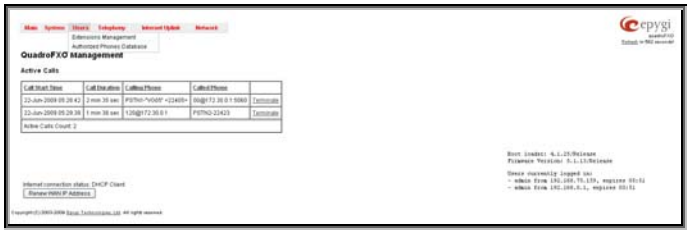
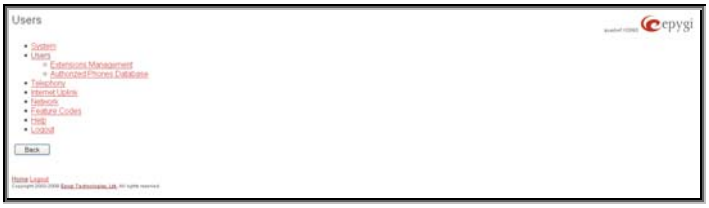


Fig. II-58: Telephone Users Menu in Dynamo Theme



F Fig. II-59: Telephone Users Menu in Plain Theme

Extensions Management

The **Extensions Management** page is used to create a variety of extensions and auto attendants on the Quadro. From this page, by clicking on the user extension, the Administrator can go to the extension settings pages.

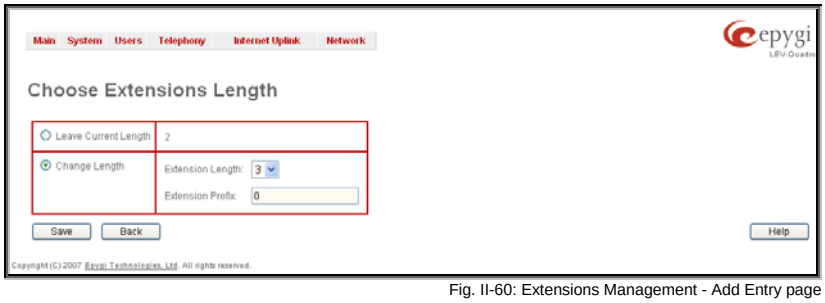


Fig. II-60: Extensions Management - Add Entry page

When this page is accessed for the first time after the Quadro's initial boot-up or the default configuration settings restore, an intermediate page is displayed.

The **Change Extension Length** page is used to define the extension settings applicable to all extensions on the Quadro. This page disappears once being saved.

The **Change Extension Length** page consists of a radio-button selection:

- **Leave Current Length** radio-button selection is used to leave the current length of extensions on the Quadro. Per default the extensions length on the Quadro is 2. In front of this selection, the actual configured length of extensions is displayed.
- **Change Length** radio-button selection is used to change the actual length of extensions on the Quadro. This selection enables the following information to be defined:

  The **Extension Length** drop-down list requires you to choose the length of the extensions on the Quadro. This number will apply to all existing extensions on the Quadro as well as to any newly created extensions. The length of the extension can be 2, 3 or 4.

  The **Extension Prefix** text field is used to define a prefix with which all existing extensions on the Quadro as well as to any newly created extensions should start. The prefix cannot start with the digits 0 or 9, otherwise an error message appears.

Please Note: By saving the settings on the **Change Extension Length** page, all existing extensions will lose the custom voice messages and voice mails in the voice mailbox. The device will be rebooted. You will not be automatically redirected to the login page, so you need to access it manually again when reboot ends. After the reboot, the **Change Extension Length** page will disappear and the **Extensions Management** page will be displayed. The **Change Extension Length** page will not appear again unless the default configuration settings are restored on the device.

Two types of user extensions, **active** and **inactive**, can be created on the Quadro. Active extensions are those that are attached to a line, can place and receive calls and use available telephony services. Inactive extensions are those that are not attached to the line. They can use some available telephony services but they cannot place and receive calls. Instead, inactive extensions have a voice mailbox available to store the messages from callers.

Quadro2x has two available lines and up to two active extensions can be established. Quadro4x has four available lines and up to four active extensions can be established. Quadro16x has sixteen available lines and up to sixteen active extensions can be established.

Attendant extensions are dedicated to the IVR system on the Quadro. These extensions are used by callers to reach Quadro's users and use the remote access and call relay services. It is possible to create Auto Attendants with the custom scenarios. By default, Quadro has one Auto Attendant extension (00) which is undeletable.

Attention: The system is limited to 100 extensions! Once the number of extensions in the Extensions table reaches 100, there will be no more possibility to add new extensions.

The **Extensions** table is a list of all extensions and their parameters.

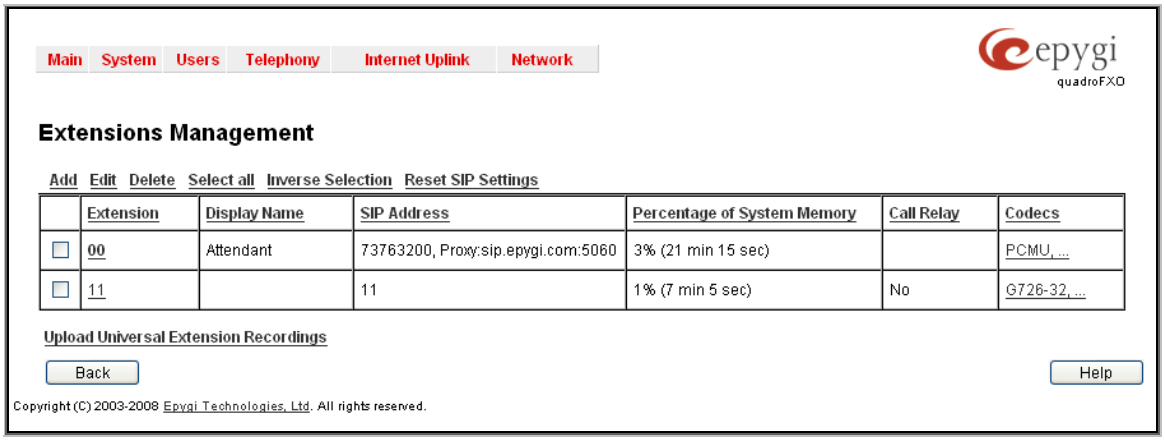


Fig. II-61: Extensions Management page

The following columns are present in the table:

- **Extension** - lists user or attendant extensions on the Quadro. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **Percentage of System Memory** - indicates the user space (in percentages) configured for each extension. The actual available duration (in minutes) for the extension voice mails, uploaded/recorded greetings and blocking messages is also displayed here. The available minutes corresponding to the selected user space are dependent on the Voice Recording codec selected from the Voice Mail Common Settings page. For example, for the same amount of marked out user space, selection of the G726 voice recording codec will provide more space for voice mails and user defined voice greetings than the G711 codec selection.
- **Call Relay** - indicates whether or not the Call Relay option is enabled on the extension.
- **Codecs** – column lists the short information (full information is seen in the tool tip) about extension specific voice Codecs. Extension codec's can be accessed and modified by clicking on the link of the corresponding extension's Codecs. The link leads to the Extension Codecs page.

Clicking on each user extension in the Extensions table will open the extension specific **Extension Settings** menu. The Pickup Group, Call Park and Paging Group extensions are displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible for this type of extensions.

Add opens the **Add Entry** page where the type and number of the new extension should be defined. This page consists of the following components:

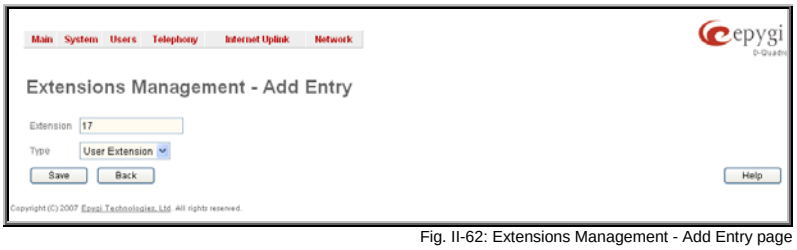


Fig. II-62: Extensions Management - Add Entry page

The **Extension** text field is used to enter a new extension number. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" will appear. If an extension with the same number already exists in the Extensions Management table, the error "Extension already exists" will appear.

Please Note: Extension number cannot start with the digits 0. You can add extensions of up to 20 digits long. However, the Call Routing won't be adjusted automatically; you may need to manually adjust the routing rules for extensions in custom length.

The **Type** drop down list is used to select the type of the extension (User Extension, Pickup Group, Call Park, Paging Group or Attendant) to be created (for details see below).

Reset SIP Settings functional button is used to reset all SIP settings of the selected extension(s) to the default values, including all settings listed under SIP Settings and SIP Advanced Settings pages (see below).

Edit opens the **Edit Entry** page where a newly created user or attendant extension settings might be adjusted. To operate with **Edit**, one or more record(s) have to be selected, otherwise the "No records selected" error message will appear.

The **Edit Entry** page consists of two frames. In the left frame settings groups are listed. Clicking on the corresponding settings group displays their configuration options in the right frame.

Please Note: Save changes before moving among settings groups.

User Extension Settings

1. General Settings

This group requires extension's personal information and has the following components:

Display Name is an optional parameter used to recognize the caller. Usually the display name appears on the called party's phone display when a call is made or a voice mail is sent.

Password requires a password for the new extension.

The extension password may only contain digits. If non-numeric symbols are entered, the "Incorrect Password: no symbol characters allowed" error will prevent making the extension.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the "Incorrect Password confirm" error will appear.

Use Kickback checkbox enables the Kickback service on the extension for the blind call transfer. When the extension transfers the call to the other extension and if there is no answer from the destination side, the call will automatically get back to the extension who initiated the transfer instead of getting into the destination's voice mailbox or being disconnected.

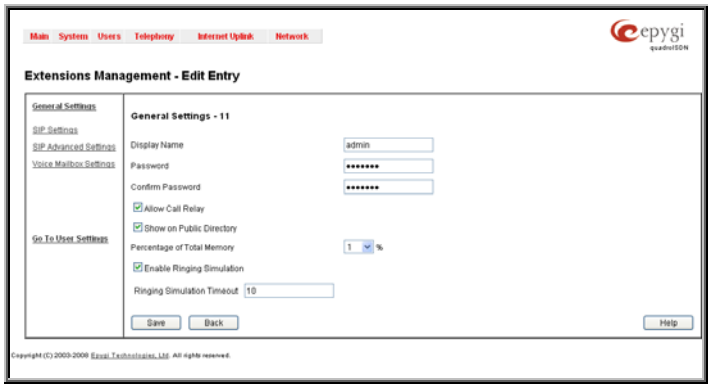


Fig. II-63: Extensions Management - Edit Entry – General Settings page

Allow Call Relay enables the current extension to be used to access the Call Relay service in the Quadro's Auto Attendant. It is recommended to define a proper and non-empty password when enabling this feature in order to protect the Call Relay service from an unauthenticated access.

When **External Call Policy** checkbox is enabled, all incoming IP calls to the corresponding extension will be handled by the external Policy Server.

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension's Quadro Web Management (accessed by the extension's login, see below Extension User's Menu). Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

The **Percentage of Total Memory** drop down list allows you to select the space for the extension's voice mails and uploaded/recorded greetings and blocking messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on Quadro. When editing an existing extension and decreasing the voice mailbox size, the system will check the present amount of voice mails in the mailbox of the extension. If the memory required for these voice mails exceeds the size entered, the system will suggest either to remove all voice messages from the extension's voice mailbox or to select a larger size so that the existing voice messages can be stored in the mailbox.

The **Enable Ringing Simulation** checkbox is available on virtual extensions only and enables extra ring tones played to the caller before the voice mail of the called virtual extension gets activated. If this checkbox is not enabled, the voice mailbox will get activated immediately the call arrives. The ring tones will be played during the timeout specified in the **Ringing Simulation Timeout** text field.

2. SIP Settings

This group is used to configure extension's SIP registration settings and consists of the following components:

User Name requires a user name for the extension registration on the SIP server. The registration user name needs to be unique on the SIP server and it is displayed on the called phone when performing an IP call.

Password indicates the password for the extension registration on a SIP server.

Registration Password is used to confirm the password. If the entered password does not correspond to the one entered in the **Password** field, the error message "The passwords do not match. Please try again" will appear.

SIP Server indicates the host address of the SIP server. The field is not limited regarding symbol usage or length. It can be either an IP address such as 192.168.0.26 or a host address such as sip.epygi.com.

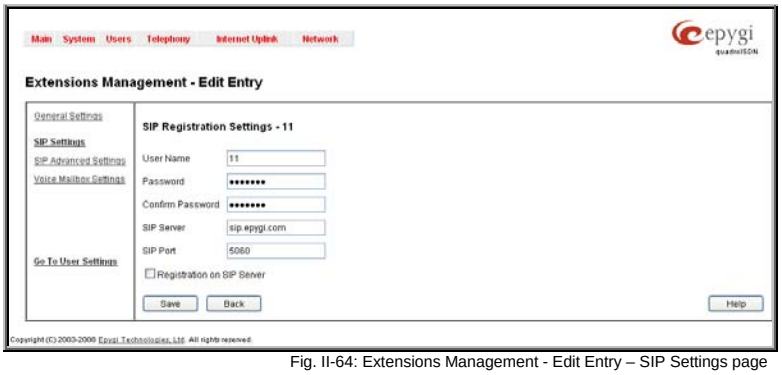


Fig. II-64: Extensions Management - Edit Entry – SIP Settings page

Registration SIP Port indicates the host port number to connect to the SIP server. The SIP server port may only contain digit values, otherwise the error message "SIP Server Port is incorrect" will be displayed when applying the extension settings. If the SIP server port is not specified, Quadro will access the SIP server through the default port 5060.

Registration on SIP Server enables the SIP server registration option. If the extension has already been registered on an SIP server, its IP address will be displayed in brackets.

3. Advanced SIP Settings

This group is used to configure advanced SIP settings (Outbound Proxy, Secondary SIP Server and Outbound Proxy for the Secondary SIP Server settings and to define other SIP server specific settings).

The SIP Outbound proxy is an SIP server where all the SIP requests and other SIP messages are transferred. Some SIP servers use an outbound proxy server to escape restrictions of NAT. For example, Free World Dialup service uses an Outbound Proxy server. If an Outbound proxy is

specified for an extension, all SIP calls originating from that extension are made through that outbound proxy, i.e., all requests are sent to that outbound proxy, even those made by Speed Calling.

The Secondary SIP Server acts as an alternative SIP registration server when the primary SIP Registration Server is inaccessible. If the connection with the primary SIP server fails, Quadro will automatically start sending SIP messages to the Secondary SIP Server. It will switch back to the primary SIP server as soon as the connection is reestablished.

Authentication User Name requires an identification parameter to reach the SIP server. It should be provided by the SIP service provider and can be requested for some SIP servers only. For others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism. **Timeout** indicates the timeout between two attempts for the SIP registration server accessibility verification. If no reply is received from the primary SIP server within this timeout, the Secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will resume being sent to it.

The **RTP Priority Level** drop down list is used to select the priority (low, medium or high) of the RTP packets sent from a corresponding extension. RTP packets with higher priority will be sent first in case of heavy traffic.

The **Do Not Use SIP Old Hold Method** checkbox enables the new recommended method of call hold in SIP, in which case the hold request is indicated with the "a=sendonly" media attribute, rather than with the IP address of 0.0.0.0 used before. The checkbox should be enabled if the remote party does not recognize hold requests initiated from the Quadro.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name) and the port numbers of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

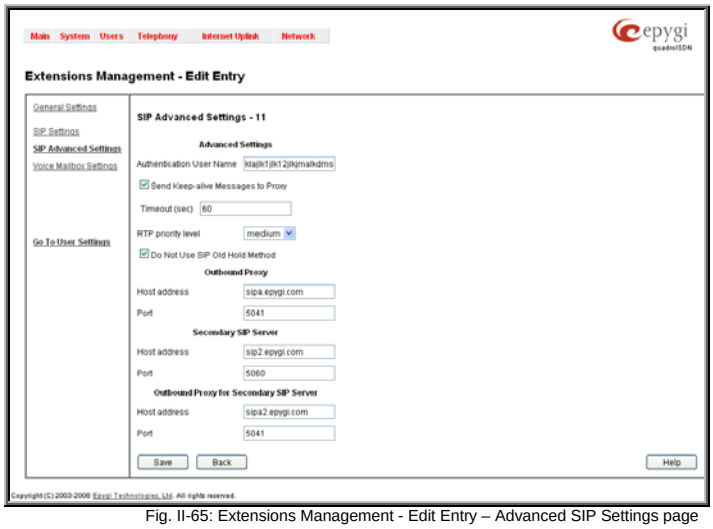


Fig. II-65: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Voice Mailbox Settings

This group is used to configure voice mailbox storage and consists of a group of manipulation radio buttons to define the location where voice mails will be collected.

- **Disable Voice Mail** – disables the Voice Mail service for the corresponding extension. With this selection, the extension user will be unable to reach their Voice Mail Settings, but will be able to access their Voice Mailbox and manage the existing voice mails.
- **Use Internal Voice Mail** – enables the Voice Mail service for the corresponding extension and defines the Quadro's internal storage as a location for the Voice Mails.

  This selection also allows you to manipulate with the **Voice Mail Configuration Wizard** used by the extension's user to setup personal settings (the password, the voice mail greeting message and the user's name for **Extensions Directory**) from the handset. By default, the **Voice Mail Configuration Wizard** is enabled when the Quadro's is in the factory reset state. It can be manually enabled from this page by pressing the **Activate** button. When the **Voice Mail Configuration Wizard** is activated, the extension's user is prompted to insert personal settings as he/she enters his/her Voice Mailbox for the first time. Unless the required information is not inserted, the button is changed to **Deactivate** and the **Configuration Wizard Status** becomes **Activated**. Use **Deactivate** button to stop **Voice Mail Configuration Wizard**. When the user inserted the required information, the **Configuration Wizard Status** on this page is changed to **Passed** and a **Reactivate** button appears. Using **Reactivate** button you might re-enable the **Voice Mail Configuration Wizard** so the user will be again prompted about his/her personal settings next time entering his/her Voice Mailbox.

  Instructions on how to insert the information prompted in the **Voice Mail Configuration Wizard** are available in the **Features Codes** (see Manual III – Extension's Users Guide).

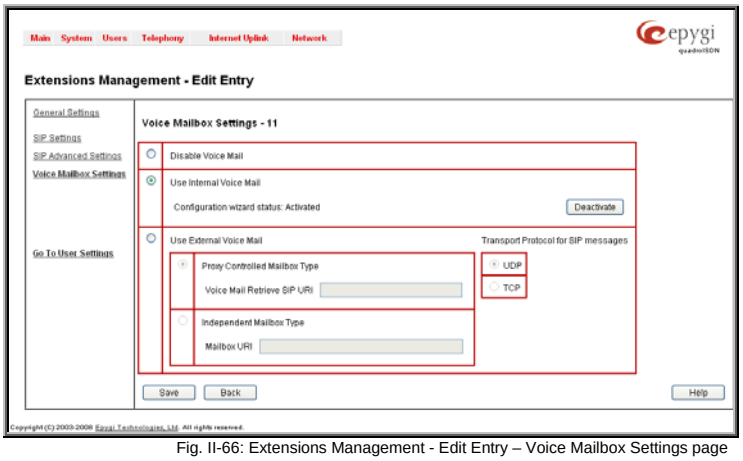


Fig. II-66: Extensions Management - Edit Entry – Voice Mailbox Settings page

- **Use External Voice Mail** – enables the Voice Mail service for the corresponding extension and is used to define a remote Voice Mail Server as a location for the Voice Mails. In this case recorded voice mails will be collected on the remote server. Radio button selection enables a sub-group of manipulation radio buttons:
  - If the remote Voice Mail Server is combined with the SIP Proxy server, it is recommended to select **Proxy Controlled Mailbox Type**. With this selection, SIP proxy will keep the recorded voice mail on itself. When extension accesses his mailbox by dialing *0, the call will be redirected to the voice mailbox on the proxy server.
  - If the remote Voice Mail Server acts as a standalone location of voice mails, it is recommended to select **Independent Mailbox Type**. With this selection, Quadro redirects the recorded voice mails to the defined remote Voice Mail server. When extension accesses his mailbox by dialing *0, the call will be redirected to the remote voice mail server.

  For each of these selections, it is required to enter the SIP URI of the Voice Mail Server where voice mails of the corresponding extension will be collected.

  Attention: By choosing the **Use External Voice Mail** option, some internal voice mailbox services may become unavailable. Instead, the services of the external voice mail server will become available to the user. Please consult with the external voice mail server administrator before enabling this option.

  The **Transport Protocol for SIP messages** radio buttons allow the transport protocol (UDP or TCP) for transmission of SIP messages to be selected.

The **Go to User Settings** link is used to make a quick jump to the extension specific Extension's Main Menu page (see below Extension User's Menu).

Voice Mail Profiles

The **Voice Mail Profiles** page can be accessed by clicking on an extension link in the Extension Management table and then choosing **Voice Mail→Voice Mail Settings**. The **Profiles for Voice Mail Settings** link on this page will lead you to the **Voice Mail Profile** page. The link is present only when the administrator accesses this page and is hidden for the extension user.

The **Voice Mail Profiles** page is used to define and configure custom voice mail profiles.

The Voice Mail Profile is a group of most common Voice Mail Settings which can be saved under a specific name. This allows you to have several versions of Voice Mail Settings configurations per extension.

Each Voice Mail Profile may have custom voice mail greeting, maximum voice mail duration, new voice mail notifications and Zero-Out settings. The Voice Mail Profiles are activated based on the call routing rule used to establish a call. This is limited to the PBX-Voicemail type of calls used for a direct access to the extension's voice mailbox. The Voice Mail Profile name should be provided in the Call Routing Wizard when defining a PBX-Voicemail routing rule. When the rule is used, caller accesses the called extension's mailbox with the settings configured in the corresponding voice mail profile.

Fig. II-67: Extensions Management - Edit Entry – License Settings page

With this service, you can pre-configure several versions of Voice Mail Settings and save them as Voice Mail Profiles. For example, if a call is originated from the PSTN network to the corresponding extension's voice mailbox, the greeting message can tell the caller: "You have reached the ... company, please leave a message." and the maximum voice mail duration is configured to 15 minutes. This voice mail profile can be saved as "ForPSTN" and its name should be defined in the routing rule responsible for incoming PSTN calls distribution. In parallel to this voice mail profile, there can be another profile designed for internal PBX calls. It will play the following voice mail greeting: "Hi, you have reached Mike's voice mailbox, please drop me a message and I shall call you back.", the maximum voice mail duration is 5 minutes and there is a Zero-Out feature configured to call Mike's cellular phone. This voice mail profile can be saved as "ForPBX" and its name should be defined in the routing rule responsible for PBX calls distribution to the local extensions. When the first routing rule is used and the call reaches the extension that has the corresponding voice mail profile, the settings of the ForPSTN voice mail profile will be activated. For the second routing rule, when the call reaches Mike's voice mailbox, the settings of the ForPBX voice mail profile will be activated.

The same profile name can be used to create profiles for different extensions. This is useful if the profiles have a similar purpose but differ in certain user-specific settings, such as voice mail greeting, Zero-Out destination number, new voice mail notification options, and so on. Creating multiple profiles with the same name gives a wide flexibility to have different voice mail settings activated depending on which extension is called.

Please note: If an extension does not have a profile specified in a call routing rule or the specified profile name is incorrect, the default Voice Mail Settings of the extension will be used.

The Voice Mail Profiles page contains a table where all Voice Mail Profiles for the corresponding extension are listed. The the following functional buttons are available:

Add opens the **Add Entry** page where a new Profile Name should be defined.

Edit opens the **Edit Entry** page where Voice Mail Profile settings should be defined. For the description of the settings found on this, please refer to the chapter on Voice Mail Settings.

Delete removes the selected Voice Mail Profile(s) from the table.

Attendant Extension Settings

For **Attendant** extensions, the **Extensions Management** - **Edit Entry** page consists of **General Settings, Attendant Scenario**, **SIP Settings** and **SIP Advanced Settings** pages. The **SIP Settings** and **SIP Advanced Settings** pages are the same as for the regular extensions described above. The **General Settings** and **Attendant Scenario** pages are described below:

1. General Settings (for attendant extension)
This group requires personal extension information and has the following components:

Display Name is an optional parameter used to define the Auto Attendant's description. Usually the display name appears on the called party's phone display when a call is made or a voice mail is sent.

The **Percentage of System Memory** drop down list is used to define the space for the Auto Attendant's system messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on Quadro.

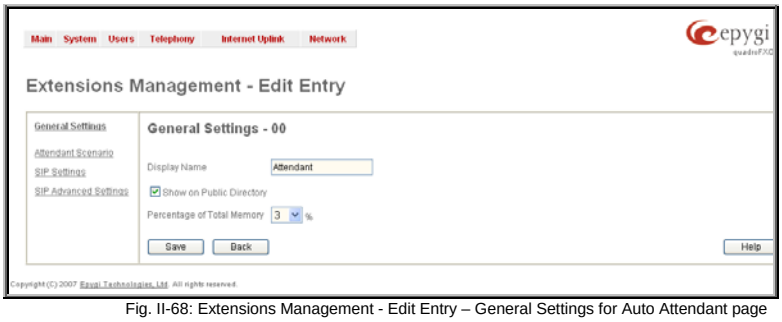


Fig. II-68: Extensions Management - Edit Entry – General Settings for Auto Attendant page

2. Attendant Scenario

This group is used to select between default and custom attendant functionality scenarios. When the **Default** scenario is selected, a group of settings should be adjusted. Here, the user defined Auto Attendant system messages can be uploaded and the list of **Friendly Phones** can be configured. For **Custom** scenario, a scenario script file (in EpygiXML coding, the coding standard can be found at Epygi Technical Support) should be defined and the custom voice messages can be uploaded.

The **Default** manipulation radio button selection enables the following components:

- The **Send AA Digits to Routing Table** checkbox selection switches the Auto Attendant to the routing mode. Any inserted digits on the Auto Attendant prompt will be parsed through the Routing Table on the Quadro.
- **Redirection on Timeout -** this group allows automatic call redirection in case no action has been performed by the caller. The group offers the following options:

  Enable Redirection on Timeout checkbox is used to enable/disable the automatic call redirection.

  Recurring Attendant Prompt Repetition Count text field indicates the number of Recurring Attendant Prompts to be consecutively played to the caller with no action from his/her side. When the Recurring Attendant Prompt is played the number of times indicated in this text field, the call will be automatically redirected to the defined destination.

  Call Type drop down list includes possible incoming call types (PBX, PSTN, SIP or Auto). PBX selection means that the call will be redirected to the local extension. **SIP** selection means that the call will be redirected to the SIP destination correspondingly. **PSTN** selection means that the call will be redirected to the PSTN destination. **Auto** selection is used for undefined call types: destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

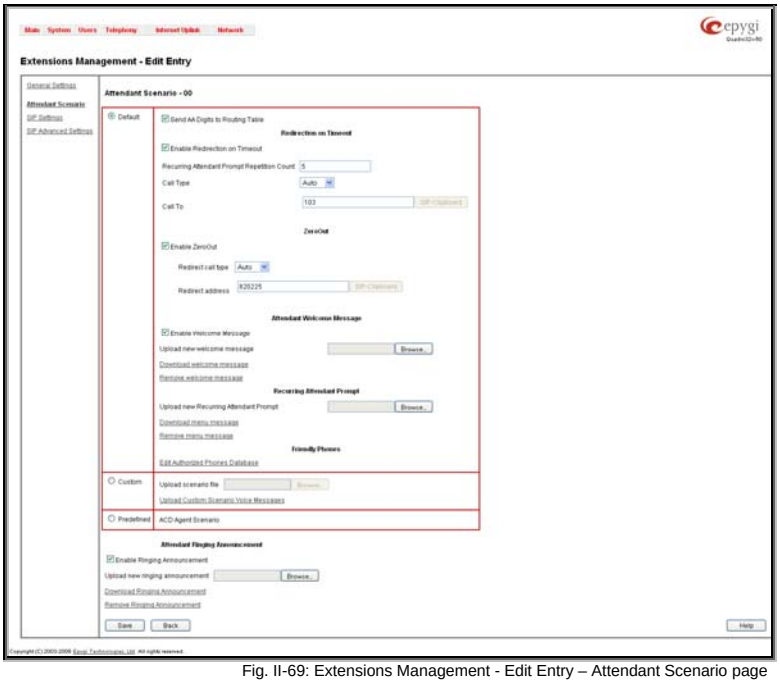


Fig. II-69: Extensions Management - Edit Entry – Attendant Scenario page

Call To text field requires the destination number dialed in the format depending on the selected Call Type. The wildcard is supported in this field.

- **ZeroOut** – this group is used to configure call redirection service on the Auto Attendant. When a caller reaches the Auto Attendant, he may want to accelerate the automatic redirection feature instead of using Auto Attendant features. To activate ZeroOut, caller should dial 0 digit (see Feature Codes) during the Auto Attendant welcome message. The caller will then be automatically transferred to the destination specified in this page.

  Enable ZeroOut checkbox selection enables the ZeroOut feature and activates the following fields to be inserted:

  Redirect Call Type drop down list includes the available call types:

  - PBX - local calls between Quadro extensions and the Auto Attendant
  - SIP – calls through a SIP server
  - PSTN – calls to PSTN
  - Auto – used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

  The **Redirect Address** text field requires the destination address where the caller should be automatically forwarded to if activating the ZeroOut feature.

  Attention: The routing patterns in the Call Routing table starting with digit "0" will not work for incoming calls to attendant if both the ZeroOut and **Send AA Digits to Routing Table** options are enabled. The ZeroOut feature has a higher priority. If it is enabled and used, the system will forward all incoming calls to attendant to the specified redirect address. As a result, calls prefixed with 0 will never reach call routing.

- **Attendant Welcome Message -** this group allows updating the active Auto Attendant welcome message (played only once when entering Auto Attendant), downloading it to the PC, or restoring the default one. The group offers the following components:

  Enable Welcome Message checkbox is used to enable/disable the Auto Attendant welcome message (the default one or the custom one uploaded from this page or recorded from the handset (see Feature Codes) being played when callers enter Quadro's Auto Attendant.

  Upload new welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.

  Browse opens the file chooser window to browse for a new welcome message file.

  The **Download Welcome Message** and **Remove Welcome Message** links appear only if a file has been uploaded previously. The **Download Welcome Message** link is used to download the message file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Welcome Message** link is used to restore the default welcome message.

- **Recurring Attendant Prompt -** this group allows updating the active recurring Auto Attendant message (played after the Attendant Welcome Message and then periodically repeated while being in the Auto Attendant), downloading it to the PC, or restoring the default one. The group offers the following components:

  Upload new Recurring Attendant Prompt indicates the file name used to upload a new recurring auto attendant prompt. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning message to appear.

  Browse opens the file chooser window to browse for a new Recurring Attendant Prompt file.

  The **Download Recurring Attendant Prompt** and **Remove Recurring Attendant Prompt** links appear only if a file has been uploaded previously. The **Download Recurring Attendant Prompt** link is used to download the Recurring Attendant Prompt file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Recurring Attendant Prompt** link is used to restore the default Recurring Attendant Prompt.

- The **Attendant Ringing Announcement** group allows uploading an optional voice message that is played to callers instead of ring-back tones when making calls through an auto attendant. The **Ringing Announcement** can be enabled for both custom and default attendants.

  Please Note: The **Attendant Ringing Announcement** is played to SIP-to-extension and PSTN-to-extension calls only. The announcement can also be played to SIP-attendant-SIP and PSTN-attendant-SIP calls if they are made by a call routing rule for which the RTP proxy is enabled.

  The group offers the following components:

  The **Enable Ringing Announcement** checkbox enables/disables the Auto Attendant optional announcement message. When this checkbox is selected but no custom announcement message is uploaded, the default message will be played to callers.

  Upload new Attendant Ringing Announcement indicates the file name used to upload an announcement. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning message to appear.

  Browse opens the file chooser window to browse for a new announcement.

  The **Download Ringing Announcement** and **Remove Ringing Announcement** links appear only if a file has been uploaded previously. The **Download Ringing Announcement** link is used to download the announcement file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Ringing Announcement** link is used to restore the default ring back tones.

- **Friendly Phones -** the **Edit Authorized Phones Database** link refers to the Authorized Phones Database page where a list of trusted external phones can be created. If external SIP or PSTN users are added to the Quadro Authorized Phones database, they are free to access the Auto Attendant Services without passing the authentication or to use the Call Back services.

The **Custom** manipulation radio button selection allows you to upload Attendant's custom scenario file and voice messages. The selections are:

- The **Upload Scenario File** indicates the file name used to upload a new scenario file. The uploaded file needs to be in EpygiXML format (the coding standard can be found at Epygi Technical Support) and is restricted to a 20KB file size. **Browse** opens the file chooser window to browse for a custom scenario file.

  Please Note: You may upload an attendant scenario file along with the voice prompt recordings as a single file. To do this, create an archive file of the "tar.gz" type containing all the necessary files and upload it from the **Upload Custom Scenario Voice Messages** page.

- The **View/Download Scenario** link appears only when a custom scenario file has been previously uploaded and is used to view or download the scenario file. The **Remove Scenario** link is used to remove a custom scenario file and return to the default Auto Attendant scenario.

- The **Upload Custom Scenario Voice Messages** link refers to the page where voice messages used in the uploaded custom scenario should be managed.

This page provides the possibility of uploading voice messages to be played in the custom Auto Attendant scenario. It also removes and downloads the uploaded files to a PC.

The **Upload Custom Scenario Voice Messages** page contains a table where uploaded custom voice messages are listed. Use the **Download** functional button to download and use **Remove** to delete the corresponding custom voice message. **Browse** opens a file chooser window to browse for a custom voice message or for an archive file with the "tar.gz" extension containing the custom attendant scenario and the voice prompt recordings.

Fig. II-70: Upload Custom Voice Messages page

The **Edit** functional button provides a possibility of editing multiple extensions at the same time. In this case, fields that cannot be edited for multiple records have **Multiple** values in the **Edit Entry** page. When editing user and attendant extensions together, the **Edit Entry** page displays only those fields that are for both user extension and attendant settings. Additionally, for the fields that need to be modified, a **Select to modify fields** checkbox alongside the corresponding field needs to be selected to submit changes, otherwise the fields will not be updated.

Delete removes the selected extensions. If no records are selected an error message occurs.

The Upload Universal Extension Recordings link leads to the page where universal default voice messages for all extensions are defined.

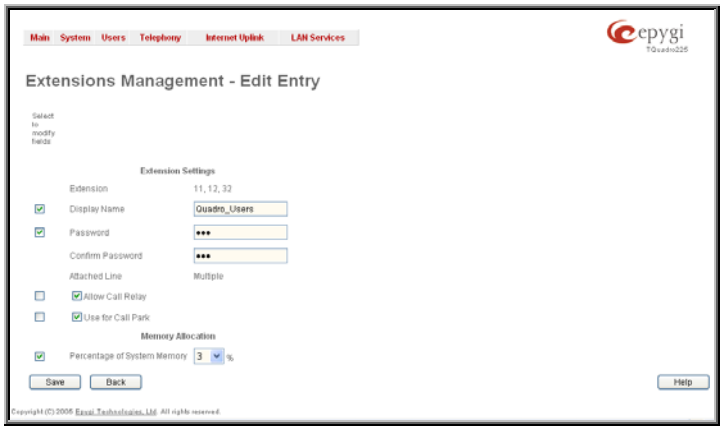


Fig. II-71: Extensions Management - Edit Entry page for multiple edit operation

To Configure an Extension

1. Press the **Add** button on the **Extensions Management** page. The **Add Entry** page will appear in the browser window.
2. Enter the desired extension number in the **Extension** text field and select the extension type from the **Type** drop down list.
3. Press **Save** to create an extension with the defined number.
4. Select the checkbox of the newly created extension in the **Extensions Management** table and press the **Edit** button. The **Edit Entry** page will appear in the browser window.
5. Move through the extension's configuration pages and fill the fields with the appropriate information.
6. To apply extension settings, press **Save**.

To Delete an Extension

1. To remove an extension with all its settings select one or more checkboxes of the corresponding extensions that should be deleted from the **Extensions Management** table. Press **Select all** if all extensions should be deleted.
2. Click on the **Delete** button on the **Extensions Management** page.
3. Confirm the deletion by clicking on **Yes**. The extension(s) will be deleted. To abort the deletion and keep the extension in the list, click **No**.

Extension Codecs

To establish IP voice communication, both partners have to use the same codec. When establishing the communication line, this codec is negotiated. If the caller does not find an appropriate codec, the communication cannot take place. If you want to be reachable by all IP calls, it is helpful to support as many codecs as possible. In this case, all the codecs that Quadro offers should be added to the **Codecs** table. Some codecs require a high transfer rate of up to 64 kbit/s. If you are certain you do not want to use these codecs, make sure they are not listed in the table **Codecs**.

The **Extension Codecs** page displays a list of **Codecs** with the state of the **Out of Band DTMF** and **FAX Support** features for Quadro extensions and the Auto Attendant.

Please Note: Use caution when configuring Auto Attendant Codecs as they are used by virtual extensions for redirecting the incoming calls.

