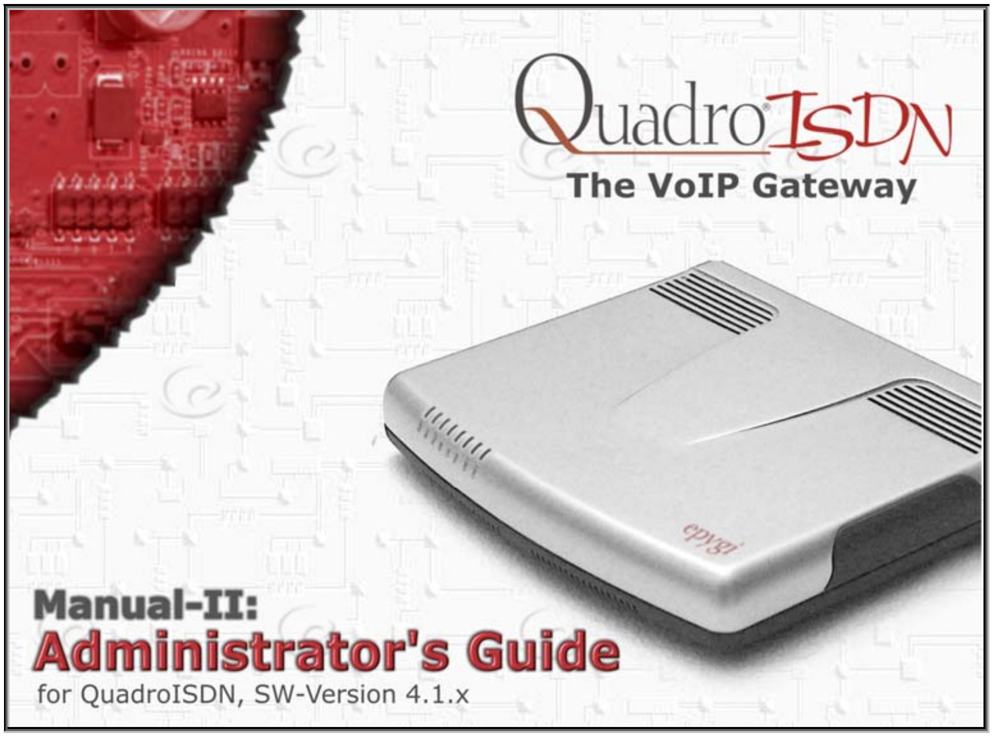


Edition 1, SW Release 4.1.3 and higher, December 2006

Table of Contents

Manual I: see Installation Guide

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

Manual II: Administrator's Guide

About this Administrator's Guide....4

Quadro's Graphical Interface 5

Administrator's Main Page 5

Recurrent Buttons 6

Recurrent Functional Buttons.... 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....11
Network Status 11
Lines Status....13
Memory Status....13
Hardware Status....14
SIP Registration Status....14
IP Routing Configuration....14
Configuration Management 16
Automatic Firmware Update 18
Legible Configuration Management 18
Events....20
Time/Date Settings 23
Mail Settings 23
Firmware Update 24
Networking Tools....25
SNMP Settings....26
Diagnostics 27
Automatic Provisioning 27
Upload Language Pack....27
User Rights Management 28

Users Menu 30

Extensions Management 30
User Extension Settings....32
Attendant Extension Settings 33
Extension Codecs....36
Authorized Phones Database 37
Call Back Services....38
Upload Universal Extension Recordings....39

Telephony Menu 40

Call Statistics 40
RTP Statistics 42
SIP Settings....42
RTP Settings 44
NAT Traversal Settings 45
ISDN Settings 47
PSTN Lines Sharing 52
Gain Control....52
Call Routing 52
Best Matching Algorithm 59
VoIP Carrier Wizard....62
RADIUS Client Settings....63
Voice Mail Common Settings 65
Dial Plan Settings....65
Hold Music Settings....65

Internet Uplink Menu 66

PPP/ PPTP Settings....66

Advanced PPP Settings 66
VPN Configuration 67
Firewall and NAT 75
Advanced Firewall Settings 75
Filtering Rules 75
Service Pool 77
IP Pool 78
LAN Services Menu 80
DNS Settings 80
DNS Server Settings 80
DHCP Settings for the LAN Interface 81
Registration Form 82
Logout 82
Extension User's Menus 83
Main Page 83
Voice Mail 83
Voice Mailbox 84
Voice Mail Settings 85
Group List 88
Your Extension 90
Call Statistics 90
Account Settings 91
Supplementary Services 92
Caller ID Based Services 92
Incoming Call Blocking 93
Outgoing Call Blocking 94
Call Hunting 94
Unconditional Call Forwarding 95
Logout 95
Quadro’s Feature Codes 96
Establishing a call 96
Voice Mail Services 96
Voice Mailbox 96
Review System Messages 97
Services for Incoming Calls 97
Quadro’s Auto Attendant Services 98
Call Codes Available in Auto Attendant 99
Appendix: System Default Values 101
Administrator Settings 101
Extension Settings 104
Appendix: Software License Agreement 105

About this Administrator's Guide

The Quadro Manual is divided into three parts:

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

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

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

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

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

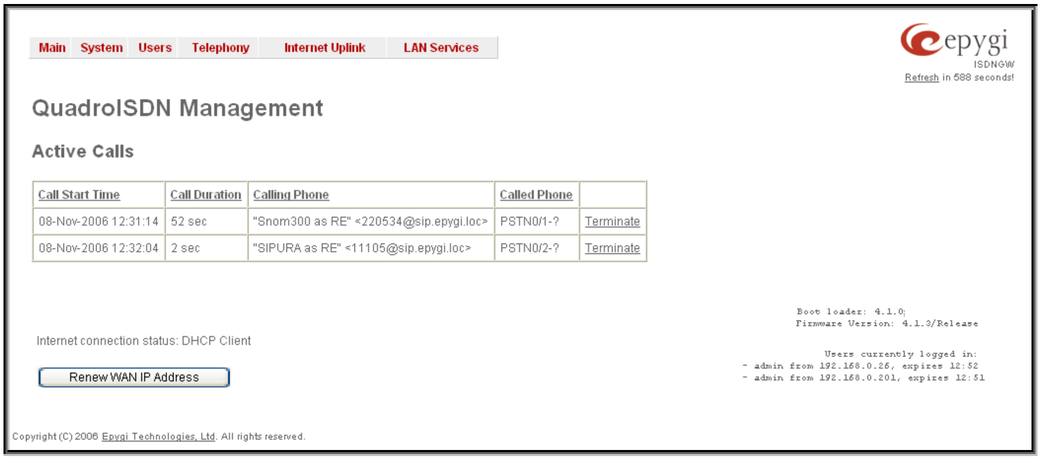
Appendix: System Default Values lists all factory defaults.

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

Quadro's Graphical Interface

Administrator's Main Page

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



Refresh in 588 seconds!

QuadroISDN Management

Active Calls

Call Start Time	Call Duration	Calling Phone	Called Phone	
08-Nov-2006 12:31:14	52 sec	"Snom300 as RE" <220534@sip.epygi.loc>	PSTN0/1-?	Terminate
08-Nov-2006 12:32:04	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	PSTN0/2-?	Terminate

Internet connection status: DHCP Client

```
Boot loader: 4.1.0;
Firmware Version: 4.1.3/Release

Users currently logged in:
- admin from 192.168.0.26, expires 12:52
- admin from 192.168.0.201, expires 12:51
```

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-1: QuadroISDN Management

System Menu

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

Telephony Menu

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

Internet Uplink Menu

- PPP/ PPTP Settings
- VPN Configuration
- Firewall and NAT
- Filtering Rules

Users Menu

- Extensions Management
- Authorized Phones Database

LAN Services Menu

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

Registration Form
(in menu tree only)

Logout

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

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

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

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

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

Recurrent Buttons

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

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

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

Recurrent Functional Buttons

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

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

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

Entering a SIP Addresses correctly

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

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

“display name” <username@ipaddress:port>
“display name” <username@ipaddress>
username@ipaddress:port
username@ipaddress
username

For your convenience, the following combinations can be used:

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

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

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

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

Administrator’s Menus

System Menu

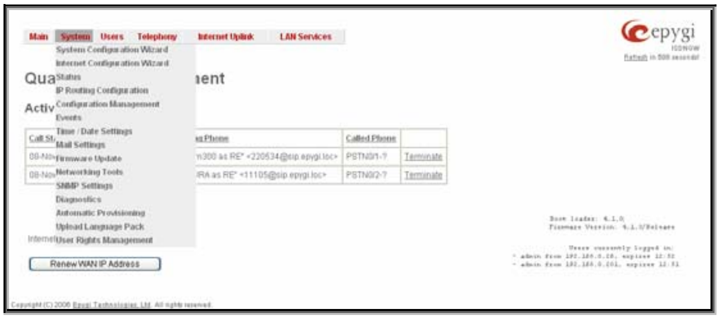


Fig. II-1: System Menu in Dynamo theme

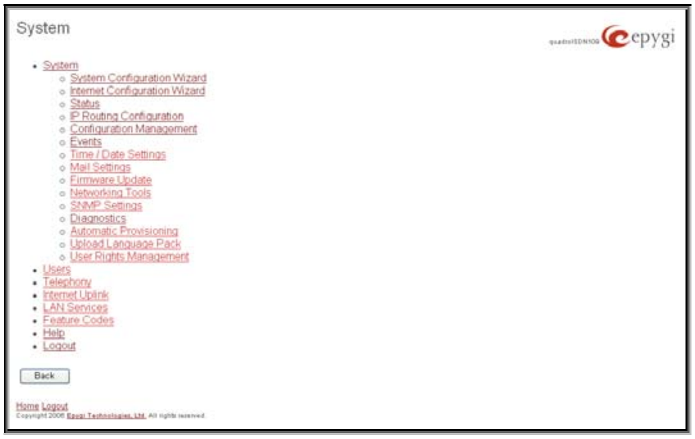


Fig. II-2: System Menu in Plain theme

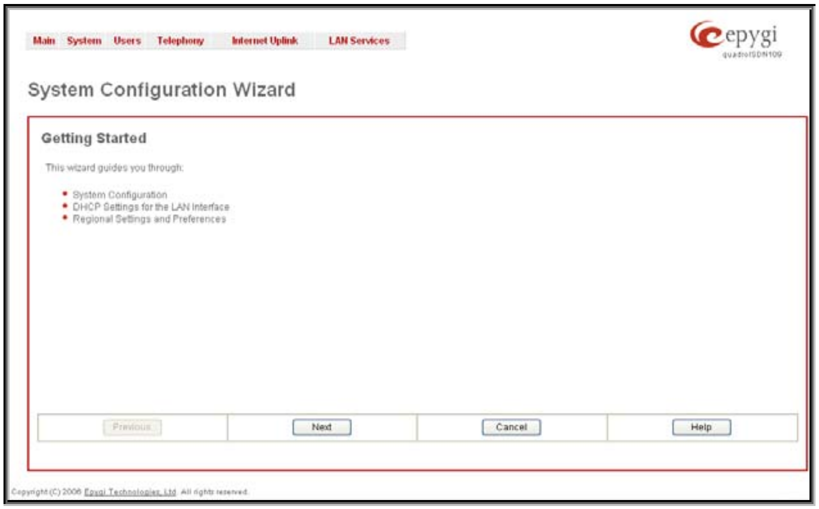
System Configuration Wizard

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

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

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.



System Configuration Wizard

Getting Started

This wizard guides you through:

- System Configuration
- DHCP Settings for the LAN interface
- Regional Settings and Preferences

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-3: 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.

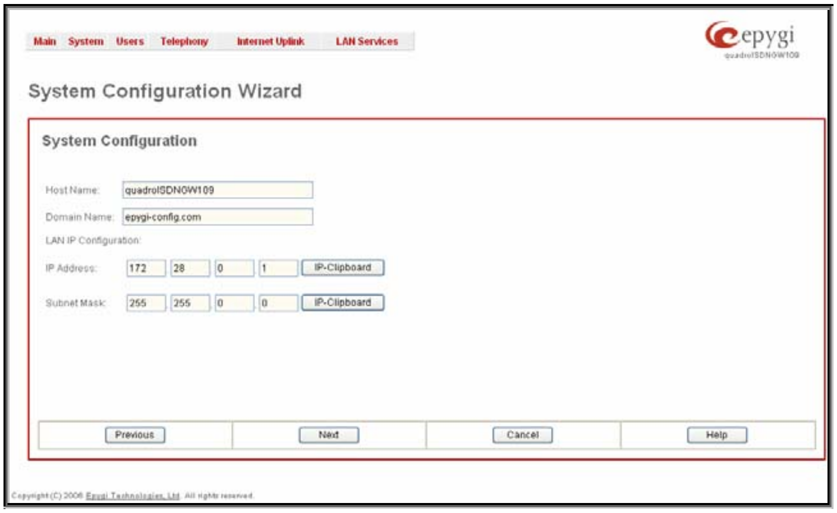
The **System Configuration** page offers the following input options:

Host Name requires a host name for the Quadro device.

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

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

Subnet Mask requires the Quadro hosts’ Subnet Mask.


Main System Users Telephony Internet Uplink LAN Services
epygi
quadroISDN0W109
Previous
Next
Cancel
Help
IP-Clipboard
IP-Clipboard
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

System Configuration Wizard

System Configuration

Host Name: quadroISDN0W109

Domain Name: epygi-config.com

LAN IP Configuration:

IP Address: 172 28 0 1

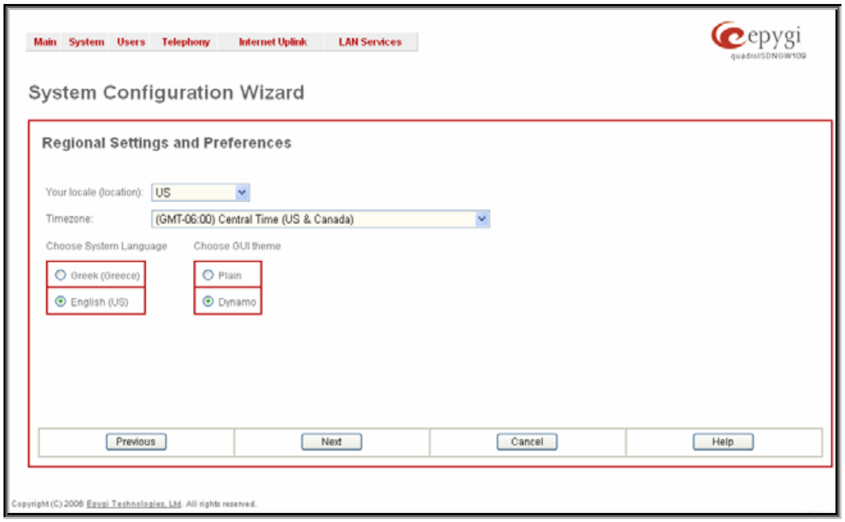
Subnet Mask: 255 255 0 0

Fig. II-4: 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.


Main System Users Telephony Internet Uplink LAN Services
epygi
quadroISDN0W109
Previous
Next
Cancel
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

System Configuration Wizard

Regional Settings and Preferences

Your locale (location): US

Timezone: (GMT-06:00) Central Time (US & Canada)

Choose System Language

○ Greek (Greece)

● English (US)

Choose GUI theme

○ Plain

● Dynamo

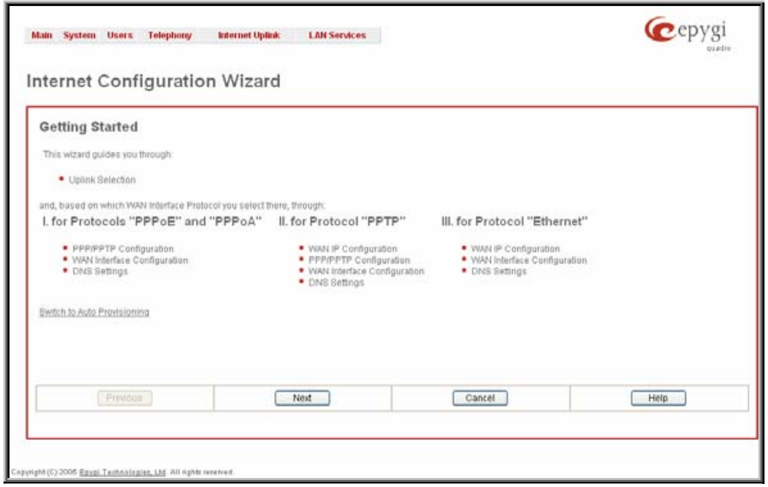
Fig. II-5: System Configuration Wizard - Regional Settings page

Internet Configuration Wizard

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

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.


Main System Users Telephony Internet Uplink LAN Services
epygi
quadro
Switch to Auto Provisioning
Previous
Next
Cancel
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Internet Configuration Wizard

Getting Started

This wizard guides you through:

- Uplink Selection

and, based on which WAN Interface Protocol you select there, through:

I. for Protocols "PPPoE" and "PPPoA"

- PPP/PPTP Configuration
- WAN Interface Configuration
- DNS Settings

II. for Protocol "PPTP"

- WAN IP Configuration
- PPP/PPTP Configuration
- WAN Interface Configuration
- DNS Settings

III. for Protocol "Ethernet"

- WAN IP Configuration
- WAN Interface Configuration
- DNS Settings

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

For WAN Interface protocol **PPTP**:

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

For WAN Interface protocol **Ethernet**:

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

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

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

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

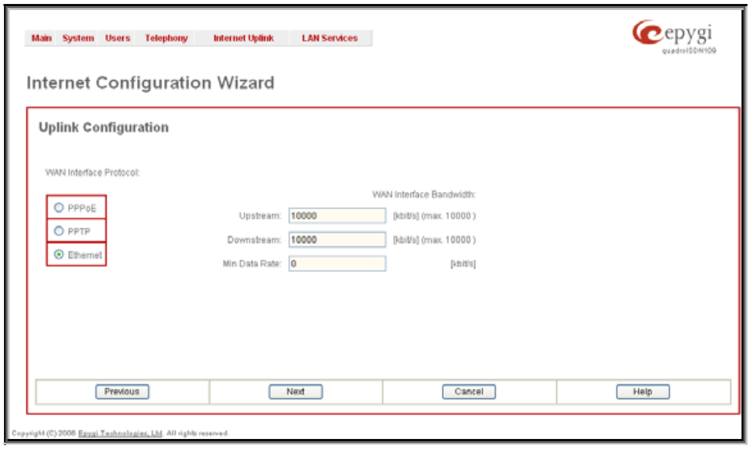
The **Uplink Configuration** page offers the following components:

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

PPPoE - turns on the PPP over an Ethernet connection.

