

Edition 1, SW Release 3.1.8 and higher, December 2006

Table of Contents

Manual I: see Installation Guide

Offers a Step-by-step guide to install and configure Quadro Conference Server basically.

Manual II: Administrator's Guide

About this Administrator's Guide	4
QuadroCS's Graphical Interface	5
Administrator's Main Page	5
Recurrent Buttons	6
Recurrent Functional Buttons of the GUI	6
Entering a SIP Addresses correctly	6
Administrator's Menus	7
System Menu	7
System Configuration Wizard	7
Internet Configuration Wizard	8
Status	10
General Information	10
Network Status	11
Memory Status	13
Hardware Status	13
SIP Registration Status	13
Configuration Management	14
Events	14
Time/Date Settings	17
Mail Settings	17
Firmware Update	18
Networking Tools	19
Diagnostics	20
Automatic Provisioning	20
Upload Language Pack	20
User Rights Management	21
Conference Management Menu	23
Conferences	23
Conference Codecs	27
SIP Settings	28
RTP Settings	29
NAT Traversal Settings	30
Statistics	32
Call Routing Table	34
Best Matching Algorithm	36
Recording Common Settings	39
Mail Default Settings	40
Internet Uplink Menu	41
PPP Settings	41
Advanced PPP Settings	41
Firewall	42
Advanced Firewall Settings	42
Filtering Rules	43
Service Pool	44
IP Pool	45
Dynamic DNS Settings	47
Network Menu	48
DNS Settings	48
DHCP Settings for the LAN Interface	48
Registration Form	49
Logout	49

Appendix: System Default Values..... 50
Appendix: Software License Agreement 53

Manual III: see Moderator's Guide

This guide explains all menus that can be accessed and configured by the conference moderator within the QuadroCS. Further, a list of all available conference codes can be found there.

About this Administrator's Guide

The QuadroCS Manual is divided into three parts:

- **Manual I: Installation Guide** gives step-by-step instructions to provision the Quadro Conference Server and configure the conferences with the Epygi SIP Server. After successfully configuring the Quadro, users will be able to automatically or manually initiate the call conferences between several IP peers, deal with the active conferences and record them if needed.
- **Manual II: Administrator's Guide** that explains all QuadroCS management menus available for administrators only. Further it includes a list of all System Default Values.
- **Manual III: Moderator's Guide** explains all menus that can be accessed and configured by the conference users within the QuadroCS. Further a list of all available call codes can be found here.

[QuadroCS's Graphical Interface](#) introduces to the QuadroCS's graphical user interface and explains all recurrent buttons.

[Administrator's Menus](#) explains each of the Administrator's management pages according to the menu structure shown on the main page of the Quadro management.

[Appendix: System Default Values](#) lists all factory defaults.

[Appendix: Software License Agreement](#) includes the contract for using QuadroCS's hardware and software.

QuadroCS's Graphical Interface

Administrator's Main Page

After logging in as an administrator, the **QuadroCS Management** with the **Active Conferences** table is displayed. Here the administrator may access the following settings and perform the following actions:

System Menu

- [System Configuration Wizard](#)
- [Internet Configuration Wizard](#)
- [Status](#)
- [Configuration Management](#)
- [Events](#)
- [Time/Date Settings](#)
- [Mail Settings](#)
- [Firmware Update](#)
- [Networking Tools](#)
- [Diagnostics](#)
- [Automatic Provisioning](#)
- [Upload Language Pack](#)
- [User Rights Management](#)

Conference Management Menu

- [Conferences](#)
- [SIP Settings](#)
- [RTP Settings](#)
- [NAT Traversal Settings](#)
- [Statistics](#)
- [Call Routing Table](#)
- [Recording Common Settings](#)
- [Mail Default Settings](#)

Internet Uplink Menu

- [PPP Settings](#)
- [Firewall](#)
- [Filtering Rules](#)
- [Dynamic DNS Settings](#)

Network Menu

- [DNS Settings](#)
- [DHCP Settings for the LAN Interface](#)

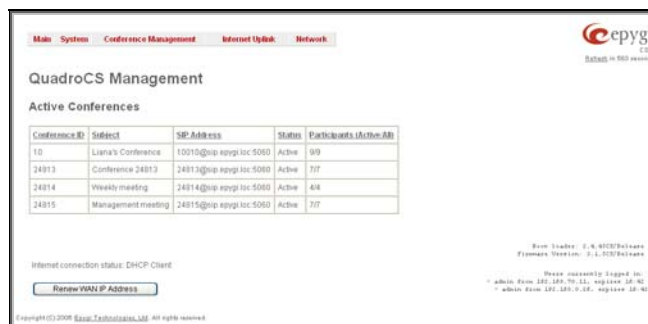


Fig. II-1: Quadro Conference Server Administrator's page




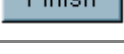
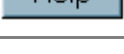

The functional button **Renew Wan IP Address** appears on the administrator's main page **Quadro Conference Server Management** if the Quadro Conference **Server** acts as a client to a DHCP server. The button **Renew WAN IP Address** is used to get a new WAN IP address, i.e., the Quadro Conference Server moves to another network.





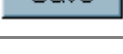
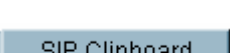
The button **Please Check Your Pending Events** will be displayed on the administrator's main menu page if any new system events exist. The link leads to the page where these new system events are listed.

The current version of the QuadroCS's firmware and of its boot loader is shown in the lower right corner of the administrator's main menu, followed by the list of **Users currently logged into the system**. Information about the IP address users accessed QuadroCS from, the username of the logged-in user and the time until the next automatic logout is provided here. The idle session timeout is set to 20 minutes. If no action is performed during that time, the user automatically will be moved to the login page and will be requested to login again.

The **Refresh** link is on some pages in the lower right corner next to the field displaying the number of seconds left until the next refresh and is used to perform a manual reload of the page.

Recurrent Buttons

Button	Description
	This button leads back to the previous page of a fixed sequence of pages (used mainly in wizards).
	This button leads forward to the next page of a fixed sequence of pages (used mainly in wizards).
	This button discards the latest not yet confirmed entries.
	This is the last button of a fixed sequence of pages that completes and saves the entries of an entire sequence.
	This button opens the help page belonging to the currently active Quadro management page.
	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
	This button returns you to the page you were previously on.
	This button confirms an operation you started before.
	This button confirms an operation you chose before.
	This button discards an operation you chose before.
	This button saves the settings modified on the currently active management page.
	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 of the GUI

In connection with tables, the following buttons - among others - usually occur:

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 a SIP Addresses correctly

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

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

```

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

The display name and the port number are optional parameters in the SIP address. If the 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.

Particularly the following combinations can be used for your convenience:

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

Please Note: Wildcards are available for caller addresses only. No wildcard characters are allowed for called party addresses. To use "*" and "?" themselves (as non wildcard characters), use "*" and "\?" correspondingly

Administrator's Menus

System Menu

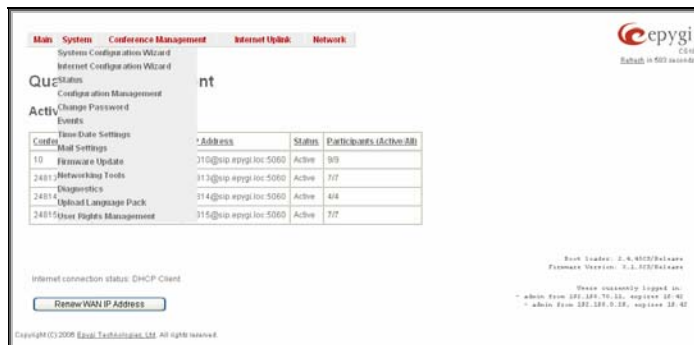


Fig. II-2: QuadroCS Management page

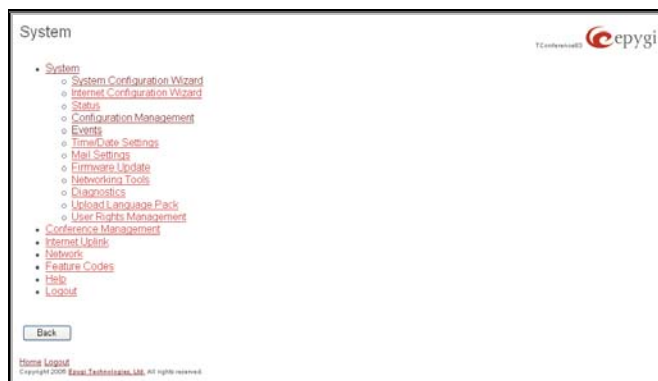


Fig. II-3: QuadroCS Management tree

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
- [DHCP Settings for the LAN Interface](#)
- Regional Settings and Preferences

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.

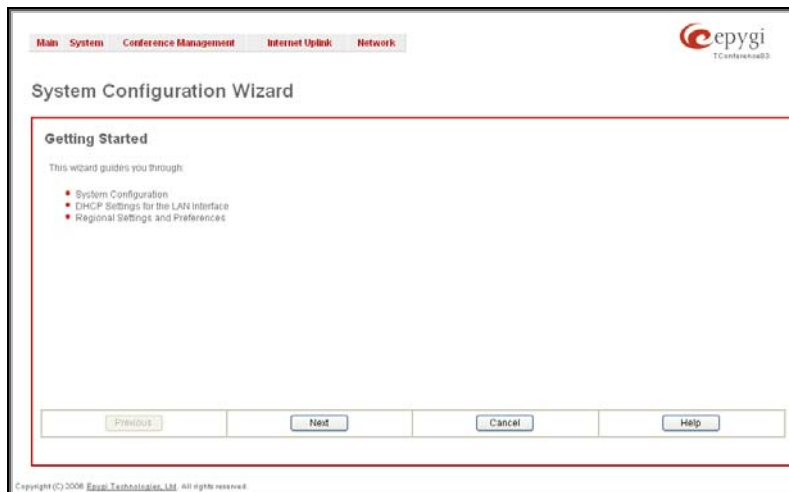


Fig.0-4: System Configuration Wizard – start page

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.
- IP Address** requires the Quadro host address for the LAN interface.
- Subnet Mask** requires the Quadro hosts' Subnet Mask.

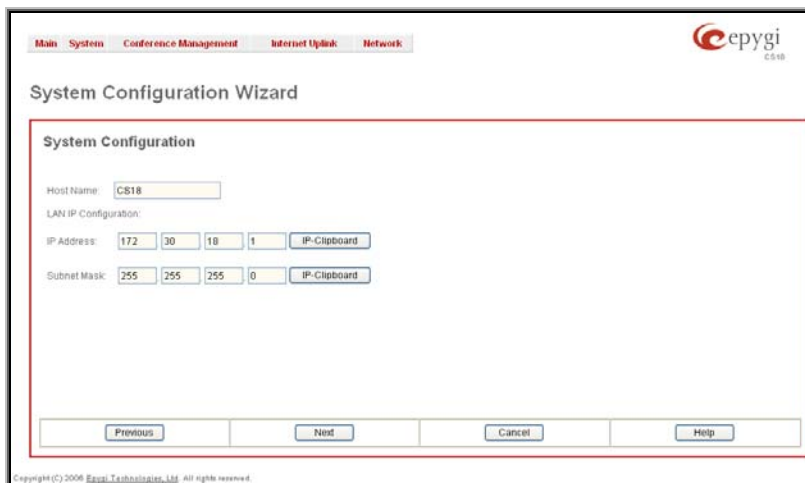


Fig.0-5: System Configuration Wizard – System Configuration page

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**. 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.

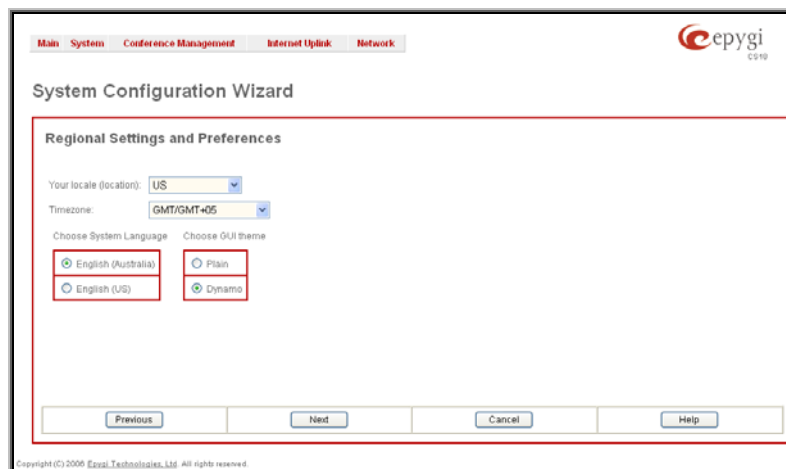


Fig. 1-5 System Configuration Wizard – Regional Settings page

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.**

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.

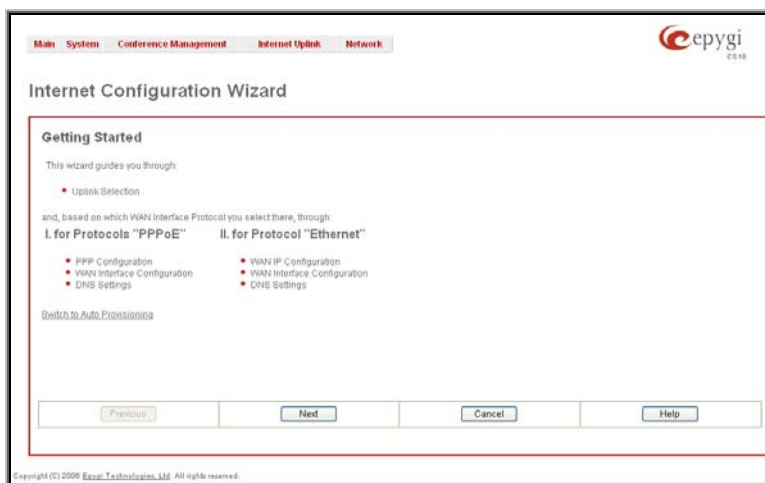


Fig. II-6: Internet Configuration Wizard - Start page

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

- Uplink configuration (see below)

For WAN Interface protocol **PPPoE**:

- [PPP 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 WAN interface connection type and the bandwidth settings. These settings will make QuadroCS 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** (see [PPP Settings](#)), 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.

Ethernet - turns on the Ethernet connection.

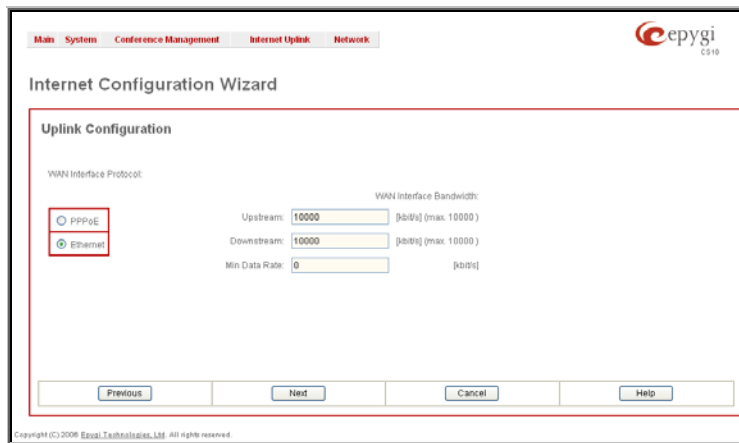


Fig. II-7: Internet Configuration Wizard - Uplink Configuration page

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 loses 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 tables 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	G723-5.3	G723-6.3	iLBC-13.33
10	105	58	66	73	81	50	-	-	-
20	84	37	45	53	60	29	-	-	-
30	77	30	38	45	53	22	19	20	27
40	73	26	34	42	50	18	-	-	-
50	71	24	32	40	48	16	-	-	-
60	70	23	30	38	46	15	12	13	21

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.

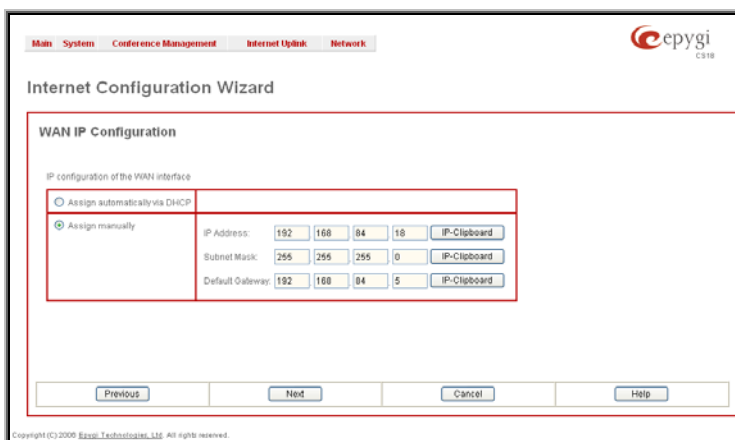


Fig. II-8: Internet Configuration Wizard - WAN IP Configuration page

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.

Please consult with your ISP administrator to get the corresponding settings.

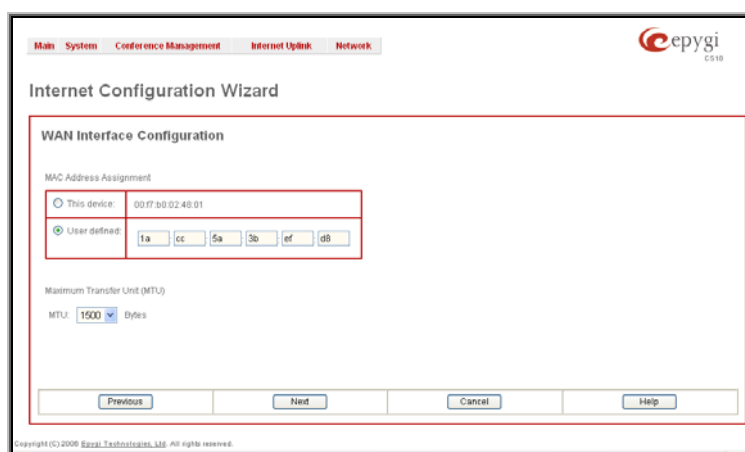


Fig. II-9: Internet Configuration Wizard - WAN MAC Address Configuration page

Status

The system status window displays non-editable tables providing extensive status information about QuadroCS: [General Information](#), [Network Status](#), [Memory Status](#), [Hardware Status](#) and [SIP Registration Status](#).

The **System Status** page consists of several tables providing system information.

General Information

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

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

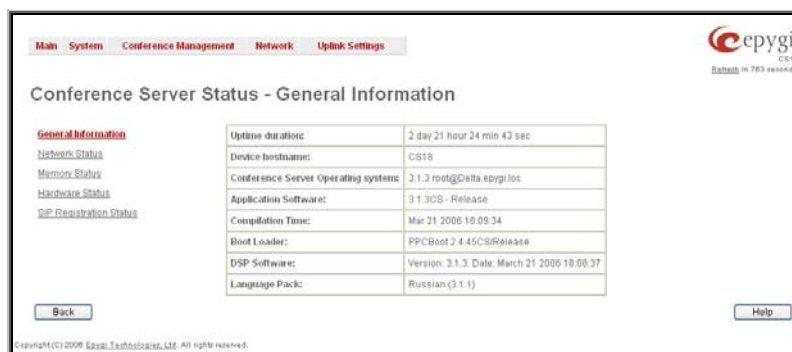


Fig. II-10: Quadro Status – General Information page

Network Status

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

Interface Name lists the Network LAN and WAN interfaces available on the QuadroCS.

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 either 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

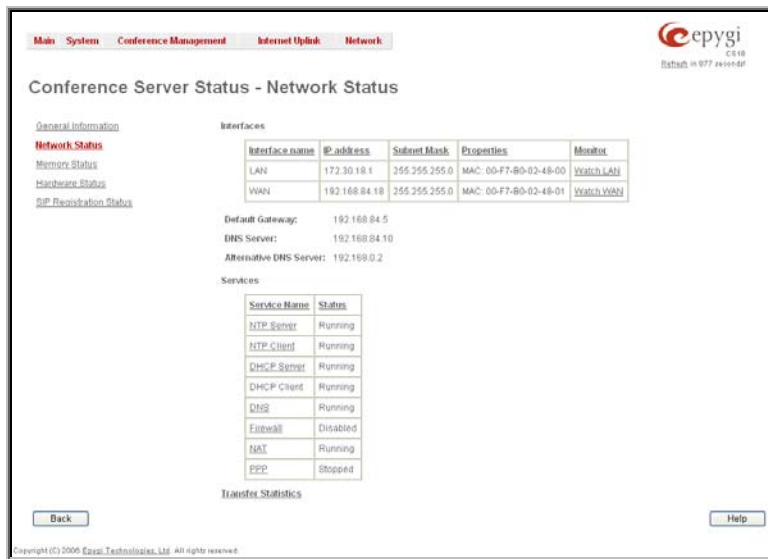


Fig. II-11: QuadroCS Status Network Status page

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 and PPP) **Status: stopped or 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

When **Show also as readable values** checkbox is selected, an additional table with statistics values will be displayed on the next page.

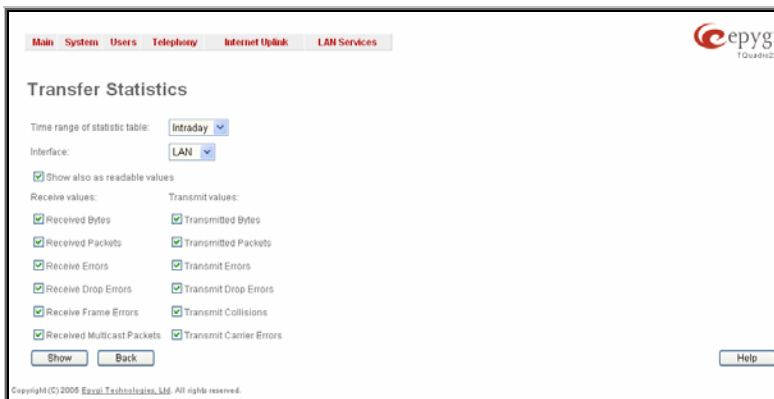


Fig. II-12: Transfer Statistics page

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.

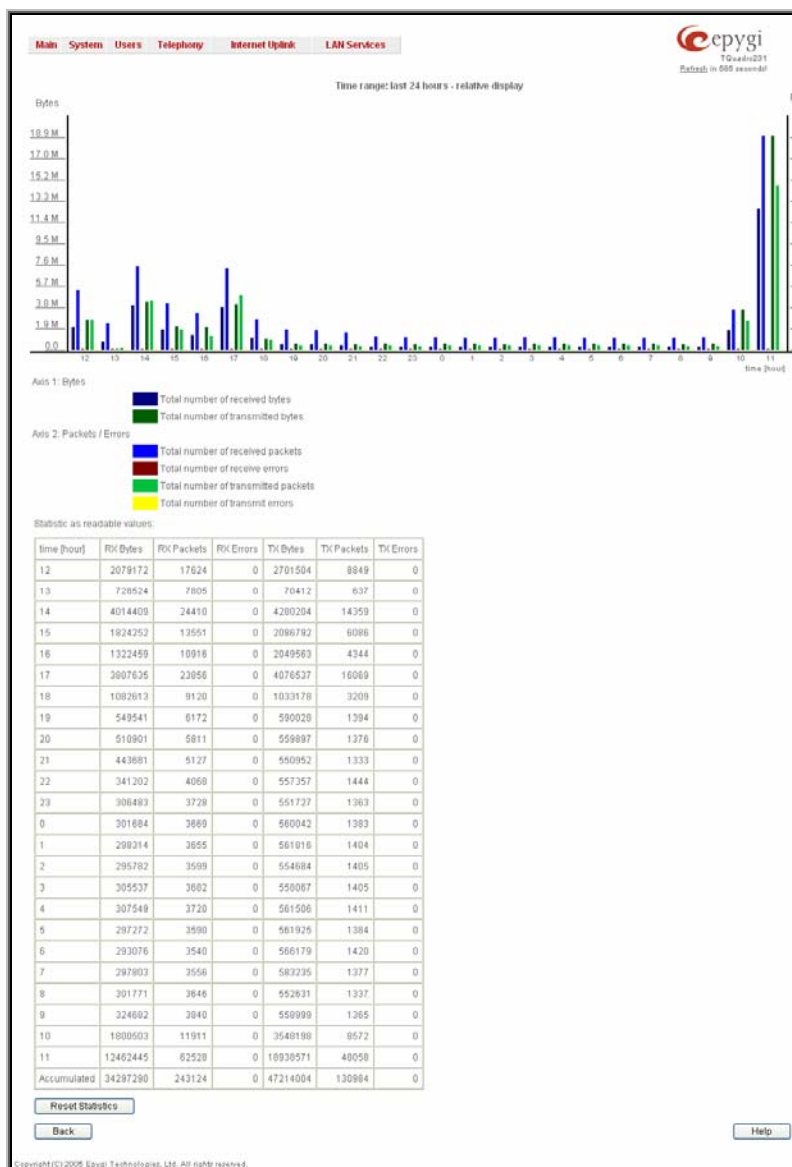


Fig. II-13: Transfer Statistics Diagram Chart

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).

Memory Status

The **Memory Status** page provides information about the total, free and used memory on the Quadro. The **Memory Size** field indicates the total available space on the Quadro, expressed in the bytes, kilobytes and megabytes.

The **Memory Status** table displays the space used by each conference. It shows the free and total space (counted in bytes, kilobytes and megabytes) for every conference. This table includes the following information:

- **Conference ID** - the column lists all available conferences on the QuadroCS. Clicking on the conference ID, the **Conference Recording Settings** page will be opened when the overall memory size allocated to that particular conference may be altered.
- **Used Space** - the column shows used by the conference.
- **Percentage of System Memory** - the column displays the space allocated to the conference.
- **Free Space** - shows the free space referring to the corresponding conference.
- **Total Space** - shows the overall space allocated to the conference. This is a summary of already used and still free spaces.

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

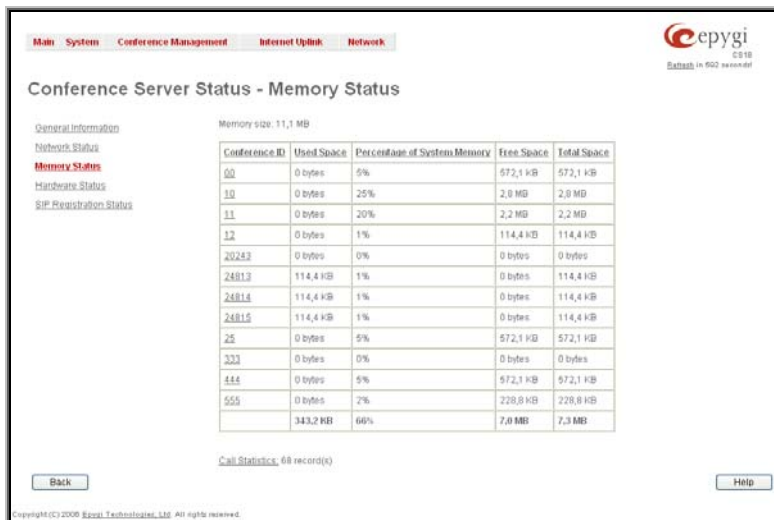


Fig.0-14 Memory Status page

Hardware Status

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

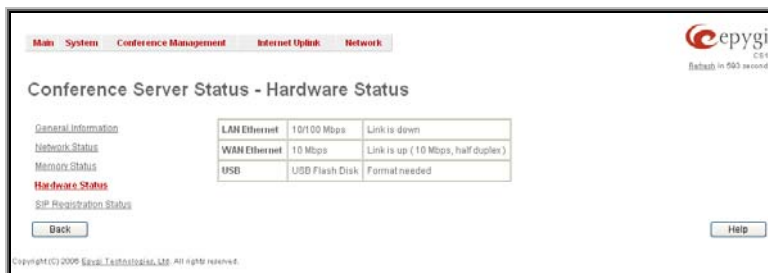


Fig. II-15: Hardware Status page

SIP Registration Status

The **SIP registration Status** is a table displaying the SIP registration status of the QuadroCS conferences.

The table contains a list of all the registered conferences of Quadro, SIP registration name for each conference, addresses of SIP servers where they are registered (if applicable), whether or not it is registered for each conference, 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 SIP Registration Settings page of the corresponding conference 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.



Fig. II-16: SIP Registration Status page

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 QuadroCS. Additionally, this page provides the possibility of restoring the factory default configuration settings.

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.

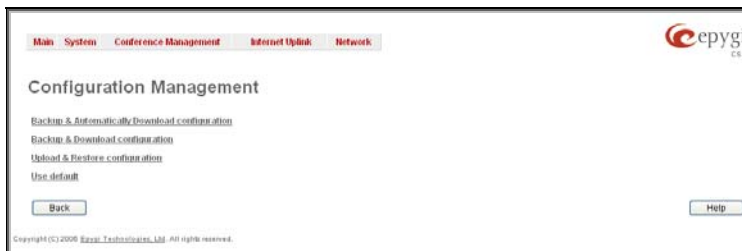


Fig. II-17: Configuration Management. page

The **Use Default** 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 QuadroCS board, this link will keep the following data:

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

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 QuadroCS. 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-18: Event warning on the main menu page

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 has occurred due to incorrect mail sending or SIP registration, the 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](#) settings when a new event occurs.

Status	Timestamp	Priority	Application	Name	Description	Reference
New	Fri Sep 1 17:20:47 2006	3	SIP	registration failure	Could not register user 7331333 on server sip.epygi.com:5060. Reason: Authorization failure	SIP Registration Status
New	Fri Sep 1 16:58:51 2006	2	SNTP	connect failure	System time could not be set. Reason: None of the servers answered	Time / Date
	Thu Aug 31 19:45:01 2006	1	SIP	registration succeeded	Successfully registered user 20243 on server sip.epygi.com:5060	SIP Registration Status
	Thu Aug 31 19:43:43 2006	1	SIP	registration succeeded	Successfully registered user 3331333 on server sip.epygi.com:5060	SIP Registration Status
	Thu Aug 31 17:38:55 2006	1	SYSTEM	usb	USB device 50893001 00 detected	
	Thu Aug 31 10:58:43 2006	1	SNTP	time set	time changed by -1.133527 secs to Thu Aug 31 10:58:42 2006 (ntp.epygi.com)	Time / Date
	Wed Aug 29 12:14:28 2006	3	MAIL	send failure	SMTPSend: connect. Connection refused	System Mail Settings
	Wed Aug 29 12:14:28 2006	1	SYSTEM	backup	Automatic backup completed	Automatic Configuration Backup
	Tue Aug 29 18:58:31 2006	3	SYSTEM	reboot	The device has been successfully started after reboot	
	Tue Aug 29 18:58:05 2006	3	SIP	registration failure	Could not register user 7331333 on server sip.epygi.com:5060. Reason: Authorization failure	SIP Registration Status
	Tue Aug 29 18:58:56 2006	1	SIP	registration succeeded	Successfully registered user 555555 on server sip.epygi.com:5060	SIP Registration Status
	Tue Aug 29 18:58:59 2006	1	SIP	registration succeeded	Successfully registered user 84025 on server sip.epygi.com:5060	SIP Registration Status
	Tue Aug 29 18:58:56 2006	1	SIP	registration succeeded	Successfully registered user 24812 on server sip.epygi.com:5060	SIP Registration Status
	Tue Aug 29 18:58:38 2006	1	SNTP	time set	time changed by 13.825810 secs to Tue Aug 29 18:58:38 2006 (ntp.epygi.com)	Time / Date
	Tue Aug 29 18:58:18 2006	1	DHCPCLIENT	got lease	New IP address assigned to WAN interface. (192.168.84.18)	Internet Configuration Wizard
	Wed Aug 27 12:07:12 2006	3	MAIL	send failure	SMTPSend: connect. Forked is unresponsive	System Mail Settings
	Wed Aug 23 12:07:11 2006	1	SYSTEM	backup	Automatic backup completed	Automatic Configuration Backup
	Mon Aug 21 18:44:11 2006	3	DHCPCLIENT	error	DHCP lease expired. IP configuration of WAN interface cleared	Internet Configuration Wizard
	Mon Aug 21 18:07:03 2006	3	SIP	registration failure	Could not register user 555555 on server sip.epygi.com:5060. Reason: Incorrect remote address	SIP Registration Status
	Mon Aug 21 18:04:28 2006	3	SIP	registration failure	Could not register user 24800 on server sip.epygi.com:5060. Reason: Destination unreachable	SIP Registration Status
	Mon Aug 21 09:22:04 2006	3	SYSTEM	reboot	The device has been successfully started after reboot	
	Tue Aug 15 19:24:39 2006	1	SIP	registration succeeded	Successfully registered user 7149504 on server sip.epygi.com:5060	SIP Registration Status
	Mon Aug 14 20:59:20 2006	1	SNTP	time set	time changed by -1.127306 secs to Mon Aug 14 20:59:19 2006 (ntp.epygi.com)	Time / Date
	Sat Aug 12 10:07:43 2006	1	SIP	registration succeeded	Successfully registered user 20243 on server sip.epygi.com:5060	SIP Registration Status
	Fri Aug 11 00:50:09 2006	1	SNTP	time set	time changed by -1.124775 secs to Fri Aug 11 00:50:08 2006 (ntp.epygi.com)	Time / Date
	Wed Aug 9 12:14:19 2006	1	SYSTEM	backup	Automatic backup completed	Automatic Configuration Backup
	Wed Aug 2 14:58:45 2006	1	SNTP	time set	time changed by 2.632182 secs to Wed Aug 2 14:58:41 2006 (ntp.epygi.com)	Time / Date
	Wed Aug 2 14:58:35 2006	1	DHCPCLIENT	got lease	New IP address assigned to WAN interface. (192.168.84.18)	Internet Configuration Wizard

Fig. II-19: System Events list

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