The table **Codecs** lists active voice codecs for the selected line that are supported by Quadro. The order of records in the **Codecs** table is important for transmitting and receiving. A codec placed at the top of the table will be used as the preferred codec. If the remote party does not support the preferred codec, the following codecs will be tried in a top to down order in the **Codecs** table.

Each record in the table has an assigned checkbox. They are used to select the record to be deleted or moved up or down.

An error occurs if no records are selected and the user activates the delete button, the "No records selected" error message appears. At least one codec must be attached to the line. When attempting to delete the last codec, the "At least one codec should stay in the codec list" error message will appear.

Enable/Disable functional button is used to enable or disabled the corresponding codec for the extension. When the codec is disabled, the extension user will not be able to use it for placing a call.

The **Move Up/Move Down** buttons are used to move the selected codec one level up/down in the table.

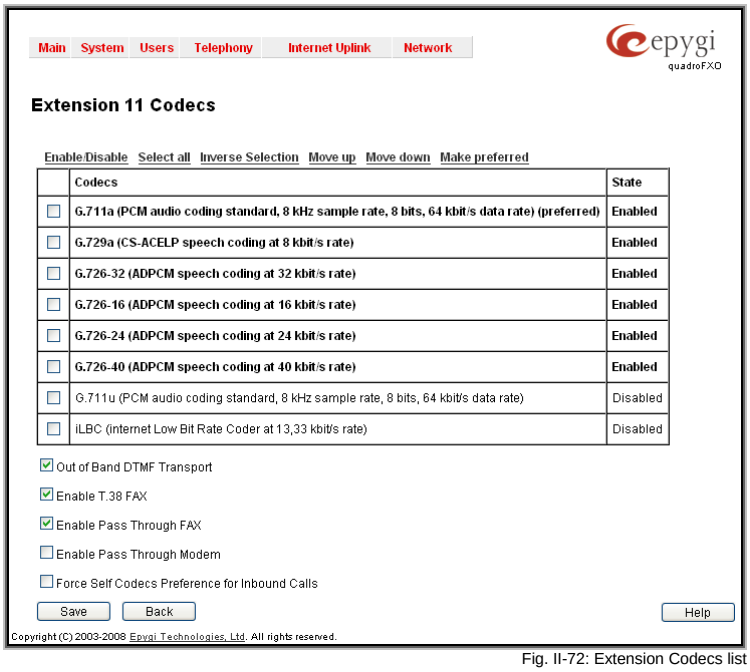


Fig. II-72: Extension Codecs list

The **Make preferred** button moves the selected codec to the top of the table, setting its priority to the highest. Clicking the **Make preferred** button when a disabled codec is selected will first enable the codec and then move it to the top.

The **Out of Band DTMF Transport** checkbox enables DTMF code transmission in parallel with the voice stream. The destination receiving the DTMF code will play it locally if it supports the feature. This is helpful to avoid DTMF's loss upon bad traffic. This feature is valuable for all codecs but it is especially recommended to enable it in case low bit rate codecs (G.729, G.723, G.726/16, etc.) are selected.

Enable T.38 FAX checkbox enables the FAX tone detection and the T.38 codec support for the FAX transmission from/to the FAX machine/modem attached to the line. It also enables the T.38 codec support for incoming unified FAX messages.

The **Enable Pass Through FAX** checkbox enables the FAX tone detection and the G.711 codec support for the FAX transmission from/to the FAX machine/modem attached to the line. It also enables the G.711 codec support for incoming unified FAX messages.

If both of the above checkboxes are enabled, the T.38 codec will be used as a preferred codec for FAX transmission. If it is not supported by the peer, the G.711 codec will be used instead. If the extension is attached to the line that has no FAX machine/modem connected (the extension is virtual), the incoming FAX can only be stored in the extension's voice mailbox. To allow FAX to be stored in the voice mailbox, the extension's user should not answer the incoming calls, so that they are forwarded to the voice mailbox.

Please note: If both of the above checkboxes are disabled, no FAX transmission to the peer's voice mailbox will be possible.

Enable Pass Through Modem checkbox is only available for Auto Attendant and extensions attached to the FXS lines. This checkbox enables the modem tone detection and the G.711 codec support for the data transmission from/to the modem attached to the line. During data transmission, Silence Suppression (see RTP Settings) and Echo Cancellation are being disabled on the line.

Please note: If the extension/attendant is intended to accept modem connections, disable the **Enable T.38 FAX** checkbox to allow the system to identify the modem tones correctly. Otherwise, the modem connection may fail.

The **Force Self Codecs Preference for Inbound Calls** checkbox enables the usage of your own preferred codecs (if available on both peers) for the IP connection establishment on the extension.

Upload Universal Extension Recordings

The **Upload Universal Extension Recordings** are to be defined by the Quadro administrator and will be present instead of the default voice messages for all extensions on the Quadro. They will be used when no custom messages have been uploaded or recorded.
The following system messages can be uploaded from this page:

- **Incoming call blocking** - played when a blocked user calls the extension
- **Outgoing call blocking** – played when extension dials a blocked destination

The **Upload Universal Extension Recordings** page consists of a table where the universal voice messages are listed.

An **Upload** functional link is present for each voice message recording that is not uploaded in the table and it is used to upload the custom system message. When a message is uploaded, the **Upload** functional link is replaced by **Download** and **Remove** functional links respectively. These are used to download to the PC and to remove the uploaded system message.

The **Memory Allocation** group includes a drop down list used to specify the **Percentage of System Memory** for the universal extension recordings. The maximum value in the drop down list is equal to the maximum available space for voice messages on Quadro.

Fig. II-73: Upload Universal Extension Recordings page

Please Note: Changing the **Percentage of System Memory** on this page will stop any recordings of universal extension voice messages from the handset.

Authorized Phones Database

The **Authorized Phones Database** page is used to create a list of trusted external phones. If they are part of the Quadro Authorized Phones database, external SIP or PSTN, then users are free to access the Quadro Auto Attendant services without requiring authentication. When adding a trusted phone to the list, an existing extension has to be chosen. The parameters (extension number and password, as well as SIP and Speed Calling Settings) will be used automatically for the trusted caller access of the Quadro Auto Attendant. A direct connection to the **Call Relay** menu can be optionally provided.

The **Authorized Phones Database** page displays the **Authorized Phones Database** table where the trusted phones are listed. Only SIP and PSTN users can be added to the **Authorized Phones Database**.

The **Authorized Phones Database** table displays all trusted callers with their settings. For example, the call type, caller address, extension they automatically login with, information if they have automatic access to Call Relay Menu of the Auto Attendant, etc.

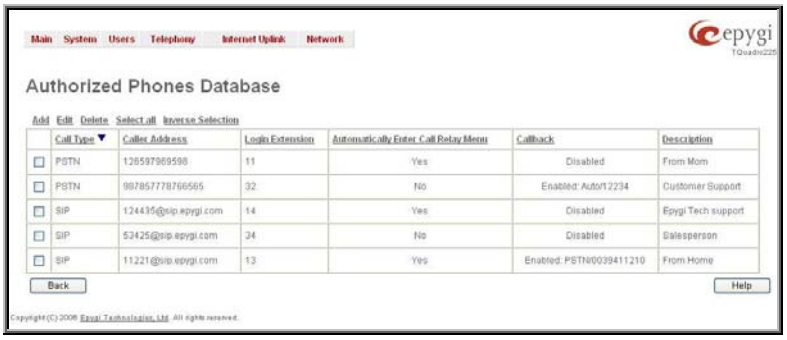


Fig. II-74: Authorized Phones Database

Each record in the table has an assigned checkbox. The checkbox is used to edit or delete the corresponding record. The “No records selected” error message occurs if the user activates the edit or delete button with no records being selected. The error message “One record should be selected” appears if the user tries to edit more than one record. The heading of each column in the table has a link. By clicking on the column heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The **Add** functional button refers to the **Authorized Phones Database- Add Entry** page where new trusted users may be entered.

The **Authorized Phones Database- Add Entry** page offers two groups of input options:

Caller Settings

The **Call Type** drop down list includes possible incoming call types (PSTN, SIP or Auto). In **SIP**, the caller connects Quadro through a SIP server and **PSTN** means the caller is a PSTN user. **Auto** is used for undefined call types and the destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

The **Caller Address** text field requires the caller’s SIP address (see chapter Entering a SIP Addresses correctly) or PSTN number to be added to the trusted phones list. The PSTN number length depends on the area code and phone number. The wildcard is supported in this field. If the caller address already exists in the **Authorized Phones Database**, the error message “The record already exists” appears when selecting the **Save** button.

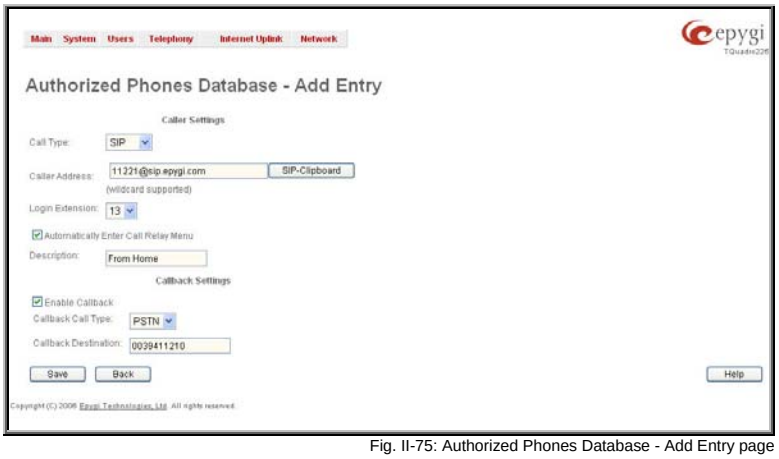


Fig. II-75: Authorized Phones Database - Add Entry page

The **Login Extension** drop down list provides all existing extensions on the Quadro. When calling the Quadro Auto Attendant, a trusted user will automatically be logged in as the selected extension, i.e., the extension number and its password will be automatically submitted by the Quadro system. The trusted user will directly access the Quadro Auto Attendant services. The SIP settings of the login extension will be used when making IP calls.

The **Automatically Enter Call Relay Menu** checkbox enables direct access for the trusted user to the Quadro Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but will still be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

Please Note: **Login Extension** drop down list and **Automatically Enter Call Relay Menu** checkbox have no sense for Auto Attendant with custom scenario configured (see Attendant Extension Settings).

The **Description** text field allows entering an optional comment.

Callback Settings

The **Enable Callback** checkbox selection gives the possibility for a specified trusted caller to use the Instant Call Back service (see chapter Call Back Services).

The **Callback Call Type** drop down list includes possible callback call types (PBX, PSTN, SIP and Auto).

The **Callback Destination** text field requires the destination number where Quadro should instantly call back to. The value inserted in this field is dependent on the selected callback call type: for **PBX**, 2-digit extension is required, for **SIP**, the SIP address is requires and for **PSTN**, a PSTN number is required. **Auto** is used for undefined call types: destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Call Routing table. If this field is left empty, the callers address will be implied as a callback destination.

Please Note: The Call Back service is functional and enabled only for PSTN callers.

To Add an Authorized phone to the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. Press the **Add** button on the **Authorized Phones Database** page. The **Add Entry** page will appear in the browser window.
4. Choose the call type and enter a caller address in the corresponding text field.
5. Select a **Login Extension** and the **Automatically Enter Call Relay Menu** checkbox (if required).
6. Enable **Call Back** service if required and define a **Call Back Destination** in the same named field.
7. Fill in an optional **Description** in the appropriate field, if required.
8. Press **Save** to submit the settings.

To Delete an Authorized phone from the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. To remove an authorized phone(s), select one or more checkboxes of the corresponding records that should be deleted from the **Authorized Phones Database** table. Press **Select all** if all records should be deleted.
4. Press the **Delete** button on the **Authorized Phones Database** page.
5. Confirm the deletion by clicking on **Yes** or cancel the action by clicking on **No**.

Call Back Services

With **Call Back** service, PSTN callers can save a call charge when calling to and through Quadro. Quadro provides the possibility of creating a list of those trusted PSTN callers that are allowed to make free of charge calls to Quadro's Auto Attendant or through its Call Relay menu to the third party IP or PSTN destination. Two types of Call Back services are available on the Quadro: **Pre-configured Call Back** and **Remote Call Back Configuration**.

Pre-Configured Call Back

For **Pre-configured Call Back**, a list of trusted PSTN callers must be configured in the Quadro's Authorized Phones Database using Web Management. The Call Back service should be enabled and a valid callback destination should be specified for each PSTN caller.

To use **Pre-configured Call Back**, the PSTN caller registered in the Authorized Phones Database simply calls to the PSTN number attached to the Quadro FXO line (the FXO line should be previously routed to the Auto Attendant from the FXO Settings page) from the global PSTN network. Let the call to ring twice and then hang up. Call Back will be instantly activated, and Quadro will call back to the defined Call Back destination. By answering the incoming call the PSTN party will be connected to the Auto Attendant menu.

Remote Call Back

The **Remote Call Back Configuration** service is used by authorized PSTN caller to configure or reconfigure by an authorized PSTN caller using a phone and calling to the Quadro's Auto Attendant. Remote Call Back Configuration is divided into two modes accessible from the Quadro's Auto Attendant: **Permanent Call Back** and **Non-Permanent Call Back**.

Please Note: Remote Call Back Configuration services are only available when the **Automatically Enter Call Relay Menu** checkbox is disabled in Authorized Phones Database for the trusted user.

Permanent Call Back service allows the callers registered in the Authorized Phones Database to create a new trusted PSTN Caller with Call Back enabled. They can also modify the Call Back destination of an existing PSTN Caller in the Authorized Phones Database. By calling Quadro's PSTN number (that is previously routed to the Auto Attendant) and entering the Auto Attendant menu, the caller can use the ***6** code (see Feature Codes) to create a new trusted PSTN Caller as well as to modify the Call Back destination for the already registered Caller in the Authorized Phones Database.

Entering the **Permanent Call Back** reconfiguration menu, the system will ask the caller to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in Call Back settings. After entering the login successfully the PSTN callers should follow the voice instructions for configuring a new entry or reconfiguring the existing entry in Authorized Phone database.

When the system accepts the settings, the corresponding entry will be logged to the Authorized Phones Database. The detected PSTN caller address must correspond to the one applied by the caller, the FXO line must be available on the Quadro, there must be network connectivity and the destination must be reachable. The PSTN caller will then be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds. Answering the incoming call, the PSTN caller will be reconnected to the Quadro's Auto Attendant.

Non-Permanent Call Back configuration service allows the trusted caller to organize one-time Call Back to the defined PSTN destination. In this situation, no entry will be logged to the Authorized Phones Database.

By calling Quadro's PSTN number (that is previously routed to the Auto Attendant) and entering the Auto Attendant menu, the caller is able to use the ***5** menu (see Feature Codes) to modify the Call Back destination for the already registered Caller in the Authorized Phones Database.

The system will ask the caller to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in the Call Back settings. After successful login, the PSTN caller should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database.

The detected PSTN caller address must correspond to the one applied by the caller, the FXO line must be available on the Quadro, there must be network connectivity and the destination must be reachable. The PSTN caller will then be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds. Answering the incoming call, the PSTN caller will be reconnected to the Quadro's Auto Attendant.

Telephony Menu

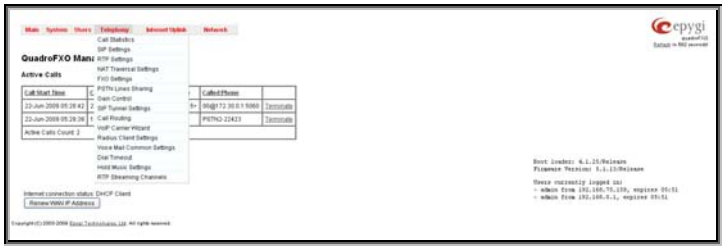


Fig. II-76: Telephony Menu in Dynamo Theme

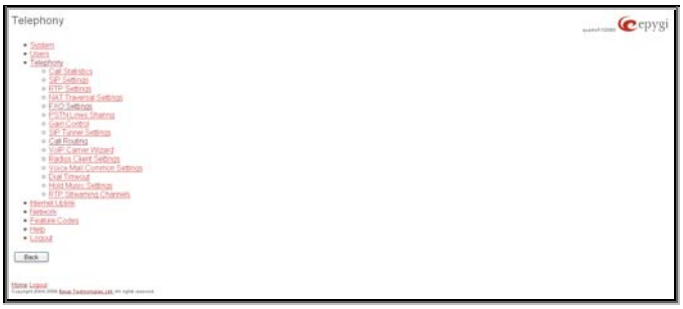


Fig. II-77: Telephony Menu in Plain Theme

Call Statistics

The **Call Statistics** page displays four tables. They provide information on successful, unsuccessful and missed incoming and outgoing calls on the first three tables, and statistics settings on the fourth page. Call statistics allows the collecting of call events on the Quadro with their parameters and to search them by various criteria.

The **Statistics Settings** page offers the following input options:

The **Enable Call Reporting** checkbox enables Call Statistics reporting. The selected number of statistics entries will be displayed in the Call Statistics tables.

The **Maximal Number of Displayed Call Records** drop down lists are used to select the number of **Successful**, **Missed** and **Unsuccessful Outgoing** statistics entries to be displayed in the corresponding **Call Statistics** tables. If the record numbers exceed the numbers specified in these drop down lists, the oldest record will be removed.

The **Download All Call Statistics** link is used to download whole displayed statistics in a file that can be viewed with a simple text editor. This type of call statistics file is more easy-to-read and can be aligned in a spreadsheet.

The **Download All Call Statistics (old format)** link is used to download whole displayed statistics in an old formatted file. This file can also be viewed with a simple text editor but contains more intricately aligned content.

The **Clear all Records** button is used to clear all statistics records.

Fig. II-78: Call Statistics Settings page

When the number of Call Statistics entries exceeds the numbers specified in the **Statistics Settings** page, the oldest entries are being automatically deleted. In order to keep the call statistics entries safe, Quadro allows you to configure an automatic download service of the call statistics.

The **Automatically Download** page is used to configure the automatic downloading of the call statistics. Two options of downloading the call statistics are available: uploading the call statistics file to the server or sending it to the mailing address. This page consists of the following components:

The **Enable Automatically Download Call Statistics** checkbox enables automatic downloading mechanism of the call statistics. **Please Note:** This service only refers to the statistics collected from the moment of enabling this service and forward; any previously generated statistics will not be downloaded.

The **Number of Call Records to Download** drop down list is used to select the portion size of the call statistics (including all types of call statistic, i.e. successful, missed and unsuccessful outgoing call statistics, in the timing order) which will be downloaded to the server or send per email. The number selected in this drop down list indicates the number of entries in the single downloaded call statistics file. If there are no enough entries in the call statistics table on the Quadro, the system will wait until the necessary number of entries will be collected and then will upload the statistics file to the server or send it to the email address.

Fig. II-79: Call Statistics – Automatically Download page

The following group of manipulation radio buttons allows you to select whether the call statistics files will be delivered by email or stored in some location on the server:

- The **Send via Email** radio button is used to send the call statistics files via email. The selection enables **Email Address** text field that requires the email address of the administrating person to receive the call statistics files.
- The **Send to Server** radio button is used to store the call statistics files on a remote server. This selection enables the following fields to be inserted:

  The **Server Name** requires the IP address or the host name of the remote server.

  The **Server Port** requires the port number of the remote server.

  The **Path on Server** requires the path on the server to store the call statistics files in.

  The **Send Method** manipulation radio buttons allow you to select the remote server type: TFTP or FTP. In case of FTP selection, the authentication username and the password need to be inserted. In case these fields are left empty, anonymous authentication will be used.

The **Download Now** button is used to perform a manually immediate download of the call statistics.

The **Number of Records** displays the current number of statistics entries in the table. For successful calls, **Total Duration, Maximum Duration, Average Duration** and **Minimum Duration** statistics are displayed on top of the table.

The **Call Statistics: Successful Calls, Missed Calls and Unsuccessful Outgoing Calls** pages consist of the general information on successful, missed and unsuccessful calls, search fields and the calls table. The search components are as follows:

From and **To** text fields are used to search by date and time. The data must be entered in either of the following formats: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The time criteria are optional. **From** requires an earlier date and time than the **To** field. If the entered data does not meet this condition, the error message “Minimal date should be less than maximal date” prevents statistics filtering.

From and **To** drop down lists are used to search by duration. The duration has to be selected from the list of values. **From** field must indicate a shorter duration than the **To** field. If the inserted data does not meet this condition, the error message “Minimal duration should be less than maximal duration” prevents statistics filtering.

Calling Phone and **Called Phone** respectively require the caller and called party’s SIP address (see chapter Entering a SIP Addresses correctly), extension or PSTN number as search criteria. Wildcard symbols are allowed here.

The **Call Statistics: Successful Calls, Missed Calls and Unsuccessful Outgoing Calls** tables are lists of successful, missed and unsuccessful incoming and outgoing calls and their parameters (Call Start Time, Call Duration, Call destinations). Each column heading in the tables is a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

The **Details** column is only present in **Successful Calls** table and provides the following information:

- Brief information about the call quality, voice codec used to receive and transmit packets and the close call reason. The close call reason appears to provide more information about the call termination reason which can be a network problem, termination by one of the call parties, voice mail service activation, etc. Clicking on the details information will open the Error! Not a valid bookmark self-reference. page where all RTP parameters of established call are provided.

Fig. II-80: Call Statistics page

- **Authenticated By** information about the callers that passed an authentication on the Quadro as configured in the Local AAA Table.
- Information about FAX statistics for the calls that have a FAX transmission handled. It only appears when there was a FAX transmission during the call. Clicking on the FAX link in the Details column will move to the FAX Statistics page.

The **Call Detail** column is present only in the **Unsuccessful Calls** table and indicates the reason why the call was unsuccessful.

The **Filter** performs a search procedure by the selected criteria. The search may be done with several criteria at the same time.

The **Download Call Statistics** links are available below all Call Statistics tables and allows you to download the displayed call statistics in a text file.

To Enable/Disable the Statistics

1. Enter the **Call Statistics Settings** page.
2. Select or deselect the **Enable Call Reporting** checkbox to enable or disable statistics recording.
3. If enabling the statistics, the maximum number of records to be stored in the statistics table should be selected from the corresponding drop down lists.
4. Press **Save** to apply the new configuration.

To Filter the Statistics

1. Enter the desired criteria fields.
2. Press the **Filter** button to search the call reports within the **Call Statistics** table.

Please Note: To return to the complete **Statistics Table**, clear all search criteria and press **Filter**.

To Reset the Statistics

1. Press the **Clear All Records** button in the **Call Statistics Settings** page.
2. Confirm the deletion by clicking on **Yes**. The call statistics will then be deleted. To abort the deletion and keep the statistics information, click on **No**.

RTP Statistics

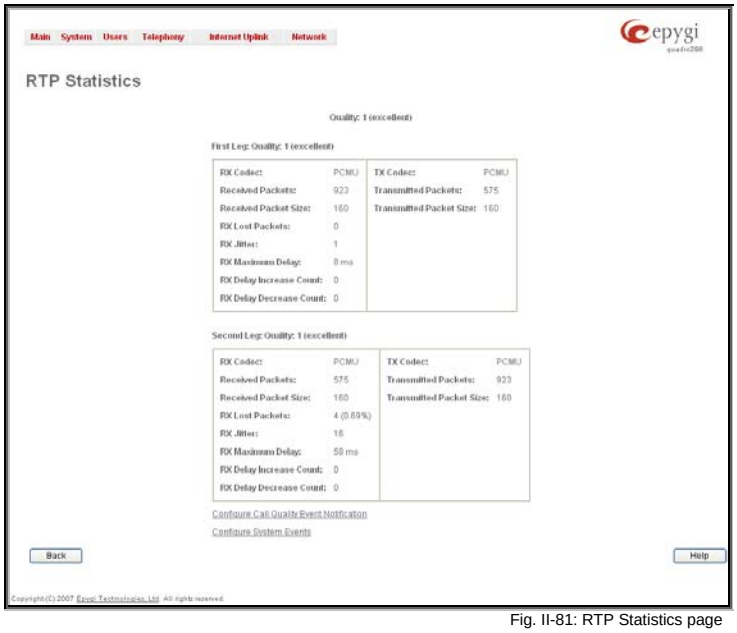


Fig. II-81: RTP Statistics page

The **RTP Statistics** page provides detailed information about the established call is provided. When Quadro serves as an RTP proxy, this page displays two groups (legs) of RTP statistics. For example, when calling from an IP Phone attached to the Quadro's IP line to an external SIP destination or from one external SIP destination to another through the Quadro's Auto Attendant. Each group of parameters describes characteristics of a piece of RTP stream composing an overall SIP session. Normally, one leg describes the RTP stream from caller to the Quadro and the other leg describes the RTP stream from Quadro to the destination.

Quality - estimated call quality, which depends on RTP statistic. Below is the legend for Call Quality definitions on the displayed RTP Statistics:

excellent – RX Lost Packets < 1% & RX Jitter < 20
good - RX Lost Packets < 5% & RX Jitter < 80
satisfactory - RX Lost Packets < 10% & RX Jitter < 150
bad - RX Lost Packets < 20% & RX Jitter < 200
very bad - RX Lost Packets > 20% or RX Jitter > 200

The **Source** and **Destination** fields indicate the two peers between which the RTP stream is transmitted. The characteristics in the table below describes to the piece of RTP stream between these peers.

Rx/Tx Codec - codec for received and transmitted RTP stream respectively.

Rx/Tx Packets - number of RTP packets received and transmitted respectively.

Rx/Tx Packet Size - size of RTP packet (payload) received and transmitted respectively.

Rx Lost Packets - number of lost RTP packets for received stream.

Rx Jitter - inter-arrival jitter is an estimate of the statistical variance of the RTP data packet inter-arrival time, measured in timestamp units.

The inter-arrival jitter is defined to be the mean deviation (smoothed absolute value) of the difference D in packet spacing at the receiver compared to the sender for a pair of packets. If Si is the RTP timestamp from packet i, and Ri is the time of arrival in RTP timestamp units for packet i, then for two packets i and j, D may be expressed as:

$D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)$

$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16$, where J(i) is Rx Jitter for packet i.

For more details about Jitter calculations, please refer to the RFC1889.

Rx Maximum Delay - maximum variance (absolute value) of actual arrival time of the RTP data packet compared to estimated arrival time, measured in milliseconds.

If Si is the RTP timestamp from packet i, and Ri is the time of arrival in RTP timestamp units for packet i, then variance for packet i may be expressed as following: $V(i) = |(Ri - R1) - (Si - S1)| = |(Ri - Si) - (R1 - S1)|$

Rx Maximum Delay = max V(i) / 8

RX Delay Increase Count – indicates the number of times the delay in jitter buffer is increased during the call.

RX Delay Decrease Count - indicates the number of times the delay in jitter buffer is decreased during the call.

Please Note: RTP Statistics is logged only when at least one of the call endpoints is located on the Quadro. For example, it will not be logged when:

- calls incoming from or addressed to the IP lines or remote extension,
- calls from an external user are routed to another external user through Quadro's routing rules.

In the first case, RTP statistics will be logged if remote extension or IP line user is calling locally to the Quadro's extension or auto attendant.

The **Configure Call Quality Event Notification** link leads to the **Configure Call Quality Event Notification** page where call quality control notification specifics can be configured.

From the **Configure Call Quality Event Notification** page you may configure event notification policy when the call quality is lower than the allowed level.

This page consists of a **Notify** checkbox, which enables the call quality monitoring mechanism for the corresponding event notifications, and a **Call Quality less than** drop down list where the least satisfactory call quality should be selected. When a call with the quality less than the level selected here is registered on the Quadro, an event notification will appear. When the **Notify** checkbox is disabled, no Call Quality events will occur on the Quadro.

Please Note: The ways of notification for the Call Quality events should be configured from the Events page.

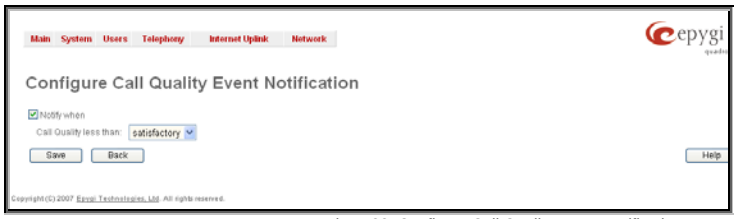


Fig. II-82: Configure Call Quality Event Notification page

The **Configure System Events** link leads to the Events page where the methods of notification for each system event can be configured.

FAX Statistics

The **FAX statistics** page is accessed from the Call Statistics page by clicking on the **FAX** link in the **Details** column for the calls that contain T.38 FAX transmission.

The **FAX statistics** page provides information about received and transmitted packets, lost, bad and duplicated packets. This statistics refers only to the T.38 FAX transmission. The FAX statistics is not available for the FAX transmitted with other protocols.

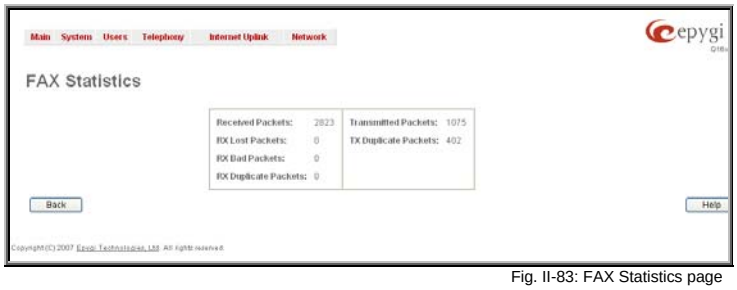


Fig. II-83: FAX Statistics page

SIP Settings

The **SIP Settings** provide information on the SIP receive UDP and TCP ports and allows you to select DNS server configurations for SIP and the SIP timers scheme.

The **UDP Port** indicates the SIP UDP (User Datagram Protocol) receive port number. By default 5060 is selected and used. The SIP UDP port cannot be in the selected RTP/RTCP port range for FXS and IP lines (see RTP Settings), otherwise the "Mapped port for SIP shouldn't be in RTP port range" error message appears.

The **TCP Port** indicates the SIP TCP (Transmission Control Protocol) receive port number. By default, 5060 is selected and used.

Please Note: Quadro will not use TCP protocol as a transport for SIP messages if the **TCP Port** field is left empty.

The **TLS Port** indicates the SIP TLS (Transport Layer Security) receive port number. By default, TLS port is not used and is empty (coded to 0). **TLS port** number should be different from the **TCP Port** number.

The **Reaml** text field requires messaging level information to be included in SIP messages sent by Quadro. This information might be used by remote side for authentication purposes.

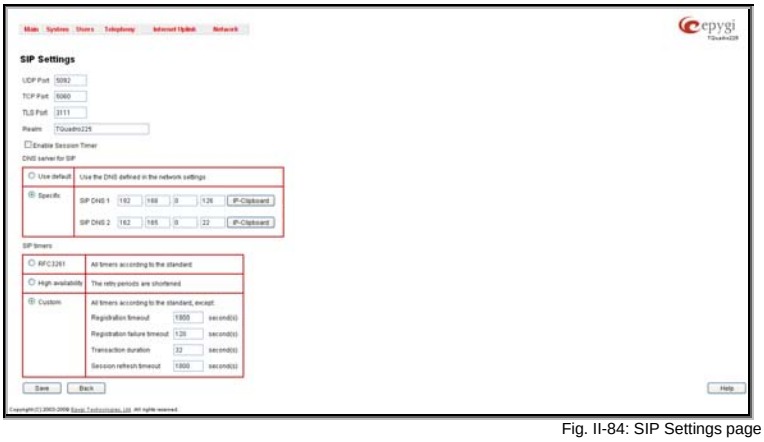


Fig. II-84: SIP Settings page

Enable Session Timer enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.

The **DNS server for SIP** radio button group allows you to choose between regular DNS servers configured in the DNS Settings page and specific DNS servers for SIP traffic.

- **Use default** is used to apply regular DNS servers for SIP traffic.
- **Specific** is used to enable SIP specific DNS servers. For this selection, both primary and secondary SIP DNS servers should be defined in the **SIP DNS 1** and **SIP DNS 2** text fields. At the least, a primary DNS server should be inserted.

The **SIP Timers** radio button group is used to define the timeouts of the SIP messages retransmission.

- **RFC 3261** will apply standard SIP timers described in the corresponding specification.

- **High availability** will apply SIP timers to shorten the call establishment, registration confirmation and registration failure procedures. This selection provides more firmness to the SIP connection but increases the network traffic on the Quadro.
- **Custom** allows manually defining the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session refresh timeout** SIP timers (in seconds).

RTP Settings

The **RTP Settings** page allows the administrator to configure the codec's packet size and silence suppression for each voice codec, to select the G726 codec standard, to define RTP/RTCP port ranges, etc. All parameters listed on this page may be modified and submitted.

The **Codec Properties** table lists all codecs with the corresponding packetization interval and information about silence suppression.

Edit opens the **Edit RTP Settings** page where the codec settings can be modified. To use **Edit**, only one codec may be selected at a time, otherwise the "One record should be selected" error message appears.

The **Packetization Interval** is the time interval between two RTP packets of the same stream. If the interval is increased, the overhead is decreased but the voice quality may deteriorate as a result. If the interval is decreased, the network load is increased and the delay is reduced.

Silence Suppression disables RTP packet transmission in case of no voice activity. This feature helps to avoid extra traffic if the RTP stream contains no voice activity. It is activated after two seconds of silence and restarted immediately if any audio appears.

The **G.726 Standard** radio buttons are used to select between packaging the G.726 codewords into octets. If you experience problems with the G.726 voice quality when one of these packaging is selected, try a different one.

- If **Use ITU_T specification** is selected, the ITU I.366.2 ("AAL2 type 2 service specific convergence sublayer for narrow-band services") type packaging of codewords is used, where packing code words into octets is starting from the most significant rather than the least significant digit in the octet.
- If **Use IETF RFC** is selected, the IETF RFC ("RTP Profile for Audio and Video Conferences with Minimal Control") type packaging of codewords is used, where packing code words is starting from the least significant position in the octet.

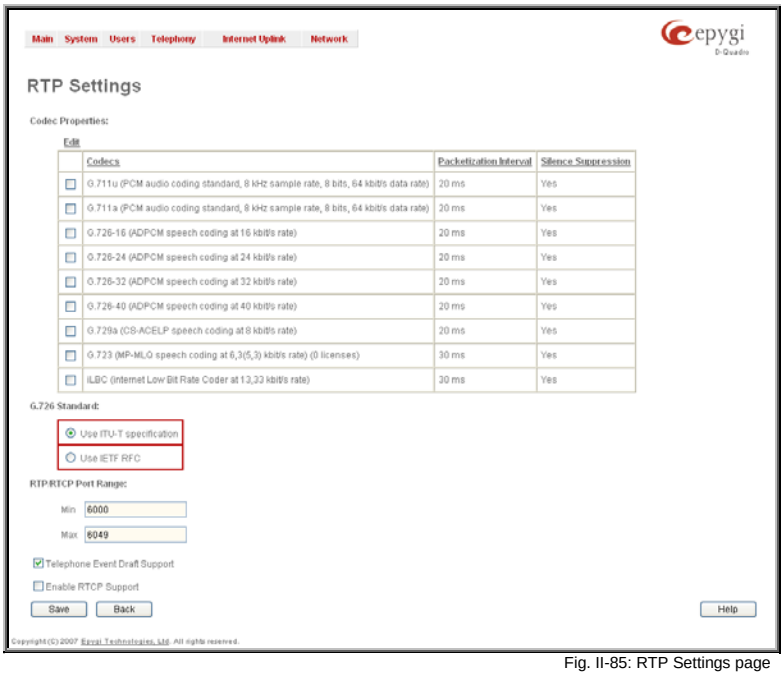


Fig. II-85: RTP Settings page

RTP/RTCP Port Range for FXS Lines:

- **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.
- **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

Since the specified maximum port has to be higher than the minimum port, the error message "Min port number should be less than max port number" will appear if this condition is not met. The port range must consist of digits only, otherwise the error "Incorrect Port Range: only Integer values allowed" will appear. The difference between Max and Min RTP ports should be 100 ports or less (according to the system's capabilities) otherwise the corresponding warning appears. RTP/RTCP Port ranges cannot include the defined SIP UDP ports (see SIP Settings) otherwise an error message will appear.

Telephone Event Draft Support enables telephony events transmission according to the draft-ietf-avt-rfc2833bis-04. The checkbox needs to be toggled if the SIP destination party phone or IVR has problems recognizing DTMFs generated by the Quadro.

Enable RTCP Support enables Real Time Control Protocol support and allows for the RTCP packets transmission. RTCP protocol is used for monitoring the RTP streams and changing RTP characteristics depending on Network conditions.

The **RTP Settings – Edit Entry** page offers a drop down list and a checkbox.

Packetization Interval contains possible values (in milliseconds) to be configured for the selected codec.

The **Enable Silence Suppression** checkbox selection enables voice activity detection for the selected codec.

Fig. II-86: RTP Settings - Edit Entry

To Edit Codec Parameters

1. Select the codec from the **Codecs Table** that is to be edited.
2. Press the **Edit** button on the **RTP Settings** page. The **Edit Entry** page will appear in the browser window.
3. Change values in **Packetization Interval** and/or enable/disable **Silence Suppression**.
4. To save the codec settings press **Save**, or to keep the initial data click **Back**.