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

Ethernet - turns on the Ethernet connection.



Internet Configuration Wizard

Uplink Configuration

WAN Interface Protocol:

○ PPPoE
○ PPTP
● Ethernet

WAN Interface Bandwidth:

Upstream: 10000 [kbit/s] (max. 10000)

Downstream: 10000 [kbit/s] (max. 10000)

Min Data Rate: 0 [kbit/s]

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

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

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

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

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

Required Bandwidth for Standard Packets:

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

Required Bandwidth for Encrypted Packets when a VPN is used:

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

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

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

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

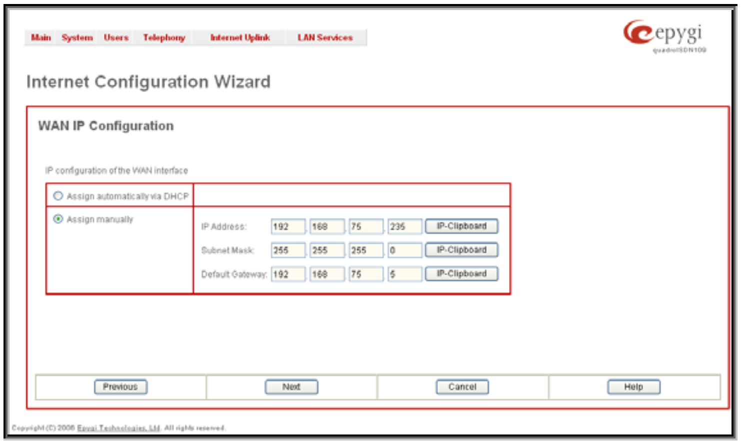
Please Note: DHCP referred to here is the one that runs on the provider’s side and not the Quadro’s personal DHCP server.

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

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

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

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



Internet Configuration Wizard

WAN IP Configuration

IP configuration of the WAN interface

○ Assign automatically via DHCP

● Assign manually

IP Address: 192 . 168 . 75 . 235

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 75 . 5

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

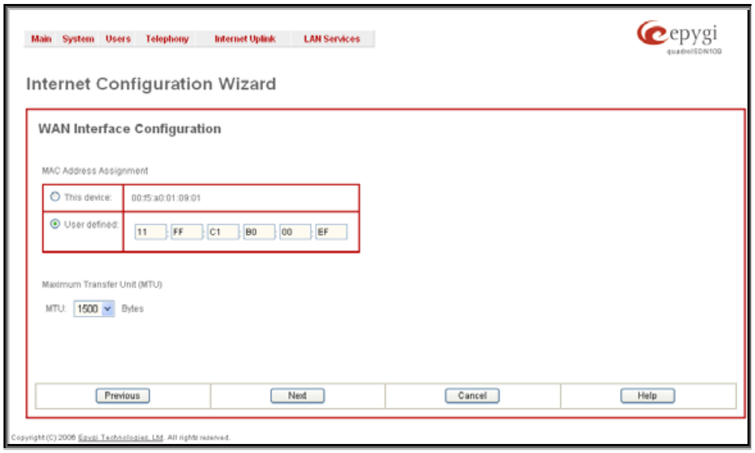
Fig. II-8: Internet Configuration Wizard - WAN IP Configuration page

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.



Internet Configuration Wizard

WAN Interface Configuration

MAC Address Assignment

○ This device: 00:f5:a0:01:09:01

● User defined: 11 : FF : C1 : B0 : 00 : EF

Maximum Transfer Unit (MTU)

MTU: 1500 Bytes

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

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

Status

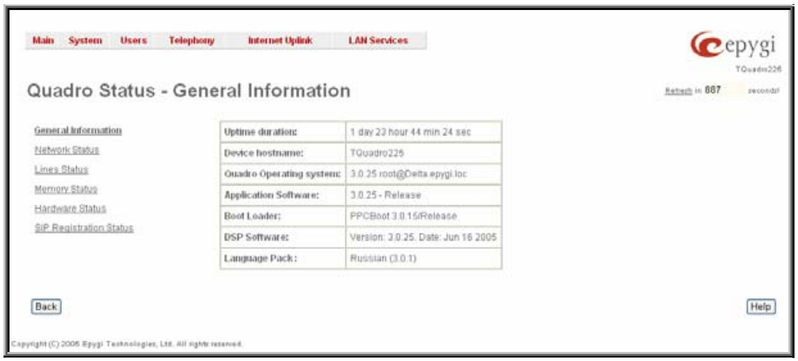
The system status window displays non-editable tables providing extensive system status information about Quadro: General Information, Network Status, Lines Status, Memory Status, Hardware Status and SIP Registration Status. The links on this page lead to device Transfer Statistics, user mailboxes and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

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

General Information

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

- **Uptime duration -** Period Quadro is on since last reboot.
- **Device hostname -** Quadro device host name.
- **Quadro Operating System -** Quadro operating system version.
- **Application Software -** Software and file system versions of the Quadro.
- **Boot Loader -** Quadro boot loader version.
- **DSP Software -** Quadro DSP software version and the date of build.
- **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.



Quadro Status - General Information

Uptime duration:	1 day 23 hour 44 min 24 sec
Device hostname:	TQuadro225
Quadro Operating system:	3.0.25 root@Delta.epygi.loc
Application Software:	3.0.25 - Release
Boot Loader:	PPCBoot 3.0.15/Release
DSP Software:	Version: 3.0.25. Date: Jun 16 2005
Language Pack:	Russian (3.0.1)

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

Network Status

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

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

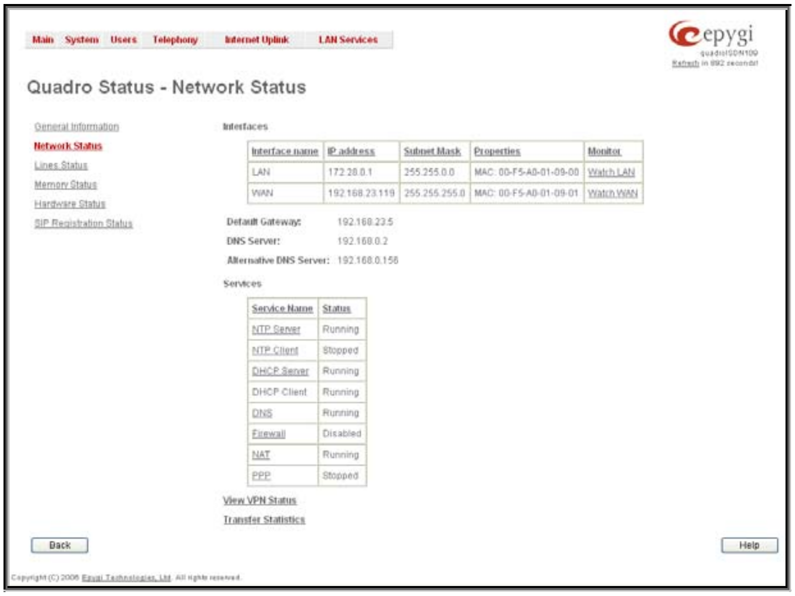
IP Address lists the IP addresses corresponding to each network interface.

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

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

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

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



Quadro Status - Network Status

Interfaces

Interface name	IP address	Subnet Mask	Properties	Monitor
LAN	172.28.0.1	255.255.0.0	MAC: 00-F5-A0-01-09-00	Watch LAN
WAN	192.168.23.119	255.255.255.0	MAC: 00-F5-A0-01-09-01	Watch WAN

Default Gateway: 192.168.23.5

DNS Server: 192.168.0.2

Alternative DNS Server: 192.168.0.156

Services

Service Name	Status
NTP Server	Running
NTP Client	Stopped
DHCP Server	Running
DHCP Client	Running
DNS	Running
Firewall	Disabled
NAT	Running
PPP	Stopped

Fig. II-11: Quadro Status Network Status page

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

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

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

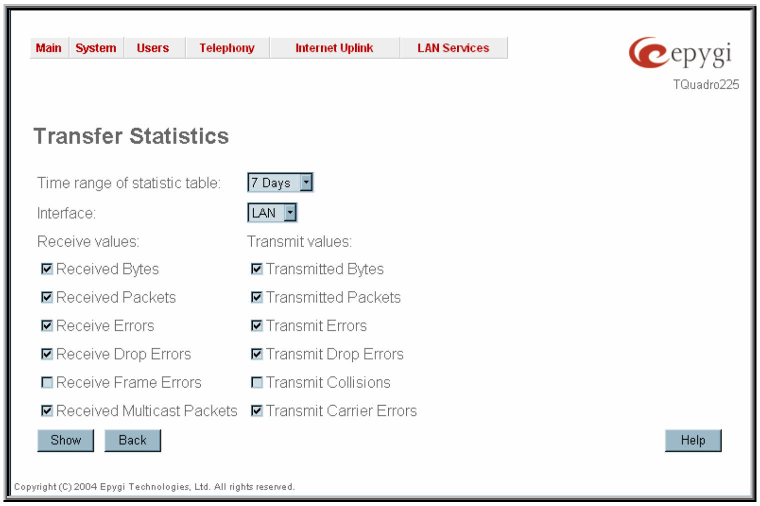
The **View VPN Status** link refers to the VPN Configuration page where all VPN (IPSec, PPTP and L2TP) connections can be viewed and edited.

The **Transfer Statistics** links to the same named page that displays 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



Transfer Statistics

Time range of statistic table: 7 Days

Interface: LAN

Receive values:	Transmit values:
☑ Received Bytes	☑ Transmitted Bytes
☑ Received Packets	☑ Transmitted Packets
☑ Receive Errors	☑ Transmit Errors
☑ Receive Drop Errors	☑ Transmit Drop Errors
□ Receive Frame Errors	□ Transmit Collisions
☑ Received Multicast Packets	☑ Transmit Carrier Errors

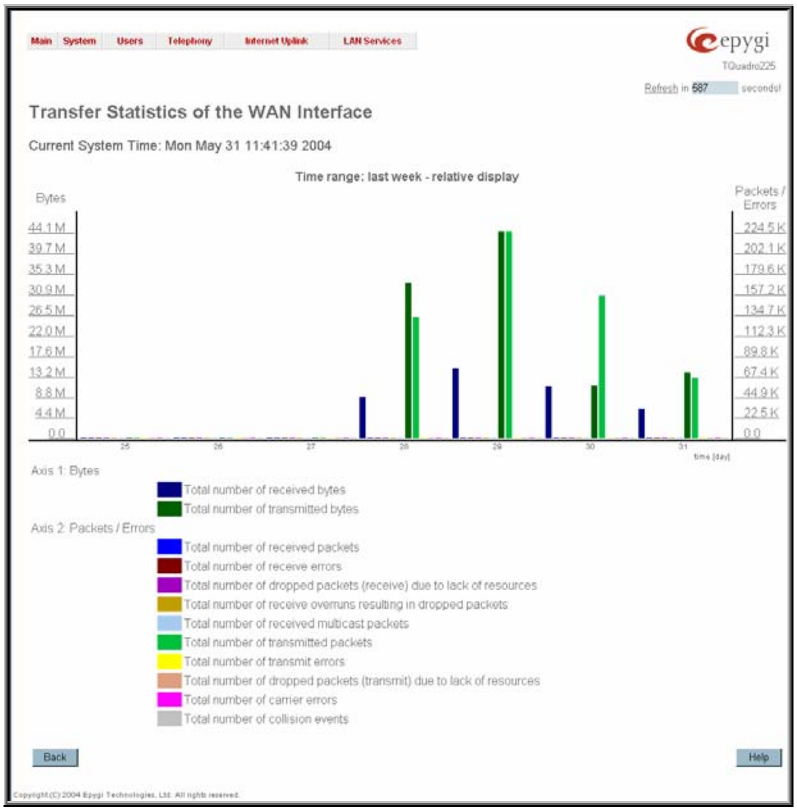
Fig. II-12: Transfer Statistics page

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.


Main
System
Users
Telephony
Internet Uplink
LAN Services
epygi
TQuadro225
Refresh in 587 seconds!
Time range: last week - relative display
Bytes
44.1 M
39.7 M
35.3 M
30.9 M
26.5 M
22.0 M
17.6 M
13.2 M
8.8 M
4.4 M
0.0
Packets / Errors
224.5 K
202.1 K
179.6 K
157.2 K
134.7 K
112.3 K
89.8 K
67.4 K
44.9 K
22.5 K
0.0
25
26
27
28
29
30
31
time [day]
Axis 1: Bytes
Total number of received bytes
Total number of transmitted bytes
Axis 2: Packets / Errors
Total number of received packets
Total number of receive errors
Total number of dropped packets (receive) due to lack of resources
Total number of receive overruns resulting in dropped packets
Total number of received multicast packets
Total number of transmitted packets
Total number of transmit errors
Total number of dropped packets (transmit) due to lack of resources
Total number of carrier errors
Total number of collision events
Back
Help
Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Transfer Statistics of the WAN Interface

Current System Time: Mon May 31 11:41:39 2004

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).

Lines Status

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

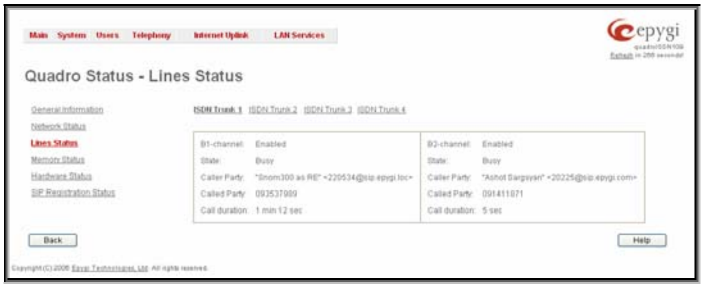
The **Line Status** for **ISDN Trunk** displays the state of the B1 and B2 channels and the information about the active calls on them. This page includes a group of static and dynamic parameters. Static parameters are always displayed. Dynamic parameters appear only when an event takes place on the channel.

Static Parameters:

- **B channel** - the state of the channel (enabled or disabled).
- **State** - the current state of the channel (free, busy or N/A).

Dynamic Parameters:

- **Caller Party** - this parameter appears when a call is received and indicates the caller address.
- **Called Party** - this parameter appears when a call is placed and indicates the destination address.
- **Call Duration** - current call duration (in seconds).



Quadro Status - Lines Status

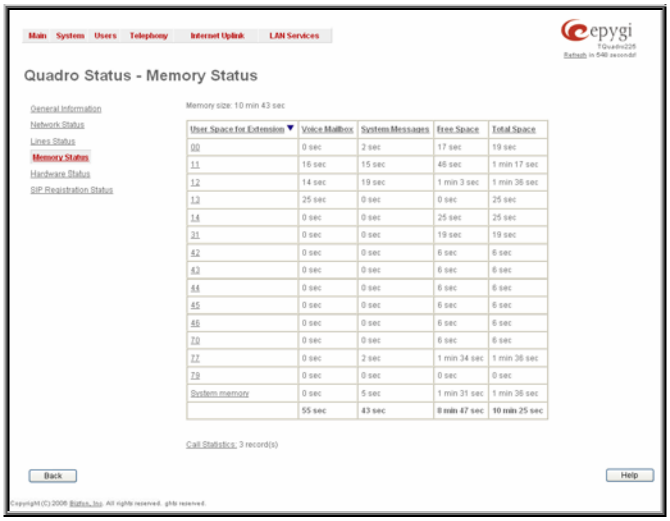
B1-channel: Enabled
State: Busy
Caller Party: "Snom300 as RE" <220534@sip.epygi.loc>
Called Party: 093537989
Call duration: 1 min 12 sec

B2-channel: Enabled
State: Busy
Caller Party: "Ashot Sargsyan" <20225@sip.epygi.com>
Called Party: 091411071
Call duration: 5 sec

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-14: Lines Status page

Memory Status



Quadro Status - Memory Status

Memory size: 10 min 43 sec

User Space for Extension ▼	Voice Mailbox	System Messages	Free Space	Total Space
00	0 sec	2 sec	17 sec	19 sec
11	16 sec	15 sec	46 sec	1 min 17 sec
12	14 sec	19 sec	1 min 3 sec	1 min 36 sec
13	25 sec	0 sec	0 sec	25 sec
14	0 sec	0 sec	25 sec	25 sec
31	0 sec	0 sec	19 sec	19 sec
42	0 sec	0 sec	6 sec	6 sec
43	0 sec	0 sec	6 sec	6 sec
44	0 sec	0 sec	6 sec	6 sec
45	0 sec	0 sec	6 sec	6 sec
46	0 sec	0 sec	6 sec	6 sec
70	0 sec	0 sec	6 sec	6 sec
77	0 sec	2 sec	1 min 34 sec	1 min 36 sec
79	0 sec	0 sec	0 sec	0 sec
System memory	0 sec	5 sec	1 min 31 sec	1 min 36 sec
	55 sec	**43 sec**	**8 min 47 sec**	**10 min 25 sec**

Call Statistics: 3 record(s)

Copyright (C) 2006 Bigfon, Inc. All rights reserved. ghb reserved.

Fig. II-15: Memory Status page

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

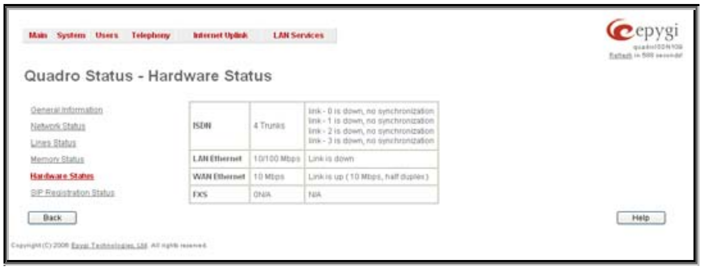
Memory Size shows total memory space (counted in minutes/seconds) available on the Quadro and assigned to all extensions.

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

The **System Memory** row indicates the space occupied by the universal extension recordings. Link refers to the Upload Universal Extension Recordings page where universal extension system messages may be uploaded.