The **Event Settings** page lists all possible events on the QuadroCS 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.

- **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** - A notification e-mail about the new event description in the email will be sent to the e-mail address specified in the [Mail Settings](#) page.

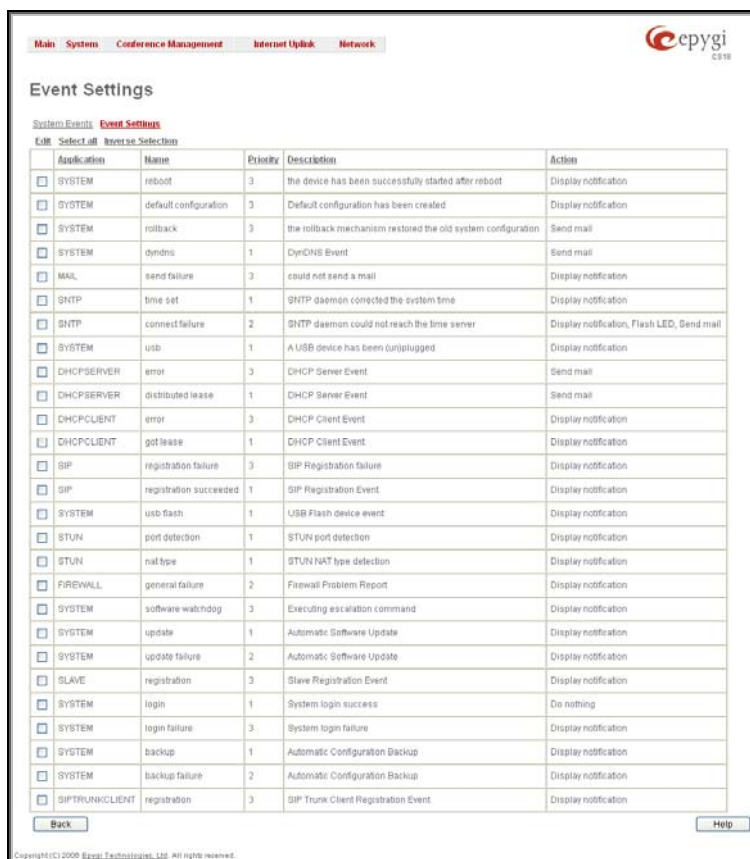


Fig. II-20: Event Configuration Settings page

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.

If QuadroCS 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.

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 administrator of QuadroCS when an event(s) takes place.

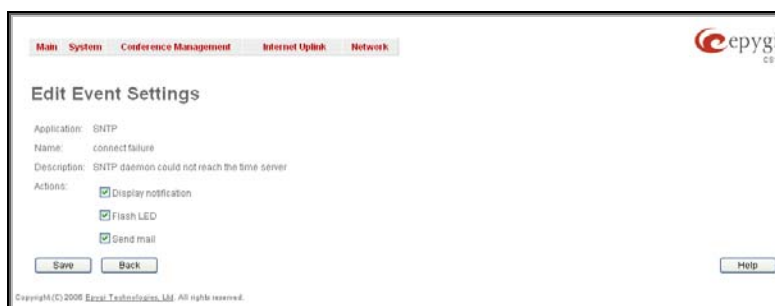


Fig. II-21: Edit Event Settings page

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

Time and Date Settings provide 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. Timezones are specified by GMT (Greenwich Mean Time) and by specific timezones for the United States and Canada.

Enable Simple Network Time Protocol Server enables the SNTP (Simple Network Time Protocol) server on QuadroCS, thus QuadroCS 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 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, QuadroCS's date/time is not being updated automatically).

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

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

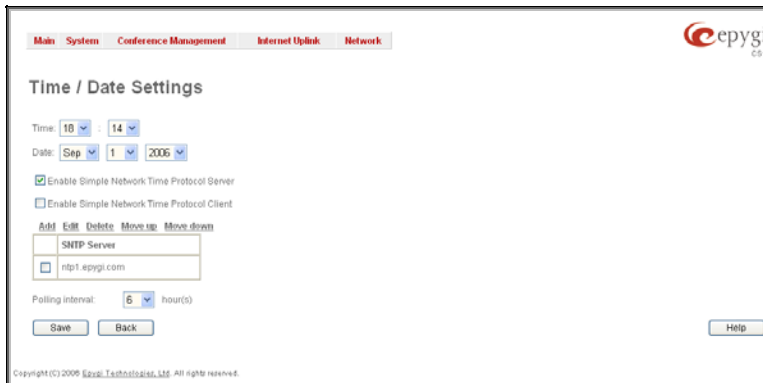


Fig. II-22: Time and Date Settings page

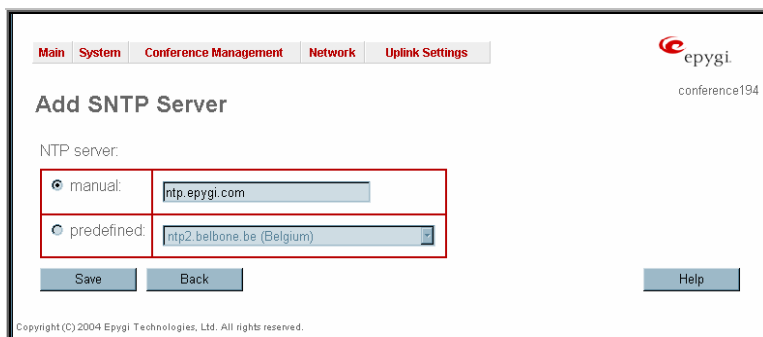


Fig. II-23: Time and Date Settings – Add Entry page

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.

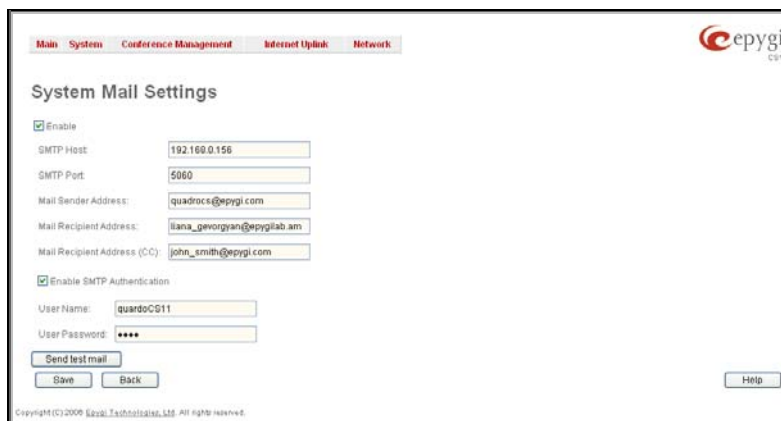


Fig. II-24: System Mail Settings page

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.

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.

Firmware Update

This window allows updating the software of QuadroCS 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. QuadroCS 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.

Please Note: Installing new firmware will take about 15 minutes. During this time, Quadro, telephony and Internet access will be disabled.

The firmware update will cause the loss of the following data:

- All internally stored recordings and custom voice messages
- DHCP leases
- Call statistics
- Pending events
- User specific GUI states

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

Please Note: If you consider the [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.

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

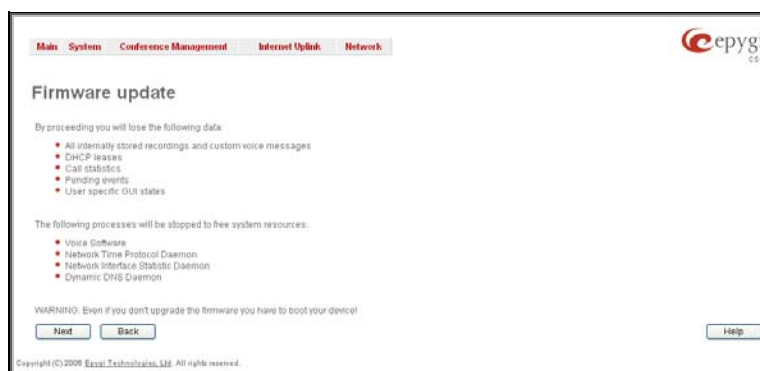


Fig. II-25: Firmware Update page 1

The second page of **Firmware update** consists of the **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. The next page will be displayed, showing the result of a verification of the image being burned.



Fig. II-26 Firmware Update page 2

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

The fields **Current Software Version** and **New Software Version** show the old software version and the version of the new image.

This page needs a confirmation to continue image updating. If you are sure that the image version is appropriate for your device press **Save**.

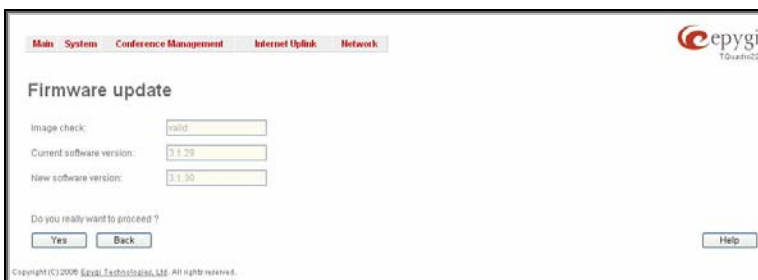


Fig. II-27: Firmware Check page

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.

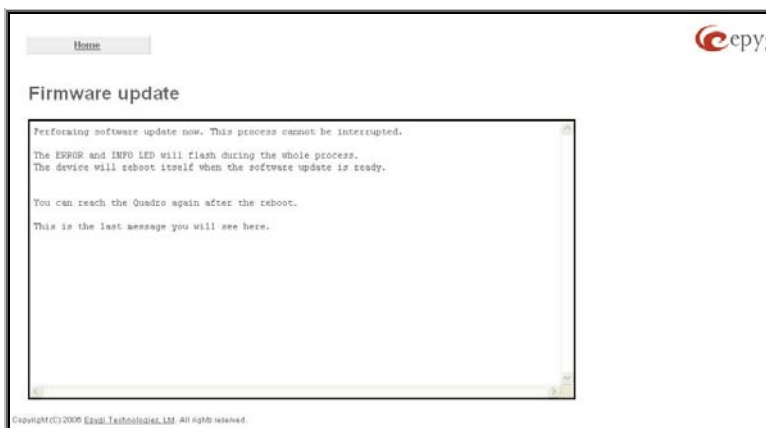


Fig. II-28: Firmware Update page

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).

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.

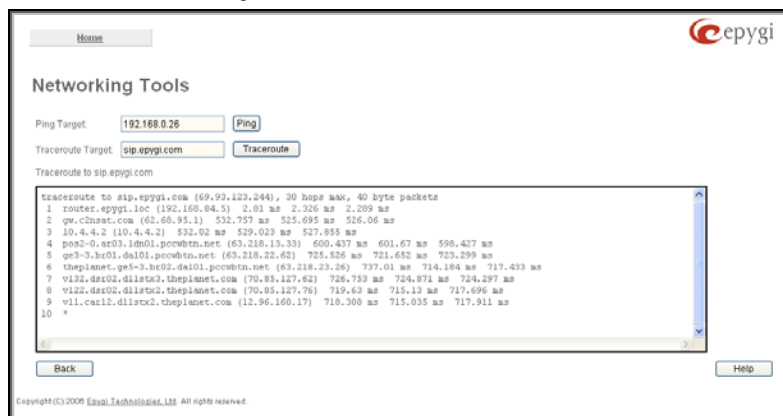


Fig. II-29: Networking Tools page

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.

Diagnostics

The **System Diagnostic** page gives a possibility of running Network and WAN protocol diagnostics to verify QuadroCS'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.



Fig. II-30: System Diagnostic page

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-31: Auto Provisioning page

Upload Language Pack

Upload Language Pack page allows you to upload a custom language for GUI and voice prompts of the QuadroCS. The language of system voice prompts can be switched to the custom Language Pack language from the GUI setting page in 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 internally stored voice mail
- DHCP leases
- 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

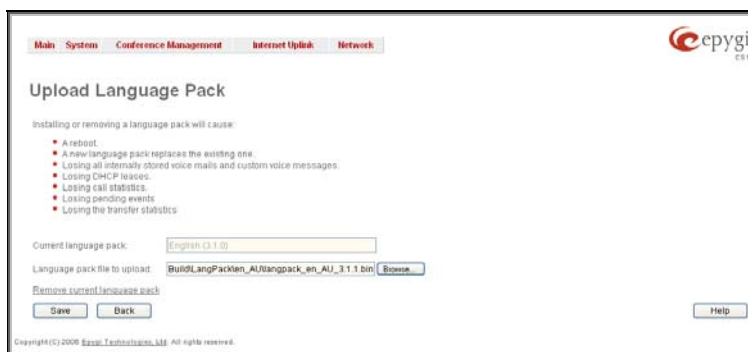


Fig. II-32: Upload Language Pack page

one (if applicable) and will reboot the QuadroCS.

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

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

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

Pressing **Save** will start uploading the custom language pack to the board. The next page displayed will show verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if applicable).

After final confirmation, the system will upload the selected custom Language Pack and it 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 QuadroCS. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the QuadroCS's configuration.

Two levels of QuadroCS 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 QuadroCS. 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.

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.

The **Store password in persistent area (Factory reset save)** checkbox is only present when modifying the Administrator's account password and is used to save the Administrator's password in the factory reset safe place.

Attention: Be EXTREMELY careful when enabling this checkbox. When it is done, the Administrator's password cannot be retrieved even after a factory reset. In this case, if the Administrator's password has been forgotten, the QuadroCS will be considered broken. Please contact Epygi Technical Support Center for replacing the device.

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.



Fig. II-33: Users page at User Rights Management

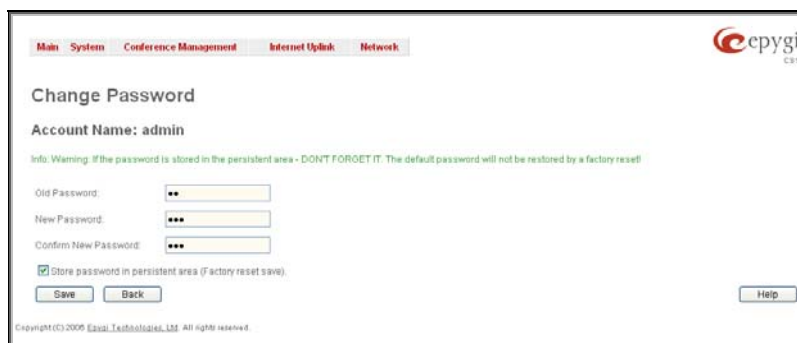


Fig. II-34: Change Password page

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.

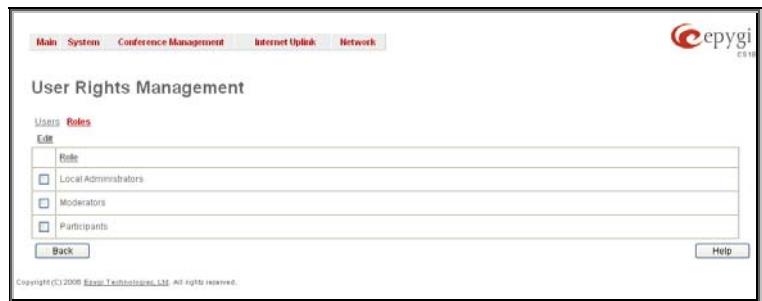


Fig. II-35: Roles page at User Rights Management

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.

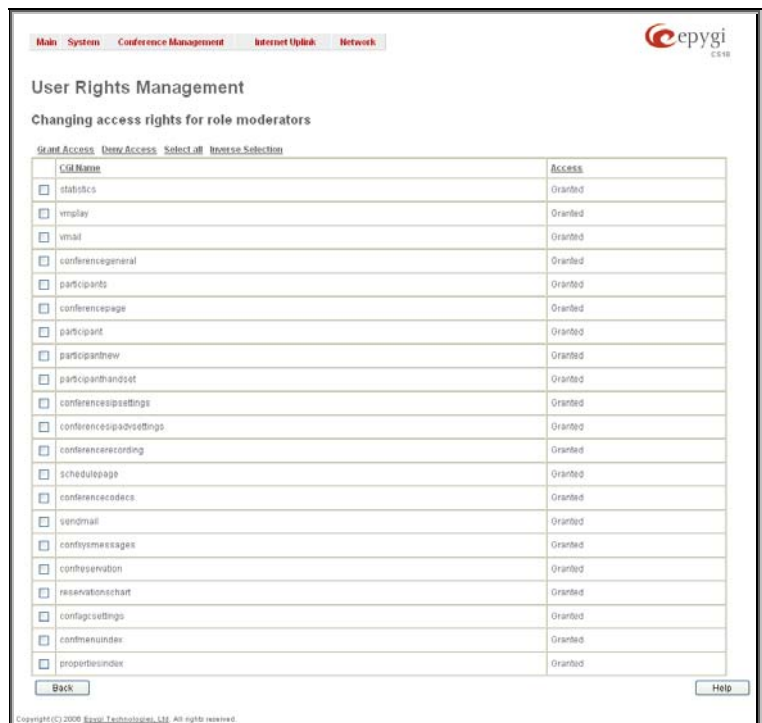


Fig. II-36: Edit Roles page at User Rights Management

Conference Management Menu



Fig. II-37: Conference Management Graphical Menu



Fig. II-38: Conference Management Tree Menu

Conferences

The **Conference** page displays a table with all existing conferences and Auto Attendants on the QuadroCS. This page allows you to create new conferences and Auto Attendants, as well as to manage the existing units.

Attendant extensions are dedicated to the IVR system on the QuadroCS, which is used by the callers to access the conferences on the QuadroCS. It is possible to create Auto Attendants with the custom scenarios. By default, Quadro has one Auto Attendant extension (00) which is undeletable.

The **All Conferences** table lists all created conferences and their parameters.

The screenshot shows the 'Conferences' management page. It includes a navigation bar, a table of conferences, and a 'Back' button. The table has columns for Conference ID, Subject, Description, SIP Address, Status, Percentage of System Memory, and Codecs.

Conference ID	Subject	Description	SIP Address	Status	Percentage of System Memory	Codecs
00		Attendant	24800@sip.epygi.loc:5060		5 %	PCMU...
444		Vonage account	12145501609@sphone.vopr.vonage.net:5061		5 %	PCMU...
555		Custom Attendant	555555@sip.epygi.loc:5060		2 %	PCMU...
10	Liana's Conference	Let's talk about design	10010@sip.epygi.loc:5060	Active	25 %	G726-40...
11	Demo Conference	Default conference with empty passwords.	7149504@sip.epygi.com:5060	Not Active	20 %	PCMU...
12	Duplicated conf from 10	Sales and Marketing discussion	24812@sip.epygi.loc:5060	Not Active	1 %	PCMU...
20243			20243@sip.epygi.com:5060	Not Active	0 %	PCMU...
24813	Conference 24813		24813@sip.epygi.loc:5060	Not Active	1 %	PCMU...
24814	Weekly meeting	Discussing weekly issues	24814@sip.epygi.loc:5060	Active	1 %	PCMU...
24815	Management meeting	Management team discussion	24815@sip.epygi.loc:5060	Not Active	1 %	PCMU...
25			84025@sip.epygi.loc:5060	Not Active	5 %	PCMU...
333	Diana's Conference	Don't touch! Hands off!	3331333@sip.epygi.com:5060	Not Active	10 %	PCMU...

Fig. II-39: Conference Management page

The following columns are present in the **Conferences** table:

- **Conference ID** – indicates the unique ID on the conference. This number is used from Auto Attendant to reach the conference.
- **Subject** - indicates an optional subject for the conference.
- **Description** - indicates an optional description of the conference.
- **SIP Address** - displays the SIP address of the corresponding conference. Column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. Else, 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 be skipped in this column. If no username is defined, the conference ID will be displayed instead.
- **Status** - indicates the status of the conference (Active, Non Active or Waiting). Clicking on the conference status link will display the **Conference Progress** page (see Manual III – Moderator's Guide) with detailed information about the conference status, participants in the conference and description of each participant. This page additionally allows administrator to drop a participant from the conference or

inviting new participants. It also allows the moderator to start/stop/resume/pause the conference recording and to terminate the conference.

- **Recording Space** - indicates the conference related memory space (in percents) dedicated for conference recordings and the conference specific custom system messages.
- **Codecs** – column lists the short information (full information is seen in the tool tip) about conference specific voice Codecs. Conference codec's can be accessed and modified by clicking on the link of the corresponding conference's Codecs. The link leads to the [Conference Codecs](#) page.

Please Note: There is a 40 conference-rooms limitation on the QuadroCS, but the amount of all participants cannot exceed 30 at the same time. Each column heading in the table is created as a link. By clicking on the column heading, the table will be sorted by the selected column. Each record in the table has a checkbox assigned to the row. The checkbox is used to edit, activate, duplicate and delete the corresponding record. Clicking on the corresponding conference ID will link you to the Moderator's page where the conference properties can be altered.

Add opens the **Conference Wizard** used to guide the user through the basic settings to create a new conference or Auto Attendant. The **Conference Wizard** consists of the following pages:

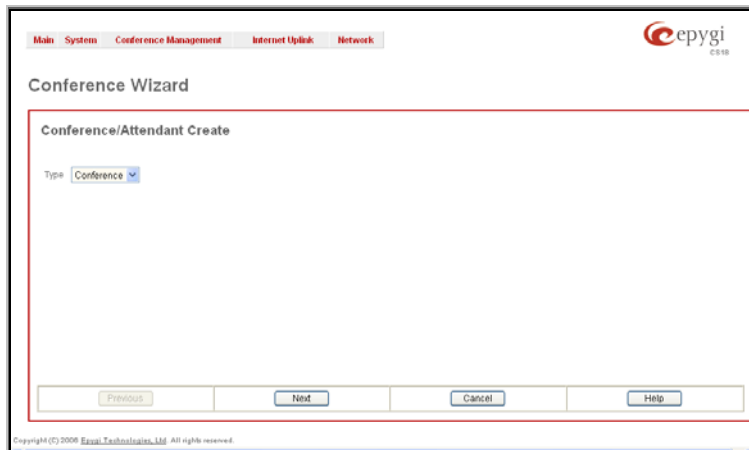


Fig. II-40: Conference Wizard - page 1

Conference Wizard – Page 1 is used to define the type of extensions created: a conference or an Auto Attendant. Depending on this selection, next pages of Conference Wizard may differ.

If you have selected “Conference” on the **Conference Wizard – Page 1** then the second page of the wizard will contain general information for the new conference to be created. In this case, the **Conference Wizard – Page 2** consists of the following components:

Conference ID is used to enter a unique ID for the call conference. This ID will be also used in Conference Server's Auto Attendant to reach the local conference. Digits allowed only. System prevents adding a conference starting with 0 digit.

Subject is an optional parameter where a brief subject of the conference can be entered.

Description is an optional parameter used to insert additional information about the conference.

Moderator Password can be entered to provide moderator access to the conference. It has to be entered twice for confirmation. The password inserted here will be used by the moderator to join the conference. The moderator can dial codes during the active conference as well as access conference specific GUI pages to control the conference (view/change conference properties, activate/deactivate it, start/stop/resume record, view conference statistics).

Participant Password can be entered to require a password for participant access to the conference. It has to be entered twice for confirmation. The password entered here should be used by the participant to join the conference. The participant can participate in the conference only according to the rights (speaker or listener) granted by the moderator. The participant also can access the conference specific GUI to view the conference properties and the other participants.

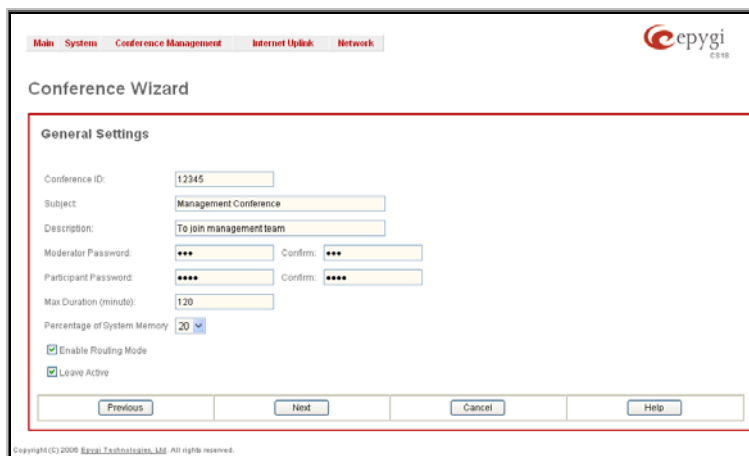


Fig. II-41: Conference Wizard - page 2 – for Conference

Max. Duration sets the conference to be limited to a maximum duration (in minutes). Leave the field empty for unlimited conference duration.

Percentage of System Memory is used to select the percentage of total QuadroCS's memory space that can be used for recording of this conference.

Enable Routing Mode checkbox enables direct access to the Quadro's internal routing tables when dialing out to a participant during a conference. When this checkbox is selected, any dialed number will be parsed through [Call Routing Table](#).

Leave Active checkbox will keep conference active, even if all participants have left it.

If you have selected "Attendant" on the **Conference Wizard – Page 1** then the second page of the wizard will contain general information for the new Auto Attendant to be created. In this case, the **Conference Wizard – Page 2** consists of the following components:

Attendant ID is used to enter a unique ID for the Auto Attendant. Digits allowed only.

Description is an optional parameter used to insert additional information about the Auto Attendant.

Percentage of System Memory is used to select the percentage of total memory space that can be used for attendant scenario and related voice prompts.

Independent on the extension type selected on the **Conference Wizard – Page 1**, the third page of the **Conference Wizard – Page 3** contains conference or attendant related SIP registration settings:

Registration User Name text field requires a user name for conference registration on the SIP server. The registration user name needs to be unique on the SIP server and is used to reach the conference over the SIP network.

Registration Password is the password for the registration on the SIP server. It must be confirmed in the **Confirm Registration Password** text field.

Registration SIP Server indicates the host address of the SIP server. The field is not limited regarding symbol usage and length. It can be either an IP address (ex: 192.168.0.26) or a host address (ex: sip.epygi.com).

Registration SIP Port indicates the host port number to connect to the SIP server. The SIP server port may only contain digit values. If the SIP server port is not specified, the QuadroCS will access the SIP server through the default port of 5060.

Registration on SIP Server enables the conference ID to be registered on the SIP server.

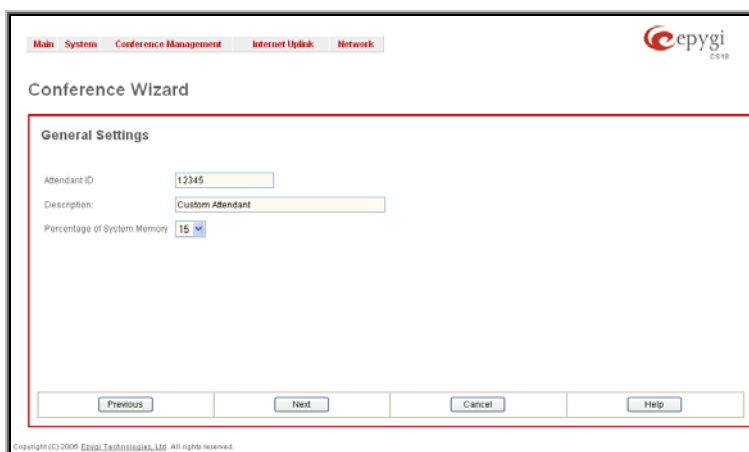


Fig. II-42: Conference Wizard - page 2 – for Auto Attendant

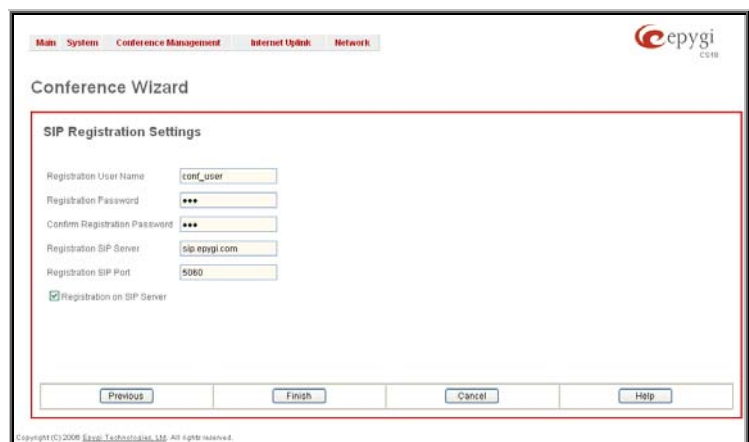


Fig. II-43: Conference Wizard – page 3

Edit button opens the **Conference Wizard** described above with the omitted first page.

Duplicate is used to generate a new conference or Auto Attendant with the settings of an exiting one. To use the **Duplicate** button only one record may be selected. Duplicating a conference, all participants, scheduling options, SIP registration settings and other configuration settings are taken from the original conference. Duplicating an Attendant, SIP registration settings of the original Attendant unit will be used.

Activate is used to activate the selected conference(s).

The **Conferences** table contains a default entry that is dedicated to the Conference Server Auto Attendant. This entry can't be deleted but its settings can be modified. To do so, click the corresponding entry in the table and **Edit Entry** page for the Auto Attendant page will be displayed.

The **Conference Attendant** page consists of four sub-pages used to configure the Quadro CS Auto Attendant:

1. General Settings

This page consists of the following components:

Attendant ID text field indicates read-only information about the Conference Server's Auto Attendant number.

Description text field is used to insert an optional description for the Auto Attendant.

Percentage of System Memory is used to select the percentage of total memory space that can be used for attendant scenario and related voice prompts.



Fig. II-44: Conference Attendant – General Settings

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. The user defined Auto Attendant greeting messages can be uploaded here. 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.

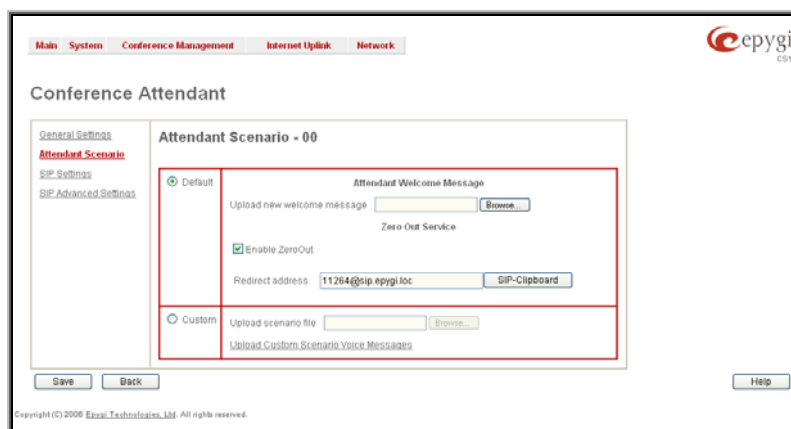


Fig. II-45: Conference Attendant – Attendant Scenario Settings

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

- 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:
 - The **Restore Default Welcome Message** checkbox allows restoring the Auto Attendant default welcome message file if another one has been previously selected. If the checkbox is selected, the file upload will be disabled.
 - 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.
- Enable Zero Out** checkbox enables **Zero Out Service** which provides a possibility to caller that has reached the Conference Server's Auto Attendant Zero Out menu (see Call Codes) to accelerate the automatic redirection feature. Entering Zero Out menu will automatically redirect call to the destination defined in the **Redirect Address** text field. If **Zero Out Service** is disabled, corresponding menu will be hidden in the Auto Attendant.

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.
- 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.

3. SIP Registration Settings

This page requires Attendant SIP registration settings and has the following components:

Registration User Name text field requires a user name for conference registration on the SIP server. The registration user name needs to be unique on the SIP server and is used to reach the Conference Server's Auto Attendant over the SIP network.

The **Registration Password** text field indicates a password for the Auto Attendant extension registration at a SIP server.

The **Confirm Registration Password** text field is used to confirm the password. If the entered password does not correspond to the one given in the **Registration Password** field, the error will appear: “The passwords do not match. Please try again”.

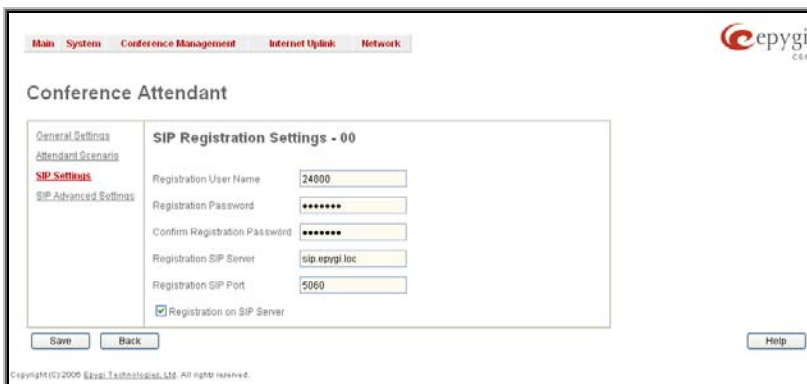


Fig. II-46: Conference Attendant – SIP Settings

The **Registration SIP Server** text field indicates the host address of the SIP Server. The field is not limited regarding symbol usage and length as it can be either an IP number, e.g., 192.168.0.26 or a host address, e.g., sip.epygi.com.

The **Registration SIP Port** text field indicates the Host Port number to connect to the SIP server. It only may consist of numerics, otherwise the error message "SIP Server Port is incorrect" will be displayed when attempting to save the SIP Registration Settings. If no SIP server port is specified, Quadro will access the SIP server through its default port 5060.

The **Registration on SIP Server** checkbox enables the SIP server registration option for the Auto Attendant.

3. SIP Advances Settings

This page requires Attendant advanced SIP settings and has the following components:

SIP Outbound Proxy Address and **SIP Outbound Proxy Port** text fields require the settings of the SIP Outbound Proxy server which acts as a SIP server where all the SIP requests and other SIP messages are transferred. Some SIP servers use outbound proxy server to escape restrictions of NAT. e.g. Free World Dialup service uses Outbound Proxy server. If an Outbound proxy is specified here, all SIP calls originated from the Conference Server's Auto Attendant are made through that outbound proxy, i.e. all requests are sent to that outbound proxy.

The **Authentication User Name** text field 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 field should be left empty.

Fig. II-47: Conference Attendant – SIP Advanced Settings

To Create a Conference

1. Press the **Add** button on the **Conferences** page. The **Conference Wizard** appears in the browser window.
2. Choose **Conference** from the **Type** drop down list.
3. Press **Next** to move forward to the second page of the **Conference Wizard**.
4. Enter the desired conference number in the **Conference ID** text field.
5. Define the conference **Subject** and **Description** in the corresponding text fields if needed.
6. Define the **Moderator** and **Participant Passwords** and confirm them.
7. Define the conference **Max. Duration** in the corresponding text field.
8. Choose a **Percentage of System Memory** for the corresponding conference recordings.
9. Enable **Routing Mode**, if needed.
10. Toggle **Leave Active** checkbox for the conference to remain active even when all participants have left.
11. Press **Next** to move to the conference **SIP Registration Settings** page.
12. Provide the **Registration Username** in the same named text field.
13. Provide the **Registration Password** and confirm it in the corresponding text fields.
14. Define the **Registration SIP Server** and **Registration SIP Port** in the corresponding text fields.
15. Enable **Registration on SIP Server**, if needed.
16. Press **Finish** to create a conference with the defined settings.

To Create an Attendant

1. Press the **Add** button on the **Conferences** page. The **Conference Wizard** appears in the browser window.
2. Choose **Attendant** from the **Type** drop down list.
3. Press **Next** to move forward to the second page of the **Conference Wizard**.
4. Define the attendant **Description** in the corresponding text field if needed.
5. Choose a **Percentage of System Memory** for the attendant scenario and custom voice prompts.
6. Press **Next** to move to the conference **SIP Registration Settings** page.
7. Provide the **Registration Username** in the same named text field.
8. Provide the **Registration Password** and confirm it in the corresponding text fields.
9. Define the **Registration SIP Server** and **Registration SIP Port** in the corresponding text fields.
10. Enable **Registration on SIP Server**, if needed.
11. Press **Finish** to create an attendant with the defined settings.

Conference Codecs