NAT Traversal Settings

The **NAT Traversal Settings** page is divided into separate pages used to configure General NAT settings, SIP NAT parameters, RTP and STUN parameters for NAT and a page where the NAT Exclusion table may be filled.

The **General Settings** page consists of a manipulation radio buttons group to select the mode of the NAT Traversal usage for the SIP traffic (any incoming and outgoing SIP messages from and to the Quadro will be routed through the NAT PC).

- **Automatic** – with this selection, system will analyze the Quadro's WAN IP address and if it is in the IP range specified for local networks (according to RFC), the SIP traffic will be routed through NAT. Otherwise, if Quadro's WAN IP address is outside the specified IP range, no SIP traffic will be routed through NAT server.
- **Force** – with this selection, all SIP traffic will be routed through NAT server.
- **Disable** – with this selection, no SIP traffic will be routed through NAT server.

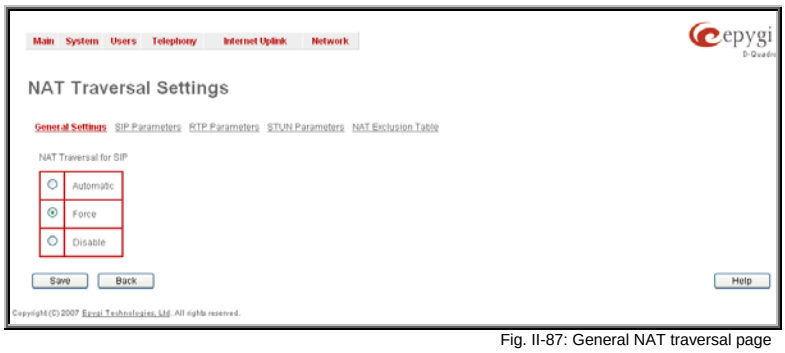


Fig. II-87: General NAT traversal page

The **SIP Parameters** page is used to configure NAT specific settings for SIP and offers two independent groups of settings:

UDP Parameters:
Manipulation radio buttons allow you to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the SIP UDP traffic over NAT. STUN settings are configured on the STUN parameters page (see below).

Selecting **Use Manual NAT Traversal** allows you to manually define the mapped settings for the SIP UDP traffic over NAT:

Mapped Host requires the IP address of the mapped host for SIP UDP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP UDP traffic over NAT.

TCP Parameters:

Mapped Host requires the IP address of the mapped host for SIP TCP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP TCP traffic over NAT.

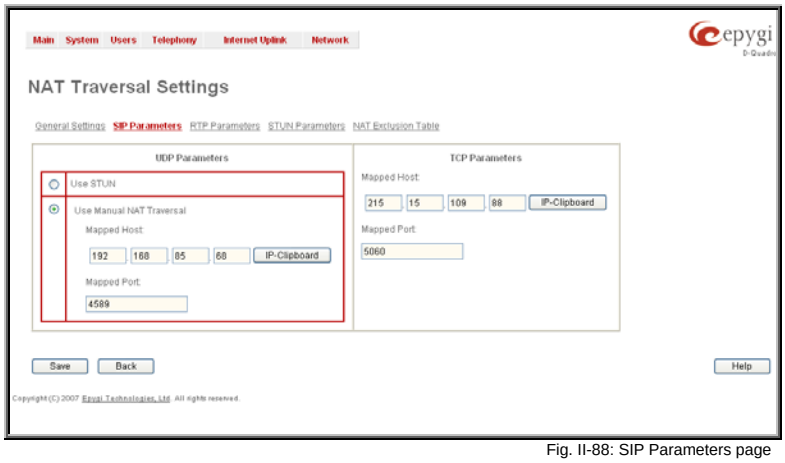


Fig. II-88: SIP Parameters page

The **RTP Parameters** page is used to choose between the STUN and Manual NAT traversal connection for the RTP traffic and to define the RTP/RTCP ports for the connection over NAT.

Manipulation radio buttons allow you to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the RTP UDP traffic over NAT. STUN settings are configured on the STUN Parameters page (see below).

Selecting **Use Manual NAT Traversal** allows you to manually define the RTP/RTCP port ranges for the RTP traffic over NAT:

- The **Mapped Host** text fields require the Mapped Host for RTP traffic over NAT.
- **Mapped RTP/RTCP Port Range for FXS Lines**:
  - **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.
  - **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

Please Note: RTP/RTCP Mapped Port ranges should be greater than or equal to the RTP/RTCP port ranges defined on the RTP Settings page.

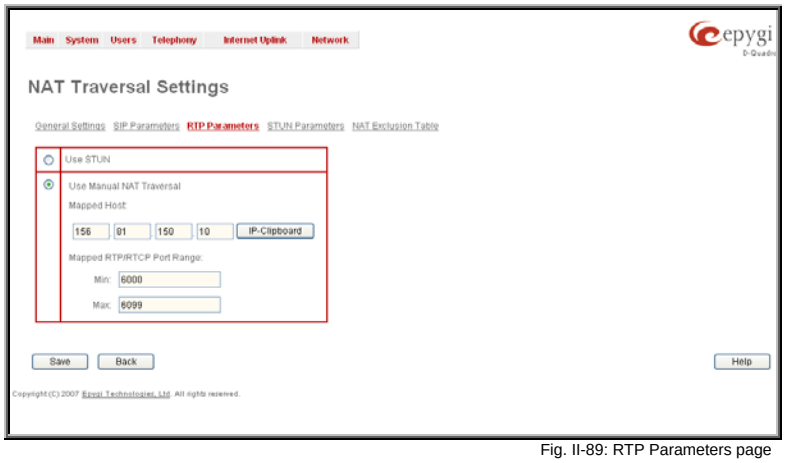


Fig. II-89: RTP Parameters page

The **STUN Parameters** page enables automatic NAT configuration through the STUN server and is used to configure the STUN (Simple Traversal of UDP over NAT) client on the Quadro. This page requires the following data to be inserted:

The **STUN Server** text field requires the STUN server's hostname or IP address. The **STUN Port** text field requires the STUN server port number.

The **Secondary STUN Server** and **Secondary STUN Port** text fields respectively require the parameters of the secondary STUN server.

The **Polling Interval** drop down list contains the possible time intervals between referrals to the STUN server.

The **Keep-alive interval** text field provides the options to select the time interval (in seconds) for keeping NAT mapping alive. The value should be in the range of 10 to 300 seconds.

The **NAT IP checking interval** text field indicates the interval (in seconds) between the NAT IP checking attempts (used to distinguish the possible NAT IP address changes and to perform registration on the new host). The value should be in the range of 10 to 3600.

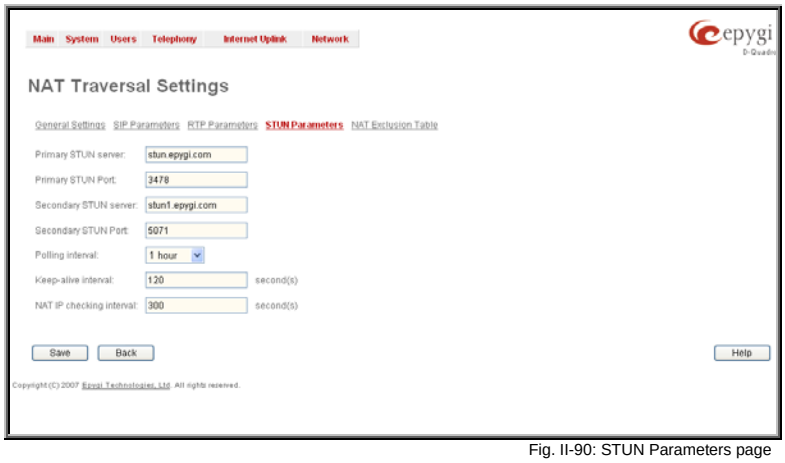


Fig. II-90: STUN Parameters page

The **NAT Exclusion Table** page includes a table where all possible IP ranges are listed that allows you to exclude some network addresses from being NATed. For example, if a Quadro user needs to make SIP calls within the local network as well as outside of that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table. Otherwise, a malfunction may occur in SIP operations.

The **NAT Exclusion Table** page offers the following input options:

Each record in the table has a corresponding checkbox assigned to its row. The checkbox is used to delete or to edit the corresponding record. Only one record may be edited at a time. An error message will appear if no selection is made or more than one is selected.

Each column heading in the table is a link. By clicking on the column heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The **Add Entry** page includes the following text fields:

Add opens the **Add Entry** page where a new IP range can be added.

Edit opens the **Edit Entry** page where the IP range can be modified. This page includes the same components as the **Add Entry** page.

The **NAT Exclusion Table** lists all possible IP ranges that are not included in the NAT process, but may be accessed directly. IP addresses that are not listed in the **NAT Exclusion Table** are accessed over NAT.

Fig. II-91: NAT Exclusion Table page

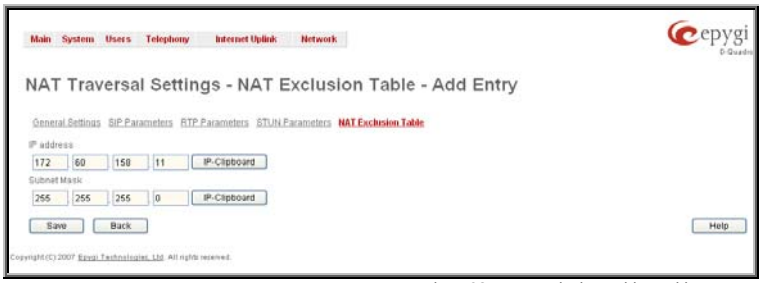


Fig. II-92: NAT Exclusion Table - Add Entry page

IP address requires the IP address that is placed behind NAT within the local network.

Subnet Mask requires the subnet mask corresponding to the specified IP address.

To Configure the NAT Exclusion Table

1. Press the **Add** button on the **NAT Exclusion Table** page. The **Add Entry** page will appear in the browser window.
2. Specify an **IP Address** and its **Subnet Mask** in the corresponding text fields.
3. Press **Save** on the **Add Entry** page to add the selected IP range to the **NAT Exclusion Table** list.

To Delete an IP Range from the NAT Exclusion Table

1. Select the checkboxes of the corresponding IP range(s) that should to be deleted from the **NAT Exclusion Table**. Press **Select all** if all IP ranges should to be deleted.
2. Press the **Delete** button on the **NAT Exclusion Table** page.
3. Confirm the deletion by pressing **Yes**. The IP range will then be deleted. To abort the deletion and keep the IP range in the list, press **No**.

FXO Settings

The **FXO Settings** are used to configure the FXO support that allows Quadro to connect to other PBXs or analog telephone lines. The **FXO Settings** also gives you the option to limit incoming or outgoing calls for the selected FXO line if required. Depending on the Quadro model, several FXO ports will be available on the board, thus giving you the option connect several PSTN lines to the Quadro and to use them simultaneously.

The administrator may assign a default recipient for each FXO line where calls from the Central Office (PSTN) will be routed. The assigned recipients become the Quadro "default users". If the Quadro Auto Attendant has been selected as a "default user", a caller from the PSTN needs to go through the attendant menu to reach the desired extension.

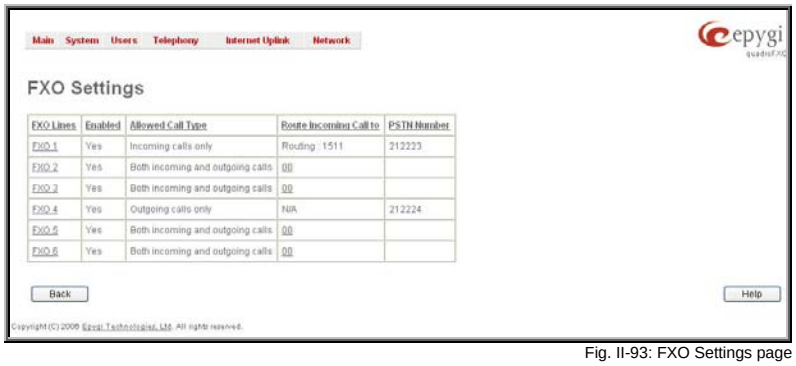


Fig. II-93: FXO Settings page

The **FXO Settings** page lists the available local FXO lines, shared FXO lines on the remote devices (if any) and their settings. If the FXO service has been disabled, the **Allowed Call Type**, **Route Incoming Call to** and **PSTN number** columns are set to N/A.

Clicking on the FXO line number will open the **FXO Settings - FXO#** page where the FXO line settings may be modified.

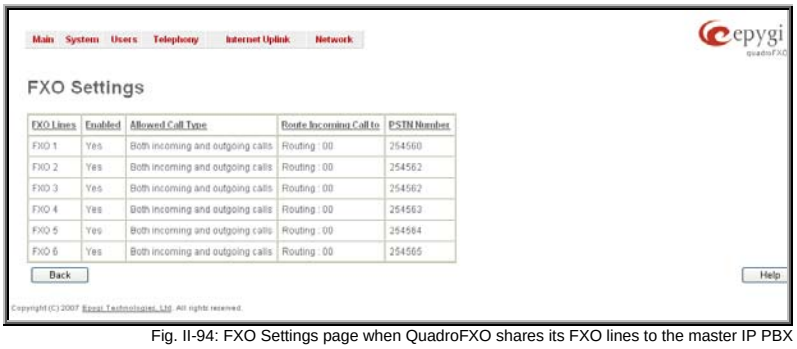


Fig. II-94: FXO Settings page when QuadroFXO shares its FXO lines to the master IP PBX

If PSTN Lines Sharing is enabled and QuadroFXO acts as an FXO line expansion device, i.e. provides its FXO lines to the remote Quadro IP PBX, the FXO Settings page becomes read-only. Any modifications in the shared FXO line's settings on the master Quadro will be immediately reflected in the FXO Settings table on the slave Quadro.

Routing:smth will be seen in the **Route Incoming Calls To** column once the Sharing Mode is enabled, where **smth** is the destination the call is routed to on the Quadro IP PBX. Exceptions are cases when **Outgoing Calls Only** is selected for **Allowed Call Type**, in this case **N/A** will be displayed in the **Route Incoming Calls To** column.

The **Enable FXO** checkbox selection activates FXO support for the selected FXO line.

The **Allowed Call Type** is used to choose the allowed call directions for the corresponding FXO line. The administrator may choose between:

- **Enabling incoming calls** (prohibiting outgoing calls) for the selected FXO line.
- **Enabling outgoing calls** (prohibiting incoming calls) for the selected FXO line.
- **Enabling both incoming and outgoing calls** for the selected FXO line.

The **Route incoming FXO Call to** manipulation radio buttons group allows you to define the destination where incoming calls addressed to the corresponding FXO line will be forwarded to.

- **Extension** – this selection allows you to choose the local PBX user or auto attendant extension to forward calls. If an inactive extension is chosen from this list, the voice mail system will answer the call addressed to the corresponding FXO line. If the Auto Attendant extension is chosen, it will become the "default user" for the corresponding FXO line on the Quadro.
- **Routing** – this selection allows you to forward the incoming calls to the destination defined through Call Routing. This selection requires you to enter a routing pattern to the corresponding field. Based on the registered PSTN users, the caller will be able to reach the destination according to configurations in Call Routing Table.

By choosing a destination, the Quadro administrator virtually assigns a default number that will start ringing when a call is initiated to the Quadro's PSTN number.

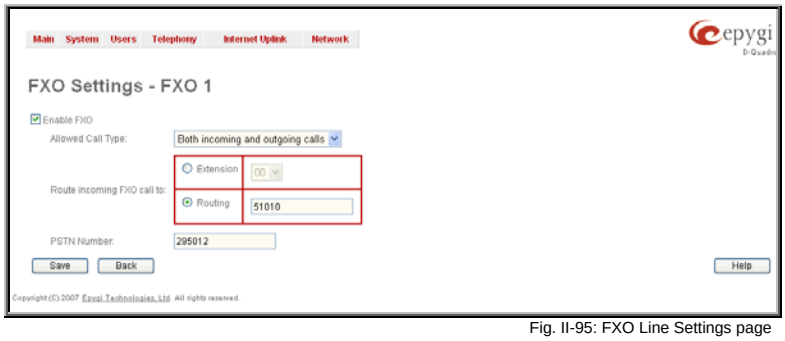


Fig. II-95: FXO Line Settings page

The **PSTN Number** text field allows you to enter the PSTN number that the current FXO line is attached to. The field value is optional and used as an identification parameter for FXO lines. The field value can be left empty.

Alternative AC Termination Mode appears if the local country (Germany, Israel, France, etc.) selected for Quadro has two COs that use different types of AC termination. Contact your CO to learn about your AC termination mode. Selecting the checkbox may help if the voice quality over FXO is poor or an echo is noticed.

To modify the FXO Settings

1. Select the FXO line number from the **FXO Settings** table. The **FXO Settings -FXO#** will appear where the line settings may be modified.
2. Enable the FXO line to receive calls from PSTN. To reject calls from/to the PSTN deselect the **Enable FXO** checkbox.
3. If FXO has been enabled, select the **Call Type** from the **Allowed Call Type** drop down list and the extension from the **Route FXO Call to** drop down list to route the FXO calls correspondingly.
4. Insert a **PSTN number** in the same named text field to identify the FXO line.
5. Enable **Alternative AC Termination Mode** if your CO so requires.
6. Press **Save** to submit the FXO line settings.

PSTN Lines Sharing

PSTN Lines Sharing page is used to configure QuadroFXO to act as an FXO expansion device for the remote Quadro IP PBX, i.e. to share its FXO lines to the master Quadro IP PBX. This provides Quadro IP PBX a possibility to call not only through local FXO lines but also through available shared FXO lines on the QuadroFXO.

When PSTN Lines Sharing is enabled, FXO Settings page becomes read-only on QuadroFXO and corresponding routing patterns are automatically created in the Call Routing table. Also following dependencies are applicable:

- Information defined in **PSTN Number** text field, as well as the configured **Allowed Call Types** for each of the FXO lines on the QuadroFXO will be transparent to Quadro IP PBX upon enabling the sharing mode.
- Independent of the configuration on the QuadroFXO, the incoming calls on all shared FXO lines will be automatically routed to the default Auto Attendant (00) once FXO sharing is activated. Occasionally, routed destinations can be then changed on Quadro IP PBX.
- Any changes applied to the configuration of shared FXO lines on Quadro IP PBX will be automatically reflected in the **FXO Settings** page and **Call Routing** table on the QuadroFXO device.

PSTN Lines Sharing page consists of the following components:

The **Provide PSTN lines for master device** checkbox is used to share the existing FXO lines to the remote Quadro.
Username and **Password** text fields are used to enter the identification parameters for the authentication on the remote Quadro IP PBX. In its turn, these authentication settings should be added in the **Authorization Parameters** table on the master Quadro IP PBX.
Master device IP text field requires the IP address of the master Quadro current FXO lines will be shared for.
Master device port text field requires the port number of the master Quadro current FXO lines will be shared for.
Registration State and **Registration Date/Time** fields indicate read-only information about the last successful registration on the master Quadro (i.e. when authentication was successful), its state and the registration date/time.

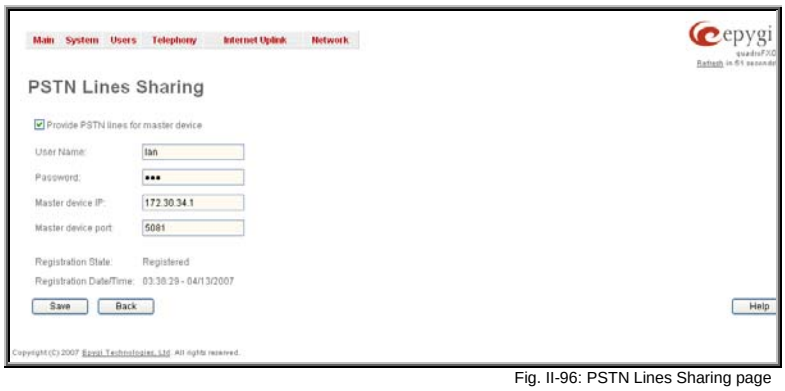


Fig. II-96: PSTN Lines Sharing page

Please Note: Any settings synchronization between the master and slave devices may take up to 60 seconds.

Gain Control

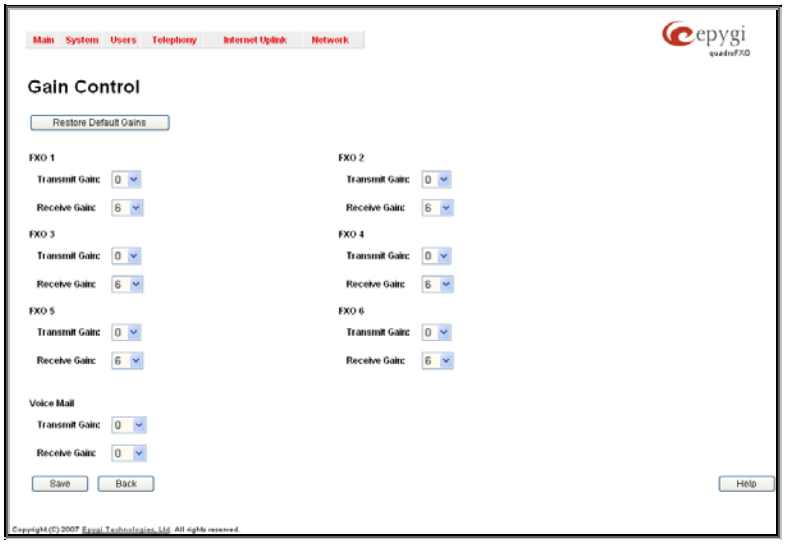


Fig. II-97: Gain Control page

The **Gain Control** settings are used to define transmit and receive gains.

For FXO lines:

Transmit Gain defines the level of voice transmitted from Quadro to the PSTN network.

Receive Gain defines the volume of voice received by Quadro from the PSTN network.

For Voice Mail:

Transmit Gain defines the volume of the phone microphone upon playing voice mails or system messages.

Receive Gain defines the phone speaker volume upon playing voice mails or system messages.

The **Gain Control** page offers **Transmit Gain** and **Receive Gain** drop down lists for each line that contains allowed gain values, which can be set up by the administrator for every line.

Please Note: If the gain control has been configured incorrectly, DTMF digits may not be properly recognized. Gain control settings are strictly dependent on the location (country) of Quadro and the phone type. If a private PBX is attached to the FXO port on the Quadro, the voice level in the handset of the phone connected to the Quadro FXS port may be too loud (depending on the PBX type and configuration). This can be adjusted by decreasing the FXO **Receive Gain** to three or to zero.

The **Restore Default Gains** button restores the default values.

SIP Tunnel Settings

The **SIP Tunneling** service is used to build a tunnel between Quardos and to use that tunnel for routing the SIP calls through the remote Quadros. When this service is enabled, slave Quadros should be registered on the master Quadro with the corresponding username/password. With the appropriate configuration done on the master Quadro, the master device can use the slave Quadros for routing the SIP calls through them and accessing peers located behind the slave Quadro or recognized by it. This enables the master Quadro to locate the slave, even when the network settings, like IP address, SIP port and other settings are changed on the slave Quadro.

When the **SIP Tunneling** service is enabled, virtual tunnels between the master and its slaves are created. A possibility to use the created SIP tunnels will be automatically enabled in the Call Routing table.

Optionally, a SIP tunnel can be mutually established on two Quadros allowing to route SIP calls back and forth. A Quadro can be at the same time configured both as a slave and as a master to the same remote device, i.e. the slave Quadro can act as a master for the master device it is registered on. For example, the Quadro1 can act as a slave for the Quadro2. In its turn, the Quadro2 can act as a slave for the Quadro1. With this configuration and the corresponding routing rules added in the Call Routing table on both devices, the SIP calls will be routed from Quadro1 to Quadro2 and vice versa.

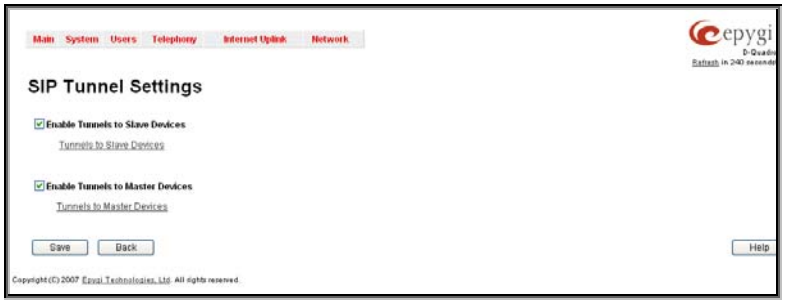


Fig. II-98: SIP Tunnel Settings page

The **SIP Tunnel Settings** page is used to enable the Quadro as a slave or master device for SIP tunneling. The page consists of the following components:

The **Enable Tunnels to Slave Devices** checkbox enables the Quadro as a master device and allows you to configure the SIP tunnels to the slave Quadros. When this checkbox is enabled the **Tunnels to Slave Devices** table needs to be configured.

The link **Tunnels to Slave Devices** moves you to the page where a list of slave devices needs to be defined.

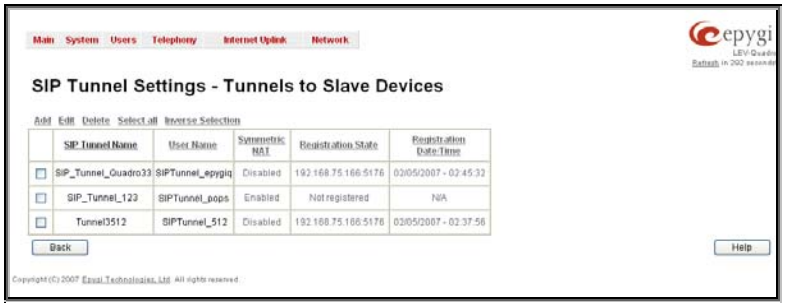


Fig. II-99: SIP Tunnel Settings – Tunnels to Slave Devices page

The **Tunnels to Slave Devices** page consists of a table where slave devices are listed with the corresponding authentication parameters.

Add functional button leads to the **Add Entry** page where a new slave device parameters needs to be provided.

The **Add Entry** page consists of the following components:

The **SIP Tunnel Name** text field requires the tunnel name for the corresponding connection. System suggests you to start the SIP tunnel name with the "SIP_Tunnel_" words, according to the automatic prefix used for the SIP tunnels on the Quadro, however this is not mandatory.

The **User Name** text field requires the authentication user name. The field in front of this text field displays the default non-editable prefix for SIP tunnels: "SIPTunnel_".

The **Password** text field requires the authentication password.

Please Note: The **User Name** and **Password** should match both on master and slave Quadros for the successful SIP tunnel establishment.

The **Symmetric NAT** checkbox should be selected when the slave Quadro is located behind the symmetrical NAT.

Fig. II-100: SIP Tunnel Settings – Tunnels to Slave Devices – Add Entry page

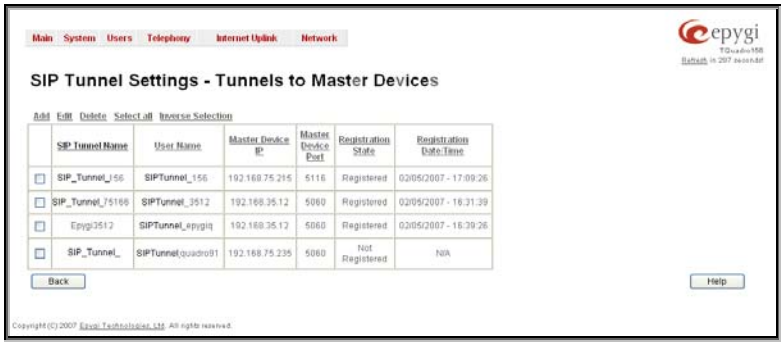


Fig. II-101: SIP Tunnel Settings – Tunnels to Master Devices page

The **Enable Tunnels to Master Devices** checkbox enables the Quadro as a slave device and allows connecting to the master Quadro via SIP tunnel. When this checkbox is enabled the **Tunnels to Master Devices** table needs to be configured.

The link **Tunnels to Master Devices** moves you to the page where a list of master devices needs to be defined.

The **Tunnels to Master Devices** page consists of a table where master devices are listed with the corresponding authentication parameters.

Add functional button leads to the **Add Entry** page where a new master device parameters needs to be provided.

The **Add Entry** page consists of the following components:

The **Enable Registration** checkbox selection is used to enable the registration to the corresponding master device.

The **Tunnel Name** text field requires the SIP tunnel name for the corresponding connection. System suggests you to start the SIP tunnel name with the "SIP_Tunnel_" words, according to the automatic prefix used for the SIP tunnels on the Quadro, however this is not mandatory.

The **User Name** text field requires the authentication user name. The field in front of this text field displays the default non-editable prefix for SIP tunnels: "SIPTunnel_".

The **Password** text field requires the authentication password.

Please Note: The **User Name** and **Password** should match both on master and slave Quadros for the successful SIP tunnel establishment.

Fig. II-102: SIP Tunnel Settings – Tunnels to Master Devices – Add Entry page

The **Master device IP** text field requires the IP address of the master device.

The **Master device port** text field requires the SIP port number of the master device.

The **Registration State** field displays information whether the slave device is registered on the master or not.

The **Registration Date/Time** field displays the time and the date of last registration on the master's device.

Call Routing

The **Call Routing** service simplifies the calling procedure for Quadro users, i.e., different types of calls (internal, SIP, PSTN or IP-PSTN) can be placed in the same way. SIP registration is not needed for extensions to make routing calls.

The **Call Routing** page offers the following components:

- When the **Route all incoming SIP calls to Call Routing** checkbox is disabled, for all incoming SIP calls Quadro will first search the incoming SIP address in the Extensions Management table. If found, the incoming SIP call will ring on the corresponding extension. If not found, Quadro will look for a matching routing rule in Call Routing table.
- When the **Route all incoming SIP calls to Call Routing** checkbox is enabled, for all incoming SIP calls Quadro will directly look for a matching routing rule in Call Routing table and will ignore the possible matches in the Extensions Management table.
- The **Call Routing Table** link leads to the **Call Routing** table where routing patterns may be manually defined.
- The **Local AAA Table** link leads to the page where local AAA (Authentication, Authorization, and Accounting) database can be managed.

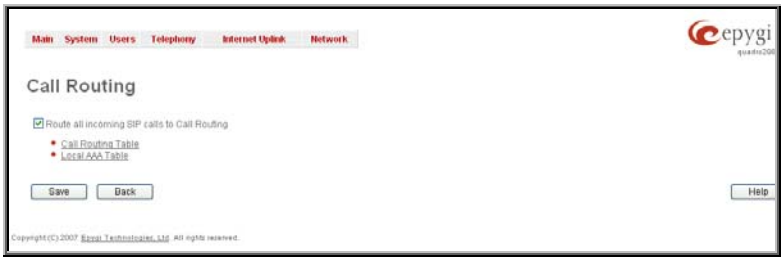


Fig. II-103: Call Routing page

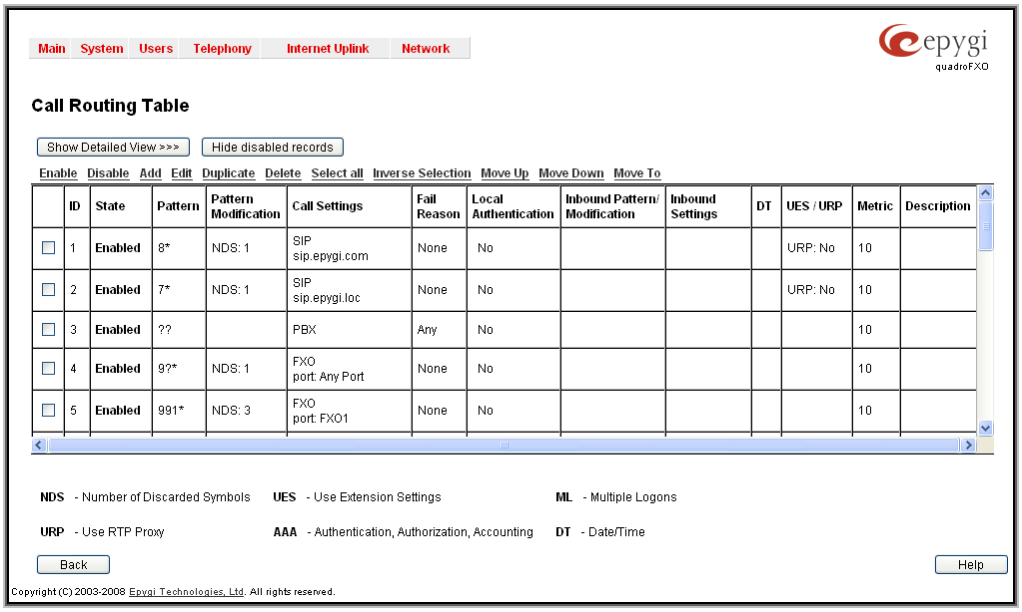


Fig. II-104: Call Routing table – brief preview

Defining patterns in the **Call Routing Table** avoids registering Quadro at the routing management server and gives you an option to establish a direct connection to the destination or to use a SIP server for call routing.
The **Call Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and inbound caller settings, RTP Proxy and Date/Time period settings, metric and description), as well as automatically created and undeletable patterns created as a result of PSTN Lines Sharing.
The alternating **Show Detailed View** and **Show Brief View** buttons are used to display entries in the Call Routing table in detailed and brief views correspondingly. The brief view displays the most important settings of the routing rules. The detailed view displays all settings of the routing rules as they are configured in the Call Routing Wizard (see below).

The alternating **Hide disabled records** and **Show all records** buttons are used to respectively hide or show disabled records in the Call Routing table. The system does not consider the disabled records when parsing the table for the call route.

If the route has an **Authentication** or an **Authentication&Accounting** selected from the **AAA Required** checkbox group, it will have a link to the **Users List** in the **Call Routing table**. The **Users List** page contains a list of authorized users defined from the **Local AAA Table** and gives the option to enable/disable authentication of each user for a particular route.

Since the **Call Routing Table** may have multiple entries that could match to same pattern, the table will be internally rearranged according to the rules with the following consequences:

- The pattern matching best to the Best Matching Algorithm will have the higher position in the rearranged list
- If multiple patterns equally match to the Best Matching Algorithm, the pattern with the lower metric will get the higher position in the rearranged list
- If the multiple patterns with the same metric have been matched to the Best Matching Algorithm, the pattern in the higher position in the table will get the higher position in the rearranged list.

The pattern in the highest position of the rearranged list will be considered as the preferred one. The second and subsequent matching patterns will be used, if the destination refused the call due to the configured **Fail Reason**.

The **Enable/Disable** functional buttons are used to enable/disable the selected route(s). Disabled routes will have no effect. Enabled routes will be parsed when initiating routing calls. The **State** column in the **Call Routing Table** displays the current state of the routes (enabled/disabled).

Add starts the **Call Routing Wizard** where a new routing pattern may be defined. The **Call Routing Wizard** is divided into several pages. Page 1 displays the following components:

The **Enable** checkbox is used to enable the newly created routing rule. By default, this checkbox is selected, so the newly created routing rule will be enabled. But if you wish to create a routing rule for a later use, disable it from this page. The new routing rule will be added to the Call Routing Table but will be disabled and will not be considered when placing calls through the call routing unless it is enabled again.

The **Pattern** text field specifies calls to which the rule should be applied. If a call, either inbound or outbound, has a destination number that matches the specified pattern, it will be completed according to the current rule. A routing pattern may contain wildcards. The complete list of characters and wildcards allowed in this text field is given in the chapter Allowed Characters and Wildcards.

Number of Discarded Symbols (NDS) requires the number of symbols that should be discarded from the beginning of the routing pattern. The field should be empty if digits do not need to be discarded. Only numeric values are allowed for this field, otherwise the error message "Error: Number of Discarded Symbols is incorrect - digits allowed only" will appear.

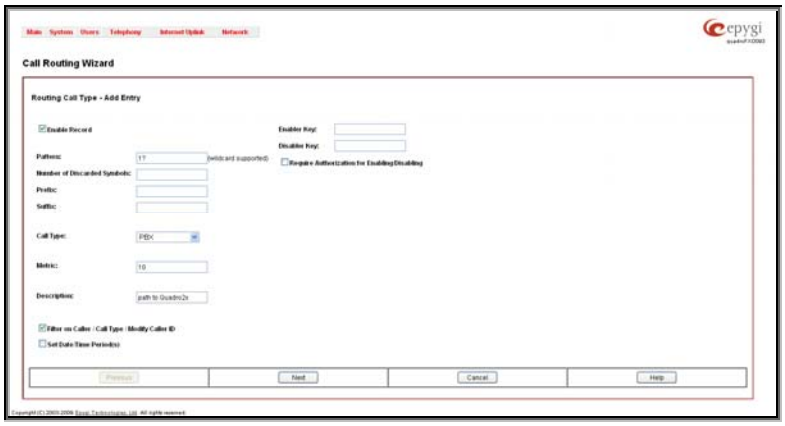


Fig. II-105: Call Routing Wizard - page 1

Prefix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in front of the routing pattern instead of the discarded digits. The following tags can be used for this field:

- <callerid:range> - used to apply the complete or a part of caller ID (the caller's number detected during the call) as a prefix. For example, <callerid:1-3> indicates that the first 3 digits of the caller ID will be considered as a prefix, <callerid:3-end> indicates that the caller ID from its 3rd digit and up to the end will be applied as a prefix. This tag can be used in combination with other digits at the beginning or at the end, as well as with wildcards.
- <dialednum:range> - used to apply the complete or a part of dialed number (the number dialed by the caller to place a call) as a prefix. For example, <dialednum:1-3> indicates that the first 3 digits of the dialed number will be considered as a prefix, <dialednum:3-end> indicates that the dialed number from its 3rd digit and up to the end will be applied as a prefix. This tag can be used in combination with other digits at the beginning or at the end, as well as with wildcards.