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

Hardware Status



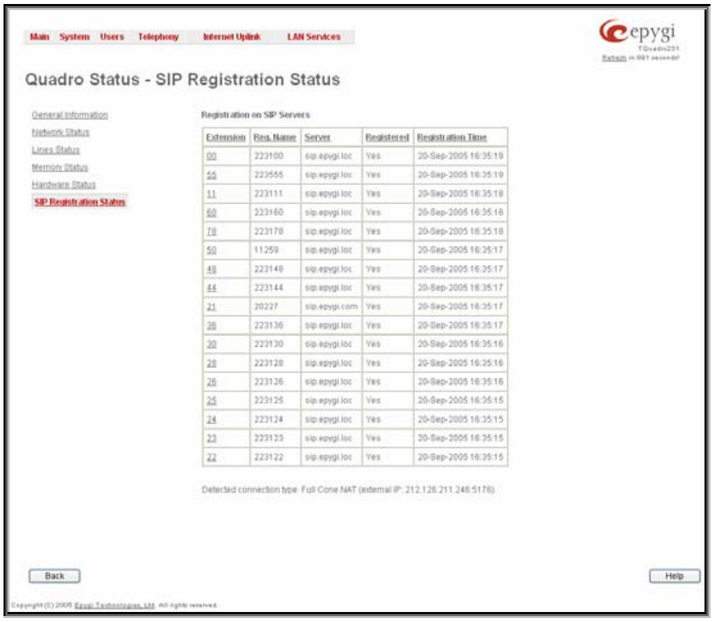
Quadro Status - Hardware Status

ISDN	4 Trunks	link - 0 is down, no synchronization link - 1 is down, no synchronization link - 2 is down, no synchronization link - 3 is down, no synchronization
LAN Ethernet	10/100 Mbps	Link is down
WAN Ethernet	10 Mbps	Link is up (10 Mbps, half duplex)
FXS	0N/A	N/A

Fig. II-16: Hardware Status page

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

SIP Registration Status



Quadro Status - SIP Registration Status

Registration on SIP Servers

Extension	Reg. Name	Server	Registered	Registration Time
00	223100	sip.epygi.loc	Yes	20-Sep-2005 16:35:19
55	223555	sip.epygi.loc	Yes	20-Sep-2005 16:35:19
11	223111	sip.epygi.loc	Yes	20-Sep-2005 16:35:18
60	223160	sip.epygi.loc	Yes	20-Sep-2005 16:35:18
78	223178	sip.epygi.loc	Yes	20-Sep-2005 16:35:18
50	11259	sip.epygi.loc	Yes	20-Sep-2005 16:35:17
48	223148	sip.epygi.loc	Yes	20-Sep-2005 16:35:17
44	223144	sip.epygi.loc	Yes	20-Sep-2005 16:35:17
21	20227	sip.epygi.com	Yes	20-Sep-2005 16:35:17
36	223136	sip.epygi.loc	Yes	20-Sep-2005 16:35:17
30	223130	sip.epygi.loc	Yes	20-Sep-2005 16:35:16
28	223128	sip.epygi.loc	Yes	20-Sep-2005 16:35:16
26	223126	sip.epygi.loc	Yes	20-Sep-2005 16:35:16
25	223125	sip.epygi.loc	Yes	20-Sep-2005 16:35:15
24	223124	sip.epygi.loc	Yes	20-Sep-2005 16:35:15
23	223123	sip.epygi.loc	Yes	20-Sep-2005 16:35:15
22	223122	sip.epygi.loc	Yes	20-Sep-2005 16:35:15

Detected connection type: Full Cone NAT (external IP: 212.126.211.246:5176).

Fig. II-17: SIP Registration Status page

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

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

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

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

IP Routing Configuration

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

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

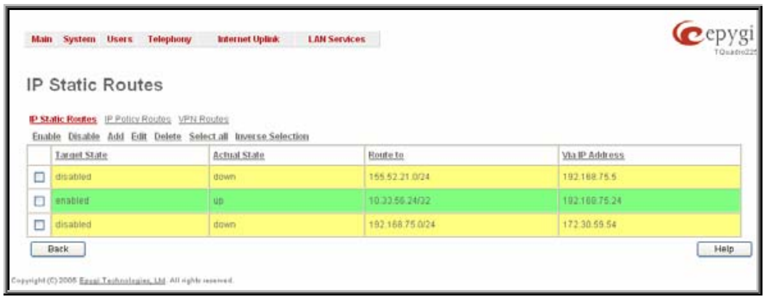
The **IP Routing Configuration** page is used to make IP Static, IP Policy and VPN routes for IP packets routing. This page consists of three tables. Entries in the tables are color coded according to the state of the route. For example, yellow indicates disabled routes, green indicates successful routes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

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

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

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

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



IP Static Routes

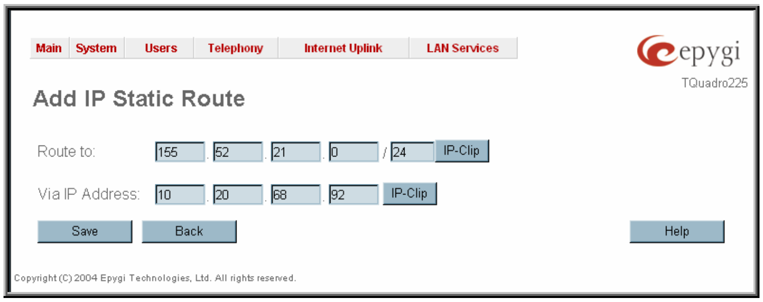
IP Static Routes IP Policy Routes VPN Routes

Enable Disable Add Edit Delete Select all Inverse Selection

	Target State	Actual State	Route to	Via IP Address
□	disabled	down	155.52.21.0/24	192.168.75.5
□	enabled	up	10.33.56.24/32	192.168.75.24
□	disabled	down	192.168.75.0/24	172.30.59.54

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-18: IP Static Routing table



Add IP Static Route

Route to: 155 . 52 . 21 . 0 / 24 IP-Clip

Via IP Address: 10 . 20 . 68 . 92 IP-Clip

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-19: Add IP Static Routing page

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

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

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

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

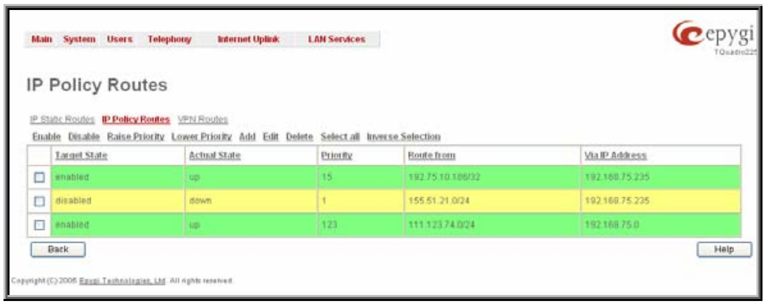
IP Policy Routes allow IP packets forwarding to the specified router depending on the source IP address as well as defining the priority for the current routing rule.

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

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

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

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



IP Policy Routes

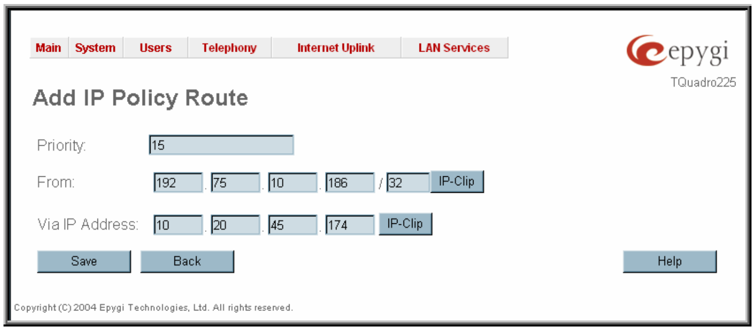
IP Static Routes IP Policy Routes VPN Routes

Enable Disable Raise Priority Lower Priority Add Edit Delete Select all Inverse Selection

	Target State	Actual State	Priority	Route from	Via IP Address
□	enabled	up	15	192.75.10.186/32	192.168.75.235
□	disabled	down	1	155.51.21.0/24	192.168.75.235
□	enabled	up	123	111.123.74.0/24	192.168.75.0

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-20: IP Policy Routing table



Add IP Policy Route

Priority: 15

From: 192 . 75 . 10 . 186 / 32 IP-Clip

Via IP Address: 10 . 20 . 45 . 174 IP-Clip

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-21: Add IP Policy Route page

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

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

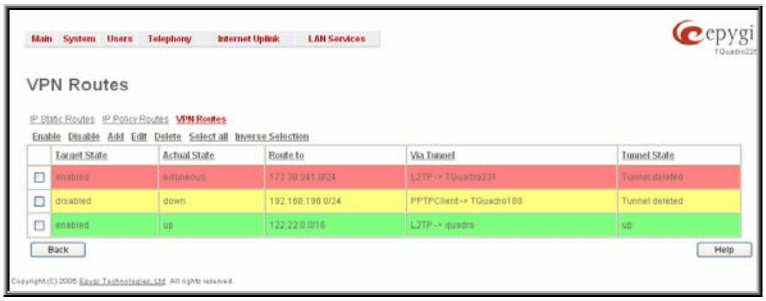
From requires the packet source IP address and subnet mask of the specified destination to match with the rule.

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

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

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

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



VPN Routes

	Target State	Actual State	Route to	Via Tunnel	Tunnel State
□	enabled	erroneous	172.30.241.0/24	L2TP -> TQuadro231	Tunnel deleted
□	disabled	down	192.168.198.0/24	PPTPClient-> TQuadro188	Tunnel deleted
□	enabled	up	122.22.0.0/16	L2TP -> quadro	up

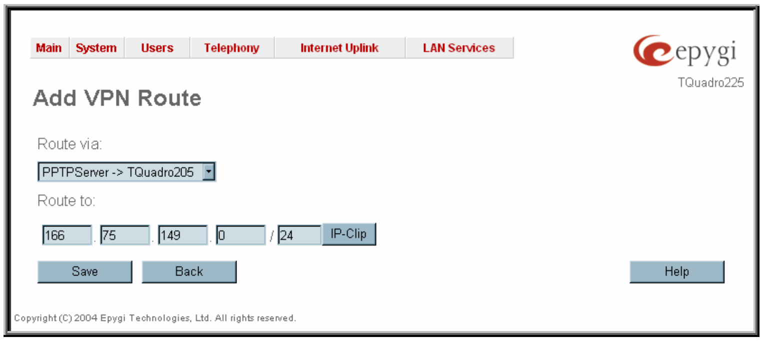
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-22: VPN Routing table

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

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

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



Add VPN Route

Route via: PPTPServer -> TQuadro205

Route to: 166 . 75 . 149 . 0 / 24

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-23: Add VPN Route page

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

To Add an IP Static Route

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

To Add an IP Policy Route

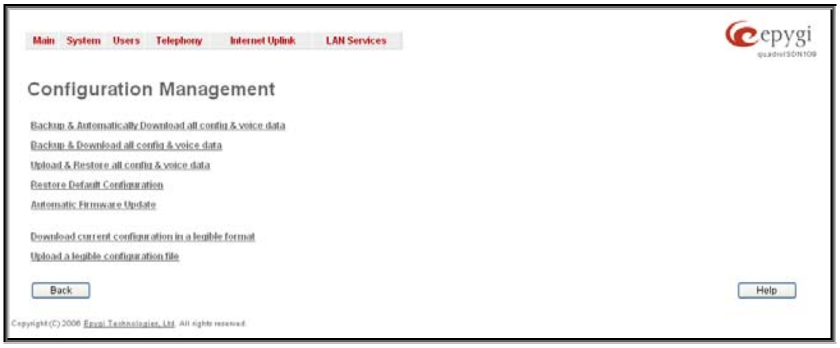
1. Select the **IP Policy Route**s link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Policy Routes** page. The **Add Entry** page will appear in the browser window.
3. Specify the policy routing rule priority in the **Priority** text field.
4. Enter the packet source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

To Add a VPN Route

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

Configuration Management

The **Configuration Management** page offers a group of possibilities addressed to the configuration management on the Quadro. From this page, administrator can manage the system configuration settings and the voice data, download and upload the legible configuration, configure the automatic configuration backup and restore the system defaults settings.



Configuration Management

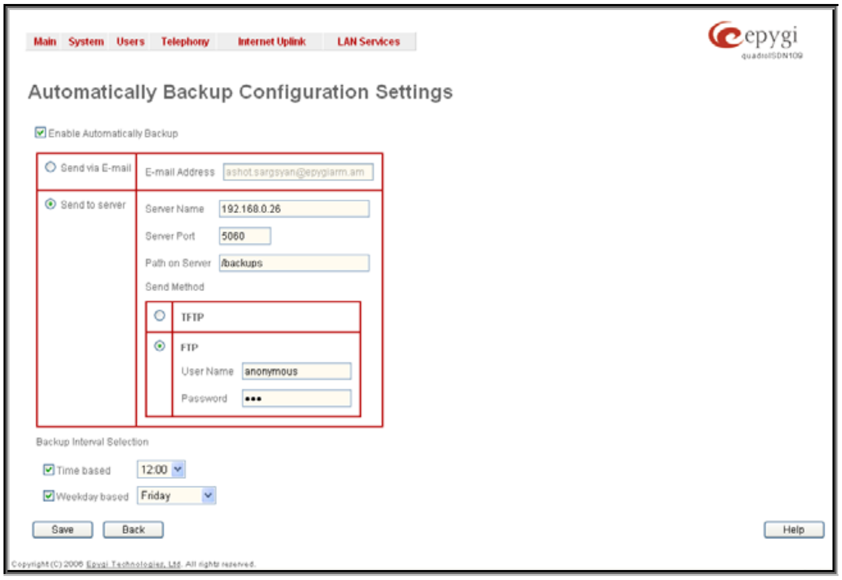
Backup & Automatically Download all config & voice data
Backup & Download all config & voice data
Upload & Restore all config & voice data
Restore Default Configuration
Automatic Firmware Update

Download current configuration in a legible format
Upload a legible configuration file

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-24: Configuration Management page

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



Automatically Backup Configuration Settings

☑ Enable Automatically Backup

○ Send via E-mail — E-mail Address: ashot.sargsyan@epygiarm.am

● Send to server — Server Name: 192.168.0.26

Server Port: 5060

Path on Server: /backups

Send Method

○ TFTP

● FTP — User Name: anonymous; Password: •••

Backup Interval Selection

☑ Time based: 12:00

☑ Weekday based: Friday

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-25: Configuration Management page

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

This page contains the following components:

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

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

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

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

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

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

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

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

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.

Attention: Configuration and voice data cannot be backed up if the size of voice data is too large. In this case, to be able to backup configuration and voice data on the Quadro, please remove some user defined system messages (by restoring the default ones, see Feature Codes), or remove some extensions from the Extensions Management table.

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

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

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

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

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

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

Automatic Firmware Update

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

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

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

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

This page consists of the following components:

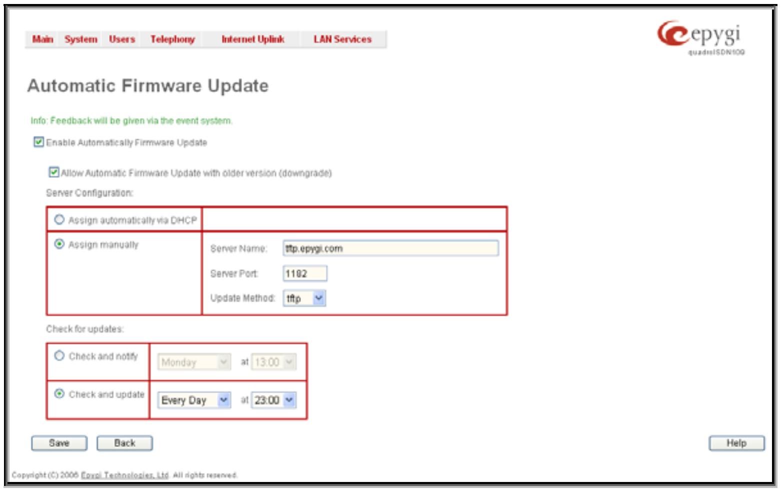
The **Enable Automatically Firmware Update** checkbox selection enables the automatic firmware update service on the Quadro.

The **Allow Automatic Firmware Update with older version (downgrade)** checkbox should be selected if any firmware older than the one currently running on the Quadro can be also installed, thus downgrading the system and forcing it to factory reset.

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

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

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



Automatic Firmware Update

Info: Feedback will be given via the event system.

☑ Enable Automatically Firmware Update

☑ Allow Automatic Firmware Update with older version (downgrade)

Server Configuration:

○ Assign automatically via DHCP

● Assign manually

Server Name: ttp.epygi.com

Server Port: 1182

Update Method: tftp

Check for updates:

○ Check and notify Monday at 13:00

● Check and update Every Day at 23:00

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-26: Upload Configuration page

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

- **Check and notify** – choose this selection if you only wish to be notified about the new available firmware on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the Quadro will check for a new firmware available on the server. The way of notification is configured from the Error! Not a valid result for table. page.
- **Check and update** – choose this selection to check and automatically install the new firmware on the Quadro as it becomes available on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the Quadro will check for a new firmware available on the server, will automatically download and install it on the Quadro.

Legible Configuration Management

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

Attention: It is strongly recommended to consult with the Quadro's Technical Support Center before uploading an edited legible configuration. Incorrect settings here may harm the current configurations.

The detailed instructions on making changes in the legible configuration files are described in the “**Introduction to Legible Configuration**” document which you can find at the Epygi Web support portal.

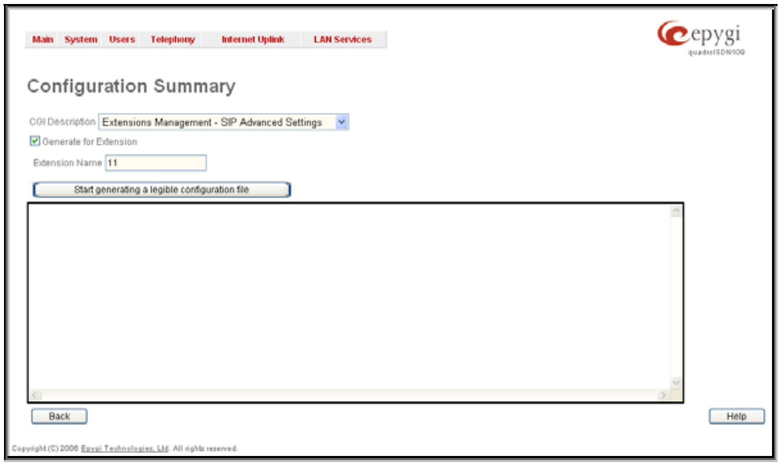
The **Download current configuration in a legible format** link on the **Configuration Management** page leads to the **Configuration Summary** page where a piece of legible configuration can be generated and downloaded or viewed.

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

The **CGI Description** drop down list includes a list of Web management pages for which the legible configuration can be manually managed. For example, selecting “RTP Settings” Web management page will generate a legible configuration file with parameters present on the RTP Settings page.