To establish IP voice communication, both parties have to use the same codec. During setup of the communication line, the codec is negotiated. If the caller does not find a matching codec, the communication won't start. If you want to be reachable by all IP callers, it is helpful to support as many codecs as possible. In this case, all codecs that Quadro supports should be added to the **Active Codecs'** table. On the other hand, some codecs require significant bandwidth- up to 64 kBit/s. If you definitely don't want to use these codecs, you must remove them from the **Active Codecs'** table.

The **Conference Codecs** page displays a list of Quadro **Active Codecs**.

The table **Active Codecs** lists active voice codecs for the selected line that are supported by Quadro. The order of records in the **Active 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 out strictly in the top down order given in the **Active Codecs**' table.

Each record in the table has an assigned checkbox. It is used to select the record to be deleted or moved up or down. The following error message results if no records are selected and the user activates the delete button: "No records selected". At least one codec must be attached to the conference, when attempting to delete the last one the error will occur: "At least one codec should stay in the codec list".

Add opens the **Add Entry** page where the user may add codecs supported by QuadroCS. The voice codec defines the voice compression algorithm for the incoming and outgoing DSP packages.

Codecs lists all codecs supported by Quadro. If no more codecs are available (all available codecs have already been transferred to the **Active Codecs**' table), the **Add Entry** page will display the message "No Available Codecs" instead of the drop down menu.

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

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 (G729, G723, G726/16, etc.) are selected.

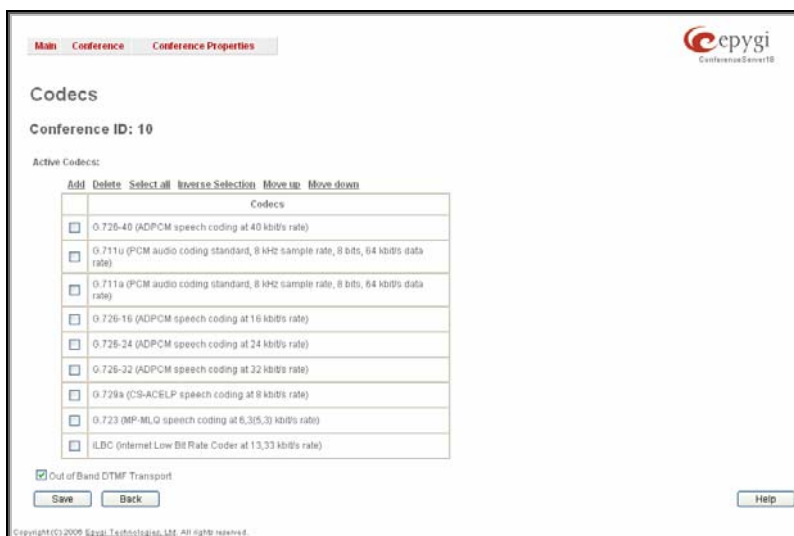


Fig. 0-48 Conference Codecs List

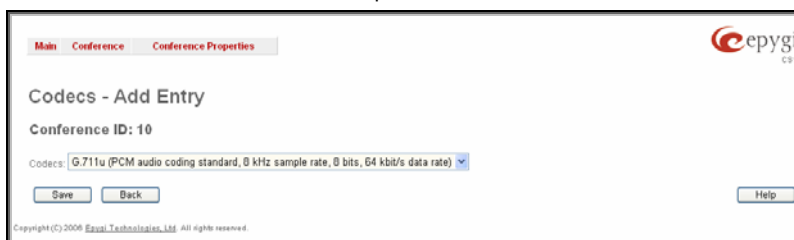


Fig.0-49 Conference Codecs – Add Codec page

SIP Settings

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

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 appears.

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.

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 to choose between regular DNS servers configured in the [DNS Settings](#) page and specific DNS servers for the SIP traffic.

- **Use default** is used to apply regular DNS servers for the 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.

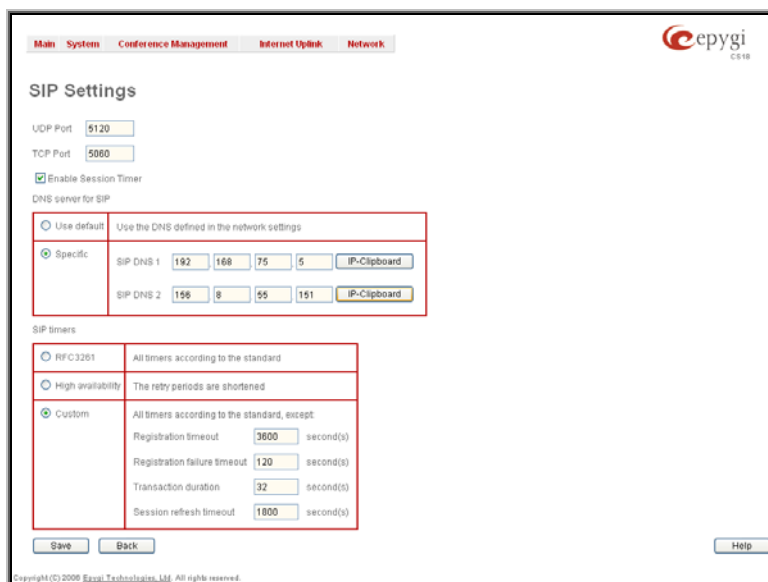


Fig. II-50: SIP Settings page

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 defining manually 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 range and to enable the RTCP support. 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 an error occurs: "One record should be selected".

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. It is activated after 2 seconds of silence and restarted immediately if any audio appears.

The **G.726 Standard** radio buttons are used to select the type of packaging the G.726 code words into octets. If you experience problems with G.726 voice quality having one of these packaging types selected, try the other 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 code words is used, where packing code words into octets is starting from the most significant rather than the least significant position 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 code words is used, where packing code words is starting from the least significant position in the octet.

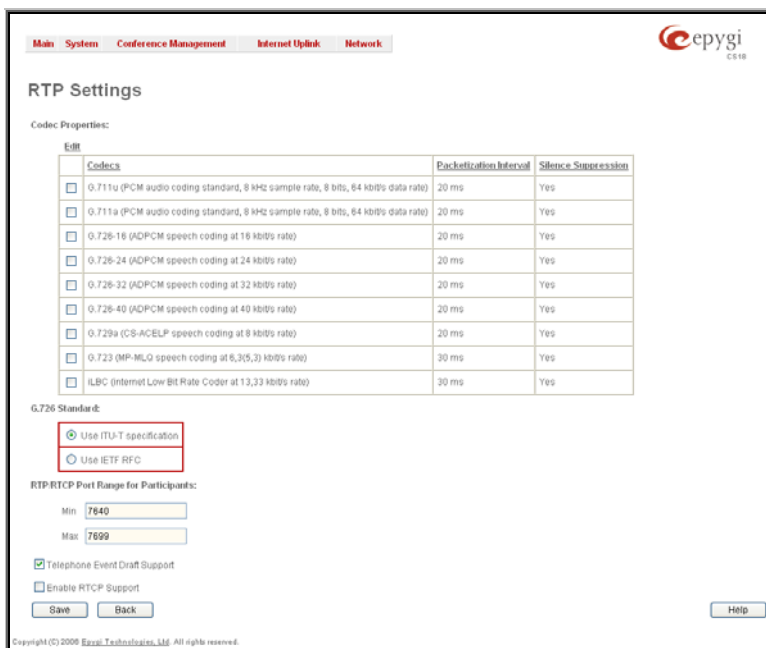


Fig. II-51: RTP Settings page

RTP/RTCP Port Range for Participants:

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.

As 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 occur if this condition is not met. The port range may consist of digits only, otherwise the error "Incorrect Port Range: only Integer values allowed" occurs. The difference between Max and Min RTP ports should be 50 ports or less (according to system capabilities) otherwise a corresponding warning appears. RTP/RTCP Port range cannot include the defined SIP UDP port. Otherwise "Mapped port for SIP shouldn't be in RTP port range" error appears.

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

The **RTP Settings – Edit Entry** page contains two drop down lists 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.

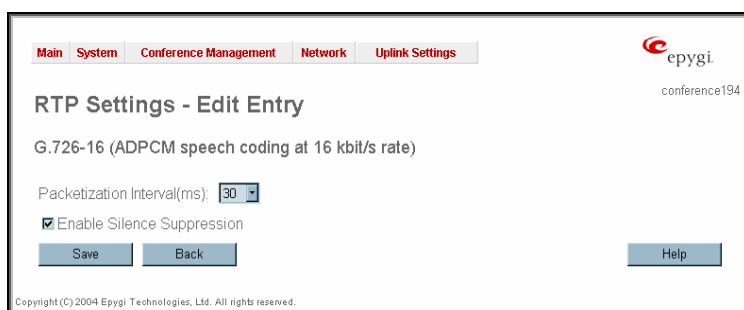


Fig. II-52: RTP Settings – Edit Entry

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 click **Back** to keep the initial data.

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 the SIP traffic will be routed through the NAT server.
- **Disable** – with this selection, no SIP traffic will be routed through the NAT server.

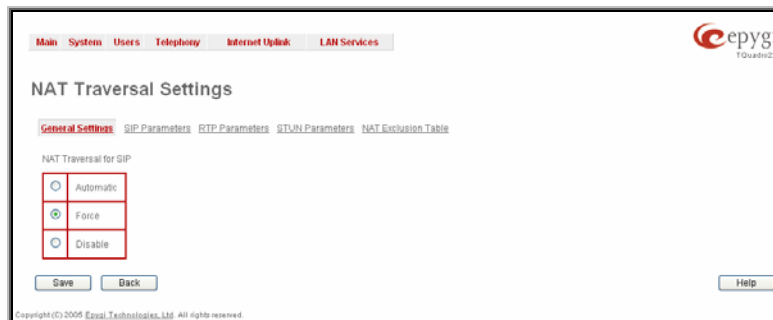


Fig. II-53: General NAT traversal page

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.

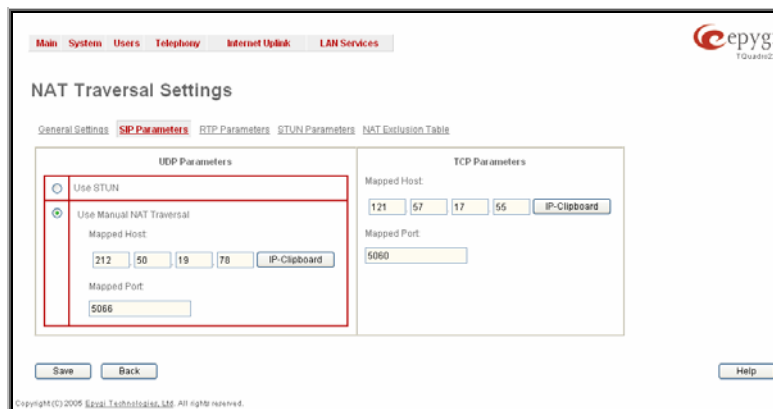


Fig. II-54: SIP Parameters page

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 Participants:**
 - **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.

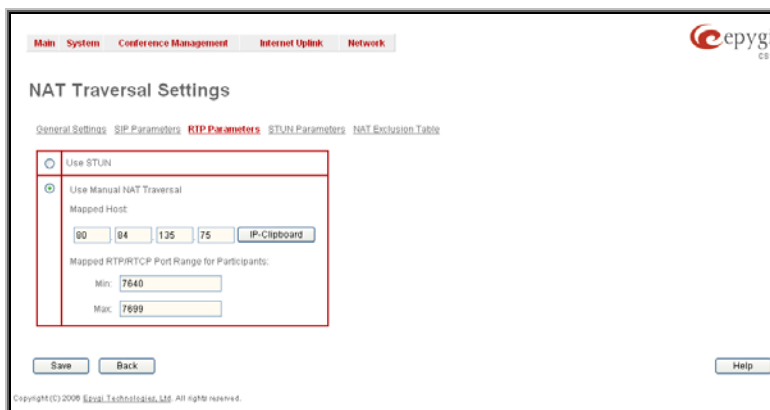


Fig. II-55: RTP Parameters page

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.

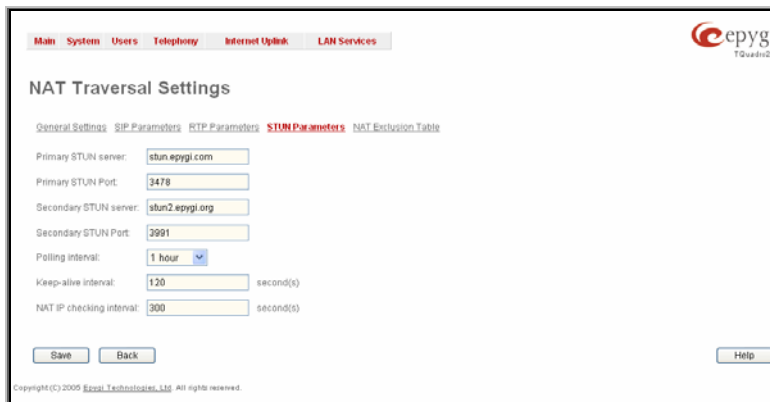


Fig. II-56: STUN Parameters page

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-57: NAT Exclusion Table 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.

Fig. II-58: NAT Exclusion Table - Add Entry page

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**.

Statistics

The **Statistics** page consists of four pages with conference statistics on the first page, successful call statistics on the second page, unsuccessful call statistics on the third page and the statistics settings on the fourth page. The Statistics allows collecting conference call events on the QuadroCS with their parameters and to search them by various criteria.

The **Statistics Settings** page contains the following components:

The **Enable Call Reporting** checkbox enables conference calls statistics reporting.

The **Maximal Number of Conference Call Records** and **Maximal Number of Nonsuccessful Call Records** drop down lists re used to select the maximum number of successful and non-successful statistics records to be collected and shown in the **Statistics** table.

If the record number exceeds the numbers specified in this drop down list, the oldest record will be deleted automatically.

The **Download Call Statistics** link is used to download all statistics in a file that can be viewed with the simple text editor.

Please Note: If you consider the statistics entries in the displayed tables to be important, it is recommended to download the statistics prior to Firmware Update which will clear all statistics on the QuadroCS.

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

Fig. II-59: Call Statistics Settings page

The **Conferences** page displays a table with detailed information (Activation Time, Conference Duration, Participants Count, Activation Reason and Activation Details) about the established conferences and gives the possibility to view the component calls of a particular conference.

To do so, click on the corresponding conference ID. To view all calls directed to or dialed out of the QuadroCS, move to the **Successful Calls** page where the call details table (Activation Time, Conference Duration, Participant, Call Start Time and Call Duration) is displayed. Failed calls can be viewed in the **Nonsuccessful Calls** page.

Each column heading in the aforementioned tables is made as a link. By clicking on the column heading, the tables will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

For both **Conferences** and **Successful Calls** pages, the statistics summary and the search components are present.

The statistics summary contains the **Number of (Call) Records** that displays the total number of conference entries or successful calls in the corresponding tables. Additionally **Conf Total Duration, Conf Maximum Duration, Conf Average Duration** and **Conf Minimum Duration** columns provide information about the total, maximum, average and minimum durations of the conferences.

The following search components allow to filter all the tables on this page:

The **ConfID** text field requires the ID of the conference call. Only numeric values are allowed for this field.

The **From** and **To** text fields above the **Activation Time** column are used to search conferences by its activation date and time. This data must be entered in the following format: dd-mm-yyyy hh:mm:ss. However, the time criteria are optional. **From** requires an earlier date and time than the **To** date and time. If the entered data does not meet this condition, the error message "Minimal date should be less than maximal date" is displayed and statistics filtering is aborted.

The **From** and **To** drop down lists above the **Conference Duration** column are used to search by conference duration. The duration has to be selected from the listed values. The **From** field has to indicate a smaller value 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.

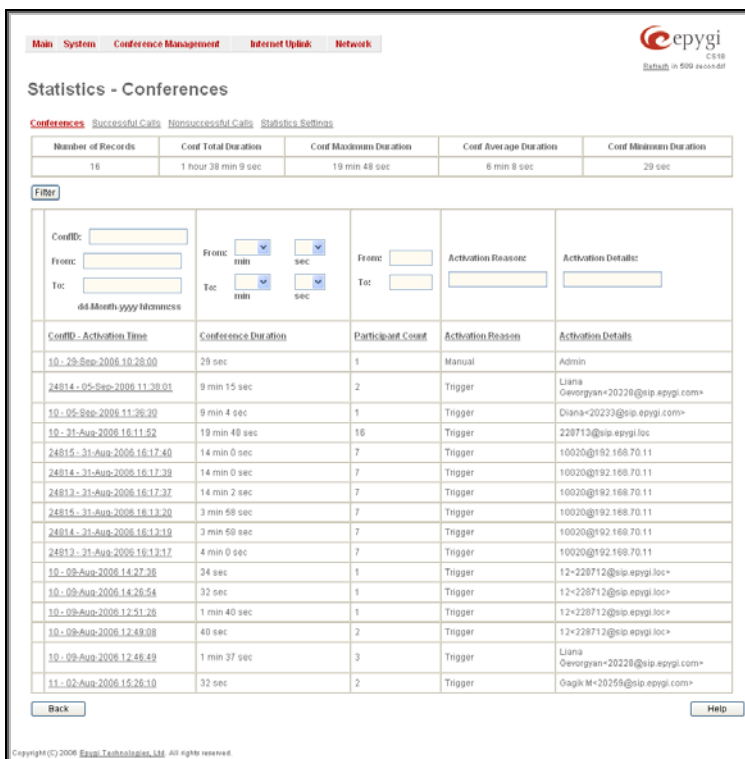


Fig. II-60: Call Statistics page

The **From** and **To** text fields above the **Participant Count** column are used to search by the number of participants in the conference. You can perform manual, trigger or scheduled searches of conferences by using the **Activation Reason** text field. Conferences can be searched by their activation details by using the **Activation Details** text field. The value in the **Activation Details** column is dependent on the **Activation Reason**. For **Manual** activation, details can be either **Admin** or **Moderator** indicating the initiator of the conference. For **Trigger** activation, details indicate the callers' address. For **Schedule** activation, details indicate the conference activation date and time.

By using the **Participant** text field located in the **Successful Calls** table call participants can be searched by their SIP addresses (see chapter [Entering a SIP Addresses correctly](#)). If the defined SIP address is inserted incorrectly, the error "Participant address is incorrect" will prevent filtering. The **From** and **To** text fields above the **Call Start Time** column in the **Successful Calls** table are used to search incoming or outgoing calls by the call start date and time. The data has to be entered in the following format: dd-mm-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.

The **From** and **To** drop down lists above the **Call Duration** column in the **Successful Calls** table are used to search by the call duration. The duration has to be selected from the listed values. The **From** field has to 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.

In the **Nonsuccessful Calls** page, entries can be searched by the Conference ID, by the participant's SIP address, the call start time and the call details (this column indicates a reason of the call failure).

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

To Enable/Disable the Statistics

1. Enter the **Statistics Settings** page.
2. Select/deselect the **Enable Call Reporting** checkbox to enable/disable conference 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 list.