Suffix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in the end of the routing pattern. For example, if the routing **Pattern** is 12345, the **Number of Discarded Symbols** is two, and the **Prefix** is 909 and **Suffix** is 0a, the final phone number will be 9093450a.

Call Type gives you the option to select the call type. The following call types are available:

- PBX - local calls to Quadro's extensions
- PBX-Voicemail **-** calls directly to the voice mailbox of the local PBX extension
- SIP – calls through a SIP server
- IP-PSTN – calls through the IP-PSTN provider to the remove PSTN global telephone network
- FXO – calls to a PSTN global telephone network

Metric allows entering a rating for the selected route in a range from 0 to 20. If a value is not inserted into this field, 10 will be used as the default. If two route entries match a user's dial string, the route with the lower metric will be chosen.

The **Description** text field requires an optional description of the routing pattern.

The **Filter on Caller / Call Type / Modify Caller ID** checkbox selection allows limiting the functionality of the current route to be used by the defined caller(s) only. If this checkbox is enabled, inbound caller information (**Inbound Caller Pattern**, **Inbound Call Type, Inbound Port ID**, etc.) will be required later in the **Call Routing Wizard**.

The **Set Date / Time Period(s)** checkbox selection allows you to define a validity period(s) for current routing patterns to take place and to define pattern date/time rules. When this checkbox is enabled, the **Call Routing Wizard** - Page 5 will be displayed.

Require Authorization for Enabling/Disabling checkbox is used to enable administrator's password authentication when enabler/disabler keys are configured for the routing rule. The service can be used locally from the handset (see Feature Codes) or remotely from Auto Attendant (see Auto Attendant Services). When this checkbox is selected, administrator's password will be requested to enable/disable the certain routing rule(s). If the administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.

Enabler Key and **Disabler Key** text fields request digit combination which should be dialed from the handset or Auto Attendant to enable or disable the certain routing rules in the Call Routing Table. You can set the same Enabler/Disabler Key for multiple routing rules (the same key may be used as enabler for one routing rule, and as disabler for another one) - this will allow managing several routing rules with the single key.

The second page of the **Call Routing Wizard** offers different components depending on the **Call Type** selected on the previous page.

Use Extension Settings drop down list is applicable to SIP and IP-PSTN call types and allows you to select the extension (also Auto Attendant) on behalf of the call that will be placed. The SIP settings of the selected extension will be used as the caller information. If an entry is not selected from this list, the original caller information will be kept. When **Keep original DID** checkbox is selected, the called destination will receive the original caller's information and not the information of the extension selected from the **Use Extension Settings** list.

When the checkbox **Add Remote Party ID** is selected, the Remote-Party-ID parameter is being delivered to the destination side upon call establishment procedure.

SIP Tunnel drop-down list appears only when the "SIP_Tunnel" **Call Type** is selected on the previous page. The list is used to select the particular SIP tunnel to route the calls through the corresponding Quadro.

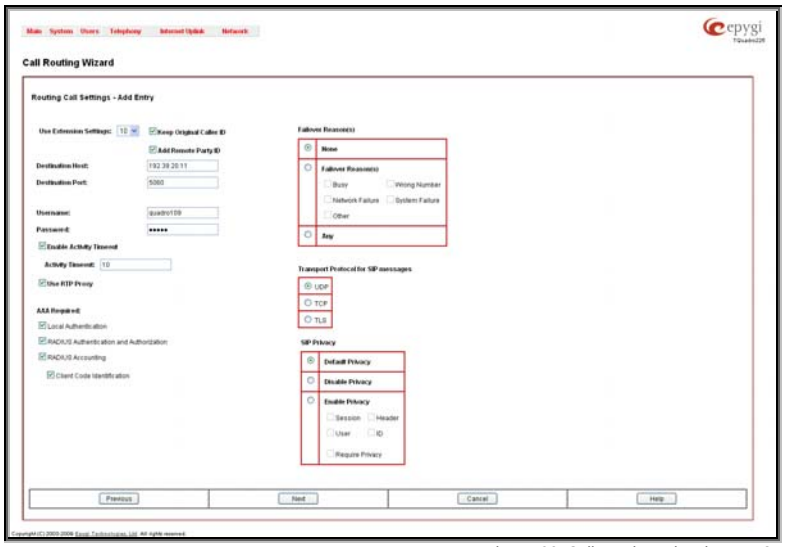


Fig. II-106: Call Routing Wizard - page 2

Destination Host requires the IP address or the host name of the destination (for a direct call) or the SIP server (for calls through the SIP server). This field is named **Modified Destination Host** if the Pattern field on the first page of this wizard contains "@" symbol.

Destination Port requires the port number of the destination or of the SIP server. This field is named **Modified Destination Port** if the Pattern field on the first page of this wizard contains "@" symbol.

User Name and **Password** require the identification settings for the public SIP server or servers requiring authentication.

Enable Activity Timeout checkbox is used to limit time-to-live period of routing pattern (makes sense if accept or failure feedback arrives too late from the destination).

Checkbox selection enables the **Activity Timeout** text field which is used to insert a routing pattern activity timeout (in the range from 1 to 180 seconds). When timeout is configured, the routing pattern will be active within the defined time frame and if no response has been received from the destination during that period, the pattern will be stopped and next routing rule might be optionally considered (depending on the **Fail Reason** configuration on the corresponding pattern).

The **Restrict the Number of Simultaneous Calls** checkbox is only available for IP-PSTN call type and is used to restrict the number of simultaneous calls to the public SIP server with the same username at the same time. This checkbox enables **Allowed Call Count** text field which requires the number of simultaneous calls allowed in a range from 1 to 64. If you leave this field empty, no limitation will apply to the number of simultaneous logons.

The **Use RTP Proxy** checkbox is available for SIP and IP-PSTN call types and is applicable when a route is used for calls through Quadro between peers that are both located outside the Quadro. When this checkbox is selected, RTP streams between external users will be routed through Quadro. When the checkbox is not selected, RTP packets will move directly between peers.

The **AAA Required** checkboxes are used to choose one or more of the following Authentication, Authorization, and Accounting (AAA) settings:

- **Local Authentication** – with this checkbox selected, callers will need to pass authentication through the Local AAA table (see below) when dialing the current pattern.
- **RADIUS Authentication and Authorization** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, callers will need to pass the authentication through RADIUS server (see above) when dialing the current pattern.
- The **RADIUS Accounting** checkbox is accessible when the RADIUS Client is enabled. With this checkbox selected, no authentication will take place, but CDRs (call detail reports) of the calls made through this routing record will be sent to the RADIUS server. This checkbox selection enables the **Client Code Identification** checkbox.

  If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.
- The **Client Code Identification** checkbox selection activates the code identification feature: a caller, after dialing the destination phone number, may optionally enter "*" and then an **Identity Code**. An **Identity Code** is an arbitrary digit string entered by the user to identify a specific call or call group. The **Identity Code** is sent with CDR to the RADIUS server and might be used by a billing program for grouping the calls having the same Identity Code.

The **Check with 3PCC** checkbox is used to request a 3PCC approval before placing a call with the specific routing rule. When this checkbox is selected and the corresponding routing rule is used to place a call, Quadro sends a request to the call controlling application for the managing person to accept or reject the specific call (it can be a popup window or any other type of dialog box, depending on the call controlling application). If the request is accepted, the call will be placed. Otherwise, if the request is rejected, the call will be skipped. In case of no feedback from the call controlling application, the call will be accepted after a timeout defined in the configuration of the call controlling application.

The **Failover Reason(s)** radio buttons indicate whether the system should use the next matching pattern if call setup with the current routing rule fails and allows choosing the reasons to be considered as a failover.

- **None** - indicates that matching patterns should not be used regardless of the failover reason.
- **Failover Reason(s)** - indicates possible failure reasons. Failure reasons vary depending on the call type selected on the previous page. If the call cannot be established due to selected Failure Reasons, the call routing table will be parsed for the next matching pattern and, if found, the call will be routed to the specified destination.
  - **Cannot Establish Connection** - failure reason is available for FXO calls and indicates cases when connection cannot be established.
  - **Busy** - available for PBX, SIP, and IP-PSTN call types and indicates cases when the dialed destination is busy.
  - **Wrong Number** - available for PBX, SIP, and IP-PSTN call types and indicates cases when the dialed number is wrong.
  - **Network Failure** - available for SIP, and IP-PSTN call types and indicates cases when system overload, network failure or timeout expiration occurred.
  - **System Failure** - available for SIP, and IP-PSTN call types and indicates cases indicated in **Network Failure** and **Other** fail reasons.
  - **Other** - available for SIP, and IP-PSTN call types and indicates cases when authorization, negotiation, not supported or request rejected or other unknown errors occur.
- **Any** stands for all failure reasons mentioned in the **Failover Reason(s)** group.

The **Transport Protocol for SIP messages** manipulation radio buttons group is available for **SIP** or **IP-PSTN** call types only and allows you to select the transport (UDP, TCP or TLS) to transmit the SIP messages through.

The **SIP Privacy** manipulation radio buttons group is only available for the **SIP** call type and allows you to select the security of the SIP route by means of hiding (or replacing, depending on the configuration of the SIP server) the key headers of the SIP messages used to establish the call.

- **Default Privacy –** with this selection, Quadro specific SIP privacy will not be applied and all privacy will rely on the configuration of the SIP Server.
- **Disable Privacy –** with this selection, SIP call security will not be disabled and all headers of the SIP message will be transparently visible to the destination.
- **Enable Privacy -** with this selection, SIP privacy will be specified for the corresponding route. This selection enables a group of checkboxes in order to choose the key headers that are to be fully or partly hidden or replaced. The **Require Privacy** checkbox selection is used to restrict the delivery of the SIP message if any of the selected headers cannot be hidden (or replaced, depending on the configuration of the SIP server) before being sent to the destination.

The **Port ID** drop down list for FXO call type is used to configure the FXO ports usage for the corresponding routing rule. **Any Port** selection means the call will be routed through the first available PSTN line. **FXO Port** checkboxes are used to select which FXO ports will be used for the corresponding rule routing. In case if multiple FXO ports are selected here, the first available port will be used.

The **FXO Lines Load Balancing** drop down list is used to enable load balancing mechanism on the PSTN lines. The None selection in this list means that no load balancing will be applied and the call will be routed through the first available PSTN line (among the selected ones). The **Round Robin** selection means that according to an internally gained statistics of most used PSTN lines, the call will be routed to the less used and currently available PSTN line (among the selected ones).

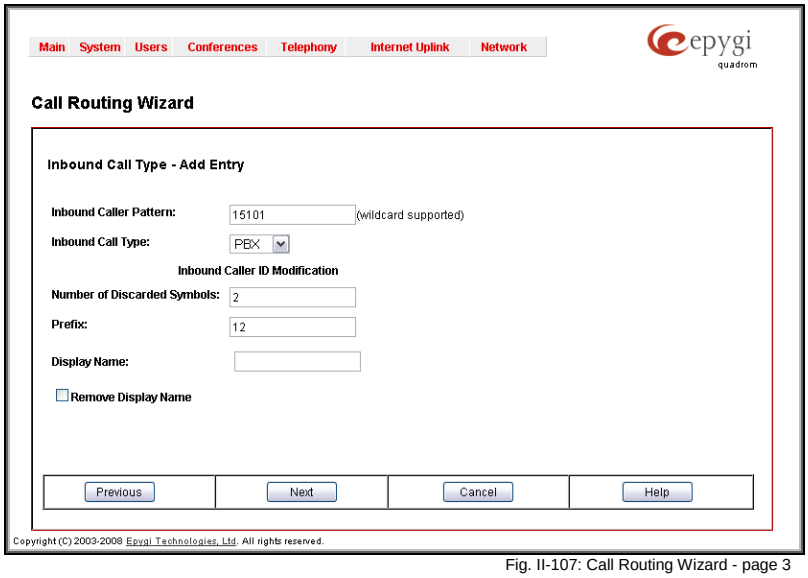


Fig. II-107: Call Routing Wizard - page 3

The **Call Routing Wizard** - Page 3 appears if the **Fill Call Source Information** checkbox had been enabled on Page 1 of the **Call Routing Wizard**. It will require information about the Inbound caller.

The **Inbound Caller Pattern** field requires the caller address for which the current route will be applied. The complete list of characters and wildcards allowed in this text field is given in the chapter Allowed Characters and Wildcards.

The **Inbound Call Type** drop down list gives you the option to select the call type (PBX, SIP, FXO) used by the inbound caller to reach the Quadro.

The settings in the **Inbound Caller ID Modification** group allow Caller IDs of inbound calls to be modified.

- The **Number of Discarded Symbols (NDS)** text field requires the number of digits that should be discarded from the beginning of the **Inbound Caller Pattern**. The field should be empty if digits do not need to be discarded. Only numeric values are allowed for this field, otherwise the error message “Error: Number of Discarded Symbols is incorrect - digits allowed only” will appear.
- The **Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Inbound Caller Pattern** instead of the discarded digits. (For example, if the routing pattern is 12345, the Number of Discarded Symbols is two, and the prefix digits are 909, the final phone number will be 909345.) Wildcards are allowed here (see chapter Entering SIP Addresses Correctly).
- The **Discard Non-Numeric Symbols** checkbox is used to discard any non-numeric symbols from the **Inbound Caller Pattern**.

- The **Display Name** text field allows you to replace an original caller's ID with the custom display name for the corresponding routing rule. This field is optional and when it is left empty, an original caller ID will be displayed on the called destination's phone, otherwise the name inserted here will appear on the phone.
- The **Remove Display Name** checkbox is used to remove caller IDs from calls made with this routing rule.

The **Next** button will open the **Call Routing Wizard** - Page 4 where different information about Inbound Caller will be required depending on the selected **Inbound Call Type**. For the **SIP** Inbound Call Type, the **Inbound Host** text field will require one or more IP addresses or host names of the SIP server where the caller is registered, or the caller's device they are direct calls, separated by a space. If the **FXO** Inbound Call Types are selected, the **Inbound Port ID** drop down list will require selecting the FXO line number correspondingly, and in the next step, a list of timeslot(s) used to receive calls from the defined caller.

The **Call Routing Wizard** - Page 5 appears if the **Set Date / Time Period(s)** checkbox previously had been enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the pattern validity period(s).
This page provides selection between **Typical** and **Custom** date/time rule definitions.

The **Typical** selection contains the following group of radio buttons that are used to select the frequency of the corresponding routing pattern that is to take place:

- **Daily**
- **Weekly** – the preferred weekday(s) should be selected for this option.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and month should be selected for this option.

In the **Available Time Period** drop down lists, the time range of the pattern validation should be defined. Any time selected in this field will be considered corresponding to the Quadro's Time/Date Settings.

The **Custom** selection provides the option to manually define the validity period(s). Use the following format to insert pattern date/time rule(s):
[Month,Month-Month,...][Day-Day,Day,...][hh:mm-hh:mm,...]; ...

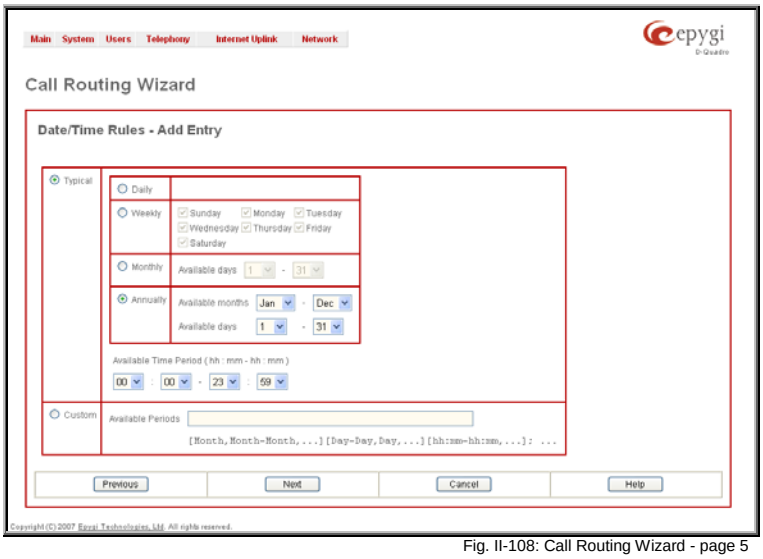


Fig. II-108: Call Routing Wizard - page 5

The **Duplicate** functional button is used to create a routing pattern with the settings of an exiting one. This is to avoid configuring a new routing entry completely by duplicating an existing entry with different settings. To use the **Duplicate** button only one record may be selected, otherwise the error message "One row should be selected" will appear. The **Duplicate** button opens the **Call Routing Wizard** where all fields except the **Pattern** field are already filled in. A **Pattern** for the new route will be required anyway.

The **Move Up/Move Down** buttons are used to move call routing patterns one level up or down within the **Call Routing** table. The sequence of the routing patterns is important when making routing calls because the **Call Routing** table is parsed from the top down and routing will take place according to the first pattern that matches the dialed number. The **Move To** button is used to move the selected entry to a different position in the Call Routing Table. This will increase or decrease the selected pattern's priority. Pressing the button will open the page where a row number should be specified together with the position the selected entry is to be placed (before or after the defined row).

The **Local AAA Table** page allows you to manage local authentication and the authorization database. Callers dialing the routes which have an AAA (Authentication, Authorization, and Accounting) option enabled, will pass the authorization on the **Local AAA Table** by using a phone number or username/password, depending on the corresponding entry configuration on this page.

The caller passes authorization automatically if the detected phone number of the caller dialing a route has the AAA option enabled and is registered in the **Local AAA Table**. If the caller ID service is disabled or the caller's phone number is not registered, the caller is asked to enter a registration user name and password.

The **Add** functional button opens the **Call Routing – Local AAA Table - Add Entry** page where a new local AAA record can be created.

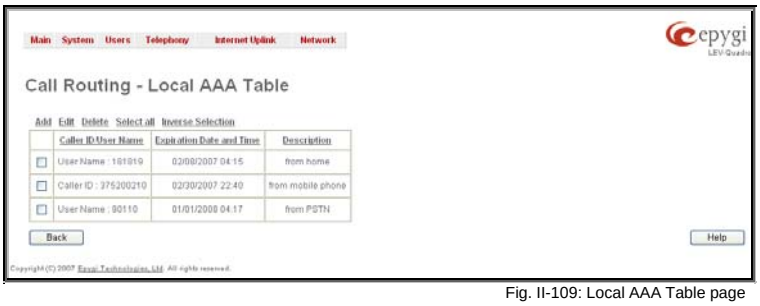


Fig. II-109: Local AAA Table page

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the type of authorization and the following other parameters:

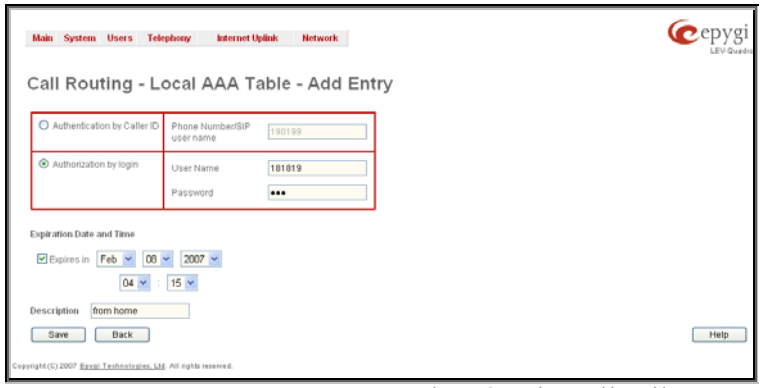


Fig. II-110: Local AAA Table - Add Entry page

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller's phone number (which is considered to be automatically detected). The **Phone Number/SIP User Name** text field requires the caller's phone number or the SIP username. Only numeric and wildcard characters (see chapter Entering SIP Addresses Correctly) are allowed for this field. '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number. The {11, 15, 23, 38, 45} pattern means that the dialed number may be 11, 15, 23, 38 or 45 to match the pattern.
- **Authorization by Login –** this selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication username. Only numeric values are allowed for this field, otherwise the error message "Incorrect Username - digits allowed only" will appear. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the error message "Incorrect Password - digits allowed only" will appear.

The **Expiration Date and Time** drop-down lists are used to set the date and time when the registration will expire.

The **Expires in** checkbox is used to enable the **Expiration Date and Time** feature.

The **Description** text field requires an optional description about the calling party.

To create a new Call Routing rule

1. Click on the **Call Routing Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Call Type** from the drop down list.
6. Define the **Metric** or leave the default.
7. Enter a **Description** if needed.
8. Enable the **Filter on Caller / Call Type / Modify Caller ID** checkbox, if the route functionality should be limited depending on inbound caller information.
9. Enable **Set Date/Time Period(s)** checkbox, if route should be functional within certain time/date interval.
10. Press **Next**.
11. Select user or attendant extension from **Use Extension Settings** drop down on behalf of which the call will be placed.
12. Specify the **Destination Host** and **Port Number**, **Username** and **Password** if **IP** or **IP-PSTN** call type has been selected. For **IP-PSTN** call type, enable **Multiple Logons** if necessary. Enable **Use RTP Proxy** checkbox, if needed.
13. Choose the Authentication and Accounting method from **AAA Required** drop down list.
14. Choose a **Fail Reason** from the corresponding drop down list.
15. Configure **Transport Protocol for SIP messages** and **SIP Privacy** parameters as needed.
16. Press the **Next** button.
17. If **Filter on Caller / Call Type / Modify Caller ID** checkbox has been previously enabled and the call type is different from the FXO, fill **Inbound Caller Pattern** in the corresponding text field, choose the needed value from **Inbound Call Type** drop down list, as well as **Number of Discarded Symbols** and **Prefix** values.
18. Press the **Next** button.
19. If **IP** has been selected on the previous step in the **Inbound Call Type** drop down list, then **Inbound Host** should be inserted in the current page. If **FXO** has been selected in the **Inbound Call Type** drop down list, then the FXO line number should be selected here.
20. If **Set Date/Time Period(s)** checkbox has been selected on the first page, pressing **Next** will open **Date/Time Rules** page where route validity should be defined.
21. Press the **Finish** button to establish a local route with the inserted settings.

To create a local AAA entry

1. Click on the **Local AAA Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Local AAA Table** page.
3. Choose the Authentication type.
4. Enter the **Phone Number** or the **Username** and **Password** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

Allowed Characters and Wildcards

The following is the set of characters and wildcards allowed in the **Pattern** and **Inbound Caller Pattern** text fields of the Call Routing Wizard:

Characters:

0…9

a…z

A…Z

+ = $; / ~ _ - . & ( ) ' ! * ? {} , [ ]

Please Note: The symbols * and ? should be prefixed with a slash (\) if they are used as ordinary characters; otherwise the system will interpret them as wildcards.

Please Note: The symbols !, {, }, [,], - and , are used to define a range of characters and cannot be used as ordinary characters.

Wildcards:

*	Any number of any characters
?	Any single character
{ }	A character or a string from the specified set of characters and strings.

The following control symbols are used to specify a set:

- Use a comma (,) to separate the elements of a set.

  Please Note: No spaces are allowed within braces.

  Example:

  The pattern is **9{1,3,11,a}**.

  Numbers matching the pattern are **91, 93 , 911, 9a.**

- Use a minus sign (-) to specify a range of characters. Each successive element of the range is obtained by increasing the previous element (the element code) by one.

  Example:

  The pattern is **2{11-15,a-d}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2145, 2155, 2a5, 2b5, 2c5, 2d5**.

- Use an exclamation point to exclude a character or a string from a set.

  Example:

  The pattern is **2{11-15,a-d,!14,!c}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2155, 2a5, 2b5, 2d5**.

Please Note: You can use the wildcard ? within the braces, but not *. Thus, **{12-104,15?,36?}** is a valid pattern, whereas **{15*,36*}** is not.

Please Note: The symbol ! cannot be used to exclude a range of symbols. For example **2{15-60,!23-32}** or **2{15-60,!23-!32}** are not valid patterns. To valid pattern will be to **2{15-22,33-60}**.

[]	The same as above with the exception that character ranges can include single-digit/character elements only.

Example:

The pattern is **2[1-5, a-c]5**.

Numbers matching the pattern are **215, 225, 235, 245, 255, 2a5, 2b5, 2c5**.

\	Precedes a control symbol (*, ?, -, ! and ,) to indicate that it is used as an ordinary character, not a wildcard.

Example:

The pattern is **1*[1-3]**

Numbers matching the pattern are: **1*1, 1*2, 1*3**

Please Note: Patterns cannot be prefixed with the * symbol. The system considers the patterns starting with * as feature codes and does not parse them through the Call Routing table.

@	Used to indicate the full SIP address (example: 20233@sip.epygi.com). This pattern is mainly used to call back users registered on the SIP server different from the one where the called party is registered.

Please Note: Patterns containing @ symbol will not be parsed among those that do not have @ symbol in the Call Routing Table. When calling from local extensions (the calling number for local extension is sipnumber@ip_address_of_Quadro, e.g. 20233@192.168.35.25), only the sipnumber part of the pattern will be parsed among other entries with @ symbol in the Call Routing Table.

Best Matching Algorithm

All calls through and within a Quadro are made according to call routing patterns that specify a destination based on a dialed number. When a user dials a number to make a call, the Quadro matches the dialed number against the existing patterns that are specified in the Call Routing table. If the dialed number matches only to a single pattern, this pattern will be used to set up a call. If several patterns have been found to match the number, the Quadro uses the Best Matching Algorithm to prioritize the matching patterns. Once the patterns are prioritized, the pattern with the highest priority will be used as a preferred route for call setup. The successive patterns will be used only if the destination specified by a higher priority pattern is unreachable.

To prioritize the matching patterns, the following criteria are sequentially applied to matching patterns. The criteria are ordered by their priorities: Each consecutive criterion is calculated only for the patterns that take the same value for the preceding criteria: that is Criterion 3 is calculated only for patterns that take the same value for Criterion 1 and Criterion 2.

Criterion 1	**The presence of asterisks ("*") in a pattern** The patterns without "*" have a higher priority.
Criterion 2	**The total number of matching digits/symbols inside and outside the braces/brackets** The more matching digits a pattern contains, the higher its priority.
Criterion 3	**The number of matching digits/symbols outside the braces/brackets** The more matching digits outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 2.
Criterion 4	**The total number of question marks ('?') inside and outside the braces/brackets** The more question marks a pattern contains, the higher its priority.
Criterion 5	**The number of question marks ("?") outside braces/brackets** The more question marks outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 4.
Criterion 6	**The number of square brackets ("[]")** The more brackets a pattern contains, the higher its priority.
Criterion 7	**The number of braces ("{}")** The more braces a pattern contains, the higher its priority.
Criterion 8	**The number of asterisks ("*")** The fewer asterisks a pattern contains, the higher its priority.
Criterion 9	**The value of the metric** The lower the metric of a pattern is, the higher its priority.
Criterion 10	**The position in the routing table** The higher the position of a pattern in the routing table is, the higher its priority.

Example. The user has dialed 1231 and the following matching patterns have been found.

The list of patterns
1
123*
{11-15}3*
?2?1
123?
[1-3]*
[1-3]???
{100-150, asd, *\?}1
12*31
1[1-3]3[0-8]
1231
*2*1
*

Step 1: The list is split into two groups separating the patterns with "*" from those without (Criterion 1). The patterns with "*" form a group with a lower priority and are pushed back to the end of the list.

Criterion 1

The list split into two subgroups
??2?1 123? [1-3]??? {100-150, asd, *\?}1 1[1-3]3[0-8] 1231
1 123* {11-15}3* [1-3]* 12*31 *2*1 *

Step 2: The two groups of patterns are arranged separately from each other by the total number of matching digits inside and outside the braces/brackets in the descending order (Criterion 2). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 2

The list of patterns	Matching digits
?**2**?**1**	2
123?	3
[**1**-3]???	1
{**100-150**, asd, *\?}**1**	4
1[**1-3**]**3**[**0-8**]	4
1231	4
__1__	1
123*	3
{**11-15**}**3***	3
[**1-3**]*	1
12*31	4
***2*1**	2
*	0

N	The list of patterns	Matching digits
1	1[1-3]3[0-8] 1231 {100-150, asd, *\?}1	4 4 4
	123?	3
	??2?1	2
	[1-3]???	1
	12*31	4
3	123* {11-15}3*	3 3
	*2*1	2
4	*1* [1-3]*	1 1
	*	0

Step 3: The new sub-lists are arranged separately from each other by the number of matching digits outside the braces/brackets (Criterion 3). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 3

The list of patterns	Matching digits
1[1-3]**3**[0-8] **1231** {100-150, asd, *\?}**1**	2 4 1
123?	-
??2?1	-
[1-3]???	-
12*31	-
123* {11-15}**3***	3 1
*2*1	-
1 [1-3]*	1 0
*	-

The list of patterns	Matching digits
1231 1[1-3]3[0-8] {100-150, asd, *\?}1	4 2 1
123?	-
??2?1	-
[1-3]???	-
12*31	-
123*	3
{11-15}3*	1
*2*1	-
1	1
[1-3]*	0
*	-

The Best Matching Algorithm will stop after executing step 3 as no new sub-lists are formed. The resultant list of prioritized patterns will be the following:

The prioritized list
1231
1[1-3]3[0-8]
{100-150, asd, *\?}1
123?
??2?1
[1-3]???
12*31
123*
{11-15}3*
*2*1
1
[1-3]*
*

VoIP Carrier Wizard

The **VoIP Carrier Wizard** is used to define access codes for available VoIP Carrier accounts which will particularly allow you to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

Attention: The VoIP Carrier Wizard is not available when the QuadroFXO is in the slave mode, i.e. it shares its FXO lines to the Quadro IP PBXs.

For each configured VoIP carrier, the wizard creates a specific IP-PSTN routing rule in the Call Routing table. This entry is available to PBX users only, which means only PBX users can make calls to the corresponding VoIP carrier. Additionally, a virtual extension automatically generated in Extensions Management will be registered on the defined VoIP Carrier's SIP server. The settings of that extension will be used to make calls from Quadro's users towards the created VoIP Carrier will be placed.

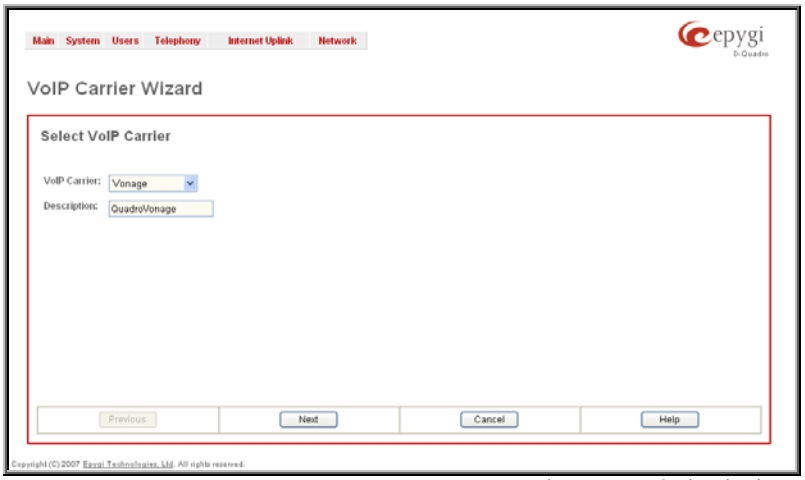
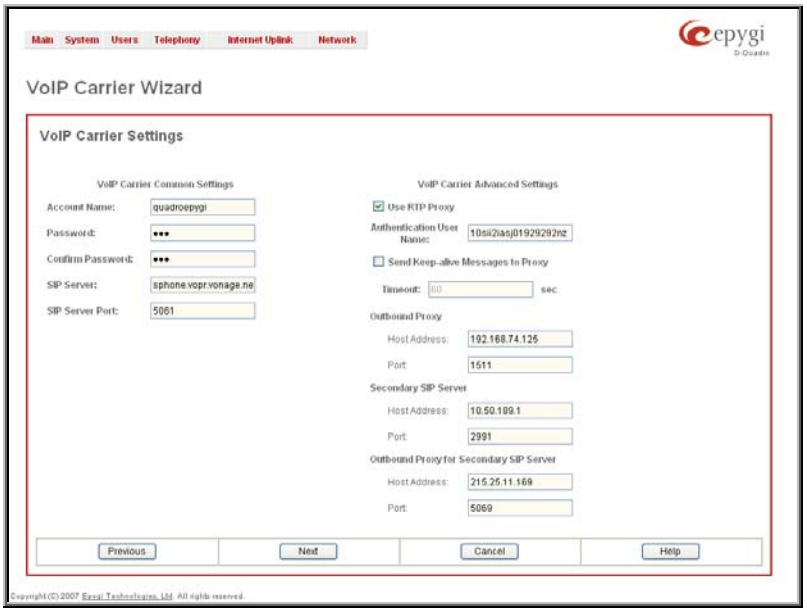


Fig. II-111: VoIP Carrier Wizard page

VoIP Carrier Wizard – Page 1 provides a following option of describing the VoIP carrier:

When predefined carrier is selected in the **VoIP Carrier** drop down list, the SIP Server and Port will be already predefined in the next page. **Manual** selection allows you to manually set up the VoIP Carrier settings.

The **Description** field allows you to insert an optional description of the VoIP Carrier.



VoIP Carrier Wizard – Page 2 is used to define VoIP Carrier Settings. The page contains following components:

1. VoIP Carrier Common Settings

The **Account Name** text field requires a username for authentication on the defined SIP server.

The **Password** text field requires a password for authentication on the defined SIP server.

The **Confirm Password** text field requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error message "Incorrect Password confirm" will appear.

The **SIP Server** text field requires an IP address or the hostname of the SIP server destination party it is registered on.

The **SIP Server Port** text field requires the port number of the SIP server destination party it is registered on.

2. VoIP Carrier Advanced Settings

The **Use RTP Proxy** checkbox is applicable only when a route is used for calls towards a configured VoIP Carrier from a peer located outside the Quadro. When this checkbox is selected, the RTP streams between external users will be routed through Quadro. When the checkbox is not selected, RTP packets will move directly between peers.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested only for certain SIP servers. For others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If a reply is not received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will continue to be sent to the server.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name), the port number of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

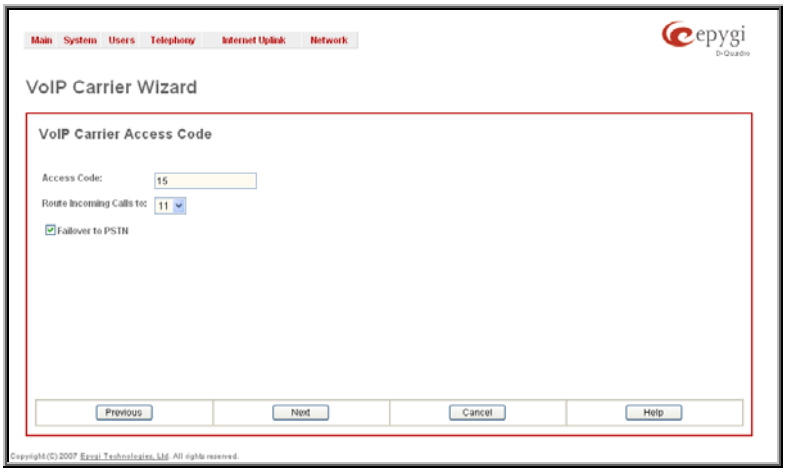
VoIP Carrier Wizard – Page 3 contains the following VoIP Carrier access code selection components:

The **Access Code** text field requires a digit combination by dialing, which the corresponding VoIP Carrier will be reached.

The **Route Incoming Calls To** drop down list allows you to select an extension (or Auto Attendant) on the Quadro where incoming calls from the configured VoIP Carrier should be routed to. For the selected extension there will be an unconditional forwarding set up which will care for incoming calls forwarding from the VoIP carrier to the corresponding extension.

The **Failover to PSTN** checkbox selection will route the call to the PSTN through local FXO line in case if the VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the Call Routing table. This maintains digit transmission to the local PSTN when an IP call towards the configured VoIP Carrier cannot be established.

Please Note: A warning message will appear when the defined **Access Code** already exists in the Call Routing table or causes a conflict with entries already in the Call Routing table. In this case, when continuing through the **VoIP Carrier Wizard**, the existing entry in the Call Routing table will automatically be overwritten by the new settings.