The **Generate for Extension** checkbox is used to limit the settings in the generated legible configuration file to one specific extension. For example, each of the extensions on the Quadro have own SIP settings or Codecs. To download the settings for a particular extension only, you need to have this checkbox selected. With this selection, the extension number should be defined in the **Extension Name** text field. If this checkbox is not selected or no extension is defined, the legible configuration file will contain the parameter of all available extensions on the Quadro (if the selected parameter applies to the extension and not to the overall system, like RTP settings).

Pressing the **Start generate a legible configuration file** button will start parsing the configuration structure of the device for the defined parameters.


Main
System
Users
Telephony
Internet Uplink
LAN Services
epygi
quadroISDN100
Start generating a legible configuration file
Back
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Configuration Summary

CGI Description: Extensions Management - SIP Advanced Settings

☑ Generate for Extension

Extension Name: 11

Fig. II-27: Configuration Summary – Parameters page

The progress will be displayed in the area below.

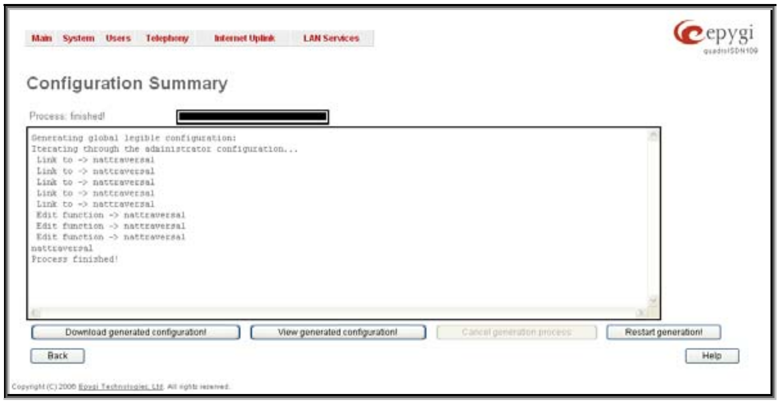
The **Cancel generation process** button appears when the configuration generation procedure starts and it is used to stop it.

The **Download generated configuration** button becomes available when the legible configuration generation is finished. It is used to download the generated file to the PC in a plain text format. Necessary changes can be made in the downloaded configuration file and then uploaded back to the system.

Attention: Make sure the changes you have done in the downloaded legible configuration file are valid and will not corrupt the system when being uploaded back to device.

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

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


Main
System
Users
Telephony
Internet Uplink
LAN Services
epygi
quadroISDN100
Download generated configuration!
View generated configuration!
Cancel generation process
Restart generation!
Back
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Configuration Summary

Process: finished!

```
Generating global legible configuration:
Iterating through the administrator configuration...
 Link to -> nattraversal
 Link to -> nattraversal
 Link to -> nattraversal
 Link to -> nattraversal
 Link to -> nattraversal
 Edit function -> nattraversal
 Edit function -> nattraversal
 Edit function -> nattraversal
nattraversal
Process finished!
```

Fig. II-28: Configuration Summary Preview page

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

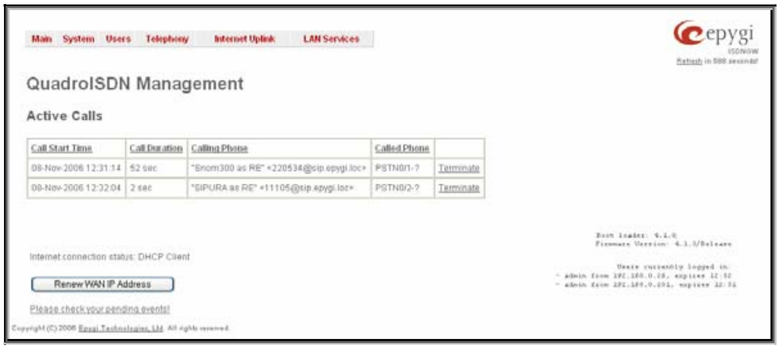
Attention: Uploading the legible configuration file will not work if the QuardoISDN is running in the slave mode, i.e. if it is sharing its ISDN lines to some Quadro IP PBX (see PSTN Lines Sharing chapter).

Events

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

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

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



QuadroISDN Management

Active Calls

Call Start Time	Call Duration	Calling Phone	Called Phone	
08-Nov-2006 12:31:14	52 sec	"Snom300 as RE" <220534@sip.epygi.loc>	PSTN0/1-?	Terminate
08-Nov-2006 12:32:04	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	PSTN0/2-?	Terminate

Internet connection status: DHCP Client

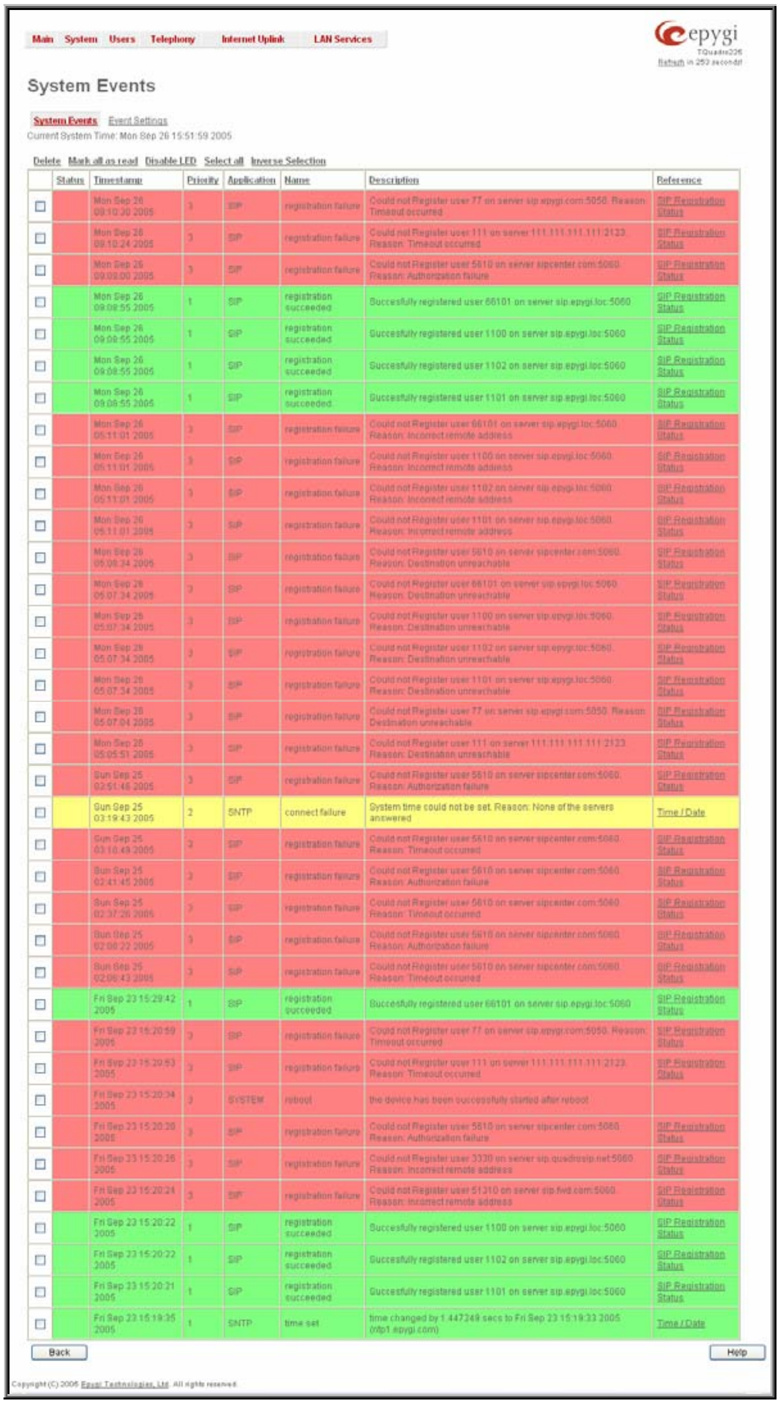
Boot loader: 4.1.0
Firmware Version: 4.1.3/Release

Users currently logged in:
- admin from 192.168.0.28, expires 12:32
- admin from 192.168.0.201, expires 12:51

Please check your pending events!

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-29: Event Warning on the Main Menu page



System Events

System Events Event Settings

Current System Time: Mon Sep 26 15:51:59 2005

Delete Mark all as read Disable LED Select all Inverse Selection

	Status	Timestamp	Priority	Application	Name	Description	Reference
□		Mon Sep 26 09:10:30 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epygi.com:5050. Reason: Timeout occurred	SIP Registration Status
□		Mon Sep 26 09:10:24 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Timeout occurred	SIP Registration Status
□		Mon Sep 26 09:09:00 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Authorization failure	SIP Registration Status
□		Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Succesfully registered user 66101 on server sip.epygi.loc:5060	SIP Registration Status
□		Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Succesfully registered user 1100 on server sip.epygi.loc:5060	SIP Registration Status
□		Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Succesfully registered user 1102 on server sip.epygi.loc:5060	SIP Registration Status
□		Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Succesfully registered user 1101 on server sip.epygi.loc:5060	SIP Registration Status
□		Mon Sep 26 05:11:01 2005	3	SIP	registration failure	Could not Register user 66101 on server sip.epygi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
□		Mon Sep 26 05:11:01 2005	3	SIP	registration failure	Could not Register user 1100 on server sip.epygi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
□		Mon Sep 26 05:11:01 2005	3	SIP	registration failure	Could not Register user 1102 on server sip.epygi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
□		Mon Sep 26 05:11:01 2005	3	SIP	registration failure	Could not Register user 1101 on server sip.epygi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
□		Mon Sep 26 05:08:34 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:07:34 2005	3	SIP	registration failure	Could not Register user 66101 on server sip.epygi.loc:5060. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:07:34 2005	3	SIP	registration failure	Could not Register user 1100 on server sip.epygi.loc:5060. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:07:34 2005	3	SIP	registration failure	Could not Register user 1102 on server sip.epygi.loc:5060. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:07:34 2005	3	SIP	registration failure	Could not Register user 1101 on server sip.epygi.loc:5060. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:07:04 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epygi.com:5050. Reason: Destination unreachable	SIP Registration Status
□		Mon Sep 26 05:05:51 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Destination unreachable	SIP Registration Status
□		Sun Sep 25 02:51:46 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Authorization failure	SIP Registration Status
□		Sun Sep 25 03:19:43 2005	2	SNTP	connect failure	System time could not be set. Reason: None of the servers answered	Time / Date
□		Sun Sep 25 03:10:49 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
□		Sun Sep 25 02:41:45 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Authorization failure	SIP Registration Status
□		Sun Sep 25 02:37:26 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
□		Sun Sep 25 02:08:22 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Authorization failure	SIP Registration Status
□		Sun Sep 25 02:06:43 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
□		Fri Sep 23 15:29:42 2005	1	SIP	registration succeeded	Succesfully registered user 66101 on server sip.epygi.loc:5060	SIP Registration Status
□		Fri Sep 23 15:20:59 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epygi.com:5050. Reason: Timeout occurred	SIP Registration Status
□		Fri Sep 23 15:20:53 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Timeout occurred	SIP Registration Status
□		Fri Sep 23 15:20:34 2005	3	SYSTEM	reboot	the device has been successfully started after reboot	
□		Fri Sep 23 15:20:30 2005	3	SIP	registration failure	Could not Register user 5610 on server sipcenter.com:5060. Reason: Authorization failure	SIP Registration Status
□		Fri Sep 23 15:20:26 2005	3	SIP	registration failure	Could not Register user 3330 on server sip.quadrosip.net:5060. Reason: Incorrect remote address	SIP Registration Status
□		Fri Sep 23 15:20:24 2005	3	SIP	registration failure	Could not Register user 51310 on server sip.fwd.com:5060. Reason: Incorrect remote address	SIP Registration Status
□		Fri Sep 23 15:20:22 2005	1	SIP	registration succeeded	Succesfully registered user 1100 on server sip.epygi.loc:5060	SIP Registration Status
□		Fri Sep 23 15:20:22 2005	1	SIP	registration succeeded	Succesfully registered user 1102 on server sip.epygi.loc:5060	SIP Registration Status
□		Fri Sep 23 15:20:21 2005	1	SIP	registration succeeded	Succesfully registered user 1101 on server sip.epygi.loc:5060	SIP Registration Status
□		Fri Sep 23 15:19:35 2005	1	SNTP	time set	time changed by 1.447249 secs to Fri Sep 23 15:19:33 2005 (ntp1.epygi.com)	Time / Date

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-30: System Events list

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

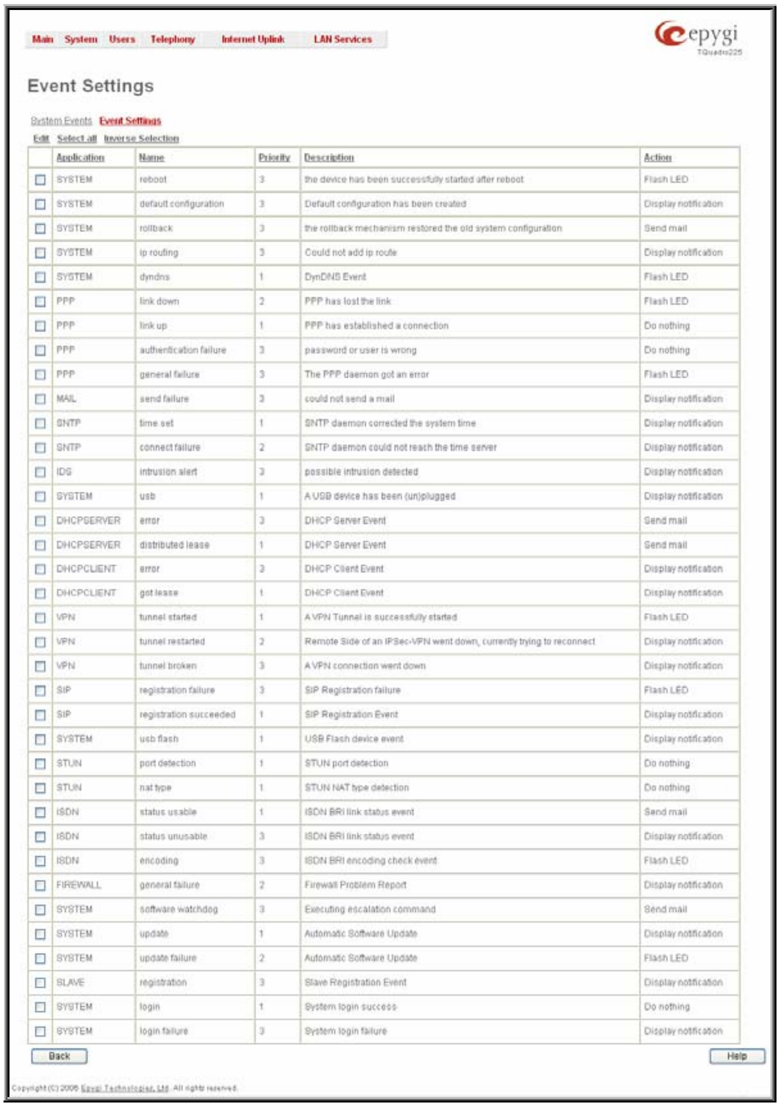
The table shows the **Status** of the event (new or read) as well as the name of the application the event refers to, event description, and the date when the event was received. For example, if the event was caused due to incorrect mail sending or SIP registration, corresponding links will be seen in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

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

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

Mark all as read marks newly occurred events as “read”.

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



Event Settings

System Events Event Settings

Edit Select all Inverse Selection

	Application	Name	Priority	Description	Action
□	SYSTEM	reboot	3	the device has been successfully started after reboot	Flash LED
□	SYSTEM	default configuration	3	Default configuration has been created	Display notification
□	SYSTEM	rollback	3	the rollback mechanism restored the old system configuration	Send mail
□	SYSTEM	ip routing	3	Could not add ip route	Display notification
□	SYSTEM	dyndns	1	DynDNS Event	Flash LED
□	PPP	link down	2	PPP has lost the link	Flash LED
□	PPP	link up	1	PPP has established a connection	Do nothing
□	PPP	authentication failure	3	password or user is wrong	Do nothing
□	PPP	general failure	3	The PPP daemon got an error	Flash LED
□	MAIL	send failure	3	could not send a mail	Display notification
□	SNTP	time set	1	SNTP daemon corrected the system time	Display notification
□	SNTP	connect failure	2	SNTP daemon could not reach the time server	Display notification
□	IDS	intrusion alert	3	possible intrusion detected	Display notification
□	SYSTEM	usb	1	A USB device has been (un)plugged	Display notification
□	DHCPSERVER	error	3	DHCP Server Event	Send mail
□	DHCPSERVER	distributed lease	1	DHCP Server Event	Send mail
□	DHCPCLIENT	error	3	DHCP Client Event	Display notification
□	DHCPCLIENT	got lease	1	DHCP Client Event	Display notification
□	VPN	tunnel started	1	A VPN Tunnel is successfully started	Flash LED
□	VPN	tunnel restarted	2	Remote Side of an IPSec-VPN went down, currently trying to reconnect	Display notification
□	VPN	tunnel broken	3	A VPN connection went down	Display notification
□	SIP	registration failure	3	SIP Registration failure	Flash LED
□	SIP	registration succeeded	1	SIP Registration Event	Display notification
□	SYSTEM	usb flash	1	USB Flash device event	Display notification
□	STUN	port detection	1	STUN port detection	Do nothing
□	STUN	nat type	1	STUN NAT type detection	Do nothing
□	ISDN	status usable	1	ISDN BRI link status event	Send mail
□	ISDN	status unusable	3	ISDN BRI link status event	Display notification
□	ISDN	encoding	3	ISDN BRI encoding check event	Flash LED
□	FIREWALL	general failure	2	Firewall Problem Report	Display notification
□	SYSTEM	software watchdog	3	Executing escalation command	Send mail
□	SYSTEM	update	1	Automatic Software Update	Display notification
□	SYSTEM	update failure	2	Automatic Software Update	Flash LED
□	SLAVE	registration	3	Slave Registration Event	Display notification
□	SYSTEM	login	1	System login success	Do nothing
□	SYSTEM	login failure	3	System login failure	Display notification

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-31: Event Configuration Settings page

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

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

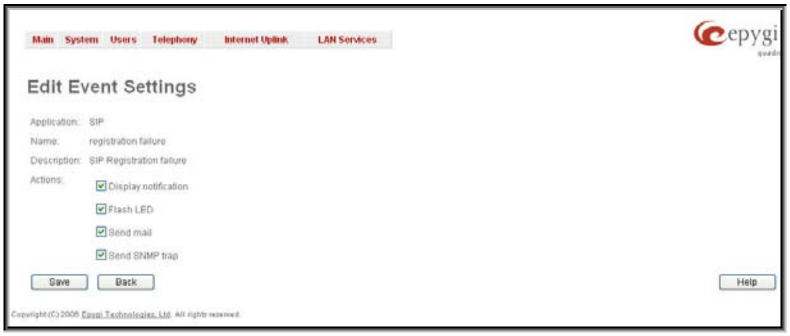
Each entry in the events’ table has a checkbox assigned to each row. By selecting the corresponding checkboxes, operations such as **Edit** may be done for one or more events.