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 **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 **Statistics Settings** page.
2. Confirm the deletion by clicking **Yes**. The conference statistics will be deleted. To abort the deletion and keep the statistics information, click **No**.

Call Routing Table

The **Call Routing** service simplifies the calling procedure for Quadro users, i.e., SIP or IP-PSTN can be accomplished in the same way. With **Local Routing**, each Quadro uses its routing resources set by the Quadro administrator in the call routing table. No SIP registration is needed to make routing calls.

Defining patterns in the **Local Routing Table** avoids registering Quadro at the routing management server and gives a possibility to establish a direct connection to the destination or to use a SIP server for call routing.

The **Call Routing Table** lists manually created routing patterns with their parameters (pattern number, state, routing settings, metric and description).

ID	State	Pattern	NDS	Prefix	Call Type	UCS	Destination Address	ML	Fail Reason	Metric	Description
1	Enabled	7*	1	2	SIP	10	sip.epygi.toc5080		Busy	10	To Epygi Tech Support
2	Enabled	8*	1		SIP		sip.epygi.com:5080		None	10	
3	Enabled	91*			SIP		192.168.75.204:5138		None	10	
4	Enabled	1*			SIP	444	sphone.vopr.vonage.net:5061		None	10	To Sales and Marketing

Fig. 0-61 Local Routing Table

Since **Call Routing Table** may have multiple entries that could match to same pattern, the table will be internally rearranged according to the rules with these 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 **Pattern** text field requires entering the routing pattern identification. To make a specified call, the appropriate routing pattern should be dialed. Wildcard symbols are allowed here (see chapter **Entering a SIP Addresses correctly**). '[', ']', ',', '-', '{', '}' are used to define a range or a quantity of numbers, '!' symbol is used for exclusion ("!5a" inserted in Pattern field means all patterns except those equal to 5a). 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 pattern; in the case of 2{3,7}, the dialed number may be 23 or 27 to match the specified pattern.

Please Note: Patterns starting with the "*" symbols cannot be used for local calls. The reason is that all local patterns starting with "*" will be considered as feature codes and will not be parsed through the Call Routing table.

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.

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.

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.

Fig. 0-62 Local Routing Wizard – Page 1

Call Type gives you the option to select the call type (PBX, PBX-Voicemail, FXO, SIP, IP-PSTN or ISDN). The **PBX** call type is dedicated for call routing to the local PBX extension, and the **PBX-Voicemail** call type is dedicated to route the calls directly to the voice mailbox of the local PBX extension.

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

Use Conference Settings drop down list allows you to select the conference (also Auto Attendant) on behalf of the call that will be placed. The SIP settings of the selected conference 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 conference selected from the **Use Conference 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.

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).

Destination Port requires the port number of the destination or of the SIP server.

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

he public SIP server with the same username at the same time.

The **Fail Reason** drop down list shows the available failure reasons, depending on the call type selection on the previous page. The following Fail Reasons may be available in this list:

- **Wrong Number** – indicates cases when the dialed number is wrong.
- **Busy** - indicates cases when the dialed destination is busy.
- **Network Failure** - indicates cases of system overload, network failure or a timeout expiration occurred.
- **Other** - indicates cases of authorization, negotiation, not supported, request rejected or other unknown errors occur.
- **System Failure** - indicates cases of Network Failure and Other fail reasons.
- **None** – available for all call types and indicates no failure reason.
- **Any** - available for all call types and indicates any of the above mentioned fail reasons.

If the call cannot be established due to some of the 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.

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 or TCP) 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 **Move Up/Move Down** buttons are used to move the local routing patterns one level up or down within the **Local Routing** table. The sequence of the routing patterns is important as the **Local 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 Local Routing Table, which will increase or decrease the selected pattern's priority. Pressing this button will open a page to specify the row number and the desired position of the selected entry (before or after the defined row).

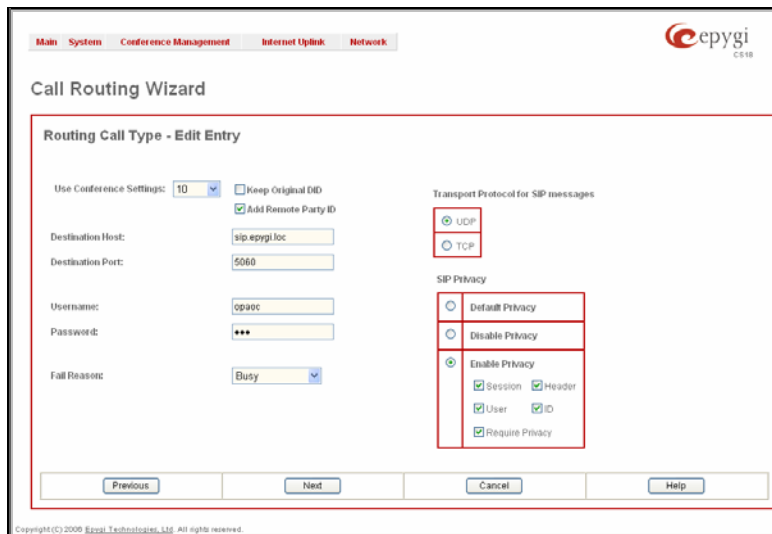


Fig. 0-63 Local Routing Wizard – Page 2

To create 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. Press **Next**.
9. Select the conference or attendant extension from the **Use Conference Settings** drop down list that the call will be placed on.
10. Specify the **Destination Host** and **Port Number, Username** and **Password**.
11. Choose a **Fail Reason** from the corresponding drop down list.
12. Configure **Transport Protocol for SIP messages** and **SIP Privacy** parameters as needed.
13. Press the **Next** button.
14. Press the **Finish** button to establish a local route with the inserted settings.

Best Matching Algorithm

The **Best Matching Algorithm** is used by the Routing Agent (RA) to sort the list of patterns that match a dialed number. Sorting is done by the following principle: **the more the pattern matches the dialed number, the higher its priority.**

To decide which of the selected patterns matches the dialed number more in comparison with the other patterns, the following list of criteria is used (List 1). The criteria are ordered by their priorities: i.e. Criterion 2 is calculated only if more than one pattern takes the same value for Criterion 1, Criterion 3 is calculated only if more than one pattern takes the same value for Criterion 2, etc. **Each consecutive criterion is calculated only if more than one pattern takes the same value for the preceding criteria.**

List 1

Criterion 1	The presence of asterisks (“**”) in a pattern The patterns without “**” have higher priority.
Criterion 2	The number of matching digits/symbols The more matching digits a pattern has, the higher its priority.
Criterion 3	The number of square brackets (“[]”) The more ranges a pattern has, the higher its priority.
Criterion 4	The number of question marks (“?”) The more question marks a pattern has, the higher its priority.
Criterion 5	The number of braces (“{}”) The more ranges a pattern has, the higher its priority.
Criterion 6	The number of asterisks (“**”) The fewer asterisks a pattern has, the higher its priority.
Criterion 7	The value of the metric The lower the metric of a pattern is, the higher its priority.
Criterion 8	The position in the routing table The higher the position of a pattern in the routing table is, the higher its priority.

The algorithm is discussed in the example below.

Example The user has dialed 1231 and the Routing Agent has found the following list of matching patterns.

The list of matching patterns found by RA
1
123*
{11-15}3*
???1
123?
[1-3]*
[1-3]???
{100-150, asd, \{?\}1
12*31
1[1-3]3[0-8]
1231
*2*1
*

The step-by-step discussion of the **Best Matching Algorithm** is as follows:

Step 1: The list is split into two groups separating the patterns with "*" from the ones without (Criterion 1). The patterns with "*" form a group with lower priority and are pushed back to the end of the list (Table 1).

???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 sorted separately from each other by the number of matching digits in descending order (Criterion 2, Table 2). The patterns that have the same number of matching digits are grouped into sub-lists (Table 3). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

The list of patterns	Criterion 2
1231	4
123?	3
???1	2
1[1-3]3[0-8]	2
{100-150, asd, \^?}1	1
[1-3]???	0
12*31	4
123*	3
*2*1	2
1	1
{11-15}3*	1
[1-3]*	0
*	0

The list of patterns	Criterion 2
1231	4
123?	3
???1	2
1[1-3]3[0-8]	2
{100-150, asd, \^?}1	1
[1-3]???	0
12*31	4
123*	3
*2*1	2
1	1
{11-15}3*	1
[1-3]*	0
*	0

The principle by which the patterns have been sorted in Step 1 is applied in all further steps with a different criterion.

Step 3: Each sub-list is sorted separately from the others by the number of brackets ("[" "]") in the pattern in descending order (Criterion 3, Table 4). The patterns that have the same number of ranges are grouped into sub-lists (Table 5). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	2
???1	0
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	1
*	0

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	2
???1	0
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	1
*	0

Step 4: Each sub list is sorted separately from the others by the number of question marks in the pattern in descending order (Criterion 4, Table 6). The patterns that have the same number of question marks are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 6

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	-
?2?1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	-
*	-

Step 5: Each sub-list is sorted separately from the others by the number braces (“{ }”) in the pattern in descending order (Criterion 5, Table 7). The patterns that have the same number of ranges are grouped into sub-lists (Table 8). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 7

The list of patterns	Criterion 4
1231	-
123?	-
1[1-3]3[0-8]	-
?2?1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
{11-15}3*	1
1	0
[1-3]*	-
*	-

Table 8

The list of patterns	Criterion 4
1231	-
123?	-
1[1-3]3[0-8]	-
?2?1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
{11-15}3*	1
1	0
[1-3]*	-
*	-

Step 6: This step is applicable to the subgroup containing patterns with “*”, the group with lower priority. Each sub-list is sorted separately from the others by the number of asterisks (“**”) in ascending order (Criterion 6). The patterns that have the same number of asterisks are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Step 7: Each sub-list is sorted separately from the others by the value of metric in ascending order (Criterion 7). The patterns that have the same value of metric are grouped into sub-lists. If a sub-list consists of one pattern it stays in its position and does not participate in further discussions.
The values of metrics are taken from the routing table.

Step 8: The patterns in each sub-list are arranged by their positions in the routing table (Criterion 8).

The subgroup containing patterns with “*” is attached to the end of the subgroup without “*” forming a single list of sorted patterns. The obtained list is the sorted list of the patterns by the Best Matching Algorithm (Table 9).

Table 9 The sorted list of patterns
1231
123?