RADIUS Client Settings

RADIUS (Remote Authentication Dial In User Service) specifies the RADIUS protocol used for authentication, authorization and accounting, to differentiate, to secure and to account for the users. The RADIUS Server provides the option for a caller from/through Quadro to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the Quadro, and according to the configuration of **AAA Required** option (see Call Routing table), the RADIUS server will be used to authenticate user and/or to account for the call. This can be accomplished by automatic detection of the caller's number or a customized login prompt where the caller is expected to enter a username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, user passwords are encrypted when sent between the client and RADIUS server to eliminate the possibility of a party viewing an unsecured network where they could determine a user's password. If no response from the RADIUS Server is returned after the Receive Timeout expires, the request is resent numerous times as defined in the Retry Count list. The client can also forward requests to an alternate server(s) if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not recognize must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the Quadro Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the Quadro.

Please Note: The RADIUS Client cannot be disabled if there is at least one route with **RADIUS Authentication and Authorization** or **RADIUS Accounting** values configured in the **AAA Required** drop down list at the Call Routing table. In order to be able to disable the RADIUS Client on the Quadro, appropriate routes should be removed first.

The other RADIUS Client settings are divided into three groups:

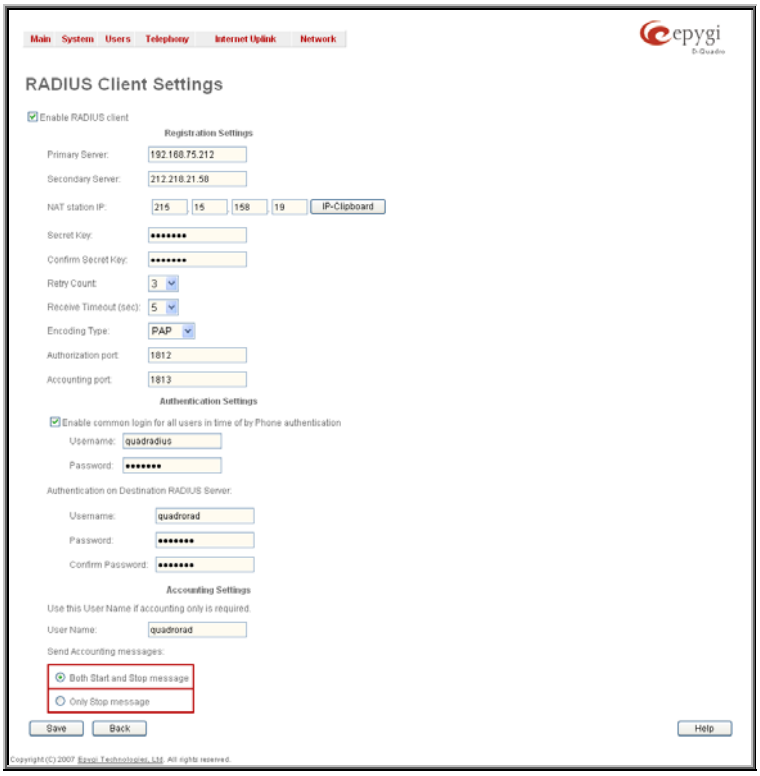


Fig. II-112: Radius Client Settings page

1. Registration Settings

The **Primary Server** requires the IP address of the primary Radius Server.

The **Secondary Server** requires the IP address of the secondary Radius Server.

NAT Station IP text fields require the NAT PC WAN IP address. If no NAT Station is specified here, Quadro's IP address will be sent to the RADIUS server.

Secret Key is used to insert the secret key between the Radius client and the server. Contact the Radius server administrator to get the secret key for your Quadro.

The **Confirm Secret Key** field is used to verify the secret key. If the entered **Secret Key** does not correspond to the one in the **Confirm Secret Key** field, the error message "The Secret Key does not match. Please try again" will appear.

Retry Count allows you to select the number of attempts authorized before canceling the registration.

Receive Timeout allows you to select the timeout (in seconds) between two attempts to register.

Encoding Type allows you to select the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type should also be requested from the Radius Server administrator.

The **Authorization Port** text field requires the port number on the RADIUS server where Quadro is to send the authentication requests.

The **Accounting Port** text field requires the port number on the RADIUS server where Quadro is to send the accounting messages.

2. Authentication Settings

The **Enable common login for all users in time of by Phone authentication** checkbox enables custom settings for the callers who passed an authorization by phone on the Quadro. This checkbox enables **Username** and **Password** text fields to insert the custom settings that will stand instead of the source caller's settings when being delivered to the RADIUS server.

The **Authentication on Destination RADIUS Server** parameters group is used to insert a **Username** and a **Password** (followed by the password confirmation) to pass authentication on the RADIUS Server of the destination Quadro. If these fields are left empty, the original authentication settings that users enter for authentication will be used.

3. Accounting Settings

The **Username** field is dedicated for accounting services only. It is used to insert an identification username for accounting purposes. When no username is specified in this field, the source username will be used for accounting.

The **Send Accounting messages** manipulation radio buttons group is used to select sending both **Start** and **Stop** accounting messages or only **Stop** accounting message.

Voice Mail Common Settings

The **Voice Mail Common Settings** page is used to configure the Voice Mail recording codec.

The page consists of the **Recording Codec** drop down list contains the existing codecs for voice mail compression. Changing the Voice Mail recording codec will directly affect the allocated memory size for users.

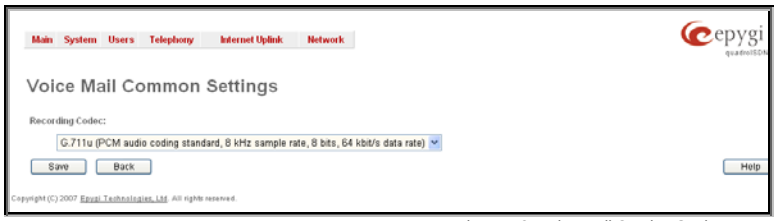


Fig. II-113: Voice Mail Coming Settings page

Dial Plan Settings

The **Dial Plan Settings** page is used to adjust the dialing timeouts for the routing calls over Quadro.

This page consists of the only drop down list used to configure the dialing timeout for the Routing calls. Values selected in the lists indicate the interval between the dialed number and it being applied to the network.

Fig. II-114: Dial Plan Settings page

System Hold Music Settings

The **System Hold Music Settings** allows you to define the hold music played to the PSTN party when it is held by the IP user. This page also allows you to define the percentage of system memory dedicated to the uploaded hold music file. This page contains following components:

The **Play Hold Music** drop down list specifies the music played to the PSTN party when it is held by remote IP user. It offers the following options:

- **Off** - no music will be played.
- **Local Music** – the hold music configured on the Quadro will be sent to the remote PSTN party while it is on hold.
- **Remote Music** – music sent by the IP party will be transparently passed to the PSTN user while it is held by the IP party.

Fig. III-115 Basic Services - Hold Music Settings page

Restore Default Hold Music File enables the default hold music. If the checkbox is selected, the text field **Upload New Hold Music File** will be disabled.

The **Upload New Hold Music File** text field can be used to enter the path where the custom hold music file is located. If the hold music file is browsed with the help of file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the hold music file.

The music file needs to be in PCMU wave format, otherwise the system will prevent uploading the file and will display the warning message "Invalid audio file or format is not supported". Additionally, the system will refuse uploading if insufficient memory is available for the Quadro and will then announce "You do not have enough space".

The **Download Hold Music File** link appears only if a file has been uploaded recently. It downloads the audio file to the PC and opens a window where the saving location can be specified.

RTP Streaming Channels

The **RTP Streaming Channels** page is used to configure channels where the broadcast RTP streams are transmitted. These channels may be then configured to be used as hold music (see Manual III – Extension User's Guide) or any other type of music played to the caller.

The **RTP Streaming Channels** page consists of a table where RTP channels are listed.

Add opens the **Add Entry** page where a new RTP channel can be added.

The **Add Entry** page includes the following text fields:

The **RTP Channel Name** text field requires the name or the number of the RTP channel.

The **Port Number** text field requires the broadcasting RTP port number.

The **Description** text field requires optional information related to the RTP streaming channel.

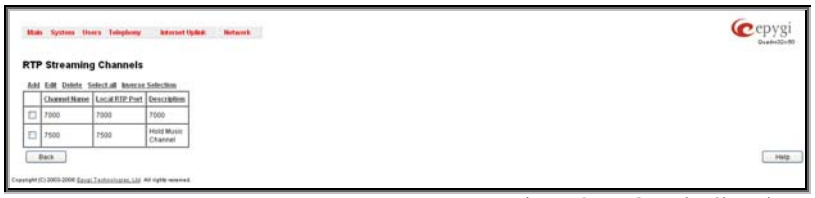


Fig. II-116: RTP Streaming Channel page

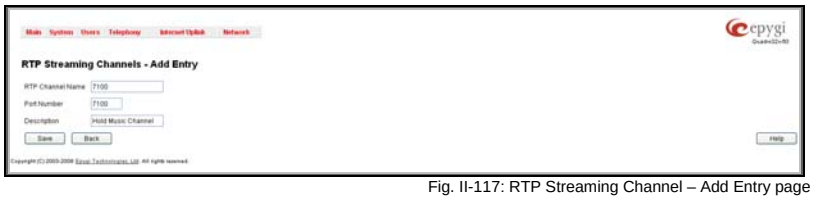


Fig. II-117: RTP Streaming Channel – Add Entry page

Internet Uplink Menu

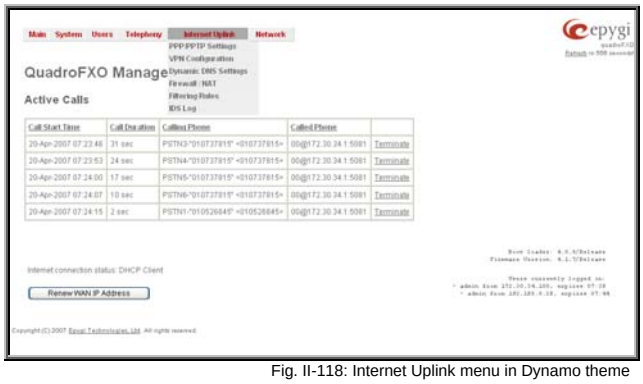


Fig. II-118: Internet Uplink menu in Dynamo theme

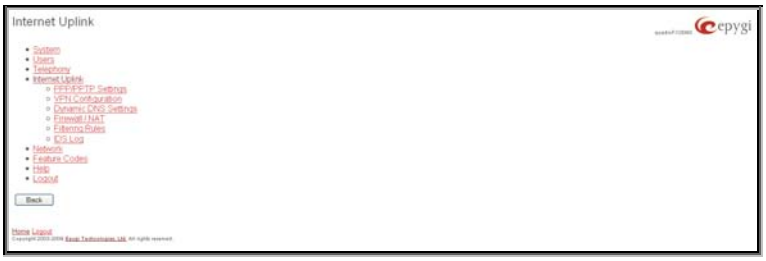


Fig. II-119: Internet Uplink menu in Plain theme

PPP / PPTP Settings

The **PPP/PPTP Settings** page is used to establish a connection over the DSL link, or any other type of uplink, to the ISP. A connection is needed to set up and make or receive calls through PPP over Ethernet. The connection may be configured for manual setup or always up. Once a connection has been established between the Quadro and the provider, Quadro users will be able to make and receive calls at any time.

The **PPP/PPTP Settings** page offers the following components:

The Advanced PPP Settings link refers to the same named page where certain parts of the negotiation process during connection establishment can be adjusted. This link is not available when accessing this page through the Internet Configuration Wizard.

The **PPTP Server** text fields are only enabled when Quadro is running with the PPTP interface and require the IP address of the PPTP server.

The **Encryption** drop down list is only enabled when Quadro is running with the PPTP interface and it is used to select the encryption for the traffic over the PPTP interface.

Authentication Settings require the Username and Password used for the authentication on the ISP server.

Dial Behavior radio buttons enables the following selections:

- **Dial Manually** - if this radio button is activated, a button will be displayed in the main management window that serves to switch the Internet connection on/off. When accessing the Internet, every station of the connected LAN has to connect to Quadro first.
- **Always connected** - Quadro stays in the always connected mode. This will allow always being online in the network.

IP Address Assignment radio buttons are used to define the IP address assignment for the PPP interface with the following options:

- **Dynamic IP Address** – the IP address to the PPP interface will be assigned dynamically by the DHCP server.
- **Fixed IP Address** – the fixed user defined IP address will be assigned to the PPP interface.

The **Keep Connection alive** checkbox enables keeping the connection alive by sending control packets dedicated for the link state verification.

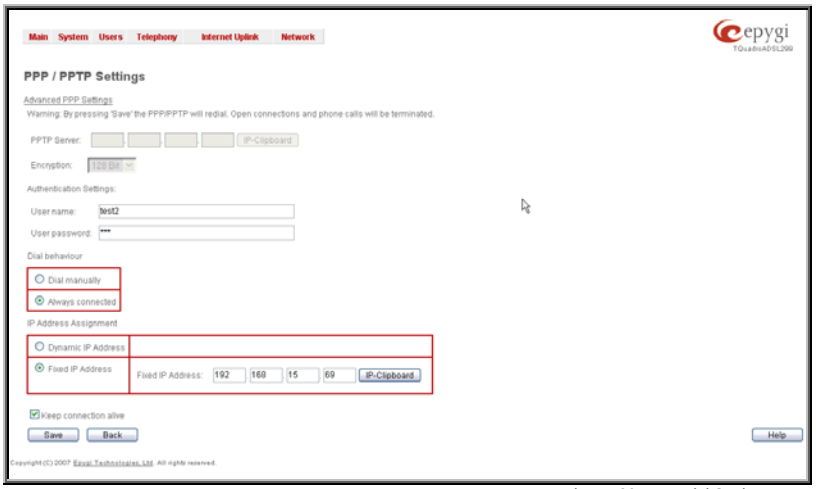


Fig. II-120: PPP Dial Settings page

Advanced PPP Settings

The **Advanced PPP Settings** are used to enable/disable certain parts of the negotiation process during connection establishment. These settings are available only if Quadro has a PPPoE WAN interface.

Attention: Disabling any of the services below may cause problems when establishing a connection including the complete connection failure. The default settings should be changed only if the ISP (Internet Service Provider) specifically requires it or if the peer system has problems with one of the services listed below. More information about these services can be found at: http://www.protocols.com/pbook/ppp.htm.

The **Advanced PPP Settings** page offers the following group of checkboxes:

Enable automatic PPP restart at checkbox is used to select the time when the PPP connection will automatically be restarted. The checkbox selection enables **LCP echo failures** text field that indicates the number of the LCP echo failure packets received before the PPP connection will be considered as dead and will be restarted.

Disable CCP (Compression Control Protocol) negotiation - this option should only be selected if the peer system is not working properly. For example, if it is not accepting the requests from the PPPD (Point-to-Point Daemon) for CCP negotiation.

Disable magic number negotiation - with this option, PPPD cannot detect a looped-back line. This option should only be selected if the peer is not working properly.

Disable protocol field compression negotiation in both the receive and the transmit direction – with this option, no protocol field compression will take place.

Disable Van Jacobson style TCP/IP header compression in both the transmit and the receive direction – with this option, no negotiation of TCP/IP header compression will take place and the header will always be sent uncompressed.

Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression - with this option, PPPD will not compress the connection-ID byte from Van Jacobson and will not ask the peer to do so.

Disable the IPXCP and IPX protocols - this option should only be selected if the peer is not working properly and cannot handle requests from PPPD for IPXCP negotiation.

Fig. II-121: Advanced PPP Settings page

VPN Configuration

A **VPN (Virtual Private Network)** is established to connect two local networks (intranets) securely over the Internet securely. The VPN routers manage authentication between servers and clients and handle data encryption for the connection. Only authorized users may access the network and the data exchange cannot be intercepted.

VPN connections are, in many ways, like every Internet connection, they are based on IP addresses, which means, the concerned VPN gateways must authenticate the IP addresses of their respective partner's VPN gateways. Each time a specific VPN is to be established, usually the same IP addresses are expected. This will not create problems if both VPN partners have fixed WAN IP addresses. There may be circumstances reasons to prefer dynamically allocated IP addresses. To enable devices that use a variable IP address as part of a VPN, they are turned into "Road Warriors". For example, at this point they are able to reach their corporate network via authentication at the company's VPN gateway device. This VPN gateway device must have a fixed IP address for Internet access. Every VPN needs at least one VPN gateway with a fixed IP address.

The partner devices of a VPN must have different WAN IP addresses, and if they are connected to local area networks, these LAN's must have different IP addresses. As all Quadro devices have the same default IP addresses on delivery, at least one of them must be reconfigured in order to set a new IP address.

Quadro supports several kinds of VPN connections such as **IPSec**, **L2TP** and **PPTP**.

The **VPN Configuration** page offers IPSec Configuration and PPTP/L2TP Configuration links that lead to the corresponding feature settings pages.

Attention: It is strongly recommended not to run different types of VPN tunnels between the same endpoints simultaneously.

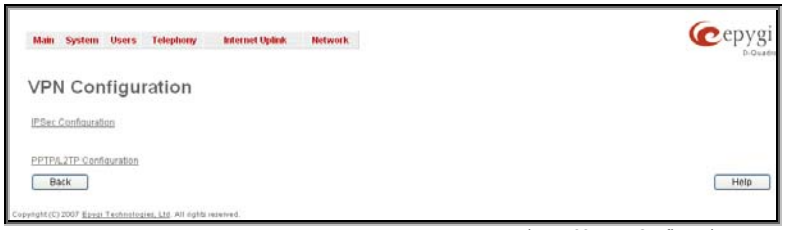


Fig. II-122: VPN Configuration page

An IPSec connection includes authentication and encryption to protect data integrity and confidentiality. VPNs are "virtual" in the sense that individuals can use the public Internet as a means of securely accessing an internal network. Once the IPSec connection is established, users have access to the same network resources, addresses, and so forth as if they were connected locally. VPNs are "private" because the data is encrypted between two VPN gateways. Encryption makes it very difficult for anyone to intercept data and capture sensitive information such as passwords. The Quadro can be set up to act as a VPN router when connected to the Internet with a fixed IP address or as an IPSec connection Road Warrior when using dynamic IP addresses.

Establishing an IPSec connection normally requires the functionality of a VPN gateway on each side of the communication line. An intelligent Internet access router, for example Quadro, delivers this function but also PCs or workstations may also be equipped with VPN gateway functionality. Home offices typically prefer dynamically allocated IP addresses.

When Quadro is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. Quadro is then prepared to establish an IPSec connection with another VPN gateway device, but also allows access to Road Warriors. A notebook /laptop used by a traveling employee could also be a Road Warrior. Access to their company's intranet via an IPSec connection can be obtained regardless of their location.

Quadro can also be set up to act as a Road Warrior. If a home office is connected to the Internet via Quadro with PPPoE (Point-to-Point Protocol) and dynamic IP addressing, setting up Quadro as a Road Warrior will allow an IPSec connection to the corporate network.

For the encryption and decryption of the data transmitted via the IPSec connection, a key is used. **RSA** used by Quadro is an asymmetric key system. It has to be available on both sides of the IPSec connection and will generate a different pair of keys on each side, a private key and a public key. During the connection establishment, some data is encrypted with the remote party's public key. They can be decrypting the data with their private key and the data encrypted there with Quadro's public key can be decrypted with Quadro's private key. Since the private key is never transmitted, it stays completely unknown to everyone, thus the system remains safe. Even if someone gets the public key, decryption cannot be possible without the private key. Quadro generates such a pair of keys automatically when it is set up. The user cannot see the private key, but must know the public key because their IPSec connection partner will need it.

Please Note: A pair of keys will always be generated, a public one and a private one. The previously generated pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

The **IPSec Configuration** link refers to the page where IPSec connections can be created and managed.

The **IPSec Configuration** page consists of two sub-pages: **Connection** and **RSA Key Management**.

The Connection sub-page provides an overview of all existing IPSec connections characterized by their **Connection Name**, the **Remote Gateway** (the IP address or the hostname of the IPSec connection partner), the **State** of the IPSec connection (Stopped, Connecting, Activated, Waiting or Connected) and the dedicated **Keying Type** (the encryption type). The content of the table can be sorted in ascending or descending order by clicking on the header of the respective column. There is a checkbox for every IPSec connection to select it for further editing.

Start activates the connection establishment of the selected IPSec connection. The **State** of the IPSec connection will change into "Connected" or "Activated" depending on the IPSec connection type. If no record is selected, the error message "One Record should be selected" appears.

Attention: It is not recommended to simultaneously start a static and a dynamic connection configured to use the same secret key. A dynamic connection may capture the static connection peer and vice versa, depending on which connection established first.

Stop disconnects the selected IPSec connection. The state of the IPSec connection will change into "Stopped". If no record is selected, the error message "One Record should be selected" will appear. More than one record may be selected at a time to be stopped.

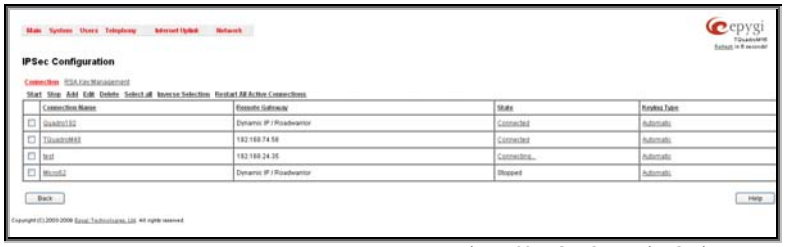


Fig. II-123: IPSec Connection Settings page

Add leads to the **Add IPSec Connection** wizard where a new IPSec connection can be defined and specified. The wizard provides several pages.

Edit leads to a set of **IPSec Connection Properties** pages to modify the parameters of the selected IPSec connection. The page includes the same components as the **Add IPSec Connection** page. To operate with **Edit**, only one record may be selected, otherwise an error message "One row must be selected" appears.

Restart all Connections restarts all active IPSec connections. The **State** of these IPSec connections will turn into **Connected** or **Activated** if the restart procedure has been successfully completed.

The first IPSec Connection Wizard page **Add IPSec Connection** has the **Connection Name** text field that requires a new mandatory IPSec connection name. If the text field is not filled in, the error message otherwise an error will occur "Error: Incorrect connection name" will appear.

Please Note: The input in the **Connection Name** field should only be in Latin characters, otherwise an error occurs and IPSec connection cannot be created.

The **Peer type** drop down list is used to choose the remote machine type for the IPSec Connection to be established. If the list does not include the required type of machine, choose **Other**.

The **VPN Network Topology** drop down list allows you to select the location of the peers participating to the VPN connection. The following options are present in the list:

- Quadro<>Peer – direct connection between Quadro and a peer.
- Quadro<>[Internet]<>Peer – connection between Quadro and peer over Internet.
- Quadro<>NAT<>[Internet]<>Peer – connection between Quadro and peer over Internet through Quadro provider's NAT.
- Quadro<>[Internet]<>NAT<>Peer – connection between Quadro and peer over Internet through peer provider's NAT.

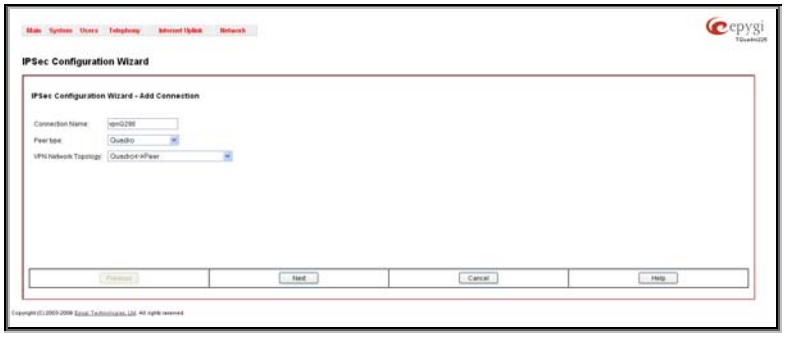


Fig. II-124: IPSec Connection Wizard - Add IPSec Connection

The second page of the IPSec Connection Wizard, **IPSec Connection Properties** serves to specify the members of the IPSec Connection and to set the basic parameters for encryption.

A group of radio buttons are used with **Dynamic IP/Road Warrior** and **Static IP/ Remote Gateway** to select if the remote Quadro (or another VPN gateway device) is connected to the Internet with a dynamic IP address and is acting as a **Road Warrior**, or is connected to the Internet with a fixed IP address and is acting as a **VPN Gateway**.

If **Dynamic IP / RoadWarrior** is selected, the **Remote Gateway IP Address** text field will automatically generate the value "any", to allow access independent from the sending IP address.

Selecting **Static IP / Remote Gateway** requires entering the IP address or the hostname of the remote Quadro (or another VPN gateway device) in the **Remote Gateway** text field.

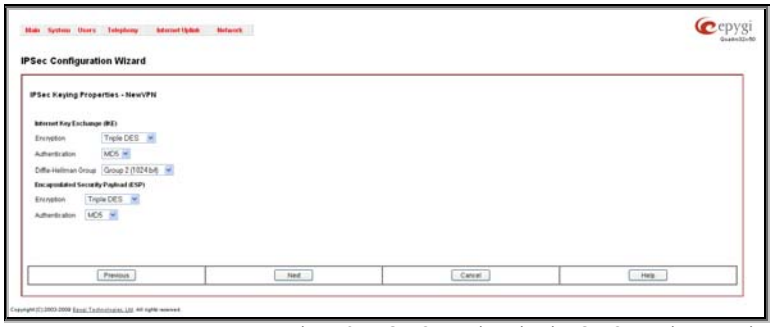


Fig. II-125: IPSec Connection Wizard -IPSec Connection Properties

Please Note: The **Static IP/ Remote Gateway** selection is not possible if this Gateway is positioned behind NAT, since the IP-address of the remote gateway is not reachable directly in this case.

Quadro <> Remote Gateway allows access from the local Quadro to the remote VPN gateway (local subnet and remote subnet are not included). This includes management access. The checkbox is disabled when "Quadro<>NAT<>[Internet]<>Peer" or "Quadro<>[Internet]<>NAT<>Peer" the is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

Local Subnet <> Remote Gateway allows access from all stations connected to the local network to the remote VPN gateway device (local Quadro and remote subnet are not included). The checkbox is disabled when "Quadro<>[Internet]<>NAT<>Peer" is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

Quadro <> Remote Subnet allows access from the local Quadro to all stations of the remote LAN (local subnet and remote VPN gateway devices are not included). The checkbox is disabled when "Quadro<>NAT<>[Internet]<>Peer" is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

Local Subnet <> Remote Subnet allows access from all stations of the local network to all stations of the remote LAN (VPN gateway devices are not included). In this case, the local and remote subnet IP addresses and subnet masks have to be entered in the corresponding text fields **Local Subnet IP** and **Remote Subnet IP**.

More than one of the above checkboxes may be selected to specify the desired communication relations.

The **Stop Connection if not successful** checkbox allows you to stop the IPSec connection attempts if the partner is still unreachable after the timeout period. If the checkbox is not selected, the system will continue to try to reach the IPSec connection partner.

The **Internet Key Exchange (IKE)** and **Encapsulated Security payload (ESP)** parameters are used to define the security of your VPN tunnel. The **Internet Key Exchange (IKE)** parameters group is used to select the **Encryption**, **Authentication** and **Diffie-Helman Group**. The **Encapsulated Security payload (ESP)** parameters group is used to select the **Encryption** and **Authentication.**

The **Encryption** drop down list offers the following standards for selection:

- **Triple DES** uses three DES encryptions on a single data block with three different keys to achieve a higher security than is available from a single DES pass (block cipher algorithm with 64-bit blocks and a 56-bit key).
- **AES 128 bit** cryptography scheme is a symmetric block cipher, which encrypts and decrypts 128-bit blocks of data.
- **AES 192 bit** cryptography scheme is a symmetric block cipher, which encrypts and decrypts 192-bit blocks of data.
- **AES 256 bit** cryptography scheme is a symmetric block cipher, which encrypts and decrypts 256-bit blocks of data.

The area **Authentication** offers the following parameters to be selected:

- **SHA** (Secure Hash Algorithm) is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPSEC.
- **MD5** (Message Digest) is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.

The **Diffie-Hellman** parameter is used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group, which is based upon the prime numbers. The higher is the group bit rate, the better is encryption. If mismatched groups are specified on each peer, negotiation fails.

The third page of the IPSec Connection wizard, **Automatic Keying**, is used to setup a type of password (**Shared Secret**) or the **RSA** public key to secure your IPSec Connection. The functionality of **Perfect Forward Secrecy** (PFS) can be added to both. Following ways of automatic keying are available.

- **Shared Secret** is a type of password consisting of any characters that both of the IPSec Connection partners must know. The authentication will be done with this shared secret. All encryption functions below will remain concealed.

  Please Note: It is also not recommended to start multiple road warrior connections with the **Shared Secret** automatic keying selected. For multiple road warriors to be started at the same time, it is recommended to use RSA keying with **Local ID** and **Remote ID** fields configured.

- **RSA** requires the public RSA key of your IPSec Connection partner.

Please Note: System prevents to start a connection with Shared Secret automatic keying selected if there is already a connection with RSA automatic keying started, and vice versa.

The **Local ID** requires an IP address, Quadro FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

Remote ID also requires an IP address, the IPSec Connection partner's FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

The **Local ID** and **Remote ID** text fields may have the values in one of the formats presented below:

- **IP address** – example: 10.1.19.32.
- **Host name** – example: vpn.epygi.com. This form requires additional resources to resolve the host name, therefore it is not recommended to use this format.
- **@FQDN** – example: @vpn.epygi.com. This form is considered as a string, and is not being resolved. It is recommended to use this form for most applications.
- **user@FQDN** - example: quadro@vpn.epygi.com. This form is also considered as a string, and is not being resolved. It has no advantages over the previous form.

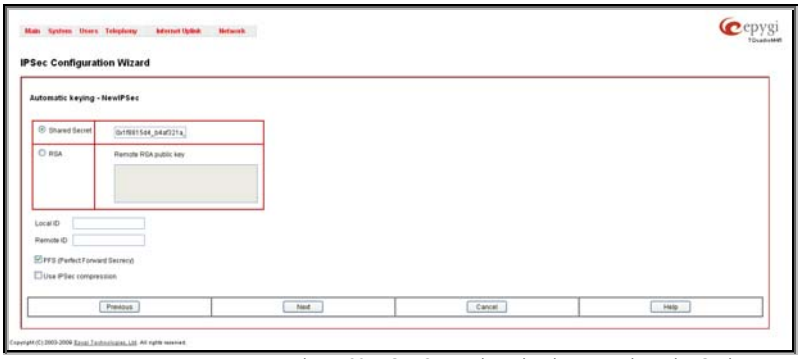


Fig. II-126: IPSec Connection Wizard - Automatic Keying Settings page

Please Note: The **Local ID** and **Remote ID** values are mandatory for **RSA** selection and are optional for **Shared Secret** selection. However, it is recommended to define the **Local ID** and **Remote ID** values for multiple road-warrior connections.

PFS (Perfect Forward Secrecy) is a procedure of system key exchange, which uses a long-term key and generates short-term keys as is required. Thus, an attacker who acquires the long-term key can neither read previous messages that they may have captured nor read future ones.

Use IPSec Compression enables IPSec data compression. This option is displayed only if the IPSec-VPN partner supports it.

The **RSA Key Management** sub-page is used to see the current RSA key and to generate a new one. This page contains the following components:

The public key is displayed in the **RSA Public Key** text field so that the user may inform their IPSec connection partner about it, for example, via fax.

The user has the option of generating a new pair of keys by specifying the key length with the corresponding radio buttons **Generate a new 1024bit RSA Key** and **Generate a new 2048bit RSA Key** and then clicking the **Generate** Button.

A valid RSA key should fit to following requirements:

- RSA key doesn't start with "0s"
- RSA key doesn't end with "=="
- RSA key contains symbols other than Alphanum, +, /, =

The **Email this to the peer** text field requires the mailing address of the IPSec connection partner. The **Send** button will insert Quadro's public RSA key into an e-mail and send it to the IPSec connection partner.

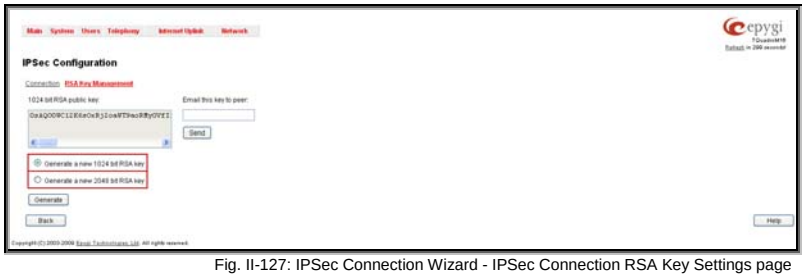


Fig. II-127: IPSec Connection Wizard - IPSec Connection RSA Key Settings page

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) is used to establish a virtual private network (VPN) over the Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers. PPTP encapsulates any type of network protocol (IP, IPX, etc.) and transports it over IP. Therefore, if IP is the original protocol, IP packets ride as encrypted messages inside PPTP packets running over IP. PPTP is based on point-to-point protocol (PPP) and the Generic Routing Encapsulation (GRE) protocol. Encryption is performed by Microsoft's Point-to-Point Encryption (MPPE), which is based on RC4.

L2TP (Layer **2 T**unneling **P**rotocol) is a protocol from the IETF, which allows a PPP session to run over the Internet, an ATM, or frame relay network. L2TP does not include encryption (as does PPTP), but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP network server (LNS) at the corporate side. Large carriers also may use L2TP to offer remote POPs to smaller ISPs. Users at the remote locations dial into the modem pool of an L2TP access concentrator, which forwards the L2TP traffic over the Internet or private network to the L2TP servers at the ISP side, which then sends them on to the Internet.

For **PPTP** and **L2TP Connections**, two parties are required: a **Client** and a **Server**. The client is responsible for establishing the connection. The server is waiting for clients, it is not able to initiate the connection itself.

Attention: L2TP tunnels have no data encryption mechanism.

The **Host Name** and a **Password** specify each side. The client should know the server's name and password (the Quadro server has no password) and the server should set the client's host name and a password. The client and server settings have to match on both sides for successful connection establishment.

Clients and Servers are identified by their hostnames, which means that only one client can be connected to the server in the same network. Servers also define the range of IP addresses that are assigned to the Server and Client hosts participating in a connection.

The **PPTP/L2TP Configuration** link displays a page where a new PPTP and L2TP connection can be configured, as well as PPTP and L2TP server settings can be adjusted. The page consists of 3 sub-pages.

The **Connections** page lists all existing connections are listed, characterized by their **Connection Name**, **Type** of the connection (PPTP or L2TP), the **Client/Server** mode, the **State** of the connection and the **Remote Hostname IP** (the IP address or the hostname of the connection peer). The state of the PPTP and L2TP Connections, except for the "Stopped" state, is established as a link that refers to the page where logout information about the connection status is displayed. Logs can be useful to determine problems on PPTP or L2TP connections failure.

Add functional button leads to the **PPTP/L2TP Connection Wizard** page, where a new connection can be established.

Please note: After creating a PPTP server connection, PPTP connections between devices placed on the Quadro LAN and external devices will no longer be possible. The PPTP pass-through service for incoming and outgoing traffic will be automatically disallowed once a PPTP server connection is created.

Fig. II-128: PPTP/L2TP Configuration page

Fig. II-129: PPTP/L2TP Connection Wizard – Page 1

The **PPTP/L2TP Connection Wizard** consists of several pages and allows you to create a new PPTP or L2TP connection.

The **PPTP/L2TP Connection Wizard – Page 1** consists of the following components:

Connection Name text field requires a connection identification name. The name of the connection cannot start with a digit symbol, however it can contain digits further in the name.

Connection Type drop down list allows to select the type of the connection (PPTP or L2TP).

The **PPTP/L2TP Connection Wizard – Page 2** consists of the following components:

The **Peer Name** text field requires the connection peer name. If you are about to create a client connection, then the server's name should be defined here. If you are creating a server connection, then the client's name should be defined here.

Please Note: When creating a connection with a Windows Server, ensure that a user with the Quadro's host name and Dial-in access exists on the server. When creating a connection with a Windows Client, ensure that the Peer name specified on this page matches the Dial-in connection's username.

Please Note: The input in the **Peer Name** field should only be in Latin characters, otherwise an error occurs and no connection can be created.

The **Password** text field requires the password for the connection establishment.

Please Note: These authentication settings should be identically configured on both peers for the successful connection establishment.

The manipulation radio buttons selection on this page allows you to choose whether the new connection will be a client or a server. For the **Client** radio button selection, no further details need to be provided. For the **Server** radio button selection, the following information needs to be provided:

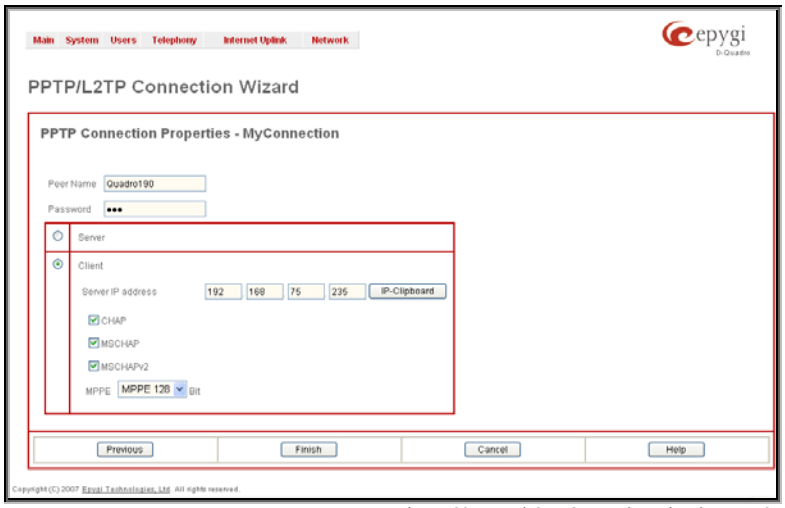


Fig. II-130: PPTP/L2TP Connection Wizard – Page 2

The **Server IP Address** text fields require the IP address of the server.