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

- **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.
- **Send SNMP Trap** – an SNMP notification will be sent to the traphost(s) listed in the SNMP Trap Settings table (see SNMP Settings).

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 Quadro cannot receive an IP address from the DHCP or PPP servers, or cannot register an extension on the SIP or Routing servers, or cannot reach the 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.



Edit Event Settings

Application: SIP

Name: registration failure

Description: SIP Registration failure

Actions:
☑ Display notification
☑ Flash LED
☑ Send mail
☑ Send SNMP trap

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-32: Edit Event Settings page

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

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

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

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

Action offers radio buttons to choose one of the actions to notify the Quadro administrator when an event(s) takes place.

To Assign an Action to the Event

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

Time / Date Settings

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

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

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

Timezone provides a selection of world time zones and is used to select the local country time zone. 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 Quadro, thus Quadro becomes the timeserver for its LAN.

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

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

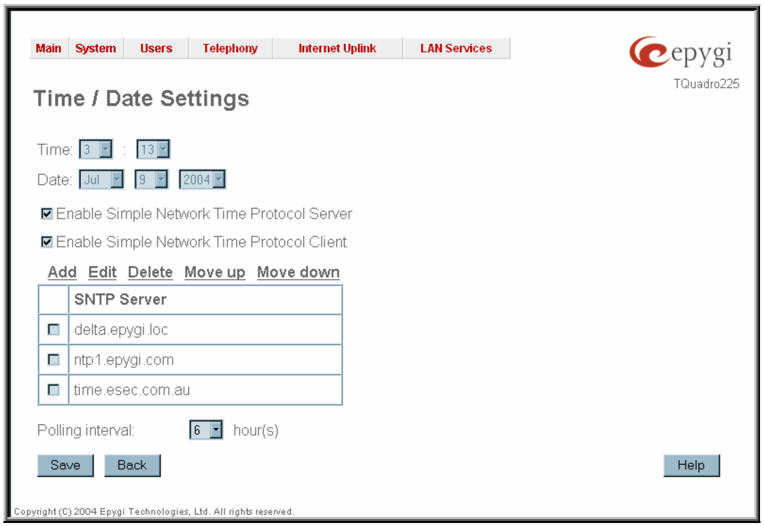
The **Add** functional button opens an **Add NTP Server** page where a new NTP server can be defined. This page offers the **NTP Server** radio buttons that are used to choose between a manual and a predefined NTP server.

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

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

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

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



Time / Date Settings

Time: 3 : 13

Date: Jul 9 2004

☑ Enable Simple Network Time Protocol Server

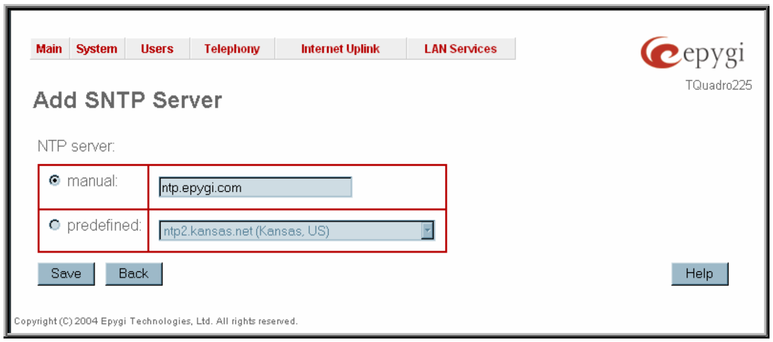
☑ Enable Simple Network Time Protocol Client

	SNTP Server
□	delta.epygi.loc
□	ntp1.epygi.com
□	time.esec.com.au

Polling interval: 6 hour(s)

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-33: Time and Date Settings page



Add SNTP Server

NTP server:

● manual:	ntp.epygi.com
○ predefined:	ntp2.kansas.net (Kansas, US)

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-34: Add NTP Server page

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

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.

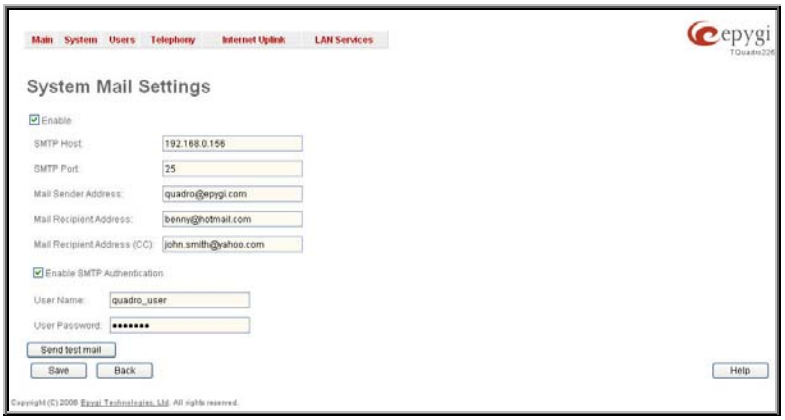
SMTP Port requires the SMTP host port number.

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.



System Mail Settings

☑ Enable

SMTP Host: 192.168.0.156

SMTP Port: 25

Mail Sender Address: quadro@epygi.com

Mail Recipient Address: benny@hotmail.com

Mail Recipient Address (CC): john.smith@yahoo.com

☑ Enable SMTP Authentication

User Name: quadro_user

User Password: •••••••

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-35: 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 Quadro by installing new firmware (image). Users registered at Epygi will receive a notice when new firmware is available and will be able to download it from the Epygi Technical Support WEB page.

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

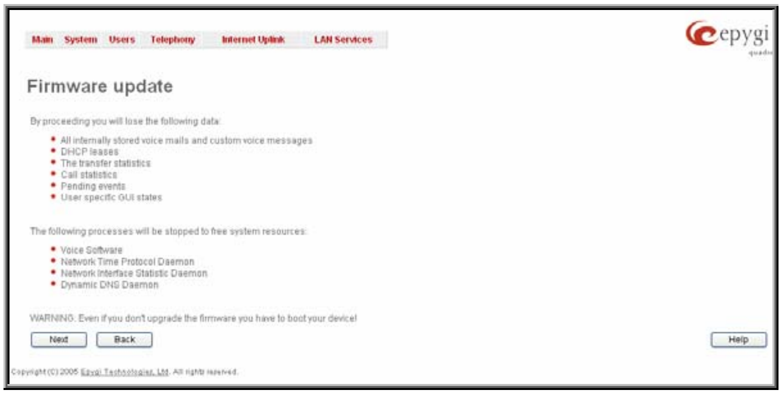
Please Note: Installing new firmware will take about 15 minutes. During this time, QuadroISDN, telephony and Internet access will be disabled.
The firmware update will cause the loss of the following data:

- All voice mails
- DHCP leases
- Transfer statistics
- Call statistics
- All 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 Call Statistics entries in the displayed tables to be important, it is recommended to download them from the corresponding page prior to starting the Firmware Update.



Firmware update

By proceeding you will lose the following data:

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

The following processes will be stopped to free system resources:

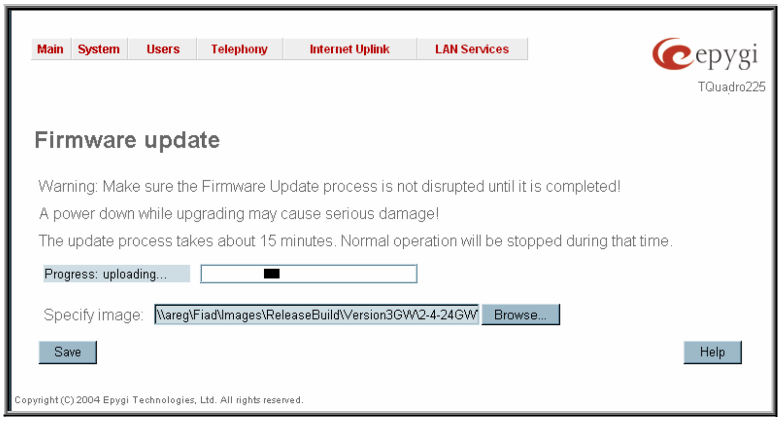
- Voice Software
- Network Time Protocol Daemon
- Network Interface Statistic Daemon
- Dynamic DNS Daemon

WARNING: Even if you don't upgrade the firmware you have to boot your device!

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-36: Firmware Update page 1

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



Firmware update

Warning: Make sure the Firmware Update process is not disrupted until it is completed!

A power down while upgrading may cause serious damage!

The update process takes about 15 minutes. Normal operation will be stopped during that time.

Progress: uploading...

Specify image: \\areg\Fiad\Images\ReleaseBuild\Version3GW\2-4-24GW\

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-37: Firmware Update page 2

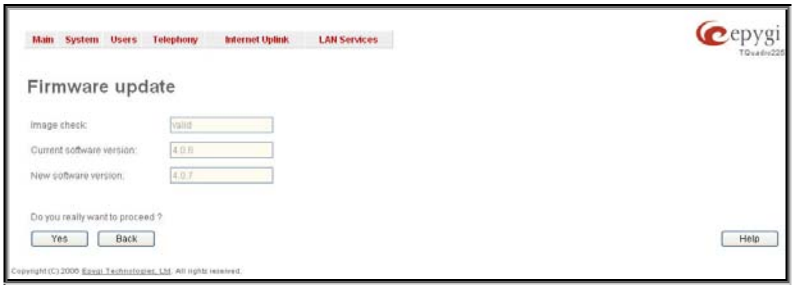
The second page of **Firmware update** has a **Browse** button used to browse the image file, and the **Specify Image** text field that will display the selected image filename.

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

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

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

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



Firmware update

Image check: valid

Current software version: 4.0.6

New software version: 4.0.7

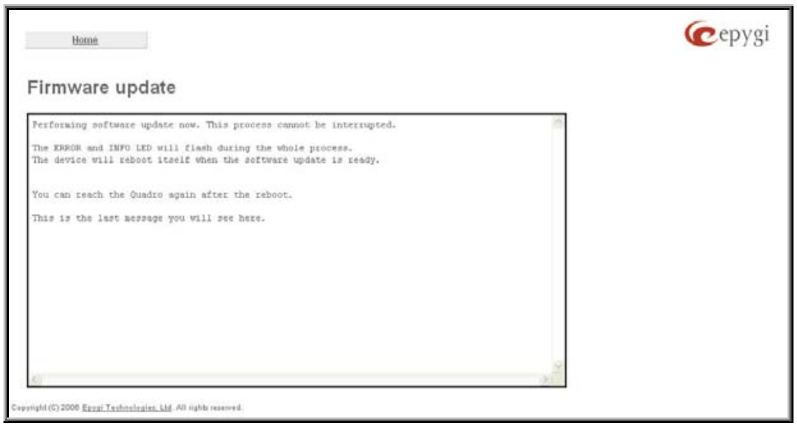
Do you really want to proceed ?

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-38: 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.



Firmware update

```
Performing software update now. This process cannot be interrupted.

The ERROR and INFO LED will flash during the whole process.
The device will reboot itself when the software update is ready.


You can reach the Quadro again after the reboot.

This is the last message you will see here.
```

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-39: 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 and NAT).

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

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

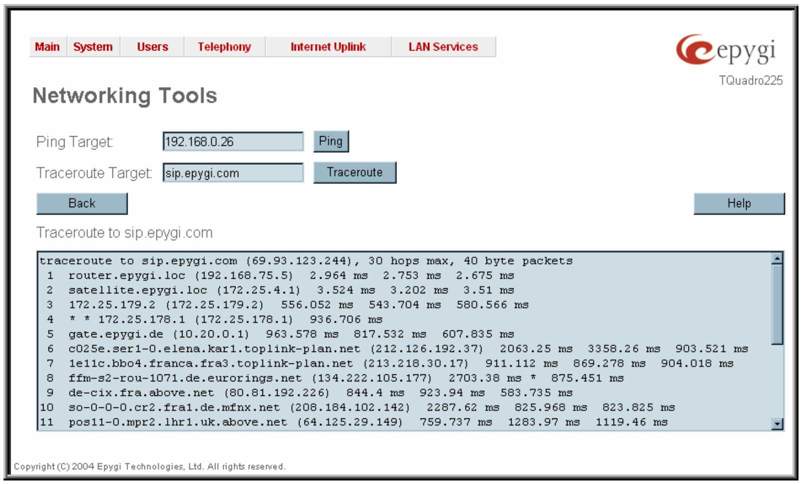
Ping Target requires the destination (IP address or host name) for the ICMP request.

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

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

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

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



Networking Tools

Ping Target: 192.168.0.26

Traceroute Target: sip.epygi.com

Traceroute to sip.epygi.com

```
traceroute to sip.epygi.com (69.93.123.244), 30 hops max, 40 byte packets
 1  router.epygi.loc (192.168.75.5)  2.964 ms  2.753 ms  2.675 ms
 2  satellite.epygi.loc (172.25.4.1)  3.524 ms  3.202 ms  3.51 ms
 3  172.25.179.2 (172.25.179.2)  556.052 ms  543.704 ms  580.566 ms
 4  * * 172.25.178.1 (172.25.178.1)  936.706 ms
 5  gate.epygi.de (10.20.0.1)  963.578 ms  817.532 ms  607.835 ms
 6  c025e.ser1-0.elena.kar1.toplink-plan.net (212.126.192.37)  2063.25 ms  3358.26 ms  903.521 ms
 7  1e11c.bbo4.franca.fra3.toplink-plan.net (213.218.30.17)  911.112 ms  869.278 ms  904.018 ms
 8  ffm-s2-rou-1071.de.eurorings.net (134.222.105.177)  2703.38 ms *  875.451 ms
 9  de-cix.fra.above.net (80.81.192.226)  844.4 ms  923.94 ms  583.735 ms
10  so-0-0-0.cr2.fra1.de.mfnx.net (208.184.102.142)  2287.62 ms  825.968 ms  823.825 ms
11  pos11-0.mpr2.lhr1.uk.above.net (64.125.29.149)  759.737 ms  1283.97 ms  1119.46 ms
```

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-40: Networking Tools page

To Check the Internet connection

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

SNMP Settings

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

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

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

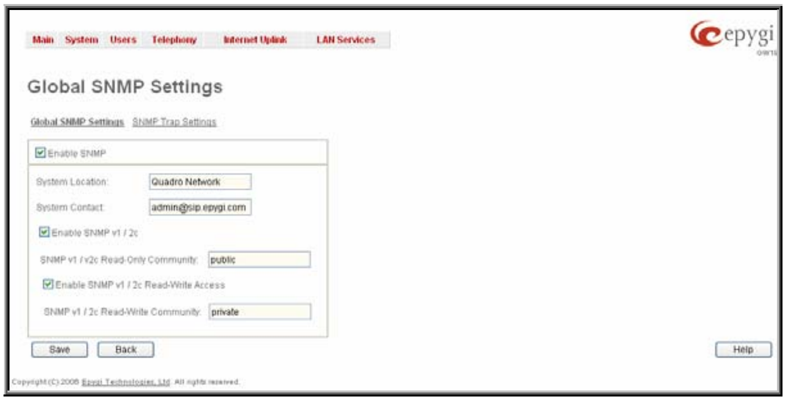
Global SNMP Settings are used to enable the SNMP agent on the Quadro, to select the SNMP protocol version for communication with the administrating application and to define the community for administrating application to connect the Quadro.

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

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

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

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



Global SNMP Settings

Global SNMP Settings SNMP Trap Settings

☑ Enable SNMP

System Location: Quadro Network

System Contact: admin@sip.epygi.com

☑ Enable SNMP v1 / 2c

SNMP v1 / v2c Read-Only Community: public

☑ Enable SNMP v1 / 2c Read-Write Access

SNMP v1 / 2c Read-Write Community: private

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-41: Global SNMP Settings page

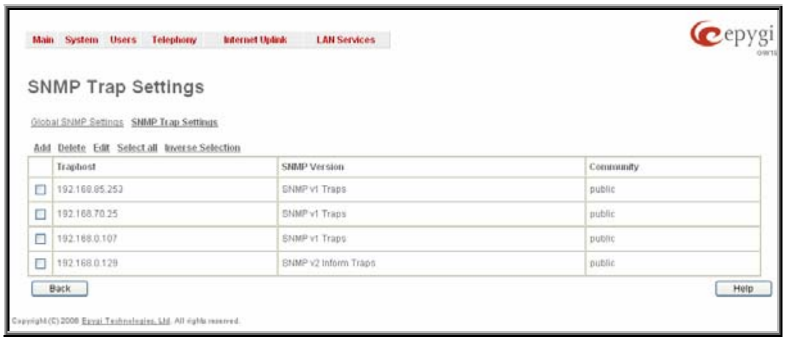
SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about Quadro’s). Field may contain some kind of password which should be matching both on Quadro and on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

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

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

SNMP Trap Settings are used to define the traphosts that should be informed when certain events occur on the Quadro. For the listed traphosts to be informed about the events on the Quadro, **Send SNMP Trap** action should be configured for the corresponding event(s) from the Error! Not a valid result for table. page.