1[1-3]3[0-8]
?2?1
{100-150, asd, *?}1
[1-3]???
12*31
123*
*2*1
{11-15}3*
1
[1-3]*
*

Recording Common Settings

The **Recording Common Settings** page is used to configure the memory allocations for recorded conferences. QuadroCS allows USB Flash Memory for conference voice data file storage. USB Flash Memory is basically a portable hard drive. Using flash memory, the USB Flash Disk is compact, lightweight, durable and easy to use. USB Flash Disk can be plugged into the available USB port on the QuadroCS.

The **Memory Allocation** manipulation radio buttons give you a choice between embedded memory or external USB storage.

- Selecting **Embedded Memory Storage** will save recorded conferences internally.
- Selecting **External USB Flash Memory** allows you to save recorded conferences on the external USB device attached to the QuadroCS. This will save the space on the QuadroCS. Selecting the External USB Flash and saving the page settings will start the USB Flash Memory automatic configuration.

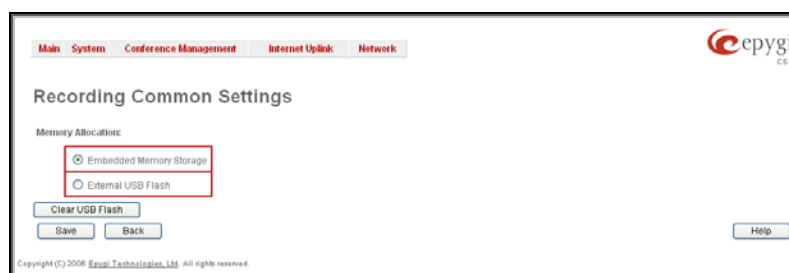


Fig. II-64: Voice Mail Coming Settings page

The USB flash memory device needs to be formatted to be available to the Quadro. A confirmation message will ask for the USB flash memory formatting verification.

Attention: Formatting will erase all existing data on you're the USB flash disk.

Quadro can reuse the USB flash memory once it s formatted. Each time the USB flash memory device is plugged into the Quadro, it will be mounted automatically. For safety purposes, removing the USB flash memory device will result in it being automatically un-mounted first. Error messages will appear when formatting, mounting, or un-mounting procedures are unsuccessful, as well as when the USB flash memory device is write protected or undetected.

Replacing or removing the USB flash memory device from the Quadro, the Quadro will automatically switch back to the **Embedded Memory Storage** and all further voice data will be stored in the Quadro's local flash memory.

Attention: It is highly recommended to select **Embedded Memory Storage** prior to unplugging the USB flash memory device. If this is not selected, the data stored on the USB flash memory device may be corrupted or lost. It is not recommended to remove one USB flash memory device and plug another one within 10 seconds; otherwise the system may fail to detect the new USB flash memory device.

When attaching the USB flash memory device to the Quadro, its voice data (if any) will be copied automatically from the Quadro's local flash to the external USB flash memory device. If the USB flash memory device is too small to fit the voice data on the Quadro, the Memory Allocation mode will still be switched to the External USB Flash, however, no voice data will be copied to the USB flash memory device.

Please Note: Since Quadro allows using both its local flash space and the External USB flash memory device, recorded conferences can be stored in both locations depending on the selected Memory Allocation mode. If the user experiences a loss of a specific recorded conference or custom Auto Attendant system messages in their configuration, verify the memory allocation mode Quadro has been acting in at the time the voice data was recorded.

The **Clear USB Flash** button appears only when the USB Flash Memory Stick is attached to the Quadro and is used for erasing the USB Flash Memory.

Below is the list of USB Flash Memory devices tested and functional with the QuadroCS.

1. San Disk Cruzer mini 256MB
2. JMTEk 128MB
3. JMTEk USBDrive 32MB
4. Apacer 64MB
5. Pen Drive 64MB
6. Seitec 256MB
7. Lexar JumpDrive 128MB
8. Orange 128MB
9. QuickDrive 128MB
10. Kingston 128MB
11. LinkSys Instant USB Disk 128MB
12. DiskGo Edge Digital Media 128MB

Attention: It is strongly recommended to use one USB Flash Memory. Two sticks cannot be used simultaneously.

Mail Default Settings

Mail Default Settings page is used to define the email templates used in the automatically generated emails from the QuadroCS to the conference participants. Two email templates can be defined on this page:

- **Conference Notification Default Mail** – delivered when the moderator chooses the **Send Notification Mail** menu option (see Manual III – Moderator's Guide).
- **Conference Activation Default Mail** – delivered by the conference Scheduling system (see Manual III – Moderator's Guide), if the **Send Mail before Conference Activation** option is enabled.

Each template should be defined in the corresponding text field. Additionally, functional tokens can be used to automatically insert the Conference ID, Subject, Description, Participants, Password, Scheduling information, as well as a possibility to display the time remained until the conference will start, etc.

All these tokens can be inserted by using the links on the right side of the page.

Please Note: Changing the body of the token will disable the token functionality and will be implied as a simple text.

The **Restore Defaults** button is used to restore the default mail templates. Using this button, all user defined mail templates will be lost.

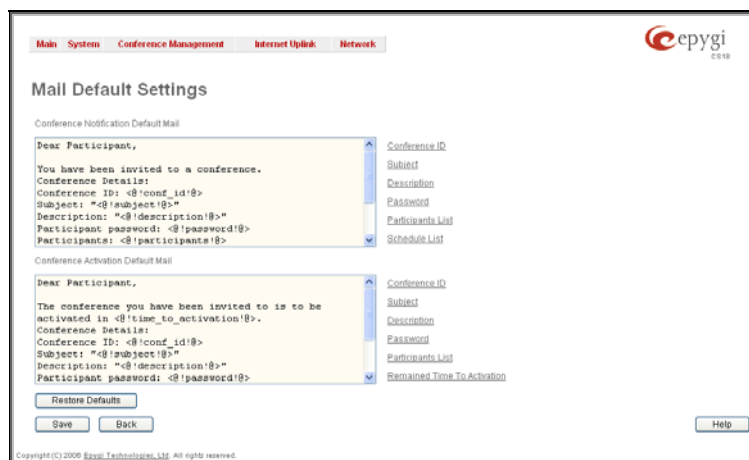


Fig. II-65: Email Default Settings page

Internet Uplink Menu



Fig. II-66 Internet Uplink Dynamo Menu

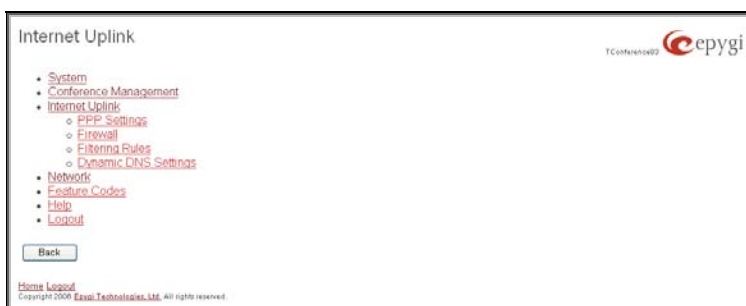


Fig. II-67: Internet Uplink Tree Menu

PPP Settings

The **PPP 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 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**.

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.

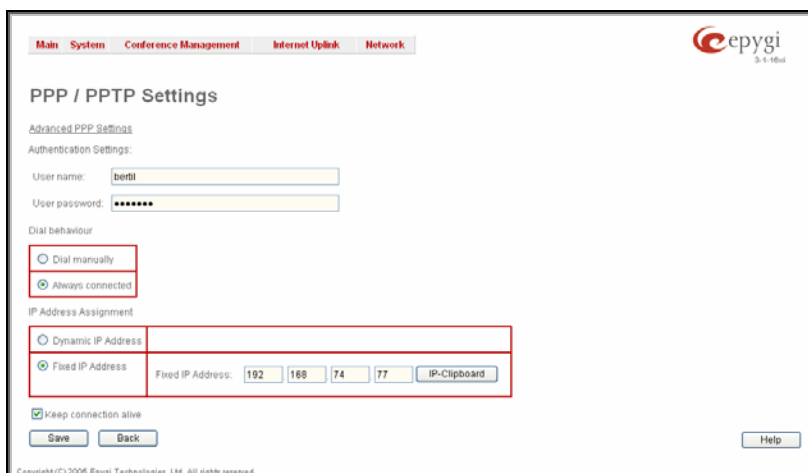


Fig. II-68: PPP Dial Settings page

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.

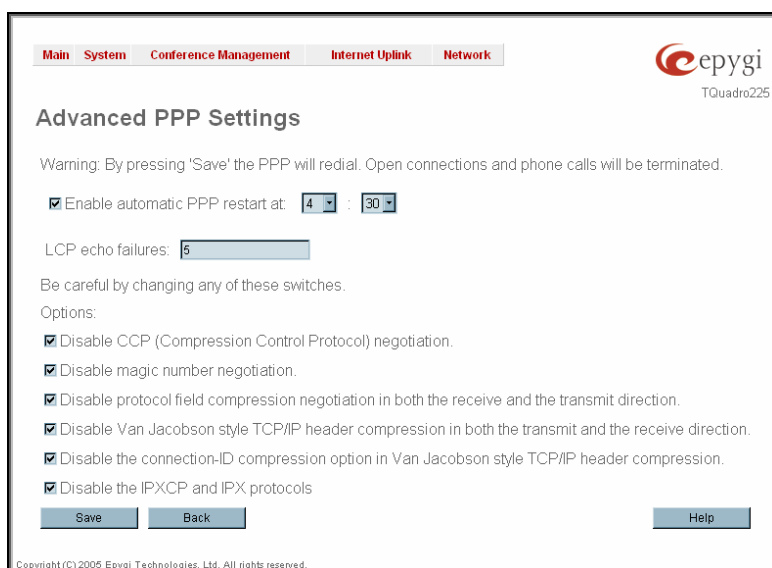


Fig. II-69: Advanced PPP Settings page

Firewall

The **Firewall Configuration** page allows setting up a firewall, configuring the security level of QuadroCS.

A **Firewall** is a security service configured by the QuadroCS 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, 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.

The **Firewall Configuration** page consists of the following components:

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:

- **Low Security** - Everything that is not explicitly forbidden is 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.**

[Advanced Firewall Settings](#) link refers to page where QuadroCS privacy can be configured.

The [View Filter Rules](#) link opens the [Filtering Rules](#) page.

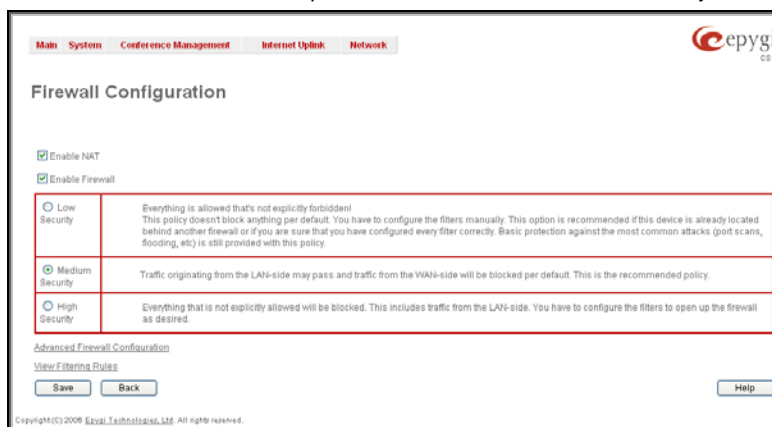


Fig. II-70: Firewall and NAT Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed toward the device. With these features enabled QuadroCS will answer with irritating message to the Ping and Portscanning operations. Page consists of the following components:

The **Ping Stealth** checkbox selection prohibits Ping operation toward QuadroCS from its WAN.

The **Fool Portscanner** checkbox selection prohibits QuadroCS portscanning from its WAN. As a reply to Portscanning operation, "network unreachable" or "host unreachable" feedback messages will be sent.



Fig. II-71: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows the configuration of filters for the incoming and outgoing traffic.

To prevent misconfiguration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. As 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 just 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**). As 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. 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.

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](#)) are leading 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 the 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 "No record(s) selected" error occurs.
- **Disable** is used to disable the rule. If no records are selected the "No record(s) selected" error occurs.
- **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**:

For example, 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.

Note: It is not allowed to forward incoming packets when 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 original port number when incoming packet is being forwarded. If this field is left empty, original port number will be used upon forwarding the packet.

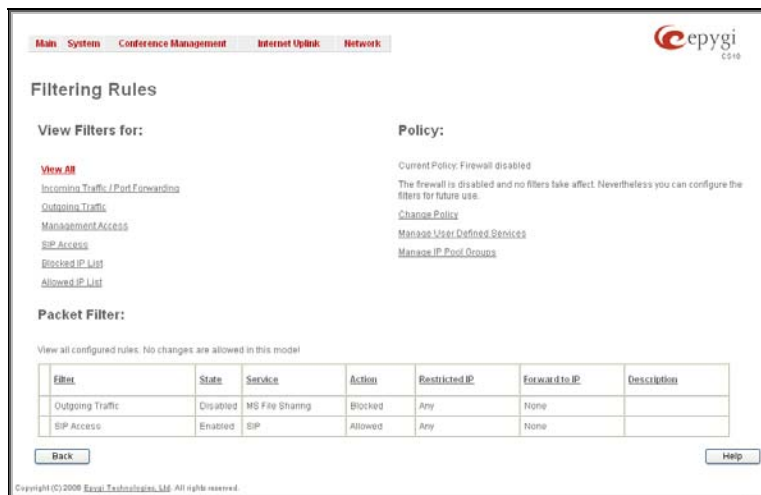


Fig. II-72: Filtering Rules page

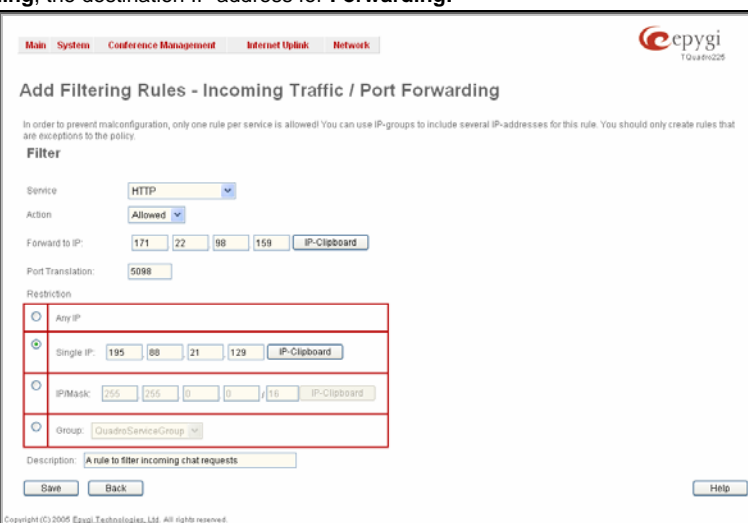


Fig. II-73: Filtering Rules - Page to add a rule for Incoming Traffic

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. **Maskbit** examples:
 255.0.0.0= /8,
 255.255.0.0 = /16,
 255.255.255.0 = /24,
 255.255.255.255= /32
- **Group** indicates the user defined groups that include IP addresses that ought to be allowed or blocked.

To Add a Filtering Rule

1. Select the **Filter** link (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List or 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, leave it as is.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, leave it as is.
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, SingleIP** or **IP/Mask** and enter the required information in the text fields or select a group.
7. 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 ought to be deleted from the rules table. Press **Select all** if all rules ought to be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion with **Yes**, or cancel it with **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:

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 an error will occur: "One row must be selected".

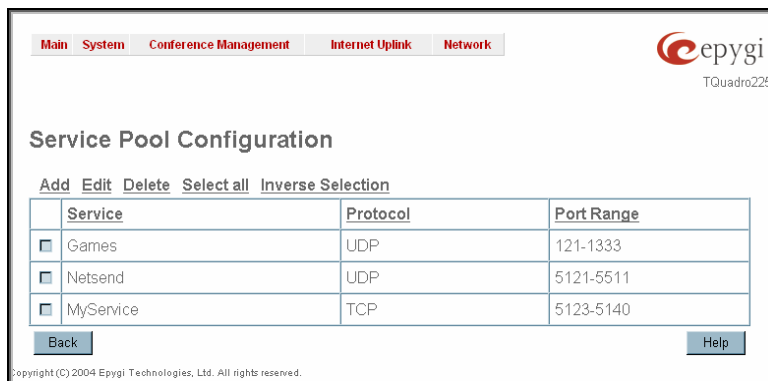


Fig. II-74: Service Pool page

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 ought to be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.

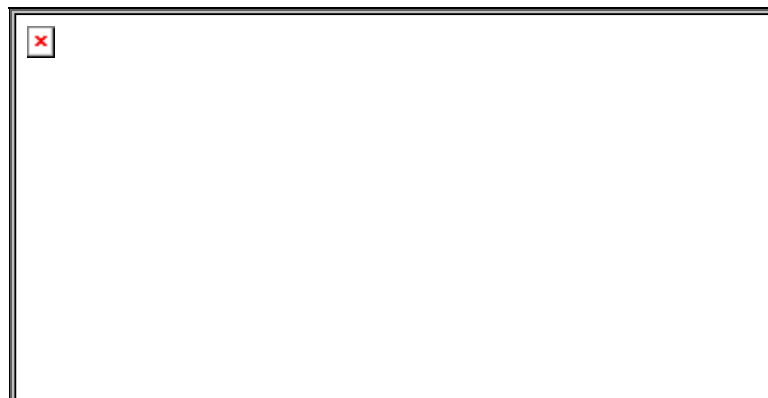


Fig. II-75: Service Pool - Page to add a new Service

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 ought to be deleted from the **Service Pool** table. Press **Select all** if all services ought to be deleted.
3. Click on the **Delete** button on the **Service Pool Configuration** page.
4. Confirm the deletion with **Yes**, or cancel it with **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. Whenever 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.

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 an error will occur: "One row must be selected".

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).

Clicking on the **Group** name will display an **IP Pool Group Configuration** page with the **Members** list for the current group.

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 an error will occur: "One row must be selected".



Fig. II-76: IP Pool Configuration page



Fig. II-77: IP Pool configuration – Add Group page

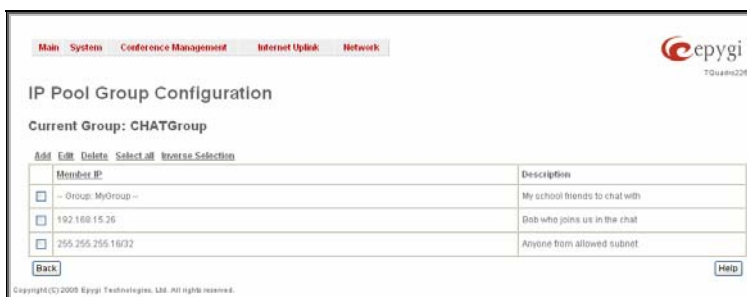


Fig. II-78: IP Pool Group Configuration page

The **Add Members** page provides the following radio buttons:

IP Address 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.

The **User-defined Group** includes previously added groups that also may be added as a member to another group.

Member description text fields can be used to enter an optional description of the member.