The **Authentication** manipulation radio buttons are only present if the **Connection Type** selected on the previous page is PPTP. They are used to select the corresponding authentication protocol by which the client communicates with the server. The **MSCHAPv2** selection enables the **Encryption** drop down list where the encryption method can be selected.

The **Start** functional button initiates the selected connection(s). If it is a client connection, then this button initiates a client activity of reaching the server. The **Start** option is applicable for multiple connections selected at the same time.

The **Stop** functional button is used to stop the selected connection(s). Stopping the server connection will disconnect all connected clients and close the PPTP/L2TP tunnel. The **Stop** option is applicable for multiple connections selected at the same time.

The **PPTP Server Configuration** page is used to configure the PPTP server settings and offers the following components:

The **PPTP Subnet** text fields are used to enter the IP address range for the PPTP server and clients within the PPTP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the PPTP connection.

Please Note: The first address specified in the PPTP Subnet will be assigned to the PPTP server; others will be assigned to the clients. The PPTP server subnet should be different from the L2TP server subnet, otherwise a corresponding error message will appear.

The **Authentication** manipulation radio buttons are used to select the corresponding authentication protocol by which the client communicates with the server. The **MSCHAPv2** selection enables **Encryption** drop down list where the encryption method can be selected.

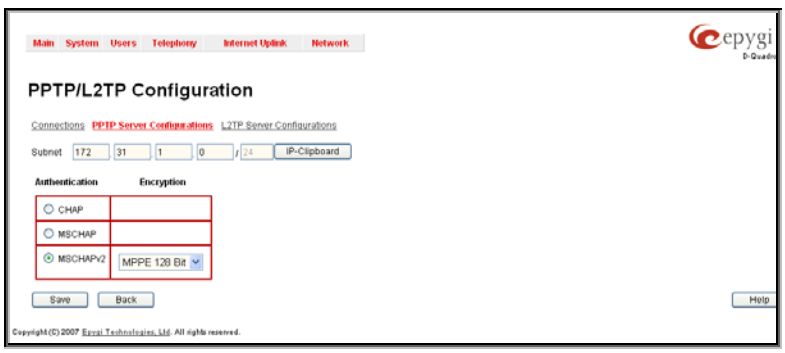


Fig. II-131: PPTP Server Configuration page

The **L2TP Server Configuration** page is used to configure the L2TP server settings and provides the following input options:

The **L2TP Subnet** text fields are used to enter the IP address range for the L2TP server and clients within the L2TP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the L2TP connection.

Please Note: The first address specified in the L2TP Subnet will be assigned to the L2TP server; others will be assigned to the clients. The L2TP server subnet should be different from the PPTP server subnet, otherwise a corresponding error message will appear.

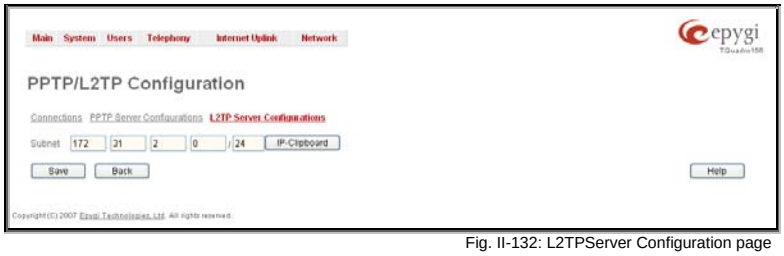


Fig. II-132: L2TPServer Configuration page

To Specify an IPSec Connection

1. Press the **Add** button on the **IPSec Connection Settings** page. The **IPSec Connection Wizard** will appear in the browser window.
2. Select a VPN **Peer Type** and assign a name to the **IPSec Connection**. Press **Next** to go to the next page of the IPSec Connection wizard.
3. Enter the remote side IP parameters, check subnets/gateways for the connection, select the NAT traversal option (if needed), and the desired keying type. Press **Next** to go to the next page of the IPSec Connection wizard.
4. If the **Automatic Keying** type has been selected, enter the automatic keying parameters and select the PFS and IPSec compression options (if needed). If the **Manual Keying** type has been selected enter the encryption and authentication keys and SPI(s).
5. To specify an IPSec connection with these parameters, press **Finish**. Press **Cancel** to abort the operation.

To Manage an RSA key for the IPSec Connection

1. Press the **RSA Key Management** button on the **IPSec Connection Settings** page. The **IPSec Connection RSA Key** will appear in the browser window.
2. Select the RSA key length and press **Generate** to generate a new RSA public key. This may take several seconds.
3. Enter a destination e-mail address in the **Email this key to peer** text field, then press **Send** to send the new RSA public key.

To Delete/Stop/Start/Enable/Disable a VPN Connection

1. Select one or more checkboxes of the corresponding connections that should to be deleted/stopped/started from the **Connections** tables. Press **Select all** to delete/stop/start all connections.
2. Click on the Delete/Stop/ Start button from the table's menu to perform the corresponding operation for the selected VPN connection(s).
3. If deleting, confirm it with pressing on **Yes**. The VPN connection will be deleted. To abort the deletion and keep the VPN connection in the list, click **No**.

Dynamic DNS Settings

The **Dynamic DNS** (DynDNS) is a service that is used to map a dynamic IP address to a host name. This service is used if you are connected to the Internet with a dynamic IP address (and PPP, DHCP client) and want to allow access from the Internet to a device behind the firewall. For example, if you want to run your own WEB server.

To enable the DynDNS service on Quadro, you first have to choose a DynDNS provider and register at their website.

The **Dynamic DNS Settings** page provides the following components:

The **Enable Dynamic DNS** checkbox selection enables the dynamic DNS service.

The **User** text field requires the username specified during the registration at the DynDNS provider.

The **Password** text field requires the password specified during the registration at the DynDNS provider.

The **Max time between updates** text field requires entering the period between two updates (in hours). The values entered in these fields should be greater than 24, otherwise the error message "Update interval times smaller than 24 hours are too small" will appear. Normally, whenever you set up a connection to the Internet, the DynDNS is updated at least once in the period indicated in this field.

The **Use predefined service** radio button leads to the manual configuration of the DynDNS service. The selection enables the following optional settings:

The **Service** drop down list contains the provider list where the administrator needs to select the one that it has been subscribed to.

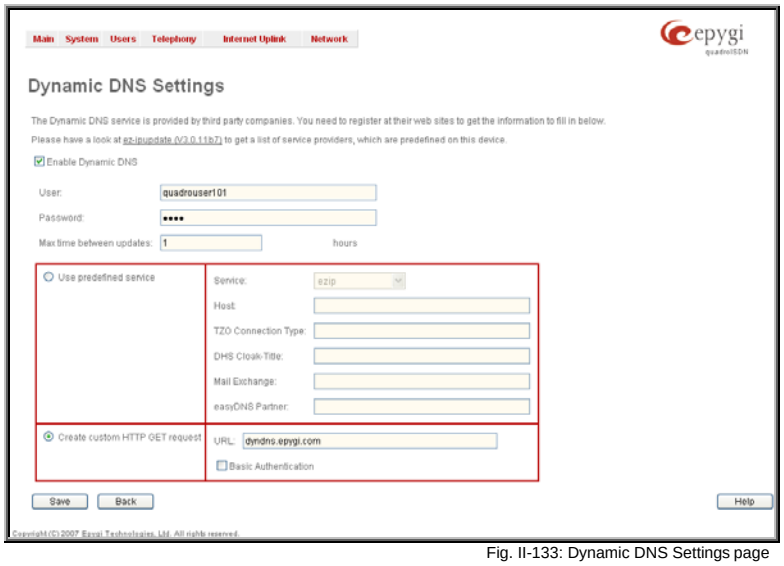


Fig. II-133: Dynamic DNS Settings page

The **Host** text field requires the name of the host on the Internet.

The **TZO Connection Type** text field is used for a special parameter required by the DynDNS provider TZO.

The **DHS Cloak-Title** text field is used for a special parameter required by the DynDNS provider DHS.

The **Mail Exchange** text field requires the address of the e-mail server where the DynDNS service provider will relay your e-mails. **Attention:** If this service is used, ensure that there is port forwarding configured for SMTP (port 25) to the internal e-mail server.

The **easyDNS Partner** text field is used for a special parameter required by the DynDNS provider easyDNS.

Selecting the **Create Custom HTTP GET Request** radio button will switch to the custom settings of the DynDNS service. Normally, the DynDNS provider uses HTTP get requests to map dynamic IP addresses to host names. If the HTTP receive request is known to you, choose the **Create Custom HTTP GET Request** radio button and enter the appropriate value into the **URL** text field.

The selection enables the following optional settings:

The **URL** text field requires the complete request to be sent to the DynDNS server. Normally it has the following format:

http://www.server.domain:port/scriptpath/scriptname?param1=value1&param2=value2

The request modifies the nameserver database so that the hostname will be resolved to the new IP address.

The **Basic Authentication** checkbox enables the encoding of the username and password entered in the text fields above, and then uses the **Basic Authentication** method to notify the provider about the user authentication settings.

Most of the DynDNS providers require an authentication for security. Authentication parameters can be provided in the **URL** text field to be used for the HTTP get request. The **Basic Authentication** checkbox can be selected if no authentication parameters to be provided.

Firewall and NAT

The **Firewall Configuration** page allows setting up a firewall, configuring the security level and enabling the NAT and IDS services of Quadro.

A **Firewall** is a security service configured by the Quadro administrator based on various criteria. The firewall allows or blocks traffic based on policies, services and/or IP addresses. The firewall has several levels of security policies (low, medium or high). The administrator may add additional service-based rules. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level.

NAT (Network Address Translation) is used to allow Quadro LAN members to connect to the Internet using Quadro's WAN IP address. The Quadro/NAT also handles forwarding incoming packets from the WAN to the PCs or devices on Quadro's LAN.

The **IDS** (Intrusion Detection System) is a type of firewall, but together with deleting dangerous packets or packets containing intrusion attacks, IDS generates a log file with information about these dropped packets and the senders responsible for those packets. The log can be viewed on the IDS Log page and notifications about them can be sent to the user in various ways such as e-mail, flashing LED and display notification.

The **Firewall Configuration** page offers the following components:

The **Enable IDS** checkbox selection enables the Intrusion Detection System. The **Enable NAT** checkbox selection enables Network Address Translation.

The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are the following:

- **Low Security** - Everything that is not explicitly forbidden will be allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

The Advanced Firewall Settings link refers to the page where Quadro's privacy can be configured.

The **View Filter Rules** link opens the Filtering Rules page.

Fig. II-134: Firewall and NAT Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed towards the device. With these features enabled, Quadro will answer with inscrutable messages to the Ping and Portscanning operations.

Please Note: Operations are available only when the firewall is enabled from the Firewall and NAT page.

This page offers the following components:

The **Ping Stealth** checkbox selection prohibits a Ping operation toward Quadro from its WAN.

The **Fool Portscanner** checkbox selection prohibits Quadro portscanning from its WAN. As a reply to a Portscanning operation, "network unreachable" or "host unreachable" feedback messages will be sent.

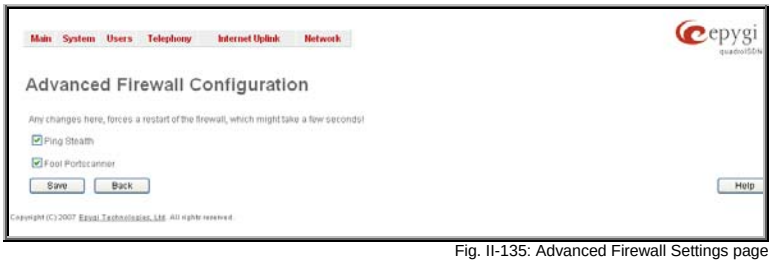


Fig. II-135: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows you to configure the filters for incoming and outgoing traffic.

To prevent inaccurate configuration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. Since the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled (additionally NAT should be enabled to use the **Port Forwarding** function in the **Incoming Traffic / Port Forwarding** filtering rules). The filtering rules are independent from the security level, so they will work if enabled, no matter what security level has been selected.

Please Note: Applying firewall rules will prevent the establishment of new connections that violate the rules. Applying rules does not kill existing connections that violate the rule.

View All displays all configured filters specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). Since it is read-only, no modifications are allowed and no functional buttons are available.

The **Incoming Traffic/Port Forwarding** filter is for incoming traffic. The rules here allow or deny systems on the Internet to reach the services of Quadro's LAN. The NAT service should be enabled on the Quadro to provide the possibility of **Port Forwarding** in the **Incoming Traffic/Port Forwarding** filtering rules. The **Port Forwarding** function will be unavailable if NAT is disabled on the Quadro.

The **Outgoing Traffic** filter is for outgoing traffic. The rules here allow or deny Quadro's LAN users to reach external services.

Management Access is used to enable management access to the Quadro from the Internet. A host on the Internet can be allowed to reach the Quadro.

Call Control Access is used to enable the access from the call controlling application from the Internet to the Quadro. The call controlling applications can be used to remotely initiate and handle calls on the Quadro and to subscribe for certain event notifications from the Quadro.

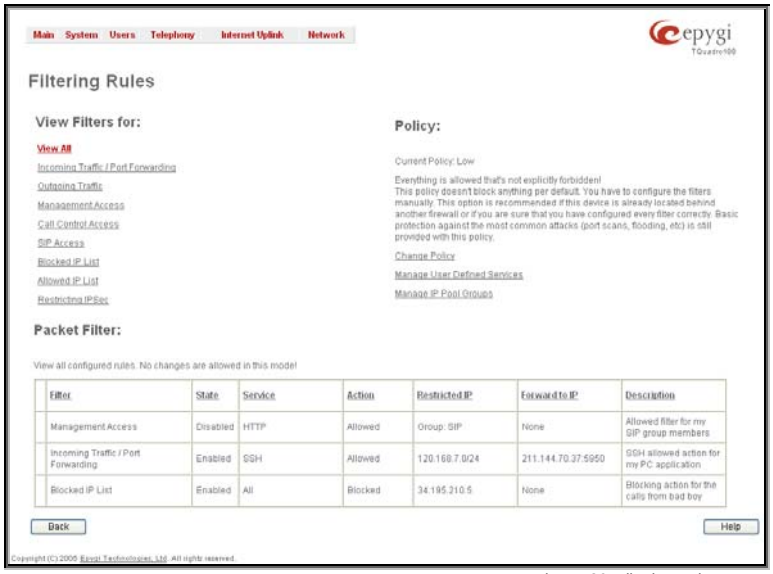


Fig. II-136: Filtering Rules page

SIP Access is to allow or deny the SIP access to or from the particular SIP servers, SIP hosts or a group of them. The **SIP Access** filtering rule may prevent or allow incoming or outgoing SIP calls to or from specified SIP server(s) or host(s).

When **Blocked IP List** is used, traffic from specific hosts may be blocked, no matter what services are opened in the other filters. NO traffic will be allowed to the specified hosts. The **Blocked IP List** service has a higher priority if the same host is also listed in the **Allowed IP List** table.

Allowed IP List allows trusted hosts to reach your network and vice versa. It is an exception to other rules and only all services may be allowed for a single host.

The **Filtering Rules** page provides several links. Each link opens its specific parameters on the same page. Only **Change Policy** (see chapter Firewall and NAT), **Manage user Defined Services** (see chapter Service Pool) and **Manage IP Pool Groups** (see chapter IP Pool) lead to separate pages. The **Filtering Rules** page also includes the currently selected firewall security (**Policy**) level and its description.

The table displayed on the bottom of this page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Disable** is used to disable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action,** a **Restriction** to certain IP address(es) or IP groups, and if adding a rule for **Incoming Traffic/Port Forwarding**, the destination IP address for **Forwarding**.

The page to add a rule for **Incoming Traffic/Port Forwarding** offers the following input options:

Service includes a list of possible services to be configured. All user-defined services also will be displayed in this list.

Action includes possible actions to setup the rule.

Forward to IP requires the destination IP address where traffic should be transferred to if it comes from the restricted host. The IP address defined in this field will be ignored for blocked action of the **Incoming Traffic/Port Forwarding** rule.

Please Note: It is not allowed to forward incoming packets when the NAT service is disabled on the Quadro.

Port Translation text field is available for "Allowed" action only and optionally requires the port number that will stand instead of the original port number when incoming packet is being forwarded. If this field is left empty, the original port number will be used when forwarding the packet.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.
- Selecting **Single IP** will require the IP address of the allowed or blocked host.
- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. The following are **Maskbit** examples:
  255.0.0.0= /8,
  255.255.0.0 = /16,
  255.255.255.0 = /24,
  255.255.255.255= /32
- **Single URL** requires the hostname of the allowed or blocked host.
- **Group** indicates the user-defined groups that include IP addresses that should to be allowed or blocked.

The **Description** field is used to insert an optional description of the filtering rule.

Fig. II-137: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filter** link (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List, Allowed IP List) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the **Filtering Rules** page. A page where a new rule may be added will appear in the browser window. The page will be named corresponding to the selected filter.
3. Select a service name from the **Service** list to configure a rule for it. If the list has a default value, do not change the default values.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, do not change the default values.
5. Enter the IP address in the **Forward to IP** field if an **Incoming Traffic Rule** is to be added.
6. Choose the restriction type by selecting **Any**, **Single IP**, **IP/Mask** or **Single URL** and enter the required information in the text fields or select a group.
7. Insert a **Description**, if needed.
8. To add a rule with these parameters, press **Save**.

To Delete Filtering Rules

1. Select the **Filter** link to delete a rule from its table. The appropriate **Filter** table will appear in the same window.
2. Check one or more checkboxes of the corresponding rules that should be deleted from the rules table. Press **Select all** if all rules should to be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

Service Pool

The **Service Pool** table is a list of all created services and their parameters. It is used to add new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or permission by defining a new filtering rule with the following:

Add opens the **Add New Service** page where new services may be added.

Edit opens the **Edit Service** page where the service parameters (except for the service name) can be modified. This page includes the same components as the **Add New Service** page. To operate with **Edit** only one record may be selected, otherwise the error message "One row must be selected" will appear.

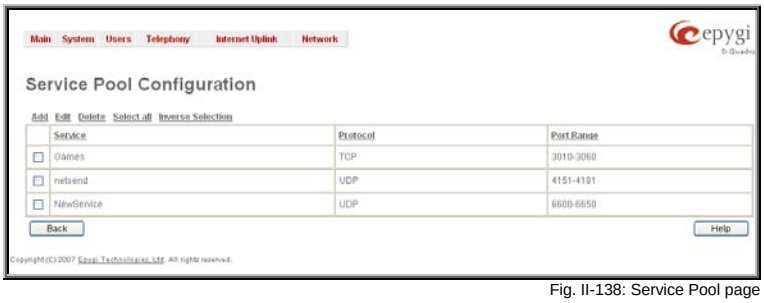


Fig. II-138: Service Pool page

The **Add** page is used to add new services and includes the following text fields and buttons:

Service Name requires a name for the service that should be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.

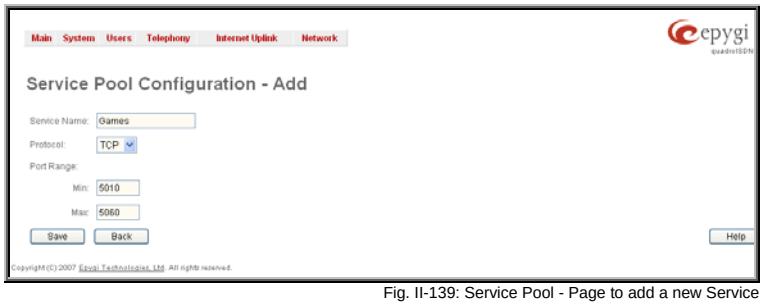


Fig. II-139: Service Pool - Page to add a new Service

To Add a new Service

1. Select the **Manage User Defined Services** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **Service Pool Configuration** page. A page where a new service may be added will appear in the browser window.
3. Define a service name in the **Service Name** text field.
4. Select the protocol type for the service from the **Protocol** drop down list.
5. Enter the port range in the **Port Range** text fields or leave one of them empty to define a particular port for the service.
6. To add a service with these parameters, click on **Save**.

To Delete a Service

1. Select the **Manage User Defined Services** link. The **Service Pool Configuration** page appears with the table of services (if any).
2. Check one or more checkboxes of the corresponding services that should be deleted from the **Service Pool** table. Press **Select all** if all services should be deleted.
3. Click on the **Delete** button on the **Service Pool Configuration** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

IP Pool

The **Manage IP Pool Groups** link opens the **IP Pool Configuration** page.

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.

Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

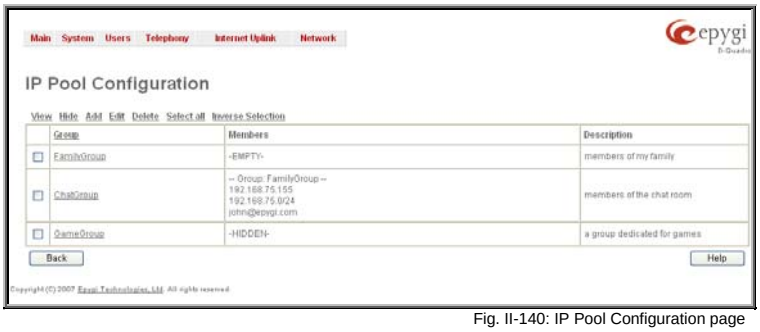


Fig. II-140: IP Pool Configuration page

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains). Deleting a group will also delete any reference to the corresponding group, including filter-rules and member relations to the other groups.

Clicking on the **Group** name will display an **IP Pool Group Configuration** page with the **Members** list for the current group.

Fig. II-141: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

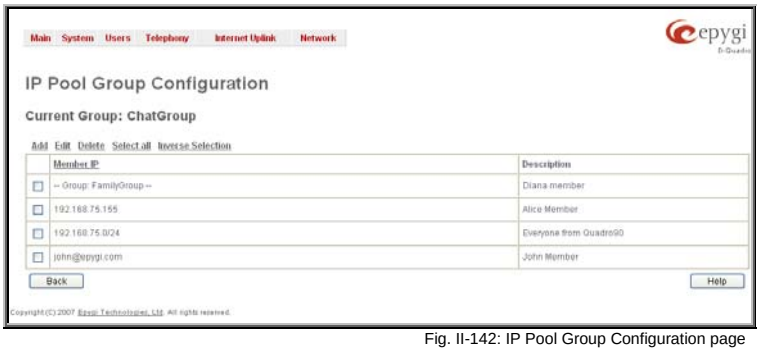


Fig. II-142: IP Pool Group Configuration page

The **Add Members** page provides the following radio buttons:

IPaddress requires the member IP address that is to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

URL Address requires the member hostname to be added to the group.

The **User-defined Group** includes previously added groups that may also be added as a member to another group.

Member description text fields can be used to enter an optional description of the member.

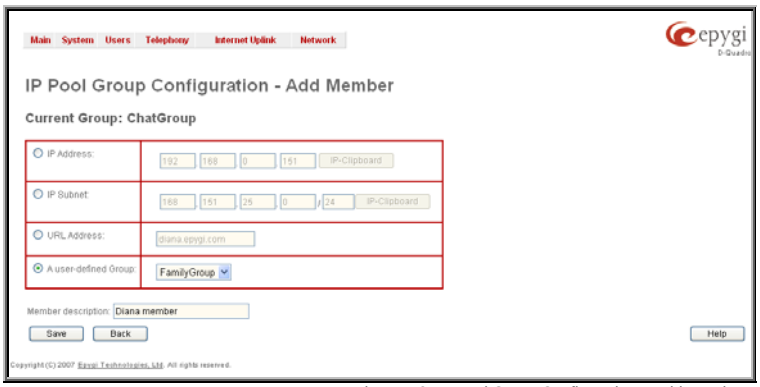


Fig. II-143: IP Pool Group Configuration – Add Member

To Add a new Group with Members

1. Select the **Manage IP Pool Groups** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **IP Pool Configuration** page. A page where a new group may be added will appear in the browser window.
3. Define a group name in the **Group Name** text field and fill in the **Group Description**, if needed.
4. To add a group with the given parameters, press **Save**.
5. Open the **IP Pool Group Configuration** page by clicking on the group name.
6. Select the **Add** button on the **IP Pool Group Configuration** page. A page opens where new members may be added to the group.
7. Enter an IP address for the member in the **IP Address** text fields, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
8. Enter a **Member Description** in the corresponding text field, if needed.
9. To add a member with these parameters to the selected group press **Save**.

To Delete a Member

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Click on the desired members that should be deleted. The **IP Pool Group Configuration** list will appear.
3. Check one or more checkboxes of the corresponding members that should be deleted from the **Members** table. Press **Select all** if all members should be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.
5. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

To Delete a Group

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Check the one or more checkboxes of the corresponding groups that should be deleted from the groups table. Press **Select all** if all groups should be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

IDS Log

The **IDS logging** page contains information about dropped packets and the senders responsible for those packets. IDS discards dangerous packets or packets including intrusion attacks. It generates a table with the IDS log report. The administrator can be notified about newly logged entries in various ways (mail, display notification and Flashing LEDs) depending on the settings in the **Event Settings** page. To make an IDS log reporting table, IDS needs to be enabled on the Firewall and NAT page.

The **IDS Logs** table is a list of new or read IDS entries and descriptions referring to them. The table provides a status row that has the value **New** if the entry is still unread or it is empty if the entry has already been read.

Mark All as Read marks all IDS logged entries as read and removes the **New** status from the **Status** row of the IDS entries table.

Delete Log is used to delete all entries from the IDS table.

A detailed log of the selected entry can be seen by clicking on the **Description** link of the corresponding entry in the **IDS Entries** table.

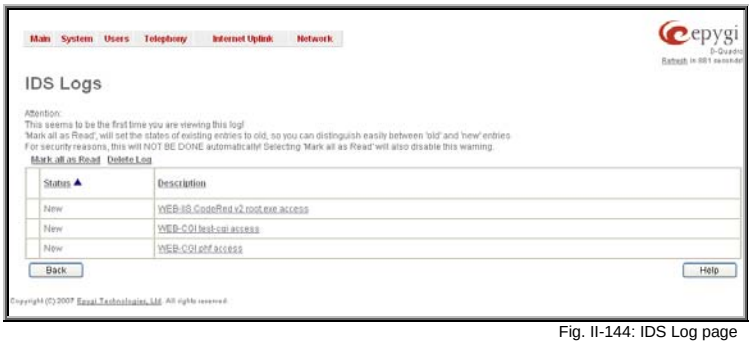


Fig. II-144: IDS Log page

The IDS Logs detailed page has a following preview:

The **Issue Detailed Log** table is a detailed list of new and read IDS entries. The table contains a **Status** row that has the value **New** if the entry is still unread or that is empty if the entry has already been read.

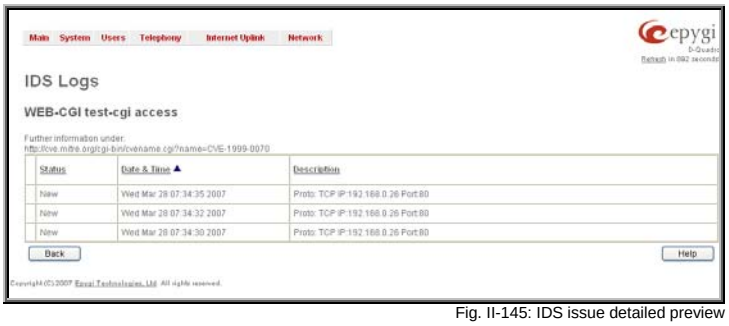


Fig. II-145: IDS issue detailed preview

Network Menu

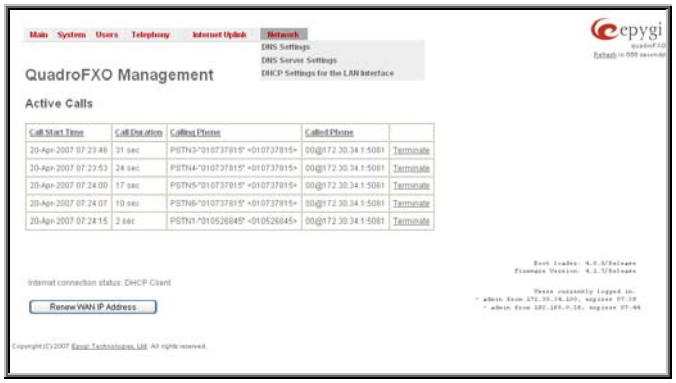


Fig. II-146: Network menu in Dynamo theme

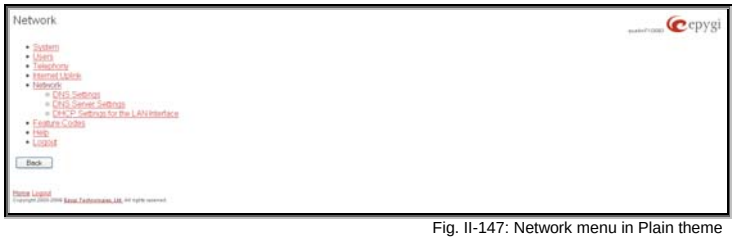


Fig. II-147: Network menu in Plain theme

DNS Settings

The **DNS Settings** page provides the option of setting up a name server for the Quadro. It offers the following components:

The **Nameserver Assignment** radio buttons are as follows:

- The **Dynamically by provider** selection automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** is a manually selected name server. The **Nameserver** text field requires the IP address of an external name server. The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.

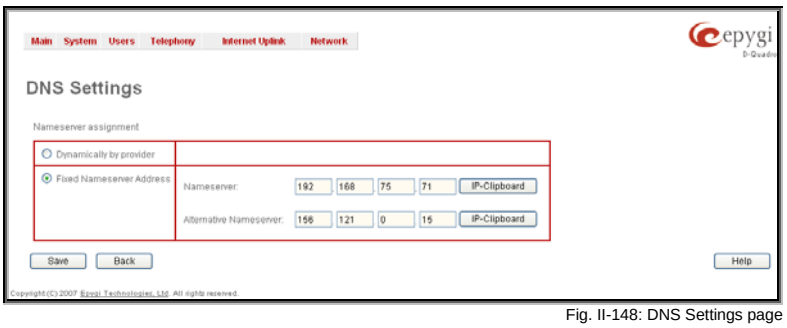


Fig. II-148: DNS Settings page

DNS Server Settings

The **DNS Server** on the Quadro provides the services to the hosts in the Quadro's LAN. With this service, Quadro returns the correct IP address to the requested domain name, so that any device in the LAN can be accessed by its hostname or alternative alias name.

The **DNS Server Settings** page is used to configure DNS server settings on the Quadro and to define a list of aliases for the devices in the Quadro's LAN. This page contains the following components:

Zone field displays the Quadro's host domain name as it is configured in the System Configuration Wizard.

Time to live (TTL) text field indicates the time (in seconds) during which the DNS server will keep the resolved names in its cache. During this time the same address will be resolved from the cache of the DNS server. When this timeout expires, the requested address will be resolved newly.

Mail Exchange (MX) text field indicates the mail server's hostname. When resolving the email address, the reference will go to the mail server defined in this field, before being sent out to the external network. The value in this field will be used in the MX record in the DNS server on the Quadro.

The table on this page lists aliases for each of the device in the Quadro's LAN to be resolves through the DNS server.

Fig. II-149: DNS Server Settings page

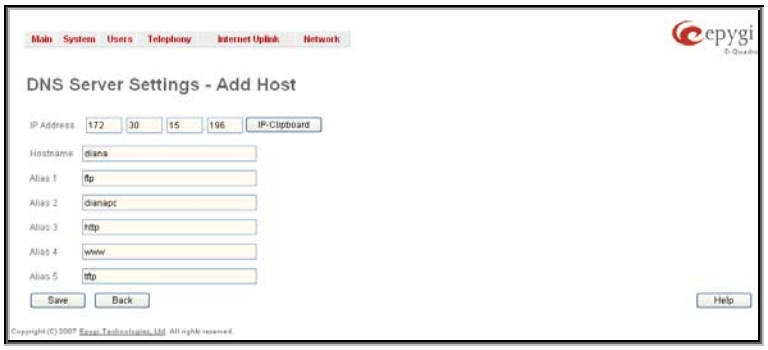


Fig. II-150: DNS Server Settings – Add Host page

Add functional link opens the page **Add Host** where a list of aliased can be defined for the certain device in the Quadro's LAN. The page contains the following components:

IP Address text fields require the IP address of the device in the Quadro's LAN.

Hostname text field requires the hostname of the device in the Quadro's LAN.

Alias text fields are used to enter up to 5 alias names by which the device in the Quadro's LAN will be resolved.

DHCP Settings for the LAN Interface

The **DHCP Settings** page provides the option of enabling a DHCP server and controlling the Quadro user's LAN settings. Therefore, Quadro LAN users will automatically be provided with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the Quadro's IP address)
- WINS server
- Nameserver (corresponds to the Quadro's IP address)
- Domain name

The **DHCP Settings** page offers the following input options:

Enable DHCP Server checkbox activates the DHCP server on Quadro. With this checkbox enabled, Quadro will be able to assign dynamic IP addresses to the devices in its LAN.

Give leases only to hosts listed in the static MAC address binding table checkbox enables the DHCP services only for the devices listed in the table below. With this checkbox selected, no DHCP services will be provided to the other devices.

IP Address Range defines a range of IP addresses that will be assigned to the Quadro LAN users. The IP range must be at least 6, otherwise the error message "Address Range too small" will prevent it from being saved. The error message "Address Range too large" will appear if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the Quadro LAN users.

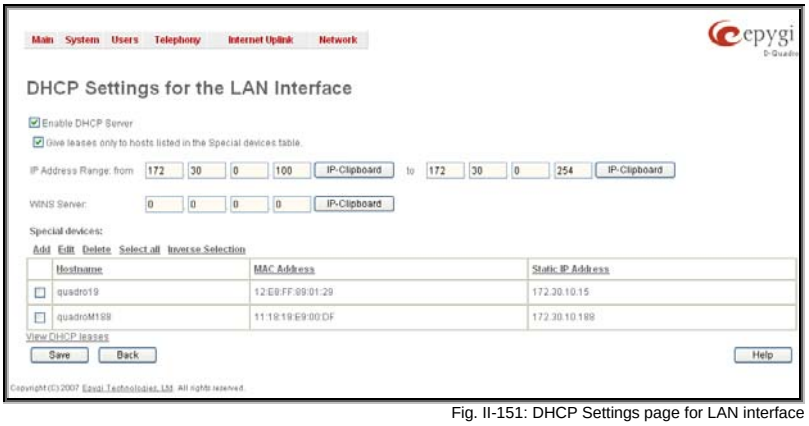


Fig. II-151: DHCP Settings page for LAN interface

The **DHCP Advanced Settings** link leads to the page where the advanced options of the Quadro's DHCP server can be configured. The page is used to modify the advanced options of the Quadro's DHCP server. It contains a table where a list of default DHCP server options is already defined.

- The **Authoritative** checkbox is used to enable/disable authoritative mode on the Quadro DHCP server. Disabling the checkbox is recommended if several DHCP servers are used on the network and the Quadro should provide network parameters to IP phones only.
- The **Ping Check** checkbox enables checking the availability of an IP address on the network before providing it to a client. If this checkbox is selected, the Quadro will first ping an IP address retrieved from the IP pool and wait for a reply. If no a reply is received within a timeout specified in the **Ping timeout** text field (by default 1 sec), the retrieved IP address will be provided to the client. If otherwise, a new IP address will be retrieved from the IP pool and the procedure will be repeated. If this checkbox is not selected, the Quadro will provide an IP address immediately when requested.

More options can be added from this page, as well as settings of the existing options can be modified. All options in the table on this page are then sent to the DHCP clients.