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



SNMP Trap Settings

Global SNMP Settings SNMP Trap Settings

	Traphost	SNMP Version	Community
□	192.168.85.253	SNMP v1 Traps	public
□	192.168.70.25	SNMP v1 Traps	public
□	192.168.0.107	SNMP v1 Traps	public
□	192.168.0.129	SNMP v2 Inform Traps	public

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

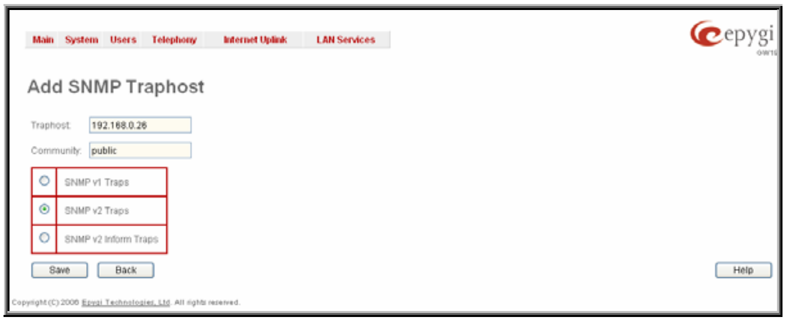
Fig. II-42: SNMP Trap Settings page

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

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

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

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



Add SNMP Traphost

Traphost: 192.168.0.26

Community: public

○ SNMP v1 Traps

● SNMP v2 Traps

○ SNMP v2 Inform Traps

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-43:Add SNMP Traphost page

Diagnostics

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

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

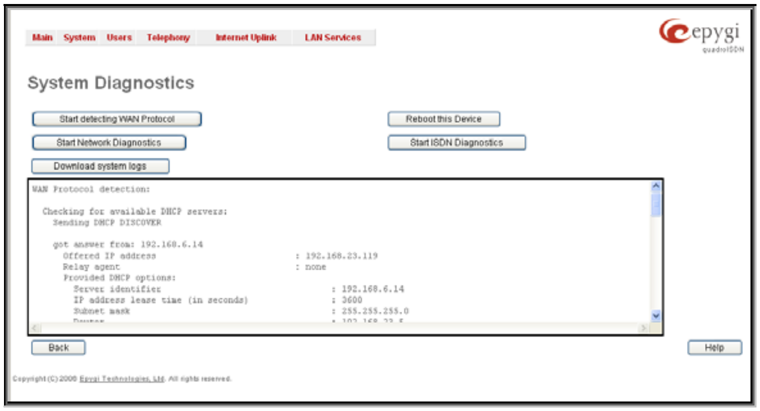
The **Start Network Diagnostics** button is used to initiate network diagnostics, i.e., to check the WAN link and IP configuration, to verify gateway, DNS primary and secondary (if configured) servers' accessibilities.

The **Start ISDN Diagnostics** button is used to initiate ISDN BRI low level diagnostic. With these tests the ISDN physical link is checked and the Frame Synchronization is verified.

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.



```
WAN Protocol detection:

  Checking for available DHCP servers:
    Sending DHCP DISCOVER

    got answer from: 192.168.6.14
      Offered IP address                          : 192.168.23.119
      Relay agent                                 : none
      Provided DHCP options:
        Server identifier                               : 192.168.6.14
        IP address lease time (in seconds)              : 3600
        Subnet mask                                     : 255.255.255.0
```

Fig. II-44: System Diagnostic page

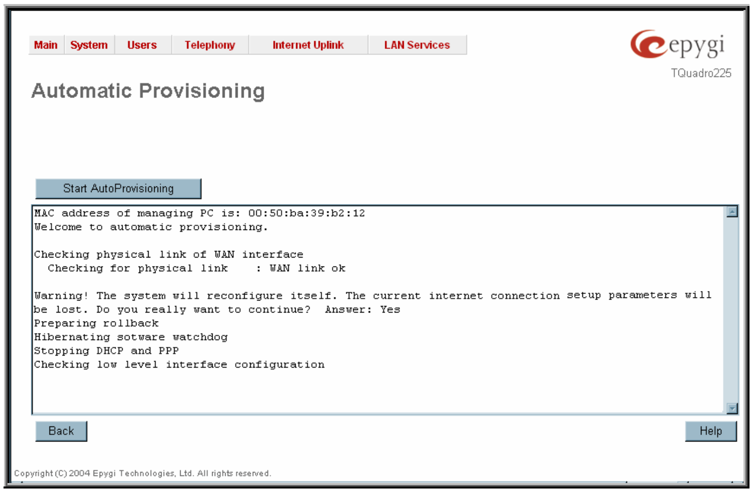
Automatic Provisioning

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



```
MAC address of managing PC is: 00:50:ba:39:b2:12
Welcome to automatic provisioning.

Checking physical link of WAN interface
  Checking for physical link    : WAN link ok

Warning! The system will reconfigure itself. The current internet connection setup parameters will
be lost. Do you really want to continue?  Answer: Yes
Preparing rollback
Hibernating sotware watchdog
Stopping DHCP and PPP
Checking low level interface configuration
```

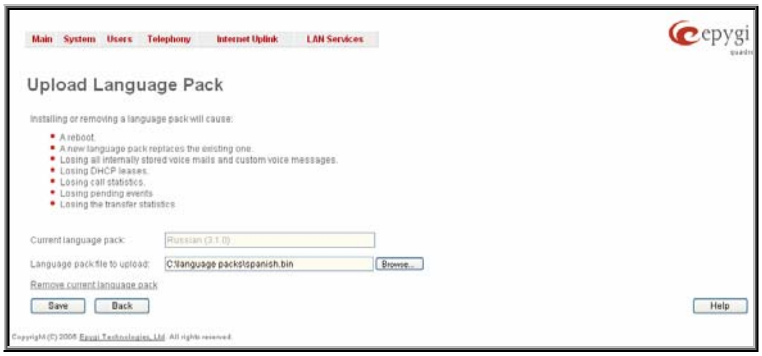
Fig. II-45: Auto Provisioning page

Upload Language Pack

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

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

- All internally stored voice mail
- DHCP leases
- Call statistics
- Pending events
- Transfer statistics



Installing or removing a language pack will cause:

- A reboot.
- A new language pack replaces the existing one.
- Losing all internally stored voice mails and custom voice messages.
- Losing DHCP leases.
- Losing call statistics.
- Losing pending events.
- Losing the transfer statistics.

Current language pack: Russian (3.1.0)

Language pack file to upload: C:\language packs\spanish.bin

Fig. II-46: Upload Language Pack page

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

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

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

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

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

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

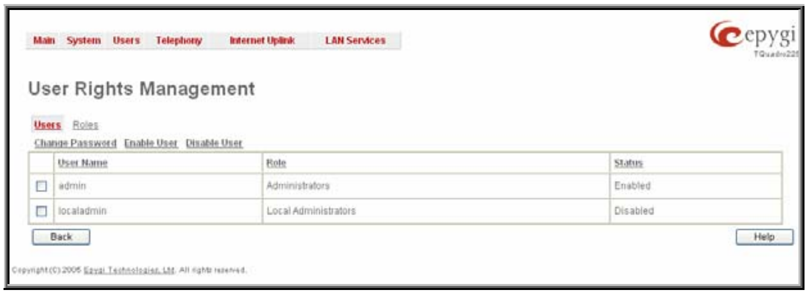
User Rights Management

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

Two levels of Quadro GUI administration are available:

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

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



User Rights Management

Users Roles

Change Password Enable User Disable User

	User Name	Role	Status
□	admin	Administrators	Enabled
□	localadmin	Local Administrators	Disabled

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-47: Users page at User Rights Management

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:

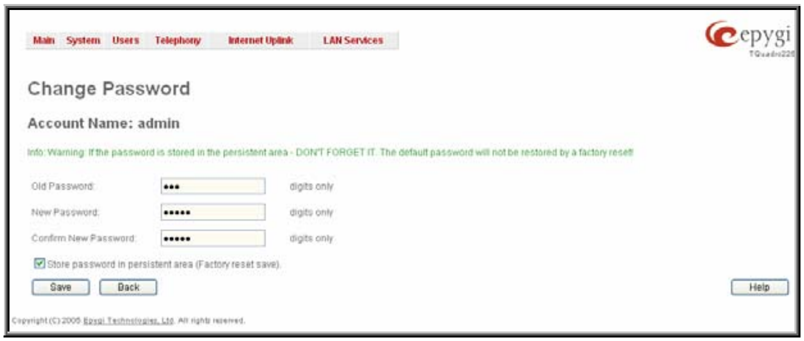
The **Old Password** text field is only present when modifying the Administrator account password and requires the current password of the Administrator. An error message prevents entering the wrong password.

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 Quadro will be considered broken. Please contact Epygi Technical Support Center for replacing the device.



Change Password

Account Name: admin

Info: Warning: If the password is stored in the persistent area - DON'T FORGET IT. The default password will not be restored by a factory reset!

Old Password: ••• digits only

New Password: ••••• digits only

Confirm New Password: ••••• digits only

☑ Store password in persistent area (Factory reset save).

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

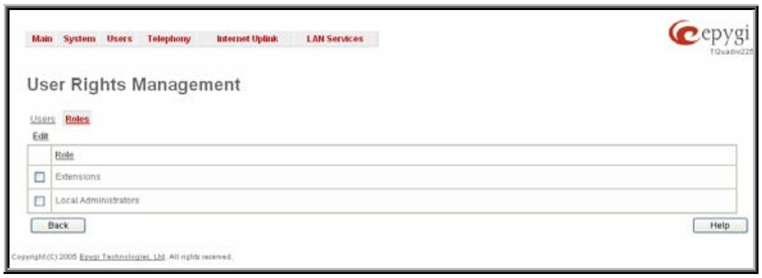
Fig. II-48: Change Password page

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

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

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

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



User Rights Management

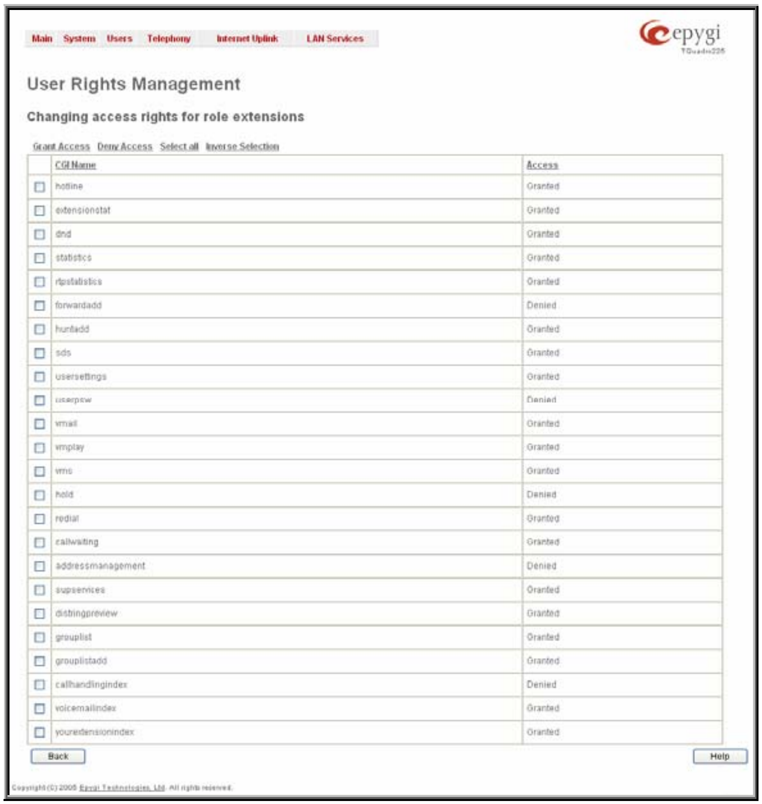
Users Roles

Edit

	Role
□	Extensions
□	Local Administrators

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-49: Roles page at User Rights Management


Main System Users Telephony Internet Uplink LAN Services
epygi
TQuadro228

User Rights Management

Changing access rights for role extensions

Grant Access Deny Access Select all Inverse Selection

	CGI Name	Access
□	hotline	Granted
□	extensionstat	Granted
□	dnd	Granted
□	statistics	Granted
□	rtpstatistics	Granted
□	forwardadd	Denied
□	huntadd	Granted
□	sds	Granted
□	usersettings	Granted
□	userpsw	Denied
□	vmail	Granted
□	vmplay	Granted
□	vms	Granted
□	hold	Denied
□	redial	Granted
□	callwaiting	Granted
□	addressmanagement	Denied
□	supservices	Granted
□	distringpreview	Granted
□	grouplist	Granted
□	grouplistadd	Granted
□	callhandlingindex	Denied
□	voicemailindex	Granted
□	yourextensionindex	Granted

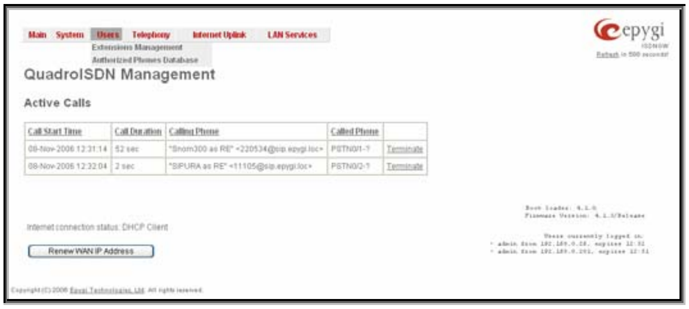
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-50: Edit 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.

Users Menu



QuadroISDN Management

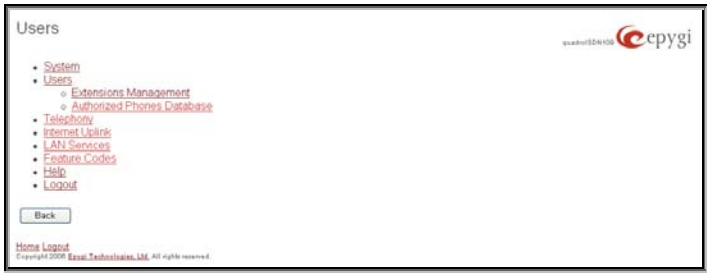
Active Calls

Call Start Time	Call Duration	Calling Phone	Called Phone	
08-Nov-2006 12:31:14	52 sec	"Snom300 as RE" <220534@sip.epygi.loc>	PSTN0/1-1	Terminate
08-Nov-2006 12:32:04	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	PSTN0/2-1	Terminate

Internet connection status: DHCP Client

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-51: Telephone Users Menu in Dynamo Theme



Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

F Fig. II-52: Telephone Users Menu in Plain Theme

Extensions Management

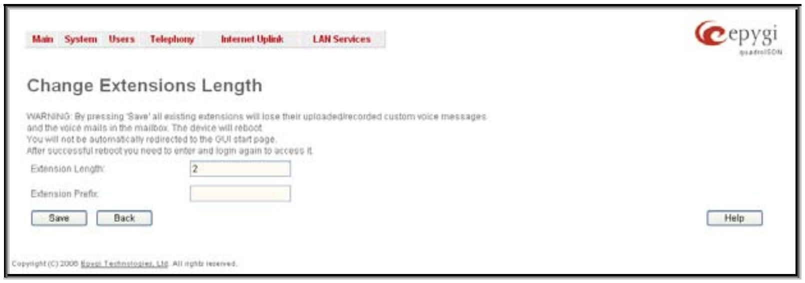
The **Extensions Management** is used to create user extensions and auto attendants on the Quadro. From this page, by clicking on the user extension, administrator can get the extension settings pages.

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

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

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

The **Extension Prefix** text field is used to define a prefix with which all existing extensions on the Quadro as well as to any newly created extensions should start. At present, there are no limitations on this field.



Change Extensions Length

WARNING: By pressing 'Save' all existing extensions will lose their uploaded/recorded custom voice messages and the voice mails in the mailbox. The device will reboot.
You will not be automatically redirected to the GUI start page.
After successful reboot you need to enter and login again to access it.

Extension Length: 2

Extension Prefix:

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-53: Extensions Management - Add Entry page

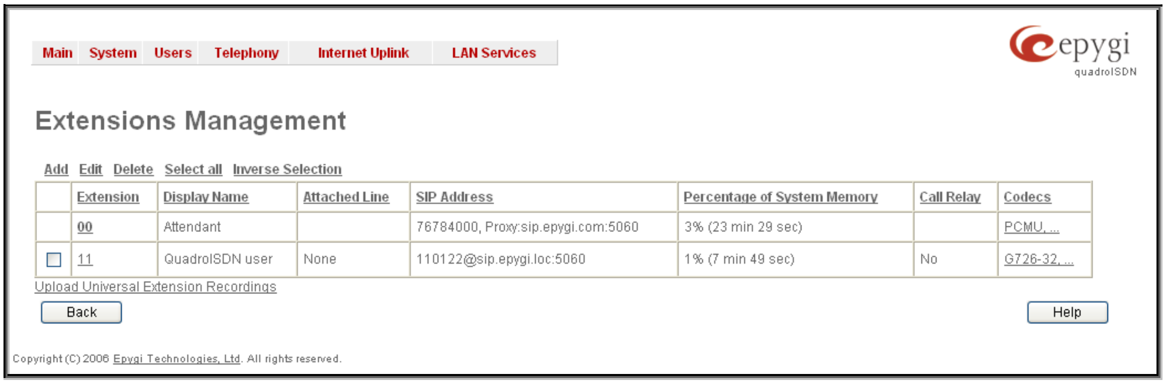
Please Note: By saving the settings on the **Change Extension Length** page, all existing extensions will lose the custom voice messages and voice mails in the voice mailbox. The device will be rebooted. You will not be automatically redirected to the login page, so you need to access it manually again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

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

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

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

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



Extensions Management

	Extension	Display Name	Attached Line	SIP Address	Percentage of System Memory	Call Relay	Codecs
	00	Attendant		76784000, Proxy:sip.epygi.com:5060	3% (23 min 29 sec)		PCMU, ...
□	11	QuadroISDN user	None	110122@sip.epygi.loc:5060	1% (7 min 49 sec)	No	G726-32, ...

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-54: Extensions Management page

The following columns are present in the table:

- **Extension** - lists the 2-digit user or attendant extensions on the Quadro. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: “username, Proxy: sipserver:port”. If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **Percentage of System Memory** - indicates the user space (in percentages) configured for each extension. For user extensions, the actual available duration (in minutes) for the blocking messages is displayed here. For attendant extensions, the actual available duration (in minutes) for the auto attendant messages is displayed here.
- **Call Relay** - indicates whether or not the Call Relay option is enabled on the extension.
- **Codecs** – column lists the short information (full information is seen in the tool tip) about extension specific voice Codecs. Extension codec’s can be accessed and modified by clicking on the link of the corresponding extension’s Codecs. The link leads to the Extension Codecs page.

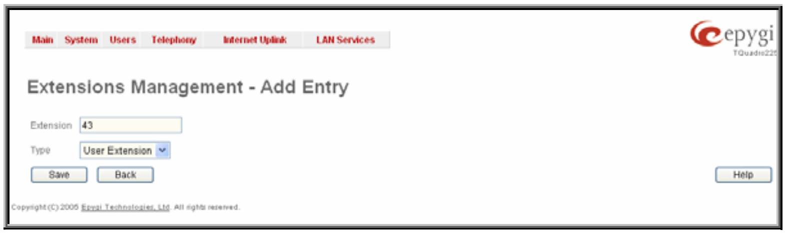
Clicking on each user extension in the Extensions table will open the extension specific **Extension Settings** menu. When Call Park service is enabled on the extension, it is displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible.