The screenshot shows the 'IP Pool Group Configuration - Add Member' page. At the top, there are navigation links: 'Main', 'System', 'Conference Management', 'Internet Upload', and 'Network'. The 'epygi' logo is in the top right corner. The page title is 'IP Pool Group Configuration - Add Member'. Below the title, it says 'Current Group: CHATGroup'. There are three radio buttons: 'IP Address', 'IP Subnet', and 'A user-defined Group'. The 'A user-defined Group' option is selected. Below the radio buttons, there are three input fields: 'IP Address' (with sub-fields for 192, 168, 70, 18), 'IP Subnet' (with sub-fields for 255, 255, 255, 0, 18), and 'A user-defined Group' (a dropdown menu showing 'MyGroup'). Below these fields is a 'Member description' field with the text 'My school friends to chat with'. At the bottom, there are 'Save', 'Back', and 'Help' buttons. A copyright notice 'Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.' is at the very bottom.

Fig. II-79: 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 ought to be deleted. The **IP Pool Group Configuration** list appears.
3. Check one or more checkboxes of the corresponding members that ought to be deleted from the **Members** table. Press **Select all** if all members ought to be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.
5. Confirm the deletion with **Yes** or quit with **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 ought to be deleted from the groups table. Press **Select all** if all groups ought to be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion with **Yes** or quit with **No**.

Dynamic DNS Settings

The **Dynamic DNS** (DynDNS) is a service that is used to map a dynamic IP address to a host name. Thus this service is only makes sense if you are connected to the Internet with a dynamic IP address (and 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 his WEB site.

The **Dynamic DNS Settings** page consists of 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 this field should be greater than 24, otherwise an error occurs: "Update interval times smaller than 24 hour are too small". 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 to which he has subscribed.

The **Host** text field requires the name of the host in 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, to which the DynDNS service provider will relay your e-mails.

Attention: If this service is used, make sure, 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 user knows this HTTP get request exactly, the radio button **Create Custom HTTP GET Request** together with the text field **URL** allows to enter it directly.

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 format:

[http://]www.server.domain:port/scriptpath/scriptname?param1=value1¶m2=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 safety reasons. The user can do that either together with the HTTP get request in the text field **URL** or select the checkbox **Basic Authentication**.

Fig.0-80 Dynamic DNS Settings page

Network Menu



Fig. II-81: Network Dynamo Menu



Fig. II-82: Network Tree Menu

DNS Settings

The **DNS Settings** page gives the possibility to setup a name server for the QuadroCS. It consists of the following components:

NameserverAssignment radio buttons:

- **Dynamically by provider** automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** - 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.

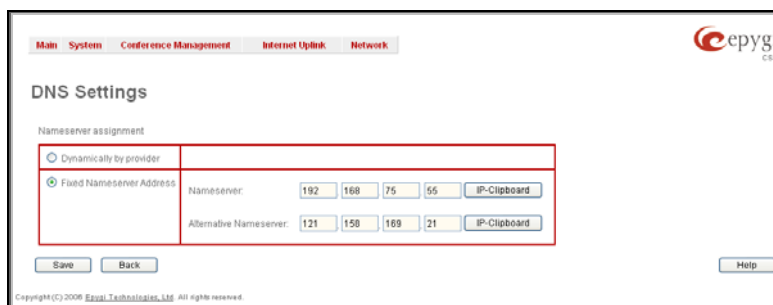


Fig. II-83: DNS Settings page

DHCP Settings for the LAN Interface

The **DHCP Settings for the LAN Interface** page gives the possibility to enable a DHCP server and control the QuadroCS user's LAN settings. Thus QuadroCS LAN users will be provided automatically with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the QuadroCS's IP address)
- WINS server
- Nameserver (corresponds to the QuadroCS's IP address)
- Domain name

The page **DHCP Settings for the LAN Interface** offers the following input options:

Enable DHCP Server activates the DHCP server on QuadroCS.

IP Address Range defines a range of IP addresses that will be assigned to the QuadroCS's LAN users. The IP range must be at least 6, otherwise the "Address Range too small" error will prevent saving. The "Address Range too large" error occurs if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the QuadroCS's LAN users.

View DHCP Leases leads to the page where the DHCP leased LAN IP addresses are listed.

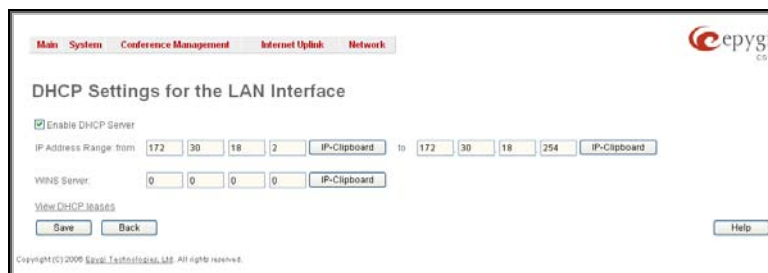


Fig. II-84: DHCP Settings page for LAN interface

The **DHCP Leased IP Addresses** page includes a list of the leased host addresses that are part of the QuadroCS's LAN. For these hosts QuadroCS acts as a server supplying them with a unique IP address. It consists of a non-editable table describing all the leased IP hosts and their parameters. The table contains the following columns:

- IP address** - host IP address, assigned by QuadroCS.
- 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 deactivated.
- Hostname** - hostname, provided by the host itself.

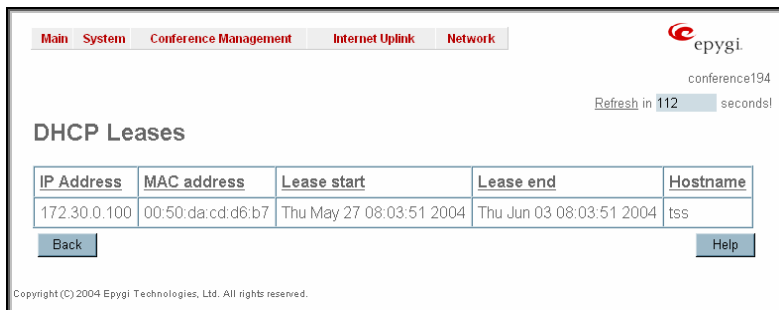


Fig. II-85: DHCP Leases page for LAN interface

Registration Form

The **Registration Form** page appears if unregistered users login and has been created for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It consists of several links offering registration options:

- Register now** leads to the Epygi Technical Support System Registration page and requires customer's information to submit the registration form.
- Remind me later** hides the registration notification until the next startup.
- Don't remind me more** hides the registration notification forever.

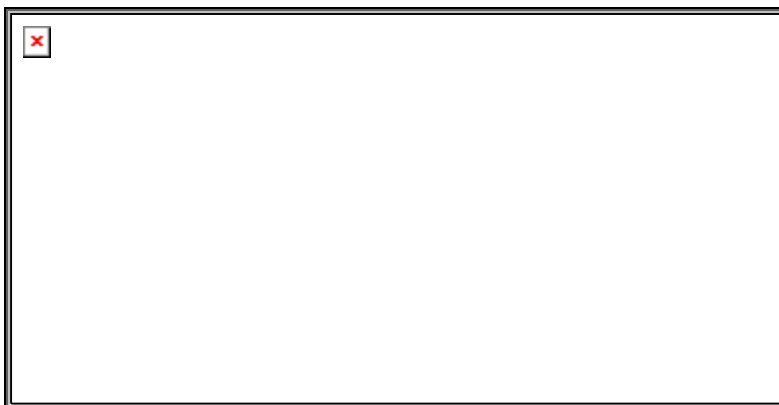


Fig. II-86: Device Registration page

Logout

This option is used to close the session between the user PC and QuadroCS and to leave the Web Management or to enter the management with another login. By selecting the button **Logout**, the startup page will be displayed and the user needs to login again.

Appendix: System Default Values

Issue	System Default Value
Admin Settings	Login name – admin Password – 19
Quadro Hostname	quadro
LAN IP Address	172.30.0.1 Subnet Mask - 255.255.0.0
DHCP Server	Enabled, IP Range - 172.30.0.100 -172.30.0.254 WINS - 0.0.0.0
Regional Settings and Preferences	Your locale - US, Time Zone - US/Central, Theme - Dynamo.
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
Event Settings	"Display notification" for all except Login event. Login event has "Do nothing" action assigned.
Time/Date Settings	NTP Server and Client – enabled, Predefined NTP Server - ntp1.epygi.com, Polling interval – 6.
Mail Settings	Disabled
Language Pack	Default - English Custom Language Pack - none
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Moderators (all accessible pages for moderators), Participants (all accessible pages for moderators in a read only mode), Local Administrators (all accessible pages for localadmin).
Conference Management	00 attendant and 11 default Conference exists.
Conference Settings – General	Subject - Demo Conference, Description - Default conference with empty passwords, Moderator and Participant passwords – none, Max Duration – undefined, Percentage of System Memory - 2%, Routing Mode – disabled, Leave Active – disabled.
Conference Settings – SIP	SIP User Name – automatically generated, SIP Registration server - sip.epygi.com, SIP server port – 5060, SIP Registration – enabled.
Conference Settings – SIP Advanced	Authentication User Name – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined.
Conference Settings – Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, G723, iLBC Out of Band DTMF Transport – enabled.
Conference Settings – Recoding	Disabled.
Conference Settings – Customization	Play First in Conference message – enabled, Welcome Message and Hold Music – default, Info File – undefined.

Issue	System Default Value
Conference Settings – Participants	No participants in the table. New Participant Allowed to Join – enabled, Max New Participant Count – 10, New Participant Type – speaker, New Participant Confirmation Type – none, New Participant Can Activate The Conference – enabled, New Participant Indication – enabled, Handset Added Participant Configuration: Participant Type – speaker, Confirmation Type – none, Participant Indication – enabled, Allowed Duplicated Participants – enabled.
Conference Settings – Schedule	No entries in the table. Allow Participants to Join before Conference Activation – disabled, Send Mail before Conference Activation – disabled, Send Mail on Behalf of – undefined.
Conference Settings – Reservation	No entries in the table.
Conference Settings – AGC	Disabled.
Attendant 00 Settings – General	Description – Attendant, Percentage of System Memory - 2%.
Attendant 00 Settings – Attendant Scenario	Scenario – default, Attendant Welcome Message – default, ZeroOut Service – disabled.
Attendant 00 Settings – SIP	SIP User Name – automatically generated, SIP Registration server - sip.epygi.com, SIP server port – 5060, SIP Registration – enabled.
Attendant 00 Settings – SIP Advanced	Same as for a default conference.
Attendant 00 Settings – Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, G723, iLBC Out of Band DTMF Transport – enabled.
SIP Settings	UDP and TCP Port – 5060, Session Timer – disabled, DNS Server for SIP – default, SIP timers – RFC 3261.
RTP Settings	Properties for all Codecs except G723 and iLBC : Packetization -20ms Silence Suppression -yes G723 and iLBC properties: Packetization - 30ms Silence Suppression – yes G276 Standard - ITU-T specification RTP/RTCP port range - 6000-6059 Telephone Event Draft Support - enabled 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.
Statistics	Enabled, 100 entries for all type of calls.
Call Routing	No entries.

Issue	System Default Value
Recording Common Settings	Memory Allocation - Embedded Memory Storage
Firewall	Enabled, Medium level, Ping Stealth – enabled, Fool Portscanner – disabled.
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
Dynamic DNS	Disabled.

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, YOU MAY NOT USE THE HARDWARE OR SOFTWARE.

- 1. 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 use the Licensed Materials only in connection with your operation of your Quadro. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.
- 2. 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 the transfer of the Licensed Materials is subject to the terms of this Agreement.
- 3. 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.
- 4. 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 under penalty of law.
- 5. Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro-4x 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.
- 6. 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.
- 7. 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, TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES AND 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.
- 8. 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 OF 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 EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.

The foregoing limitation, exclusion and disclaimers apply to the maximum extent permitted by applicable law.
- 9. 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.

10. **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.
11. **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.
12. **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.
13. **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.
14. **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.