The following functional buttons are available:

Add opens a page **Add Entry** page where a new DHCP server option can be defined. The **Add Entry** page contains a group of manipulation radio buttons to select between the predefined DHCP server options or to define your own DHCP server option:

- **Predefined** - this selection allows you to select from the predefined DHCP server options.
  - The **Option Name** drop down list contains the most common DHCP server options.
  - The **Option Value** text field requires the value for the selected option. The type and format of the value inserted in this field is dependent on the option selected from the **Option Name** drop down list.
- **Custom** - this selection allows you to define a new DHCP server options. The following parameters are required to be inserted for a new option:

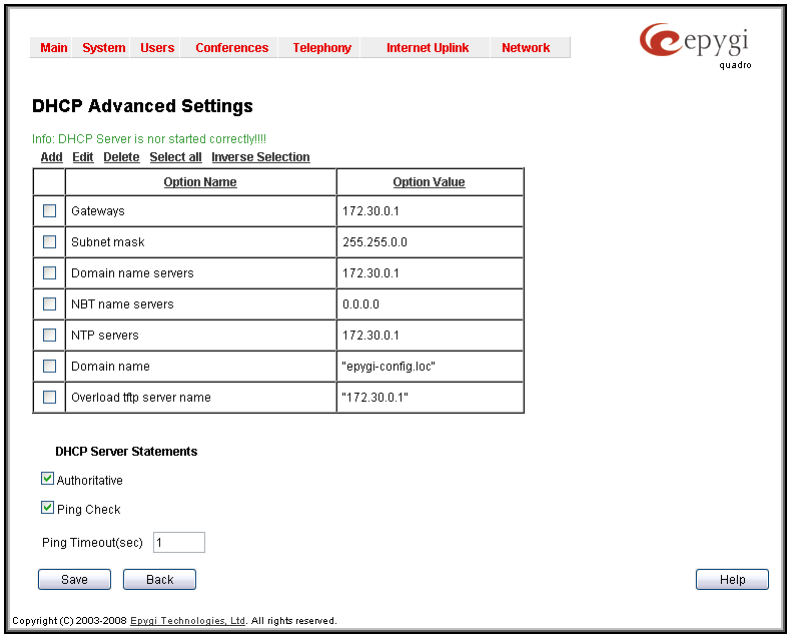


Fig. II-152: DHCP Advanced Settings

  - The **Option Code** text field is used to insert a code of the option. It may have values in a range from 0 to 255.
  - The **Option Value Type** drop down list is used to select the type of the option value. It may be an IP address, a boolean or integer value, etc.
  - The **Option Value** text field is used to insert the value of an option. Depending on the selected Option Value Type, this field should have the corresponding value. Warning messages will prevent saving if the value inserted in this field does not correspond to the requirements of the Option Value Type. If an array should be inserted here, the values should be separated with a comma.

Edit opens a page **Edit Entry** where existing DHCP server option settings can be modified. This page includes the same components like the **Add Entry** page does.

The **Special Devices** table on this page allows you to set a static IP address binding on the MAC address of the device in the Quadro's LAN. When this table is configured, the devices with defined hostnames and MAC addresses will always get the same LAN IP address from the DHCP server. Otherwise, devices not listed in this table will get dynamic LAN IP addresses. This table is also displayed in the System Configuration Wizard.

Add functional button opens an **Add Host** page where a new static MAC address binding can be defined. The page consists of the following components:

Hostname text field requires the hostname of the device in the Quadro's LAN.

MAC Address text fields require the MAC address of the device in the Quadro's LAN.

Static IP Address text fields require a fixed IP address of the device in the Quadro's LAN.

Please Note: If you leave this field empty, the device in the Quadro's LAN will get the first available IP address from range defined in the **DHCP Settings** page (see above).

Fig. II-153: Static MAC address binding – Add Host page

View DHCP Leases leads to the page where the DHCP leased LAN IP addresses are listed.

The **DHCP Leased IP Addresses** page includes a list of the leased host addresses that are part of the Quadro's LAN. For these hosts, Quadro acts as a server supplying them with a unique IP address. It displays a read-only table describing all the leased IP hosts and their parameters. The table contains the following columns:

IP address - host IP address, assigned by Quadro.

MAC address - host MAC address, provided by the host itself.

Lease Start - date and time when the leased IP address has been activated.

Lease End - date and time when the leased IP address has been or will be deactivated.

Binding State – indicates the state of the DHCP lease.

Hostname - hostname, provided by the host itself.

Fig. II-154: DHCP Leases page for LAN interface

Registration Form

The **Registration Form** page appears when administrating an unregistered Quadro, and it has been created for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It provides several links offering the following registration options:

Register now leads to the Epygi Technical Support System Registration page and requires customer's information to submit the Quadro registration form.

Remind me later hides the registration notification in the Quadro through System Configuration Wizard or Internet Configuration Wizard until the next administrating activities.

Don't remind me more hides the registration notification forever.

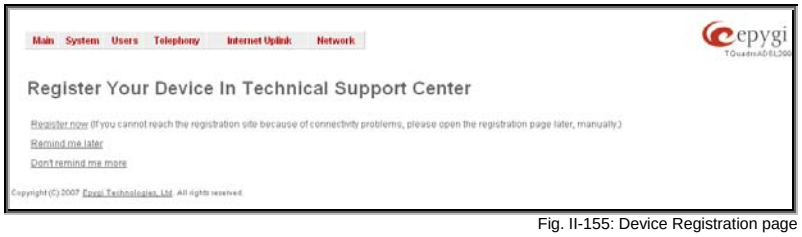


Fig. II-155: Device Registration page

Logout

This option is used to close the session between the user PC and Quadro and to leave the QuadroFXO Web Management or to enter the management with another login. By selecting the **Logout** button, the startup page will be displayed and the user needs to login again.

Extension User's Menus

When logging in as an extension user the page **Extension Settings** is displayed with the Main Page table as a startup. This page displays a list of available codecs for the corresponding extension, the list of other extensions on the Quadro, their Display names, the SIP registration username and line number (if attached), as well as the FXO lines state and the destination to route incoming calls. For FXO lines, allowed call types are displayed here.

Voice Mail

- Voice Mailbox
- Voice Mail Settings
- Group List

Your Extension

- Call Statistics
- Account Settings

Supplementary Services

- **Caller ID Based Services**
  - Incoming Call Blocking
  - Outgoing Call Blocking
  - Call Hunting
  - Unconditional Call Forwarding

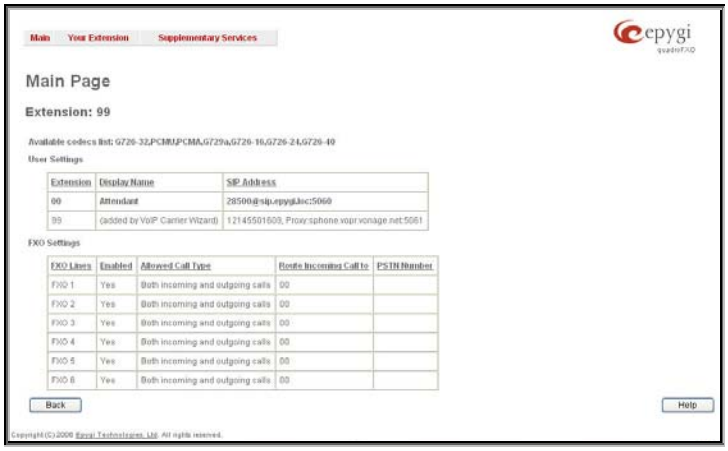


Fig. III-1: Quadro Extension User's page

Main Page

The **Main Page** provides read only information about the extension codecs, other existing extensions and available FXO lines on the Quadro depending on the active interface.

The **Main Page** displays a list of available codecs for the corresponding extension, the list of other extensions on the Quadro, their Display names, the SIP registration username and line number (if attached). It also displays the FXO lines state and the destination to route incoming calls. For FXO lines, allowed call types displayed here.

Voice Mail

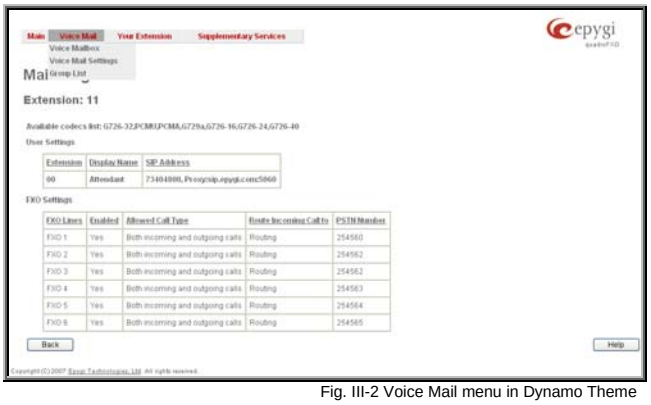


Fig. III-2 Voice Mail menu in Dynamo Theme

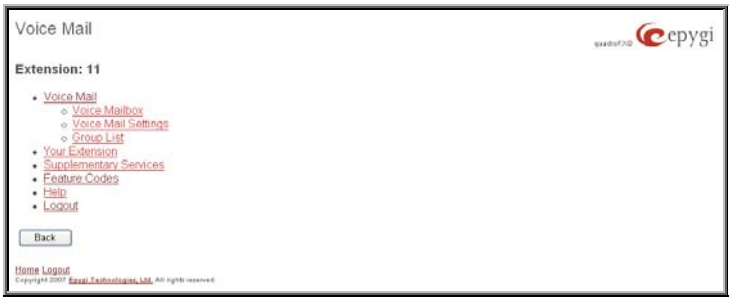


Fig. III-3 Voice Mail menu in Plain Theme

The **Voice Mail Service** provides a possibility to leave brief voice messages on the mailbox of an unavailable or busy Quadro extension. The caller hears a greeting message (configurable by the extension user) and a signal initiating the Voice Mail recording. The extension user may configure the maximum duration of the voice message, as well as the Voice Mail system activation timeout (see chapter Voice Mail Settings).

Received voice messages are stored in the Voice Mailbox. They can be accessed by the * 0 key combination from the phone handset and via Quadro management. Voice messages can to be played, marked (from GUI only), deleted, replied to (from handset only) or forwarded by the user. Messages with a facsimile (FAX) attached will be displayed in a special way in the Voice Mailbox on web management access and will be indicated by a special voice signal when accessing the message from the handset. The Incoming FAX message can be viewed and downloaded to the PC from the Voice Mailbox at Web management access as a *.tif picture file.

Quadro's Voice Mail service also allows reviewing system messages used for telephony services functionality. The voice mail greeting, incoming and outgoing blocking messages, user's name and out of office greeting can be played, recorded and restored. Greeting messages are played to the caller announcing that the called extension is unavailable and asking to leave a voice mail. Blocking messages are played when receiving or making incoming/outgoing calls from/to the restricted destination. User's name is played when surfing the Extensions Directory. The personal out of office greeting is played instead of the main greeting message, when out of office option is selected on the extension.

Voice Mailbox

Quadro provides caller the possibility of leaving voice messages when called extension is busy or unavailable. A voice mail greeting message, and a voice signal indicating voice mail recording initiation, are played back to the caller.

All voice mail functionality settings, such as enabling the greeting message, adjusting the maximal voice mail duration, voice mail system activation timeout, etc, are configurable by the user through the extension's Voice Mail Settings.

Received voice mails are stored and are accessible in the extension's Voice Mailbox. Quadro supports two ways of accessing the extension's Voice Mailbox: through the phone handset and through Quadro Web Management. With both options, the user is free to manipulate with voice mails located in the Voice Mailbox, such as playing, deleting, forwarding, etc.

When accessing the Voice Mailbox through the phone handset, additional settings to manipulate the user defined system messages are provided. The user can define their own Voice Mail Greeting, Incoming and Outgoing Blocking messages as well as the User's recorded name. Each of these system messages can be played, recorded and restored. Voice Mail Greeting messages are played back to the caller announcing that the called extension is unavailable and asking to leave a voice mail. Blocking messages are played back to the caller when receiving or making incoming/outgoing calls from/to the restricted destination.

Instructions on accessing and navigating within the voice messages and Voice Mailbox Services via the phone handset are described in the Feature Codes.

Please Note: When playing newly received voice mails (via a phone handset or with the use of the **Play** button in this page) will deprive the "New" state of the voice mail.

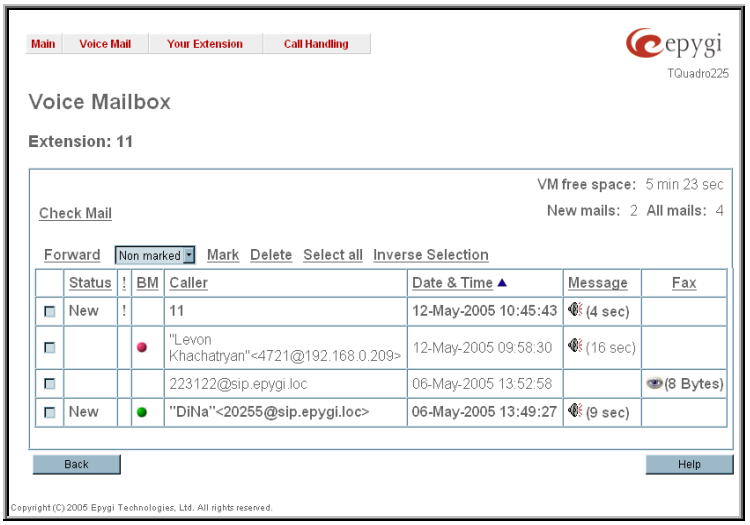


Fig. III-4 Extension Voice Mailbox

The **Voice Mailbox** can hold **New** (not yet played) and **Old** (already played) voice mails. The **Status** column in the Voice Mailbox table indicates the current state of the voice mails. All new mails in the table are displayed in bold font. Playing a voice mail cancels both the **New** status and bold font.

Voice mails can be selected to be played, deleted, marked as important or book-marked, etc. Additionally they can be forwarded to desired email addresses.

VM free space provides information on the number of minutes/seconds of free voice mailbox space.

The following functional buttons and fields are available:

Check Mail refreshes the mailbox and updates the number of newly arrived mails (if any).

New Mails shows the number of newly arrived mails since the user's last access to the voice mailbox.

All Mails shows the number of all mails existing in the mailbox.

The **Voice Mailbox** tables display all voice mails in the mailbox:

Status - indicates whether the voice mail is **New** and not yet played. New mails are displayed in bold font.

! - indicates whether message has an urgent priority or not.

BM (bookmark) - shows marked records. The fields can include some indications (image signs) depending on the type of being marked.

Caller – is the address of the caller who left the voice mail.

Date & Time – is the voice mail receipt date and time.

Message – indicates voice mail duration (in minutes/seconds) and a speaker sign used to play (using any available media player supported by your Operation System) the received voice mail or to download the audio file to the PC.

FAX (facsimile) – indicates whether a FAX message is attached to the voice mail, and if so, displays the size of the FAX message (in KBs) and an icon used to view the incoming FAX message or download the graphical file to PC.

The column headings of the voice mail tables are created as a link. By clicking on the column heading the table will be sorted by the selected column. Upon sorting (ascending, descending) arrows will be displayed next to the column heading. Each row in the Voice Mailbox tables can be selected by a checkbox for editing, deleting or marking.

The following functional buttons serve to modify the table entries:

Forward link allows forwarding a selected voice mail to one or more email addresses with some enclosed message in the email body. The link refers to the page where email addresses should be defined (use a space or a comma to separate the mailing addresses in the text field), email subject and some message can be inserted. Voice mails will get automatically converted to the G.711 codec before being attached to the email. The Voice Mail forwarding feature is active only when Mail Service is enabled otherwise the "Mail Service is disabled" error appears.

Mark submits the values chosen out of the drop down list aside (Important or Bookmark) to the selected records.

Delete removes the selected voice mail record(s).

Select All checks all existing entries in the table.
Inverse Selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

To Play a Voice Mail

1. Click on the speaker icon of the corresponding voice message.
2. Depending on you browser's settings the .wav file will be played directly or an application will ask you to save the .wav file on the local PC. In the second option, please specify the path and run the media file from the specified location to play it.

To Mark a Voice Mail Record

1. Select the checkbox of the corresponding record in the **Voice Mailbox** table that should to be marked. Press **Select all** if all extensions should to be marked.
2. Select the desired marking type from the **Mark** drop down list.
3. Select the **Mark** button to initiate the marking operation. Depending on the selected marking type the record(s) will show an image sign in the corresponding **BM** field.

To Delete a Voice Mail Record

1. Select the checkbox of the corresponding record(s) in the **Voice Mailbox** table that should to be deleted. Click on **Select all** if all records should to be deleted.
2. Select the **Delete** button.
3. Confirm the deletion with **Yes**. The selected voice messages will be deleted. To abort the deletion and keep the messages in the inbox, select **No**.

Voice Mail Settings

The **Voice Mail Settings** permits enabling the **Voice Mail Service** for the callers if the called extension is not available or does not answer. The voice mail system will be activated allowing the caller to leave a voice message. This page also provides information on the voice mailbox settings such as maximal mail message duration and various settings for the voice mailbox as well as a possibility to send voice mails via e-mail.

Please Note: **Voice Mail Settings** are only available when the Voice Mailbox is enabled on the extension. If you find Voice Mail Settings are unavailable please refer to your system administrator.

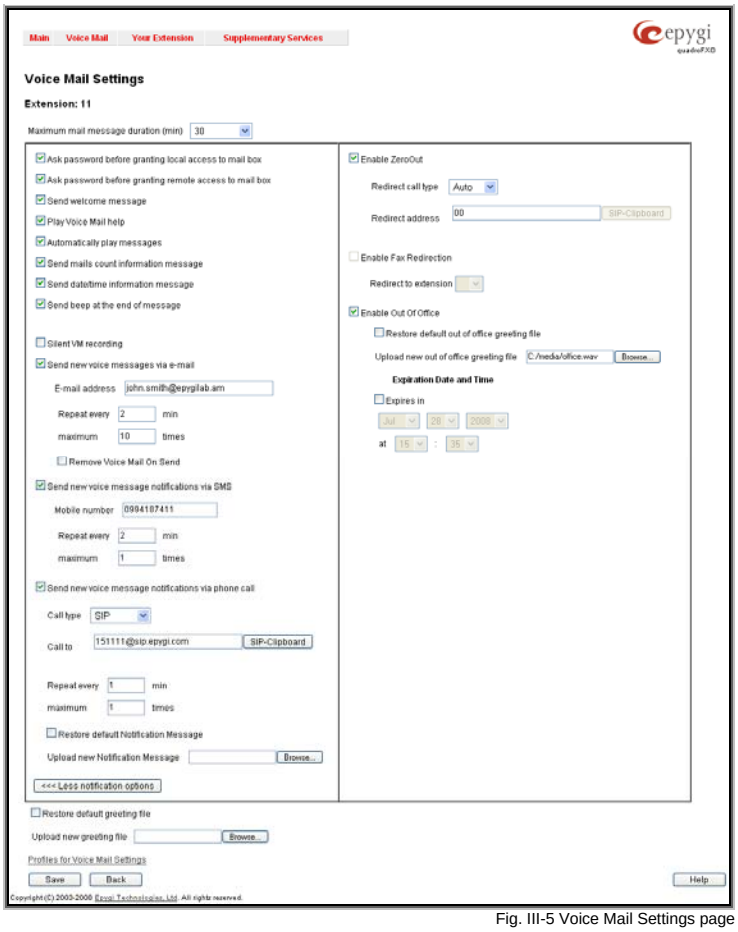


Fig. III-5 Voice Mail Settings page

The **Voice Mail Settings** page offers the following input options:

Maximum mail message duration lists the possible values for the maximum mail duration (counted in minutes) during which a voice mail will be recorded. The **Unlimited** selection allows voice message recording as long as the user's space remains.

Ask password before granting local access to mailbox protects local access of the user's voice mailbox. If the checkbox is checked a user password will be required to access the voice mailbox via * 0 digit combination.

Ask password before granting remote access to mailbox protects remote access of the user's voice mailbox. If the checkbox is checked a user password will be required to access the voice mailbox when reaching it through the Auto Attendant.

Send welcome message enables a welcome message to be played to the user when accessing the mailbox locally.

Play Voice Mail Help is an optional setting that plays voice mail help instructions to the user when entering the Voice Mailbox. This option guides the user through the mailbox, explaining how to play and delete the voice mails as well as modifying system messages.

Automatically play messages will auto play of all voice mails. Whenever entering the voice mailbox, the system will sequentially play the date/time when the message was received followed by the voice mail itself in the order sorted by the priority level (starting with the message in highest priority) or. If no priority is specified, they will be played in the order in which messages were received, i.e. starting with first (oldest) message. When the last message is played, the Voice Mail help will be replayed.

Send mails count information message announces the number of **New** (unread) voice messages in the mailbox when entering the mailbox.

Send date/time information message announces the time and date a voice message was received and is played before every voice message.

Send beep at the end of message enables an optional parameter that activates a "beep" sound after each played voice message.

When the **Silent VM recording** checkbox is selected, callers who have reached the extension's voice mail service will not hear an invitation to record a voice mail and the following beep sound. The voice mail recording will start without any additional notification.

Send new voice message via email is an option to send new voice mail files via e-mail to the defined recipients. Mails will be automatically converted to the Windows wave (PCMU) format before being attached to the e-mail. Checkbox activates the following input options:

Email Address requires the e-mail address(es) of the person(s) that should to receive the newly arrived voice mails on their e-mail account(s). Use a space or a comma to separate the mailing addresses in the text field.

The next two fields are used for retransmission of the voice mail via email. Number of times text field requires the maximum number of times the voice mail will be delivered via email to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the voice mail is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field.

Remove Voice Mail on send removes the voice mail from the user mailbox after sending it to the e-mail recipient(s).

Attention: The e-mail can only handle up to 3 minutes long voice mails. If the voice mail is longer than 3 minutes, it will be truncated and only the first 3 minutes of it will be sent to the indicated e-mail address. However, in the e-mail body the recipient will receive the information that the attached voice mail is truncated and the total length of the voice mail. Please note that the voice mails longer than 3 minutes will not be removed from the voice mailbox once they are sent per e-mail even if the **Remove Voice Mail on send** checkbox is selected. This gives you a possibility to listen to the ending of the voice mail directly from your voice mailbox (from the handset or by downloading it from the Web management).

Please Note: This service will work only when **System Mail** is enabled on the Quadro. Contact your system administrator if you have problems with voice mail delivery via email.

Send new voice message notification via SMS allows the voice mail notification delivery via SMS to the defined mobile number. Checkbox activates the following input options:

Mobile Number text field requires the destination's mobile number.

The next two fields are used for retransmission of SMS notifications. The number of times text field requires the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the notification is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field.

Please Note: This service will work only when **SMS Service** is enabled on the Quadro. Contact your system administrator if you have problems with voice mail notifications delivery via SMS.

Send new voice message notification via phone call enables the voice mail notification delivery via a phone call to the defined phone number. The checkbox activates the following input options:

Call Type drop down list includes the available call types:

- PBX - local calls to Quadro extensions;
- SIP – calls through a SIP server;
- Auto – for undefined call types. The destination (independent on whether it is a PBX number or SIP address) will be reached through Routing;
- Callback – automatic call to the voice mail author. This can be used as a notification that the recipient has received the voice mail but has not yet played it.

Call To text field requires the destination's phone number depending on the selected call type. For **Callback** call type, no destination's phone number is required.

The next two fields are used for retransmission of phone notifications. Number of times text field indicates the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the notification is specified to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field. For **Callback** call type, the first notification is sent to the voice mail author after the first expiration of the interval defined in the **Repeat every** text field. For calls with call type different from Callback, the first notification will be sent immediately.

Restore default Notification Message restores the default notification message. If the checkbox is selected, the file upload will be disabled.

Upload new Notification Message will show the attached notification file selected by the current extension. Please note that a different notification message can be uploaded in case this service serves as a notification to the extension user (to inform about the new voice mail received) or if it serves as a notification for the voice mail author to be informed that the message has been received by the Quadro but is not yet played by the extension user. The uploaded file needs to be in the PCMU wave format, otherwise the system will prevent uploading with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading in case insufficient space is available on Quadro for the corresponding extension and gives a "You do not have enough space" warning.

Browse browses for the notification file that must be in PCMU wave format.

Download Notification Message appears only if a file has been uploaded previously. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

The **ZeroOut** voice mail feature allows a caller that has reached the called extension's voice mailbox to accelerate the automatic redirection feature instead of leaving a message in the extension's Voice Mailbox. To activate this feature, the caller should dial 0 digit (see Feature Codes) during the voice mail greeting which invites the caller to leave a message. The caller will then be automatically transferred to the destination specified in this page.

Enable ZeroOut checkbox selection enables the ZeroOut feature and activates the following fields to be inserted:

Redirect Call Type drop down list includes the available call types:

- PBX - local calls between Quadro extensions and the Auto Attendant
- SIP – calls through a SIP server
- PSTN – calls to PSTN
- Auto – used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

The **Redirect Address** text field requires the destination address where the caller should be automatically forwarded to if activating the ZeroOut feature.

The **Enable FAX Redirection** checkbox is used to redirect the incoming FAX (facsimile) when the FAX tone is detected after Voice Mail has been activated. The checkbox selection enables the **Redirect to extension** drop down list where extensions with enabled FAX Support are listed and is used to select the extension where the incoming FAX should be forwarded.

The **Enable Out of Office** checkbox allows activation of the Out of Office message which acts as an optional Voice Mail Greeting message in the period while the user is out of office, on vacations, etc. When this checkbox is selected, a user-defined Out of Office message will be played (if uploaded or recorded from the phone handset, otherwise a default Out of Office message will be used) to the caller which reached the called extension's Voice Mailbox.

Restore default Out of Office file restores the default Out of Office message file. If the checkbox is selected, the file upload will be disabled.

Upload new Out of Office Greeting file will show the attached Out of Office message file selected by the current user. The Out of Office message file will be played to a caller when entering the voice mail system. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent its uploading and will give the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading when insufficient space is available on Quadro for the corresponding extension. In this situation, the "You do not have enough space" warning will be received. Optionally, the Out of Office message can be recorded from the phone handset (see Quadro's Feature Codes).

Browse browses for the Out of Office message file that must be in PCMU wave format.

Download Out of Office Greeting file appears only if some file has been uploaded previously. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

Expiration Date and Time selection is used to set the expiration date and time of the Out of Office message validity. When the expiration date/time expires, the Out of Office message automatically gets disabled and Voice Mail regular greeting gets activated again.

Restore default Greeting file will restore the default greeting file. If the checkbox is selected, the file upload will be disabled.

Upload new greeting file will show the attached greeting file selected by the current user. The greeting file will be played to a caller when entering the voice mail system. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will be received. The system also prevents uploading in case insufficient space is available on Quadro for the corresponding extension. In this situation, the "You do not have enough space" warning will be received. Optionally, a greeting file can be recorded from the phone handset (see Quadro's Feature Codes).

Browse browses for the greeting file that must be in PCMU wave format.

Download Greeting File appears only if a file has been previously uploaded. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

The **Voice Mail Profiles** link is present only when the administrator accesses this page. It is hidden for the extension user's access. This link leads to the page where custom voice mail profiles and their settings can be defined.

Group List

Group List allows you to define Groups with the specified addresses inside. The **Group List** is used to send or forward voice messages (see Feature Codes) to the number of addresses simultaneously. Groups may consist of a variety of PBX and SIP addresses.

The **Group List** page consists of a table where all defined Group Keys and the corresponding addresses are listed.

Press on a link in the **Addresses** column to access the **Address List for the Group** page and to modify the addresses of the corresponding group. If Group doesn't include addresses, "no address is available" will be displayed in the **Addresses** column.

The **Add** functional button opens the **Group List - Add Entry** page where a new Group Key can be defined.

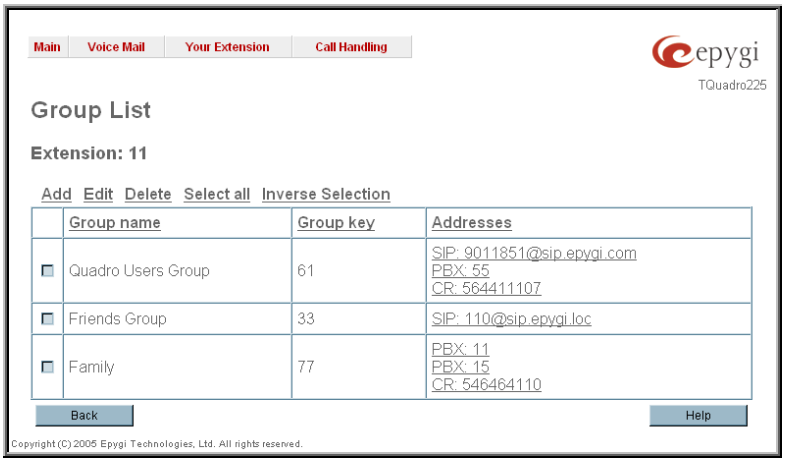


Fig. III-6 Group List page

The **Group List - Add Entry** page consists of two text fields used to insert the **Group Key** and the **Group Name** (optionally). The **Group Key** should include numeric characters only and should be unique in the Group List table.

Please Note: Groups with keys equal to extension numbers on Quadro have a higher priority and will be applied when sending or forwarding a voice message to the corresponding destination.

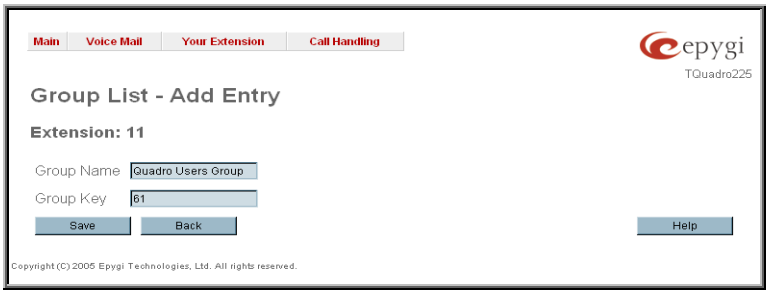


Fig. III-7 Add Group page

Fig. III-8 Addresses List page

The **Address List for the Group** page contains a table of addresses where new address may be added to the group and existing ones may be edited or deleted.

The **Add** functional link moves to the **Address List for the Group – Add Entry** page where new address may be defined.

Address List for the Group – Add Entry page consists of he following components:

Call Type lists the available call types:

- PBX - local calls between Quadro extensions and Auto Attendant
- SIP – calls through a SIP server
- Auto – used for undefined call types. The destination (independent on whether it is a PBX number or SIP address) will be reached through Routing.

The **Address** text field is used to define the address that ought to be included in the group. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the Quadro extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined.

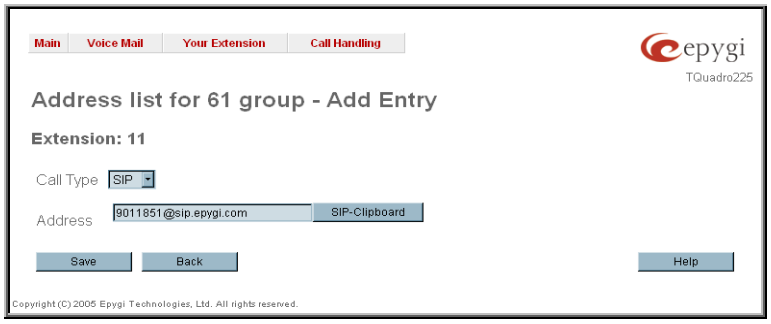


Fig. III-9 Add Address page

To Configure a Group

1. Press Add in the Group List page. **Group List - Add Entry** page will be displayed in the browser window.
2. Fill in the **Group Key** and **Group Name** (optionally) in the same named field.
3. Press **Save**.
4. Click on the link in the row corresponding to the newly created Group.
5. Press Add in the **Address List for the Group** page. **Address List for the Group – Add Entry** page appears.
6. Choose a **Call Type** from the corresponding drop down list.
7. Define the group member address in the **Address** text field.
8. Press **Save**.

Your Extension

Fig.0-10 Your Extension menu in Dynamo theme

Fig. III-11 Your Extension menu in Plain Theme

Call Statistics

The page **Call Statistics** allow collecting the call events and their parameters over the Quadro, i.e. incoming and outgoing calls reporting. It contains three tables and provides reports on successful, not successful and missed incoming and outgoing calls for the current extension only. The page also gives a possibility to filter the collected **Call Statistics** based on various criteria. The search components are as follows.

The **From** and **To** text fields are used to search by date and time. The data must be inserted in the following format: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The **From** field has to indicate an earlier date and time than the **To** field. If the entered data does not correspond with this condition, the "Minimal date should be less than maximal date" error message prevents statistics filtering.

The **From** and **To** drop down lists are used to search by duration. The duration needs to be specified from the listed values. The **From** field has to indicate a shorter duration than the **To** field. If the entered data does not correspond with this condition, the "Minimal duration should be less than maximal duration" error message prevents statistics filtering.

Called Phone requires the called party's SIP address, extension or PSTN number as a search criteria.

Calling Phone requires the caller party's SIP address, extension or PSTN number as a search criteria. For **Called** and **Calling Phone** wildcards are available (see chapter Entering SIP Addresses Correctly). If the defined caller or called addresses are inserted incorrectly the "Calling (Called) address is incorrect" error will prevent filtering.

Fig. III-12 Extension's Call Statistics page

The **Call Statistics- Successful Calls, Missed Calls and NonSuccessful Calls** tables list the successful, missed and not successful incoming and outgoing calls and their parameters (Call Start Time, Call durations, Calling and Called phones) for the current extension. Each column heading in the tables are created as links. By clicking on the column heading, the table will be sorted by the selected column. After sorting (ascending or descending) arrows will be displayed close to the column heading.

Number or records displays the current number of statistics entries in the table. For Successful calls **Total Duration, Maximum Duration, Average Duration** and **Minimum Duration** are displayed at the top of the table.

Call Detail column is present in the **Non Successful Calls** table only and indicates the reason of the call being unsuccessful.

Filter performs a search procedure by the selected criteria. The search may be conducted with several criteria at once.

To Filter the Statistics

1. Enter the desired search criteria.
2. Click on the **Filter** button to search call reports within the **Call Statistics** table.

Please Note: To return to the complete statistics table clear all search criteria and press **Filter**.

Account Settings

The **Account Settings** page provides information on the extension display name, allows changing the user password, enabling user password protection for incoming/outgoing calls and downloading/uploading of a file with the user-defined voice greetings. All parameters listed on this page may be modified and submitted. The page consists of the following components:

Extension shows a non-editable parameter providing information about the current user extension number.
Display Name defines an optional parameter used to identify the calling party. Usually the display name appears on the phone display if a call is placed or a voice mail is sent. The field is not limited regarding symbol usage but its length is limited to 20 characters.
User Permissions selection indicates password protection for:

- **Incoming Calls** enables password protection for incoming calls. If the service is enabled a user password is required to be able to accept the incoming calls.
- **Outgoing Calls** enables password protection for outgoing calls. If the service is enabled a user password is required to be able to make calls.

Fig. III-13 Extension Account Settings page

The **File to upload** text field can be used to type in the path where backed up file with voice messages is located. If voice greetings are browsed with the help of a file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the previously downloaded file with custom voice messages.

Attention: Uploading the selected file will replace your custom voice messages. Uploading custom messages downloaded from the other Quadro will overwrite messages that have not been configured by the user with the current device defaults. This means that if some default messages were used on one Quadro, they may be completely different on the other one upon the uploading of the voice data.

The link **Download custom voice messages** appears only when there are some user-defined custom greetings recorded and is used to download a compressed file with all user specified voice messages. The link opens the file-chooser window to specify the saving location.

The link **Change Password** refers to the page where the user password can be changed.

The **Change Password** page requests the following information:
Old Password requires the existing password for the extension access (this field is not displayed when the administrator updates the user's password from the User specific configuration page).
New Password is used to change the existing one. The password should only consist of digits with a length between 0-20 digits.
Confirm New Password is used to confirm the new password. If the entered **New Password** does not match to the one entered in the **Confirm Password** field the error "The passwords do not match. Please try again" will appear.

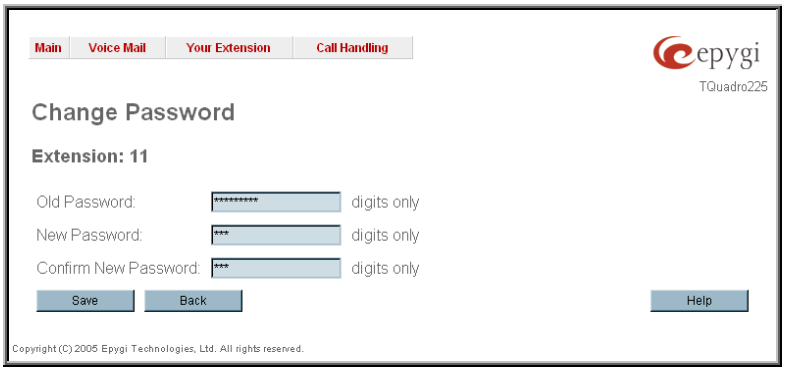


Fig. 3-14 Change Password page for extension access

Please Note: If the extension is allowed to be used for the Call Relay service from the Quadro's Auto Attendant, it is highly recommended to define a proper and non-empty password on this page.

Supplementary Services

Fig. III-15 Supplementary Services menu in Dynamo Theme

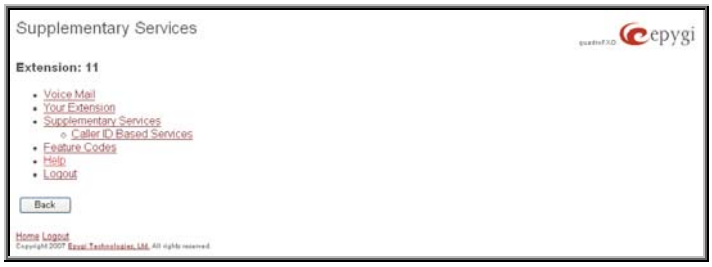


Fig. III-16 Supplementary Services menu in Plain Theme

Caller ID Based Services

The **Caller ID Based Services** page provides a possibility to configure a set of telephony settings from the same page. Incoming and Outgoing Call Blocking Settings, Unconditional Call Forwarding and Call Hunting services are configurable from this page.