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

The **Extension** text field is used to enter a new extension number. The extension number is a two-digit number. If non-digit symbols have been entered, the error “Incorrect Extension: no symbol characters allowed” will appear. If the extension length is shorter than 2 digits, the error “Incorrect Extensions length” will prevent the creation of the extension. If an extension with the same number already exists in the Extensions Management table, the error “Extension already exists” will appear.

Please Note: Each extension number cannot start with digits 0, 8 or 9.

The **Type** drop down list is used to select the type of the extension (user or attendant) to be created (for details see below).



Extensions Management - Add Entry

Extension 43

Type User Extension

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-55: Extensions Management - Add Entry page

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

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

Please Note: Save changes before moving among settings groups.

User Extension Settings

1. General Settings

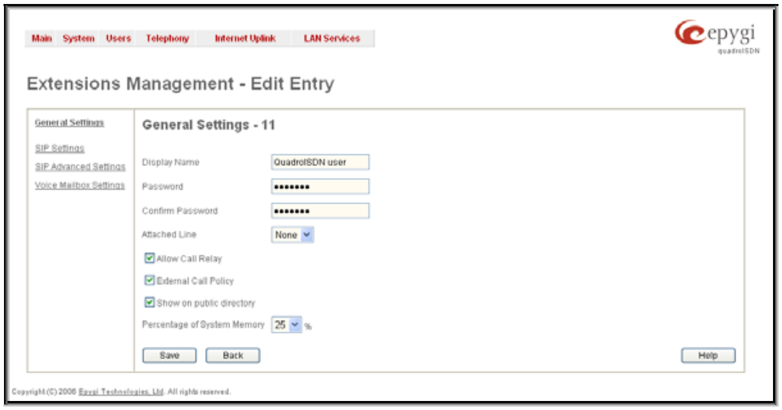
This group requires extension‘s personal information and has the following components:

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

Password requires a password for the new extension.

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

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



Extensions Management - Edit Entry

General Settings - 11

Display Name: QuadroISDN user
Password: •••••••
Confirm Password: •••••••
Attached Line: None
☑ Allow Call Relay
☑ External Call Policy
☑ Show on public directory
Percentage of System Memory: 25 %

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-56: Extensions Management - Edit Entry – General Settings page

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

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension’s Quadro Web Management (accessed by the extension’s login, see Manual III – Extension User’s Guide). Besides this, the details of the extension will be displayed in the Public Directories on the Snom and Aastra SIP phones. Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

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

2. SIP Settings

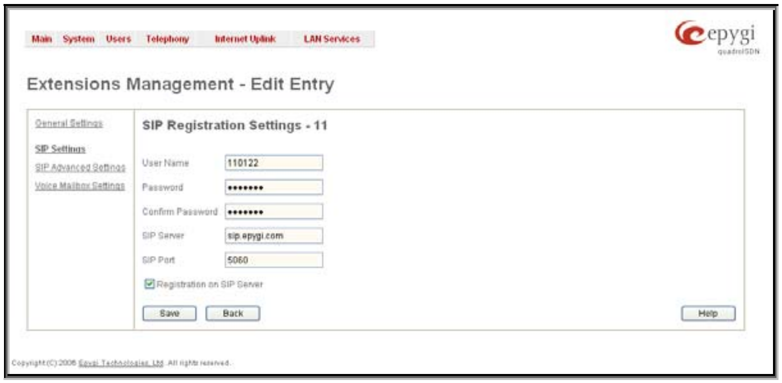
This group is used to configure extension’s SIP registration settings and consists of the following components:

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

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

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

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



Extensions Management - Edit Entry

SIP Registration Settings - 11

User Name: 110122
Password: •••••••
Confirm Password: •••••••
SIP Server: sip.epygi.com
SIP Port: 5060
☑ Registration on SIP Server

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-57: Extensions Management - Edit Entry – SIP Settings page

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

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

3. Advanced SIP Settings

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

The SIP Outbound proxy is an SIP server where all the SIP requests and other SIP messages are transferred. Some SIP servers use an outbound proxy server to escape restrictions of NAT. For example, Free World Dialup service uses an Outbound Proxy server. If an Outbound proxy is specified for an extension, all SIP calls originating from that extension are made through that outbound proxy, i.e., all requests are sent to that outbound proxy.

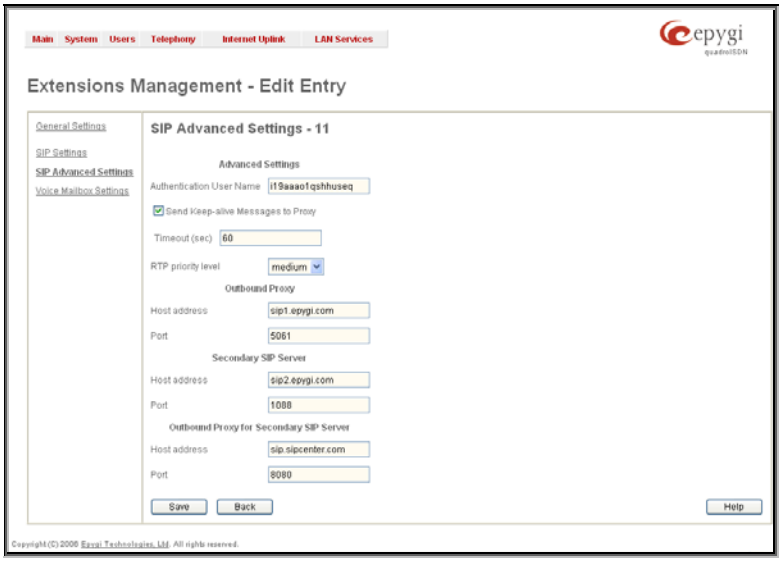
The Secondary SIP Server acts as an alternative SIP registration server when the primary SIP Registration Server is inaccessible. If the connection with the primary SIP server fails, Quadro will automatically start sending SIP messages to the Secondary SIP Server. It will switch back to the primary SIP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

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

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

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

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



Extensions Management - Edit Entry

SIP Advanced Settings - 11

Advanced Settings

Authentication User Name: i19aaao1qshhuseq

☑ Send Keep-alive Messages to Proxy

Timeout (sec): 60

RTP priority level: medium

Outbound Proxy

Host address: sip1.epygi.com

Port: 5061

Secondary SIP Server

Host address: sip2.epygi.com

Port: 1088

Outbound Proxy for Secondary SIP Server

Host address: sip.sipcenter.com

Port: 8080

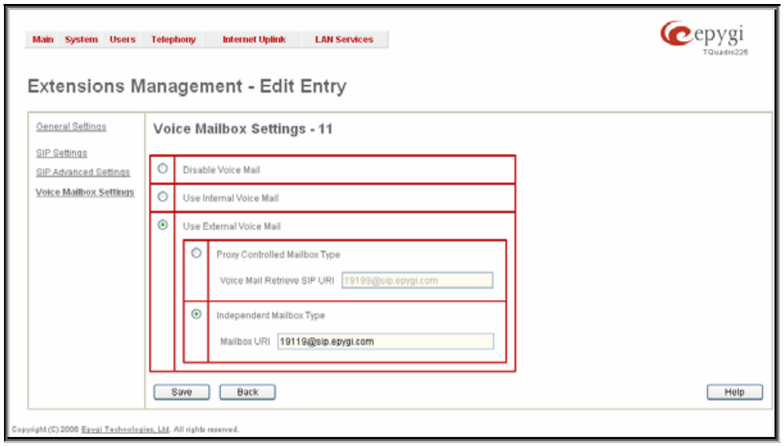
Fig. II-58: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Voice Mailbox Settings

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

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

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



Extensions Management - Edit Entry

Voice Mailbox Settings - 11

○ Disable Voice Mail

○ Use Internal Voice Mail

● Use External Voice Mail

○ Proxy Controlled Mailbox Type

Voice Mail Retrieve SIP URI: 19199@sip.epygi.com

● Independent Mailbox Type

Mailbox URI: 19119@sip.epygi.com

Fig. II-59: Extensions Management - Edit Entry – Voice Mailbox Settings page

Attendant Extension Settings

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

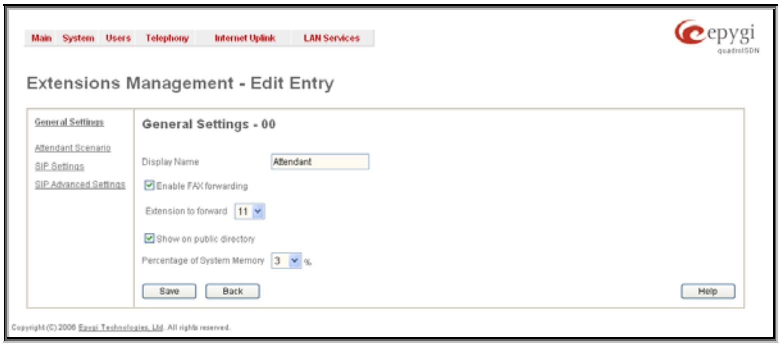
1. General Settings (for attendant extension)
This group requires personal extension information and has the following components:

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

With the **Enable FAX Forwarding** checkbox enabled, the system moves the incoming FAX to the selected extension if a FAX tone is detected on the Auto Attendant.

The **Extension to forward** drop down list is used to choose the extension where the incoming FAX addressed to the Quadro's Auto Attendant will be forwarded. The list contains only those extensions that have FAX support enabled. FAX support can be enabled from the Extension Codecs page.

Please Note: FAX forwarding is applicable only for incoming calls from PSTN and IP networks. It is not valid for PBX calls.



Extensions Management - Edit Entry

General Settings - 00

Display Name: Attendant

☑ Enable FAX forwarding

Extension to forward: 11

☑ Show on public directory

Percentage of System Memory: 3 %

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-60: Extensions Management - Edit Entry – General Settings for Auto Attendant page

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

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

2. Attendant Scenario

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

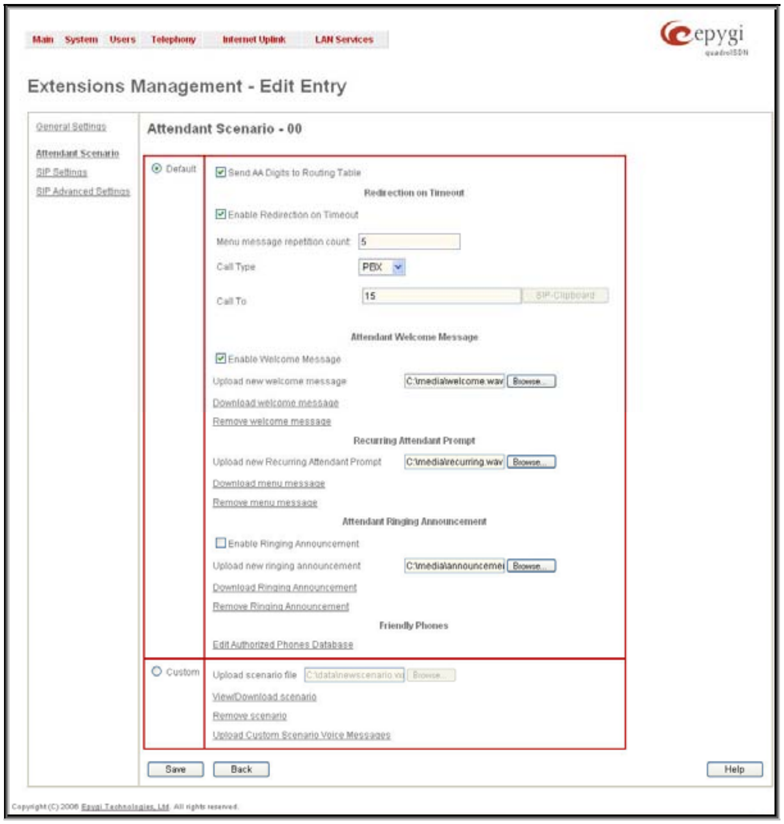
The **Default** manipulation radio button selection enables following components:

- The **Send AA Digits to Routing Table** checkbox selection switches the Auto Attendant to the routing mode. Any inserted digits on the Auto Attendant prompt will be parsed through the Routing Table on the Quadro.

- **Redirection on Timeout** - this group allows automatic call redirection in case if no action has been performed by the caller. The group offers the following options:

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

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



Extensions Management - Edit Entry

Attendant Scenario - 00

● Default

☑ Send AA Digits to Routing Table

Redirection on Timeout

☑ Enable Redirection on Timeout

Menu message repetition count: 5

Call Type: PBX

Call To: 15

Attendant Welcome Message

☑ Enable Welcome Message

Upload new welcome message: C:\media\welcome.wav

Recurring Attendant Prompt

Upload new Recurring Attendant Prompt: C:\media\recurring.wav

Attendant Ringing Announcement

□ Enable Ringing Announcement

Upload new ringing announcement: C:\media\announceme

Friendly Phones

○ Custom

Upload scenario file: C:\data\newscenario.xı

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-61: Extensions Management - Edit Entry – Attendant Scenario page

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

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

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

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

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

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

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

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

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

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

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

- **Attendant Ringing Announcement -** this group allows updating an optional announcement message (played instead of ring back tones when calling through Auto Attendant), downloading it to the PC, or restoring the default ring tones. The group offers the following components:

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

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

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

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

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

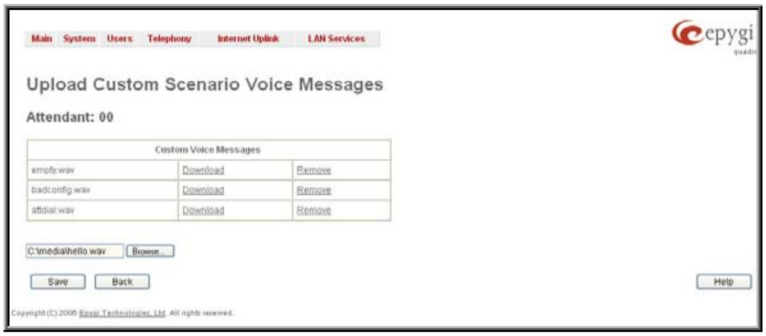
- The **Upload Scenario File** indicates the file name used to upload a new scenario file. The uploaded file needs to be in EpygiXML format (the coding standard can be found at Epygi Technical Support) and is restricted to a 20KB file size. **Browse** opens the file chooser window to browse for a custom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

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

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

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

The **Upload Custom Scenario Voice Messages** page contains a table where uploaded custom voice messages are listed. Use the **Download** functional button to download and use **Remove** to delete the corresponding custom voice message. **Browse** opens a file chooser window to browse for a custom voice message.



Upload Custom Scenario Voice Messages

Attendant: 00

Custom Voice Messages		
empty.wav	Download	Remove
badconfig.wav	Download	Remove
attdial.wav	Download	Remove

C:\media\hello.wav

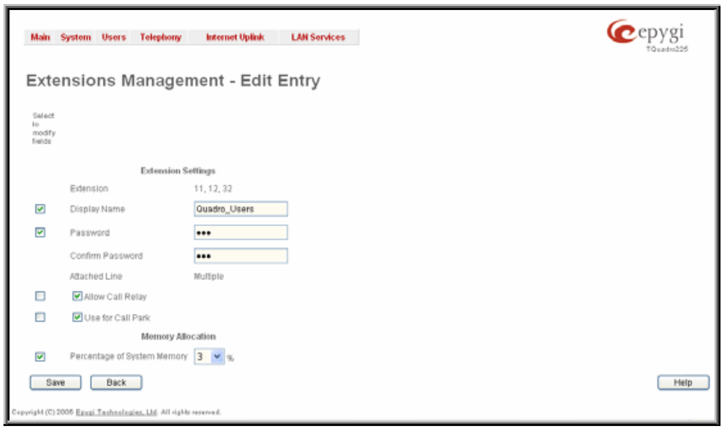
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-62: Upload Custom Voice Messages page

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

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

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



Extensions Management - Edit Entry

Select to modify fields

Extension Settings

	Extension	11, 12, 32
☑	Display Name	Quadro_Users
☑	Password	•••
	Confirm Password	•••
	Attached Line	Multiple
□	☑ Allow Call Relay	
□	☑ Use for Call Park	

Memory Allocation

☑	Percentage of System Memory	3 %

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-63: Extensions Management - Edit Entry page for multiple edit operation

To Configure an Extension

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

To Delete an Extension

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

Extension Codecs

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

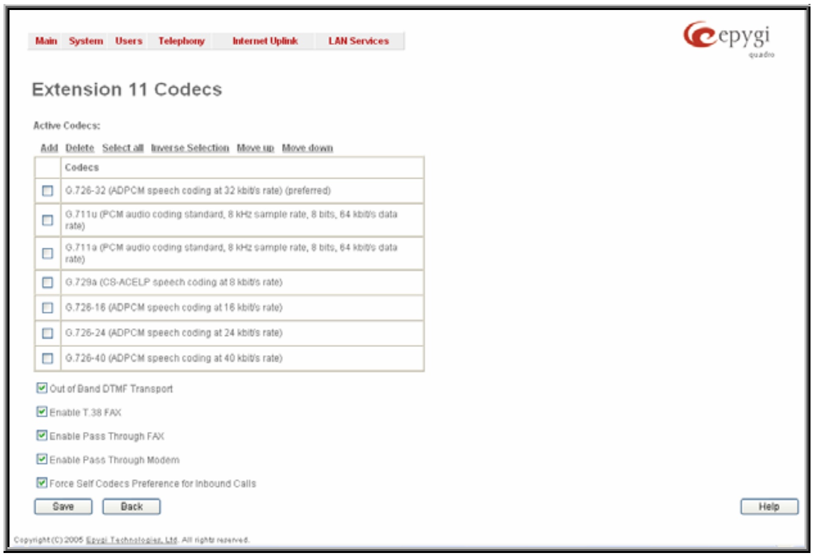
The **Extension Codecs** page displays a list of **Active Codecs** with the state of the **Out of Band DTMF** and **FAX Support** features for Quadro extensions and the Auto Attendant.

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

The table **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 in a top to down order in the **Active Codecs** table.