The **Caller ID Based Services** page contains a table where all caller or called destinations and the states (ON or OFF) of caller ID based services for each of them are listed. Caller or called destinations are used to configure caller ID based services based on them. The column headings of the table are designed as links. By clicking on the column heading the table will be sorted by the selected column. Upon sorting (ascending or descending) arrows will be displayed close to the column heading.

The table also has **Any Address** entry that is undeletable. It is used to configure caller ID based services for all addressed. When adding a new caller address **Any Address** is changed to **Other Addresses**. Now there could be different configurations for the specified addresses and for all others.

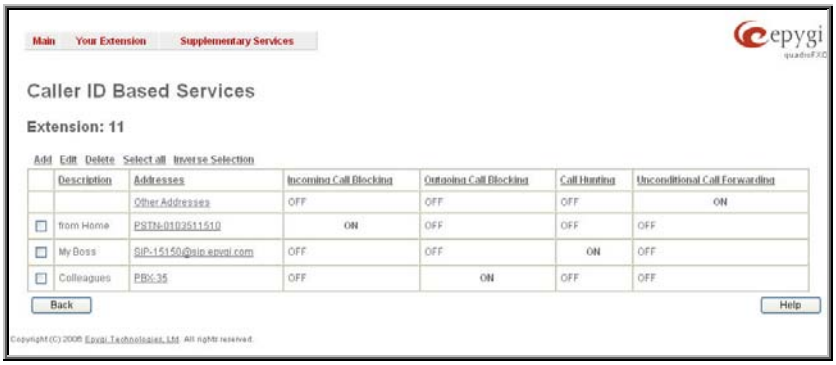


Fig. 3-17 Caller ID Based Services page

Add opens the **Caller ID Based Services** - **Add Entry** page where a new address can be defined. Page consists of the following components:

The **Description** text field requires optional information about the address owner.

Call Type lists the available call types:

- PBX - local Quadro extensions and Auto Attendant
- SIP – caller or called destinations reached through a SIP server
- PSTN – caller or called destination dialed from or to PSTN
- Auto – used for undefined call types. In this case, for incoming calls from specific address, configuration of caller ID based services will apply either to PBX, SIP or PSTN callers. For outgoing calls, the called destination will be reached through Routing.

Addresses text field requires a SIP address (see chapter Entering SIP Addresses Correctly), an extension or a PSTN number, for whom supplementary services should be applied. If the address already exists in the table, selecting **Save** will give the error "Caller address already exists". Wildcard is allowed in this field (see chapter Entering SIP Addresses Correctly). Entering "*" as PBX or PSTN addresses will apply configuration of supplementary services to all extensions or PSTN users.

The extension number should be inserted in the **Addresses** text field for the PBX call type. The PSTN number length depends on the area code and phone number.

Fig. 3-18 Caller ID Based Services – Add Entry page

When clicking on the **Address** in the **Caller ID Based Services** table, the caller ID based services configuration pages for the corresponding extension will be displayed.

The **Caller ID Based Services for Address** page consists of two frames. In the left frame all caller ID based services are listed. Clicking on the corresponding caller ID based service, its settings will be displayed in the right frame.

Please Note: Pay attention to save changes before moving among caller ID based services configuration pages.

Fig. 3-19 Caller ID Based Services for Address page

Below is the guidance on configuration of each caller ID based service available to the user.

To Configure Caller ID Based Services

1. Press the **Add** button on the **Caller ID Based Services** page. The **Caller ID Based Services - Add Entry** page where new address can be defined will appear in the browser window.
2. Define an optional **Description** of the address.
3. Select the call type from the **Call Type** drop down list.
4. Enter the SIP address, extension or PSTN number (dependant on the chosen call type) in the **Address** text field according to the entering rules.
5. To add an address to the **Caller ID Based Services** table, click **Save**.
6. Click on the newly created **Address** in the **Caller ID Based Services** table to open the **Caller ID Based Services for Address** page.
7. From the left frame, choose a Caller ID Based Services and enable, configure and adjust corresponding service(s) settings in the right frame. Pay attention to **Save** configuration each time moving among Caller ID Based Services configuration pages.

To Edit Caller ID Based Services

1. Select the checkbox of the corresponding address that has to be edited in the **Caller ID Based Services** table. The **Caller ID Based Services - Edit Entry** page will appear in the browser window.
2. Change the **Description** of the address, if needed.
3. Change the **Call Type** and the **Address** defined in the corresponding fields.
4. **Save** changes.
5. If the reconfiguration of **Caller ID Based Services** is needed, click on the corresponding **Address** in the **Caller ID Based Services** table to open the **Caller ID Based Services for Address** page.
6. From the left frame, choose a Caller ID Based Services and change service(s) settings in the right frame, if required. Pay attention to **Save** configuration each time moving among **Caller ID Based Services** configuration pages.

Incoming Call Blocking

Incoming Call Blocking allows blocking unwanted incoming calls for a Quadro extension. This page provides the necessary settings for incoming call blocking. It indicates if the service is enabled for the particular caller and whether or not the custom message will be used to inform the caller about the call being blocked. If the service for the particular caller has been enabled by the administrator and has been stated as protected, it cannot be disabled by the user.

Please Note: Since the administrator can protect the service from being disabled by you, contact the administrator if callers complain that they cannot reach you.

The **Enable Service** checkbox selection blocks all calls to the current extension from corresponding **Address** listed in Caller ID Based Services table Incoming Call Blocking service is configured for.

The **Send Message to Caller Party** checkbox is available when the service is enabled and initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without notification.

The **Restore Default Blocking Message File** restores the default incoming call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Message File** requires the name of the desired voice message file. The file needs to be in PCMU wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will be received. The system also prevents uploading if there is not enough space available for the corresponding extension. You will then receive the "You do not have enough space" warning.

Browse is used to browse custom voice message used for incoming call blocking.

The **Download Voice Message File** link only appears if a file has been previously uploaded. The link is used to download the audio file to the PC and opens a window where the saving location can be specified.

Fig. 3-20 Incoming Call Blocking page

Outgoing Call Blocking

Outgoing Call Blocking allows blocking unwanted outgoing calls for a Quadro extension towards the destination **Address** service is configured for. This page provides the necessary settings for the outgoing call blocking service. It indicates whether service is enabled for the particular caller and whether or not a custom message will be used to inform caller about the call being blocked. If the service for particular caller has been enabled by administrator and has been stated as protected, it cannot be disabled by the user.

Please Note: Since the administrator can protect the service from being disabled by you, contact the administrator if you have problems establishing certain calls.

The **Enable Service** checkbox selection blocks all calls to the corresponding **Address** listed in Caller ID Based Services table from current extension.

The **Send Message to Caller Party** checkbox is available when service is enabled and it initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without a warning.

The **Restore Default Blocking Message File** restores the default outgoing call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Message File** requires the name of the desired voice message file. The file needs to be in PCMU wave format, otherwise the system will prevent uploading it and "Invalid audio file, or format is not supported" warning message will be received. The system also prevents uploading if there is not enough space available for the corresponding extension. The "You do not have enough space" warning will then be received.

Browse is used to browse custom voice message used for outgoing call blocking.

The **Download Custom Blocking Message File** link appears only if a file has been previously uploaded. This link is used to download the audio file to the PC and opens a window where the saving location can be specified.

Fig. 3-21 Outgoing Call Blocking page

Call Hunting

The **Call Hunting** service provides the possibility of incoming call consecutive ringing on several extensions depending on the calling party. The **Call Hunting** page contains a table where all the participants in the call hunting group for the corresponding extension should be defined.

Attention: By configuring the **Call Hunting** service, **Unconditional Call Forwarding** will be automatically disabled on the current extension.

Selecting **Enable Service** activates the Call Hunting service on the current extension.

The table displayed here lists the extensions to where the call must be consecutively duplicated in case of a call from the corresponding caller. The **Line Status** column shows whether or not the extension is **Attached**, **Not Attached** or Attendant. An extension can't ring if it is **Not Attached**, it must be attached to the line by the administrator from the **Extensions Management** page.

As the order of the entries in the **Call To** table define the consecutive ringing order, **Move Up/ Move Down** is available to move the checked **Call To** extension either one level up or down.

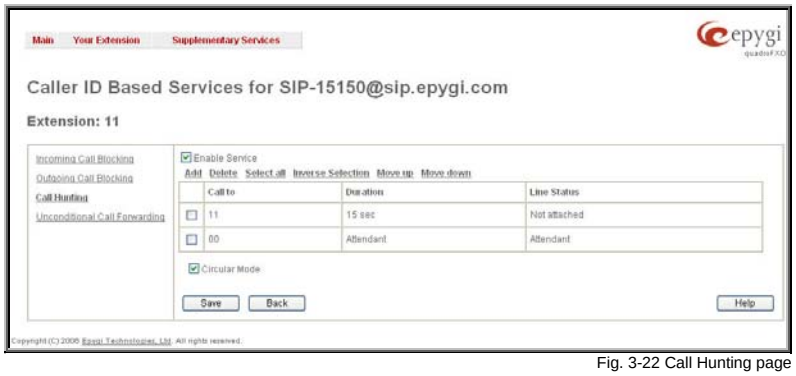


Fig. 3-22 Call Hunting page

Add opens the **Add Entry** page to add called extensions (an attendant or a user extension). It has manipulation radio buttons to select the type of extension to be added to Call Hunting, and contains the following components:

- The **Call To** drop down list contains Quadro's attendant or user extensions, depending on the radio button selected. It is possible to add the same extension more than once to the **Call To** table. The extension will ring - depending on the order - as often as configured.
- The **Duration** drop down list is available for user extensions only and is used to select the period (in seconds) during which the corresponding user's extension should ring.

When saving the call hunting configuration, a message will notify the user that the Many Extensions Ringing and the Call Forwarding services have been disabled.

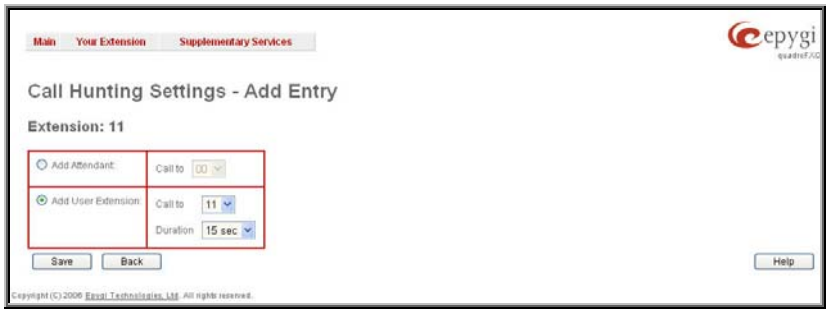


Fig. 3-23 Call Hunting – Add Entry page

The **Circular Mode** checkbox enables the call hunting start over when the last extension in the Call Hunting table has been called and there is still no answer. When this checkbox is not selected, call hunting will terminate once the last extension in the Call Hunting table does not answer the call, the incoming call will then be redirected to the Voice Mailbox of the extension call it originally called (if enabled) or it will be disconnected.

Attention: The Circular Mode will not work if the list of called destinations contains at least one Auto Attendant extension, otherwise the hunted call will be answered by the Auto Attendant and will terminate there.

Unconditional Call Forwarding

Unconditional Call Forwarding is a service of Quadro that allows the automatic unconditional transfer of incoming calls to varying other destinations.

The following rules are applicable to all call forwarding types:

- By setting up unconditional call forwarding service, **Call Hunting** services will be automatically disabled. The exception is cases when unconditional call forwarding is enabled from the handset (see Feature Codes).
- PSTN destinations (with **PSTN** or **Auto** call type) have priority in **Forward to** list. If there are different destinations in the **Forward to** list, the call will be forwarded to PSTN destination (in the same time any available SIP or PBX destinations will receive a short ring). If the PSTN destination was not successful, the next PSTN destination will be dialed, otherwise if there are no more PSTN destinations in the table, the call will be forwarded to any available SIP and PBX destinations simultaneously.
- If there are multiple entries with any combination of PBX or SIP call types, then all destinations will ring simultaneously and the call will be established with the destination that will pick up the call the first.

Fig. III-24 Unconditional Call Forwarding page

Enable/Disable functional button is used to enable/disable the corresponding forwarding destinations. This is helpful to avoid removing forwarding destination(s) if they are not applicable at the moment.

Add opens the **Add Entry** page to add forwarding destinations. It consists of the following components:

Call Type lists the available call types:

- PBX - forwarding destination is a local Quadro extensions or Auto Attendant
- SIP – forwarding destination is reached through a SIP server
- PSTN – forwarding destination is a PSTN user
- Auto – used for undefined call types. In this case, the routing pattern will be considered and parsed through the Local Routing Table

The **Forward To** text field requires the SIP address (see chapter Entering SIP Addresses Correctly), a PBX extension or a PSTN number, where an incoming call from a certain caller should be unconditionally forwarded. If the address already exists in the table, selecting **Save** will display the error "Caller address already exists". A wildcard is allowed in this field (see chapter Entering SIP Addresses Correctly). Entering "*" as PBX or PSTN addresses will apply the configuration of Caller ID Based services to all extensions or PSTN users.

Fig. III-25 Call Forwarding – Add Entry page

The extension number should be inserted in the **Forward To** text field for the PBX call type. The PSTN number length depends on the area code and phone number.

Send Notification Via SMS checkbox enables SMS notifications sending to the user's mobile phone when unconditional call forwarding on the corresponding extension from the certain caller takes place. This checkbox selection enables the **Mobile Number** text field where the user's mobile phone number should be defined. If you feel this service is not working, contact your system administrator to configure the SMS Settings.

Send E-mail checkbox enables email notifications sending to the user's mailbox when unconditional call forwarding on the corresponding extension from the certain caller takes place. This checkbox selection enables the **E-mail Address** text field where the user's email address should be defined. If you feel this service is not working, contact your system administrator to configure the Mail Settings.

When saving the unconditional call forwarding configuration, a message will notify the user that Many Extension Ringing and Call Hunting services have been disabled.

Logout

This option is used to close the session between the user PC and Quadro and to leave the Quadro Web Management or enter into the management with another login. By selecting the **Web Management** link, the startup page will be displayed and the user will need to login again.

Quadro's Feature Codes

This chapter describes how Quadro's feature codes allow the user to navigate through Quadro's services with the help of a phone handset. These services are **Establishing a Call**.

Establishing a call

To make a call, dial the **Routing Number**.
Routing Numbers and available routs to, from and through Quadro are listed in the **Call Routing Table**, which is configured and managed by Quadro's Administrator. To get information about dialing rules, please turn to administrator.

Please Note: You may accelerate establishing a connection by a pound (#) sign dialed at the end of the number.

Voice Mail Services

*0 Enter Voice Mail Services *		
1 Voice Mailbox	3 Personal Settings	4 Change Password

* After the first boot-up of the Quadro or if the Voice Mail Configuration Wizard is manually enabled by Quadro's administrator, entering the Voice Mail Services for the first time will activate the Voice Mail Configuration Wizard which will prompt the essential user's personal settings. Below are instructions on how to proceed with the Voice Mail Configuration Wizard from the handset.

*0 Enter Voice Mail Services for the first time after Quadro's first boot-up, reset factory default or Voice Mail Configuration Wizard activation	
Dial the extension user's new **Password** and press #	
Confirm the extension user's new **Password** and press #	
Record a **Voice Mail Greeting** and press #	
* Apply recorded Voice Mail Greeting and move forward to the next step	# Record Voice Mail Greeting again
Record a **User's name** and press #	
* Apply recorded User's name and exit	# Record User's name again

The **Voice Mail Services** are divided into three parts: **Voice Mailbox**, **Personal Settings** and **Password Change**. Each of these parts has a hierarchy that is described below.

*0 Enter Voice Mail Services		
*0 Exit Voice Mail Services	*1 Go to the top of the Voice Mail Services Tree	*2 Go one level up in the Voice Mail Services Tree

The following key combinations are available to navigate through **Voice Mail Services** menus.

Voice Mailbox

*** 0 Enter Voice Mail Services**		
1 Voice Mailbox Menu		
1 Send a Message or Leave a Reminder	2 Play First Message	3 Get Date/Time Info
4 Play Previous Message	5 Play Current Message	6 Play Next Message
7 Print the attached FAX (and press START button on the FAX machine)	8 Play Last Message	9 Delete Current Message
*	0 Reply or Forward a Message	#

After entering the voice mail services (using the keys * 0) press the key 1 to enter the Voice Mailbox menu. The following key combinations are available to navigate within the new messages:

The **Voice Mailbox** menu has the following sub-hierarchy in the **Reply or Forward a Message** and the **Send a Message or Leave a Reminder** menus:

0 Reply or Forward a Message			
0 Call Back immediately	1 Reply by Voice Mail	2 Forward a Message (any FAX attached to the message will be also forwarded)	
	Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.	Dial **Destination Number**	
	# Record a Message	# Record a Message	Dial additional **Destination Number**
			# Record a Message
		Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.	

1 Send a Message or Leave a Reminder		
Dial **Destination Number**		# Leave a reminder
# Record a Message	Dial additional **Destination Number**	Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.
	# Record a Message	
Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.		

Please Note: This service is restricted regarding sending a message to PSTN destinations. A message will be successfully received by the destination if all of the following criteria are met:

- The connection to the destination is successful;
- The voice mail service is enabled on the destination;
- There is enough space in the voice mailbox of the destination;
- The duration of the forwarded/replied message is less than the maximum voice mail duration set up at the destination.

Personal Settings

Use the digit 3 to enter the area where the personal system messages can be modified. A voice notification will play the list of available system messages that may be modified so the user can select the desired system message by the corresponding buttons:

*0 Enter Voice Mail Services				
3 Review System Messages				
1 Greeting Message	3 Incoming Blocking Message	4 Outgoing Blocking Message	5 Your Name	6 Out of Office Message
1 Listen to Current Greeting Message	1 Listen to Current Incoming Blocking Message	1 Listen to Current Outgoing Blocking Message	1 Listen to Current Name recorded	1 Listen to Current Out of Office Message
2 Record a New Greeting Message	2 Record a New Incoming Blocking Message	2 Record a New Outgoing Blocking Message	2 Record a New Name	2 Record a New Out of Office Message
3 Restore Default Greeting Message	3 Restore Default Incoming Blocking Message	3 Restore Default Outgoing Blocking Message	3 Restore Default Name	3 Restore Default Out of Office Message
# Stop Recording or Playback Greeting Message	# Stop Recording or Playback Incoming Blocking Message	# Stop Recording or Playback Outgoing Blocking Message	# Stop Recording or Playback Name Message	# Stop Recording or Playback Out of Office Message

Change Password

Use the digit 4 to enter the area where the extension's user may change its password. This password is used to access personal configuration settings (also voice mailbox) through the Quadro Web Management and the voice mailbox through the handset.

4 Change Password
Dial **Old Password** and press pound
Dial **New Password** and press pound
Confirm **New Password** and press pound

Services for Incoming Calls

Calling to the extension	Calling to the extension's Voice Mailbox	
1 Skip the greeting message and enter the called extension's Voice Mailbox (authentication required)	0 (during the greeting message) Calling to the Zero Out destination	# Skip the greeting message and record a Voice Mail

Quadro's Auto Attendant Services

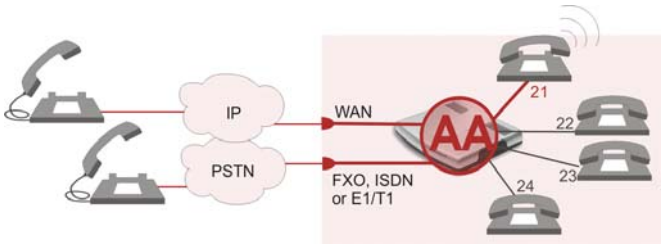
Quadro's Auto Attendant is addressed to provide remote access to the Quadro voice connectivity services. Specifically it supports remote connection to Quadro extensions, their mailboxes and making pass-through calls to other destinations. Remote access to the Quadro auto attendant is possible through IP and PSTN calls.

Quadro's Auto Attendant can be accessed locally, remotely from the IP network (by dialing Auto Attendant's SIP address) and from the PSTN network (by dialing Quadro's PSTN number) if the calls addressed to the Quadro's PSTN number are routed to the Auto Attendant.

Attention: If the Auto Attendant authentication attempts have been failed for the five times, Quadro's Auto Attendant will become unavailable for the next 5 minutes.

The automated attendant services are divided into the feature groups listed below. The **Connection Service** is supported by the voice messages help which helps caller to navigate within area using the handset buttons. Other feature groups are available using the appropriate call code, but are not supported by voice messages. Thus, they are hidden for external callers.

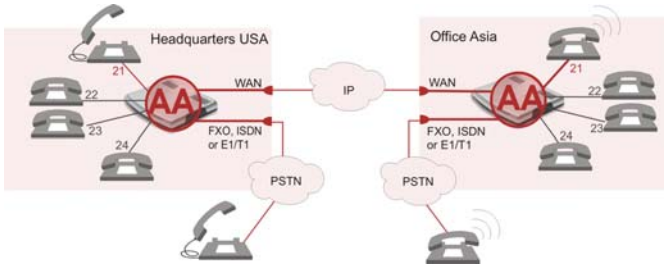
Connection Service provides access to all extensions of the Quadro device without restrictions: All Quadro extensions may call each other dialing the extension number. And all external callers (using PSTN or IP calling) can reach every Quadro extension dialing Quadro's phone number and using the Auto Attendant's voice menu to be connected to the desired extension by entering the extension number.



Call Relay

As the Quadro Auto Attendant is registered at Epygi's SIP server by default, it may be used as a kind of private switching center, if the Auto Attendant is routed to the particular telephone line (FXO, ISDN or E1/T1) as a "default user". Then it allows e.g. establishing cost-saving long-distance calls: Via PSTN to the Quadro Auto Attendant (e.g. USA headquarters), via IP to the remote Quadro Auto Attendant (e.g. Office Asia) and via PSTN to the desired destination (see call codes below).

Access to **Call Relay** needs authorization.



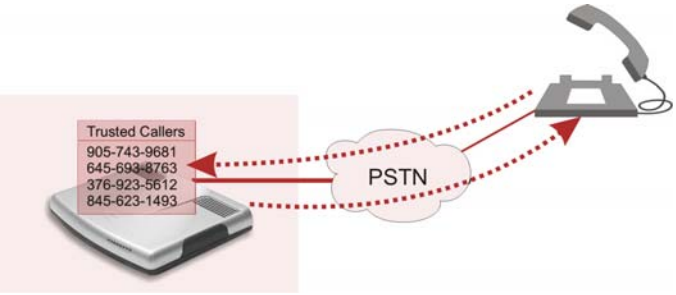
Remote Configuration Menu

This menu allows extension owners to remotely enable/disable the Unconditional Call Forwarding Service for **Any Address** or **Other Addresses** entries of the

Caller ID Based Services table on the corresponding extension, as well as to change the certain forwarding number in the Unconditional Call Forwarding table. The menu requires extension authorization.

Call Back

With the Quadro's Call Back service the PSTN callers can save the call charge when calling to/through the Quadro to the third party IP or PSTN destinations. The Quadro allows you to configure a list of those trusted PSTN callers that are allowed to make free of charge calls through Quadro. Two types of Call Back configurations are available on the Quadro: **Pre-configured Call Back** and **Remote Call Back Configuration**.



Pre-configured Call Back

For **Pre-configured Call Back** service, a list of trusted PSTN callers must be configured in the Quadro's Authorized Phones Database using Web Management. The Call Back service should be enabled and a valid callback PSTN destination should be specified for each PSTN caller.

To use Pre-configured Call Back, the PSTN caller registered in the Authorized Phones Database should simply call to the PSTN number attached to Quadro FXO line (the FXO line should be previously routed to the Auto Attendant) from the global PSTN network, let the call ring twice and then hang up. Call Back will get instantly activated, and Quadro will call back to the defined Call Back destination. By answering the incoming call the PSTN party will be connected to the Auto Attendant menu.

Remote Call Back Configuration

Call Back settings may be configured/reconfigured by authorized PSTN caller over a phone by calling to the Quadro's Auto Attendant. There are two options for configuring Call Back remotely:

- Permanent Call Back
- Non-Permanent (Instant) Call Back

Please Note: Remote Call Back Configuration services are only available when the **Automatically Enter Call Relay Menu** checkbox is disabled in Call Back settings for the trusted user.

Permanent Call Back

This service allows the callers registered in Authorized Phones Database to create a new trusted PSTN Caller with Call Back enabled and/or to modify the Call Back destination of an existing PSTN Caller in the Authorized Phones Database. By calling Quadro's PSTN number (that is previously routed to the Auto Attendant) and entering the Auto Attendant menu, caller is able to use the *6 code to create a new trusted PSTN Caller as well as to modify the Call Back destination for the already registered Caller in the Authorized Phones Database.

Entering the Permanent Call Back reconfiguration menu, the system will ask to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in Call Back settings.

After passing the login successfully the PSTN callers should follow the voice instructions for configuring a new entry or reconfiguring the existing entry in Authorized Phone database.

When the system accepts the settings, the corresponding entry will be logged to the Authorized Phones Database. The PSTN caller will be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds if the detected PSTN caller address corresponds to the one applied by the caller (and if FXO line is available on the Quadro, network connectivity is fine and destination is reachable). Answering the incoming call, the PSTN caller will be connected to the Quadro's Auto Attendant.

Non-Permanent Call Back

Non-Permanent Call Back configuration service allows the trusted caller to organize one-time Call Back to the defined PSTN destination. No entry will be logged to the Authorized Phones Database in this case.

By calling Quadro's PSTN number (that is previously routed to the Auto Attendant) and entering the Auto Attendant menu caller is able to use the *5 menu to modify the Call Back destination for the already registered Caller in the Authorized Phones Database.

The system will ask to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in Call Back settings.

After passing the login successfully the PSTN callers should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database.

The PSTN caller will be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds if the detected PSTN caller address corresponds to the one applied by the caller (and if FXO line is available on the Quadro, network connectivity is fine and destination is reachable). Answering the incoming call, the PSTN caller will be connected to the Quadro's Auto Attendant.

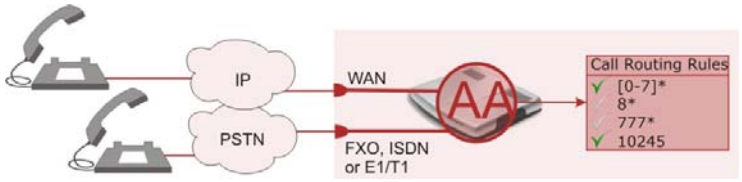
Call Routing Management Menu

This menu is used to manage the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry.

Dialing *7 at the Auto Attendant welcome message, will ask for an enabler/disabler key used to enable or disable the routing rule(s) correspondingly. Since multiple routing rules may have the same enabler/disabler key combinations (the same key may be used as enabler for one routing rule, and as disabler for another one), dialing the certain key will affect all pre-configured routing rules.

If the routing record has an authorization enabled on the enabler/disabler key, administrator's password will be required to be inserted after the key. Once the administrator's password is dialed, system plays a confirmation about the accepted configuration and the state of the certain routing rule(s) is getting modified.

If administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.



Call Codes Available in Auto Attendant

For external calls addressed to the Auto Attendant or incoming calls from mainline routed to the Auto Attendant or local by dialing the 2-digit attendant extension, following key combinations are available to access and manipulate within Auto Attendant services:

Incoming call to Auto Attendant Services or dial locally	Keys
Extensions Menu - establishing a connection to an extension on the called Quadro	- (already in)
Call Relay Menu - mainly for external calls (IP/FXO or IP/ISDN), local calls are allowed, too. Service allows you to avoid hanging up and redo the entire dialing, if Quadro detects an error in the dialed number or the user decides to cancel the call and start a new one: Entering the combination * * the call will be interrupted and the user will get an invitation to make a new one. This is applicable during dialing, after the ring tone has started, and after the call has been established.	* 2
"* *" digit combination is applicable: During the dialing, After ring tones start, After call establishment. **Under the following restrictions:** This feature can be used when accessing the AA from the PSTN line to make IP or local calls This feature can be used when calling to PSTN through the AA This feature is not available on the second Quadro Auto Attendant (calling from one Auto Attendant to another)	
Remote Configuration Menu – allows remote enabling/disabling of Unconditional Call Forwarding service for **Any Address** or **Other Addresses** entries in the Caller ID Based Services table on the extension and to modify the certain forwarding destination.	* 4
Non-Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to change the callback destination for a one-time callback. After the caller hangs up, Quadro will call back to the newly specified number, but this change will not be logged into Authorized Phones Database.	* 5
Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to reconfigure Authorized Phones Database entries by modifying the caller's and/or callback numbers. As a result, the caller will be able to initiate a callback, only by calling from the newly specified caller number.	* 6
Call Routing Management Menu – allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain routing rules by dialing key combinations pre-configured on each routing entry.	* 7
Quits the Auto Attendant and starts a dial tone.	Flash 4

Remote Configuration Menu

* 4 **Remote Configuration Menu** (when this menu is accessed, the Unconditional Call Forwarding service is already getting toggled)	
1 Toggle (enable or disable) the Unconditional Forwarding service again	2 Change the Forwarding Number
	Dial a new **Forwarding Number** and press #
	Confirm the new Forwarding Number with # or press * to dial a new Forwarding Number.

Please Note: Using the **Change the Forwarding Number** option will change the first entry in the **Unconditional Call Forwarding** table with **Auto** call type to the inserted **Forwarding Number**. Any other entries with **Auto** call type, as well as with other call types will not be modified.

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name -admin Password - 19
Quadro Hostname	quadroFXO
Quadro Domain Name	epygi-config.com
LAN IP Address	172.28.0.1 Subnet Mask - 255.255.0.0
DHCP Server	Enabled, Give leases only to hosts listed in the Special devices table – disabled, IP Range - 172.28.0.100-172.28.0.254, WINS - 0.0.0.0. No static mappings defined.
Regional Settings and Preferences	Locale – US, TimeZone – Central Time (US&Canada), Theme – Dynamo, Choose Theme on Login - disabled.
WAN Interface Protocol	Ethernet
WAN Interface Bandwidth	Upstream – 10000, Downstream – 10000, Min Data Rate – 0.
WAN IP	Automatically through DHCP
Mac Address	Assigned by device, MTU - 1500 Bytes.
DNS Server	Dynamically
IP Routing Configuration	No Routes
Configuration Management	Automatically Backup Configuration – disabled.
Event Settings	”Display notification” for all except the following events which have “Do nothing” action assigned: Login Password Authentication Failure PPP Link Establishment PPP Link Brake
Time/Date Settings	NTP Server and Client – enabled, Predefined NTP Server - ntp1.epygi.com, Polling interval – 6.
Mail Settings	Disabled.
SMS Settings	Disabled.
Automatic Firmware Update	Disabled.
SNMP Settings	Disabled.
System Logs Settings	User Logging – enabled, Developer Logging – disabled, Archived Logging – disabled, Comment – undefined, Remote Logging – disabled.
Language Pack	Default - English Custom Language Pack - none
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Extension (all accessible pages for extension), Local Administrators (all accessible pages for localadmin).
Extensions Management	Extension Length – 2, once applied extension 00 appears
Attendant 00 Settings – General	Display name – Attendant, Enable FAX Forwarding – disabled, Show on Public Directory – enabled, Percentage of System Memory – 3%.

Parameter	System Default Value
Attendant 00 Settings – Attendant Scenario	Scenario – default, Send AA digits to Routing Table – enabled, Redirection on Timeout – disabled, ZeroOut – disabled, Welcome Message – enabled, Welcome Message, Recurring Attendant Prompt and Attendant Ringing Announcement – default.
Attendant 00 Settings – SIP	Registration username and password - automatically generated, SIP server - sip.epygi.com, SIP Server port – 5060, SIP Server Registration – disabled.
Attendant 00 Settings – SIP Advanced	Authentication User Name – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Do Not Use SIP Old Hold Method – disabled, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined, Port for Secondary SIP Server – 5060.
Attendant 00 Settings - Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, iLBC – enabled, Out of Band DTMF Transport – enabled, T.38 FAX – disabled, Pass Through FAX – disabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Universal Extension Recordings	Default, Percentage of System Memory – 1%.
Authorized Phones Database	No entries.
Call Statistics	Enabled, 100 entries for all type of calls, Automatic Downloading of Call Statistics – disabled.
SIP Settings	UDP and TCP Port – 5060, TSL Port – undefined, Realm – quadro, Session Timer – disabled, DNS Server for SIP – default, SIP timers – RFC 3261.
RTP Settings	Properties for all Codecs except iLBC : Packetization -20ms Silence Suppression -yes iLBC properties: Packetization - 30ms Silence Suppression – yes G.726 Standard - ITU-T specification RTP/RTCP port range - 6000-6099 RTCP Support - disabled
NAT Traversal Settings	NAT Traversal for SIP – Automatic SIP and RTP Parameters - Use STUN SIP TCP Port – 5060 STUN Parameters: Primary STUN Server - stun.epygi.com Primary STUN Port – 3478 Secondary STUN Server – undefined Secondary STUN Port - undefined Polling Interval: 1 hour Keep-alive interval: 120 seconds NAT IP checking interval: 300 seconds No entries in NAT Exclusion table
FXO Settings	6 FXO lines – all enabled, incoming and outgoing calls allowed and routed to 00 Attendant on all.
PSTN Lines Sharing	Provide PSTN lines for master device – disabled.
Gain Control	FXO lines: Transmit Gain: 0 Receive Gain: 6 Voice Mail: Transmit Gain: 0 Receive Gain: 0

Parameter	System Default Value
SIP Tunnel Settings	Enable Tunnels to Slave Devices – disabled, Tunnels to Slave Devices – no entries, Enable Tunnels to Master Devices – disabled, Tunnels to Master Devices – no entries.
Call Routing	Route all incoming SIP calls to Call Routing - enabled Local Routing table – no entries. Local AAA Table - no entries.
RADIUS Settings	RADIUS client – disabled.
Voice Mail Common Settings	Voice Mail Recording - G729a.
Dial Timeouts	4 seconds.
System Hold Music Settings	Play Hold Music – Local Music, Hold Music file – default.
3PCC Settings	Secure Connection – disabled, Request Timeout – 10, Feature Key – Not Added, WAN Port – Not Opened.
RTP Streaming Channels	Undefined.
IPSec, PPTP and L2TP	No connections. RSA Key Management - 1024 bit key defined PPTP Server Configuration Subnet – 172.31.1.0/24, Authentication - MSCHAPv2, MPEE 128 bit L2TP Server Configuration Subnet – 172.31.2.0/24.
Dynamic DNS	Disabled.
Firewall	Disabled, Ping Stealth – enabled.
IDS	Enabled.
NAT	Enabled.
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all), SIP Access (Allowed for all), No user defined services and IP pool groups
DNS Server Settings	Time to live (TTL) – 86400 seconds, Mail Exchange (MX) – undefined, No aliases defined.
DHCP Advanced Settings	DHCP Options: Gateways – 172.28.0.1 Subnet mask – 255.255.0.0 Domain name servers – 172.28.0.1 NBT name servers – 0.0.0.0 NTP servers – 172.28.0.1 Domain name – epygi-config.loc DHCP Server Statements: Authoritative – enabled. Ping Check – enabled, Ping timeout – 1 sec.

Extension Settings

Parameter	System Default Value
Voice Mail Settings	Maximal mail message duration - 5 min, Ask password before granting local access to mail box – disabled, Ask password before granting remote access to mail box – enabled, Send welcome message – disabled, Play Voice Mail help – enabled, Automatically play messages - enabled, Send mails count information message – disabled, Send date/time information message – enabled, Send beep at the end of message – enabled,

Parameter	System Default Value
	Silent VM Recording – disabled, Send new voice messages via e-mail – disabled, Send new voice message notifications via SMS – disabled, Send new voice message notifications via phone call – disabled, Zero Out – enabled, to 00 default Attendant, FAX redirection – disabled, Out of Office – disabled, Greeting message – default. Voice Mail Profiles – undefined.
Group List	No entries.
Account Settings	Display Name – undefined, User Password Protection – disabled both for incoming and outgoing calls, Custom Voice Messages – default.
Caller ID Based Services	No entries in the table. For Any Callers – all services are disabled, Blocking Voice Messages – default.

Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD.
Software License Agreement

THIS IS A CONTRACT. CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, SIMPLY DO NOT USE THE HARDWARE OR SOFTWARE.

- **License.** Epygi Technologies, Ltd. (the "Licensor"), hereby grants to you a non-exclusive right to use the Quadro Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may only use the Licensed Materials in connection with your operation of the Quadro or any Quadro SIP Gateway product. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.

- **Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or transfer of the Licensed Materials is subject to the terms of this Agreement.

- **Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.

- **No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language.

- **Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro or any Quadro SIP Gateway product. If you sell your license rights in the Licensed Materials you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

- **Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.

- **Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

  EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

- **LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.
  The foregoing limitation, exclusion and disclaimers apply to the maximum extent permitted by applicable law.

- **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

- **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227-19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.

- **Entire Agreement.** It is understood that this Agreement, along with the Quadro Installation Guide and User's Manual, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.

- **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.

- **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.

- **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.

If you have any questions about this Agreement, please write to Epygi at 6900 North Dallas Parkway, Suite 850, Plano, Texas 75024 or call Epygi at 972.692.1166.