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

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



Extension 11 Codecs

Active Codecs:

	Codecs
□	G.726-32 (ADPCM speech coding at 32 kbit/s rate) (preferred)
□	G.711u (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)
□	G.711a (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)
□	G.729a (CS-ACELP speech coding at 8 kbit/s rate)
□	G.726-16 (ADPCM speech coding at 16 kbit/s rate)
□	G.726-24 (ADPCM speech coding at 24 kbit/s rate)
□	G.726-40 (ADPCM speech coding at 40 kbit/s rate)

☑ Out of Band DTMF Transport

☑ Enable T.38 FAX

☑ Enable Pass Through FAX

☑ Enable Pass Through Modem

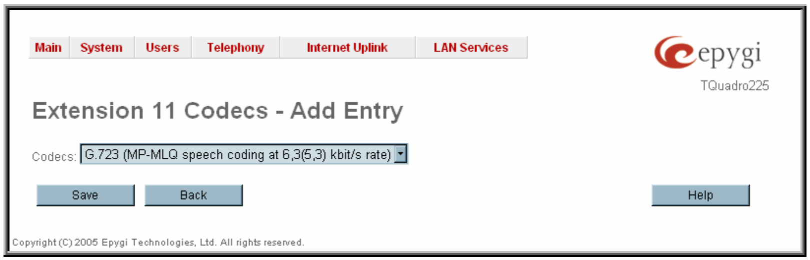
☑ Force Self Codecs Preference for Inbound Calls

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-64: Extension Codecs list

Add opens the **Add Entry** page where the user may add codecs supported by Quadro. 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.



Extension 11 Codecs - Add Entry

Codecs: G.723 (MP-MLQ speech coding at 6,3(5,3) kbit/s rate)

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-65: Extension Codecs - Add Codec page

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

Enable T.38 FAX checkbox enables the FAX tone detection and the T.38 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line. **Enable Pass Through FAX** checkbox enables the FAX tone detection and the G711 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line.

If both of these checkboxes are enabled, T.38 codec will be used as preferred codec for FAX transmit/receive and if not acceptable by the peer, G711 codec will be used instead.

Please Note: If both of these checkboxes are disabled, no FAX transmission to the peer’s voice mailbox will be possible. Checkboxes are applicable for FAX transmission/receipt over an IP network only.

Enable Pass Through Modem checkbox enables the modem tone detection and the G711 codec support for the data transmission from/to the modem attached to the line. During data transmission, Silence Suppression (see RTP Settings) and Echo Cancellation are being disabled on the line.

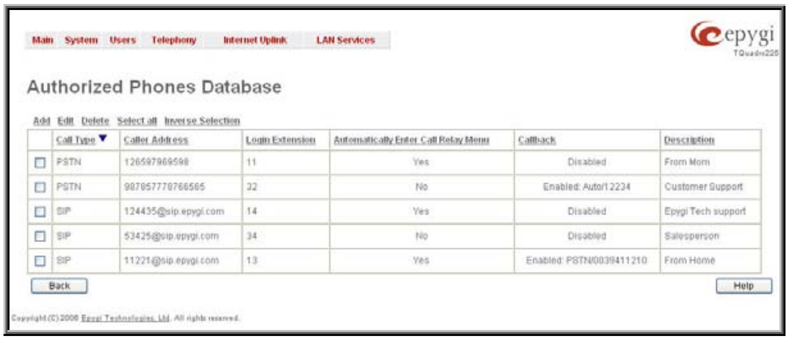
The **Force Self Codecs Preference for Inbound Calls** checkbox enables the usage of your own preferred codecs (if available on both peers) for the IP connection establishment on the extension.

Authorized Phones Database

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

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

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



Authorized Phones Database

	Call Type ▼	Caller Address	Login Extension	Automatically Enter Call Relay Menu	Callback	Description
□	PSTN	126597969598	11	Yes	Disabled	From Mom
□	PSTN	987857778766565	32	No	Enabled: Auto/12234	Customer Support
□	SIP	124435@sip.epygi.com	14	Yes	Disabled	Epygi Tech support
□	SIP	53425@sip.epygi.com	34	No	Disabled	Salesperson
□	SIP	11221@sip.epygi.com	13	Yes	Enabled: PSTN/0039411210	From Home

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-66: Authorized Phones Database

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

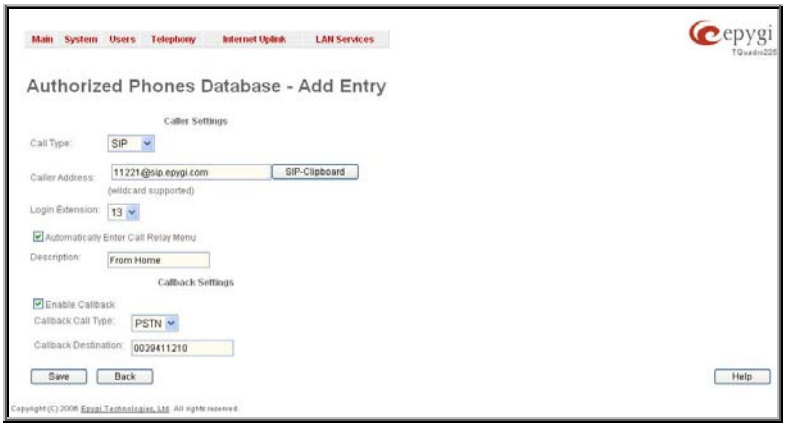
The **Add** functional button refers to the **Authorized Phones Database- Add Entry** page where new trusted users may be entered.

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

Caller Settings

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

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



Authorized Phones Database - Add Entry

Caller Settings

Call Type: SIP

Caller Address: 11221@sip.epygi.com

(wildcard supported)

Login Extension: 13

☑ Automatically Enter Call Relay Menu

Description: From Home

Callback Settings

☑ Enable Callback

Callback Call Type: PSTN

Callback Destination: 0039411210

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-67: Authorized Phones Database - Add Entry page

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

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

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

Callback Settings

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

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

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

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

To Add an Authorized phone to the database

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

To Delete an Authorized phone from the database

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

Call Back Services

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

Pre-Configured Call Back

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

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

Remote Call Back

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

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

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

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

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

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

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

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

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

Upload Universal Extension Recordings

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

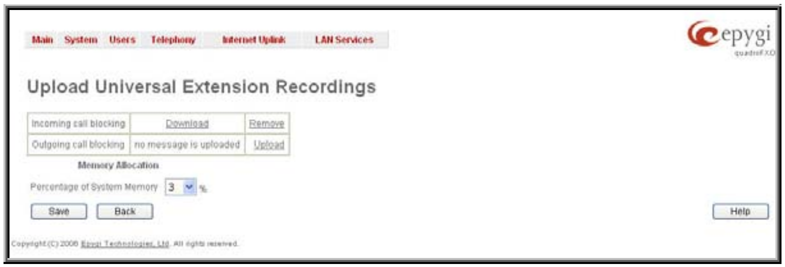
The following system messages can be uploaded from this page:

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

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

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

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



Upload Universal Extension Recordings

Incoming call blocking	Download	Remove
Outgoing call blocking	no message is uploaded	Upload

Memory Allocation

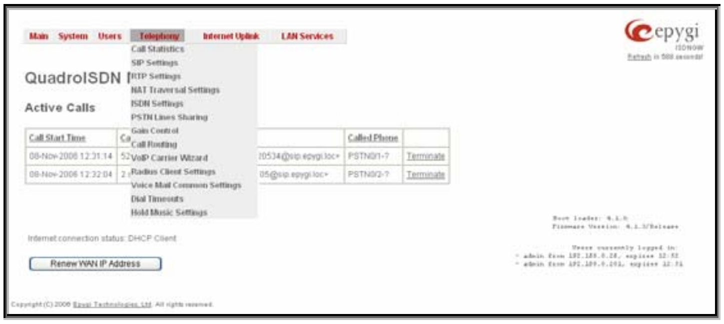
Percentage of System Memory 3 %

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-68: Upload Universal Extension Recordings page

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

Telephony Menu

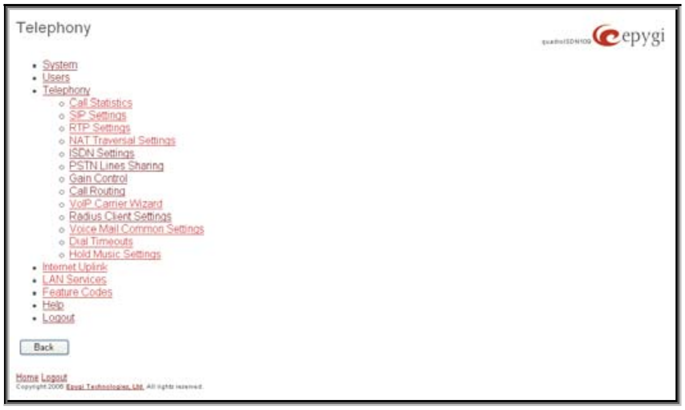


Call Start Time	Ca		Called Phone	
08-Nov-2006 12:31:14	52	20534@sip.epygi.loc>	PSTN0/1-7	Terminate
08-Nov-2006 12:32:04	2	05@sip.epygi.loc>	PSTN0/2-7	Terminate

Internet connection status: DHCP Client

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-69: Telephony Menu in Dynamo Theme



Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-70: Telephony Menu in Plain Theme

Call Statistics

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

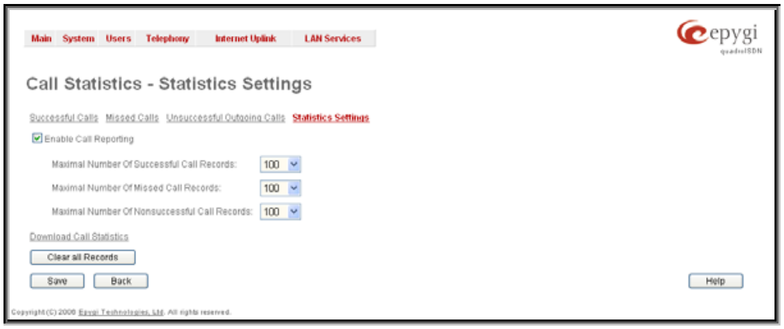
The **Statistics Settings** page offers the following input options:

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

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

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

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



Call Statistics - Statistics Settings

☑ Enable Call Reporting

Maximal Number Of Successful Call Records: 100

Maximal Number Of Missed Call Records: 100

Maximal Number Of Nonsuccessful Call Records: 100

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-71: Call Statistics Settings page

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

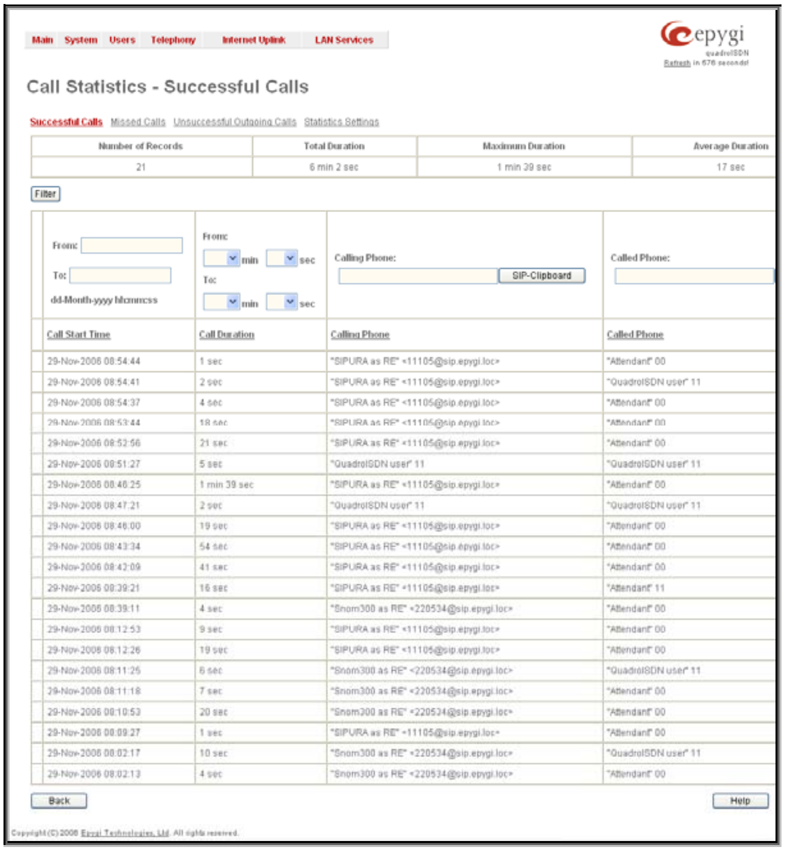
The **Call Statistics: Successful Calls, Missed Calls and Unsuccessful Outgoing Calls** pages consist of the general information on successful, missed and unsuccessful calls, search fields and the calls table. The search components are as follows:

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

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

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

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



Call Statistics - Successful Calls

Number of Records	Total Duration	Maximum Duration	Average Duration
21	6 min 2 sec	1 min 39 sec	17 sec

From:
To:
dd-Month-yyyy hh:mm:ss

From: min sec
To: min sec

Calling Phone:

Called Phone:

Call Start Time	Call Duration	Calling Phone	Called Phone
29-Nov-2006 08:54:44	1 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:54:41	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"QuadroISDN user" 11
29-Nov-2006 08:54:37	4 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:53:44	18 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:52:56	21 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:51:27	5 sec	"QuadroISDN user" 11	"QuadroISDN user" 11
29-Nov-2006 08:48:25	1 min 39 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:47:21	2 sec	"QuadroISDN user" 11	"QuadroISDN user" 11
29-Nov-2006 08:46:00	19 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:43:34	54 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:42:09	41 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:39:21	16 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 11
29-Nov-2006 08:39:11	4 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:12:53	9 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:12:26	19 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:11:25	6 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"QuadroISDN user" 11
29-Nov-2006 08:11:18	7 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:10:53	20 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:09:27	1 sec	"SIPURA as RE" <11105@sip.epygi.loc>	"Attendant" 00
29-Nov-2006 08:02:17	10 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"QuadroISDN user" 11
29-Nov-2006 08:02:13	4 sec	"Snom300 as RE" <220534@sip.epygi.loc>	"Attendant" 00

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-72: Call Statistics page

The **Network Details** column is only present in the **Successful Calls** table and provides brief information about the call quality and codecs used to receive and transmit packets. Clicking on the successful call details will open the RTP Statistics page where detailed information about the established call is provided. The **Call Detail** column is present only in the **Non Successful Calls** table and indicates the reason why the call was unsuccessful.

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

To Enable/Disable the Statistics

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

To Filter the Statistics

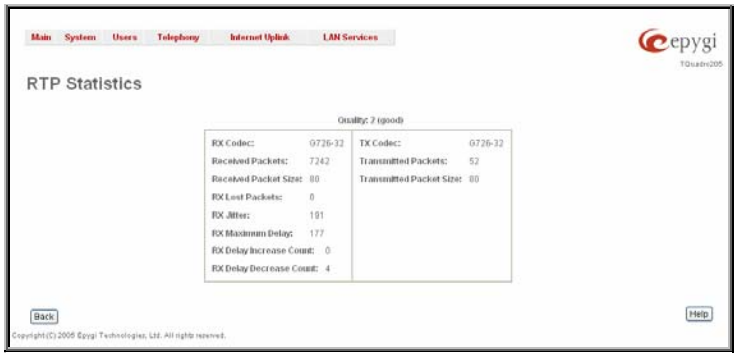
1. Enter the desired criteria fields.
2. Press the **Filter** button to search the call reports within the **Call Statistics** table.

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

To Reset the Statistics

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

RTP Statistics



RTP Statistics

Quality: 2 (good)

RX Codec:	G726-32	TX Codec:	G726-32
Received Packets:	7242	Transmitted Packets:	52
Received Packet Size:	80	Transmitted Packet Size:	80
RX Lost Packets:	0		
RX Jitter:	191		
RX Maximum Delay:	177		
RX Delay Increase Count:	0		
RX Delay Decrease Count:	4		

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-73: RTP Statistics page

The **RTP Statistics** page provides detailed information about the established call is provided.

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

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

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

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

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

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

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

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

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

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

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

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

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

Rx Maximum Delay = max V(i) / 8

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

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

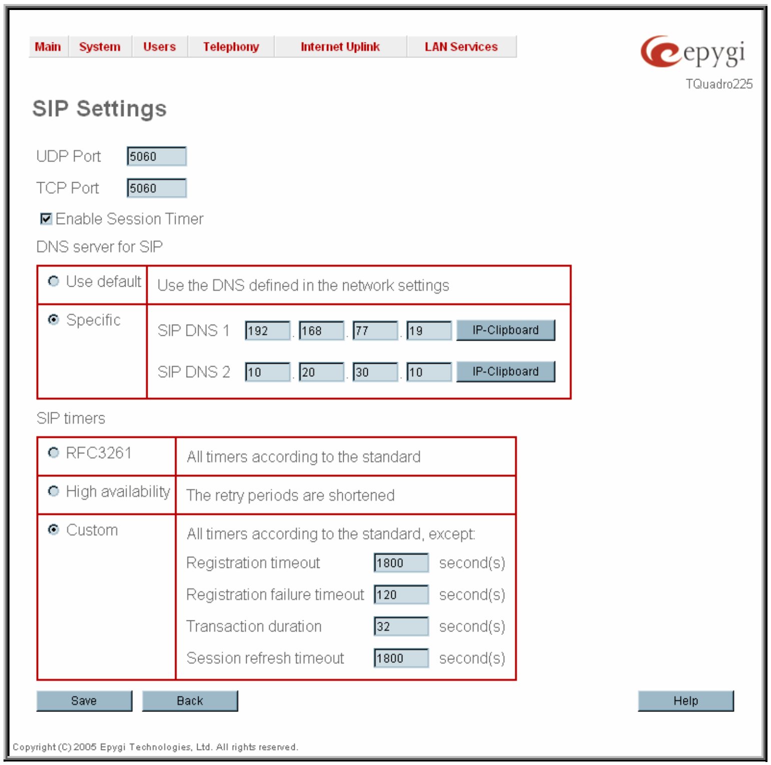
Please Note: RTP Statistics is logged only when at least one of the call endpoints is located on the Quadro. For example, it will not be logged when:

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

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

SIP Settings

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



SIP Settings

UDP Port 5060

TCP Port 5060

☑ Enable Session Timer

DNS server for SIP

○ Use default	Use the DNS defined in the network settings
● Specific	SIP DNS 1 192 . 168 . 77 . 19 IP-Clipboard SIP DNS 2 10 . 20 . 30 . 10 IP-Clipboard

SIP timers

○ RFC3261	All timers according to the standard
○ High availability	The retry periods are shortened
● Custom	All timers according to the standard, except: Registration timeout 1800 second(s) Registration failure timeout 120 second(s) Transaction duration 32 second(s) Session refresh timeout 1800 second(s)

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-74: SIP Settings page

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

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

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

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

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

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

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

- **RFC 3261** will apply standard SIP timers described in the corresponding specification.
- **High availability** will apply SIP timers to shorten the call establishment, registration confirmation and registration failure procedures. This selection provides more firmness to the SIP connection but increases the network traffic on the Quadro.
- **Custom** allows manually defining the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session refresh timeout** SIP timers (in seconds).

RTP Settings

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

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

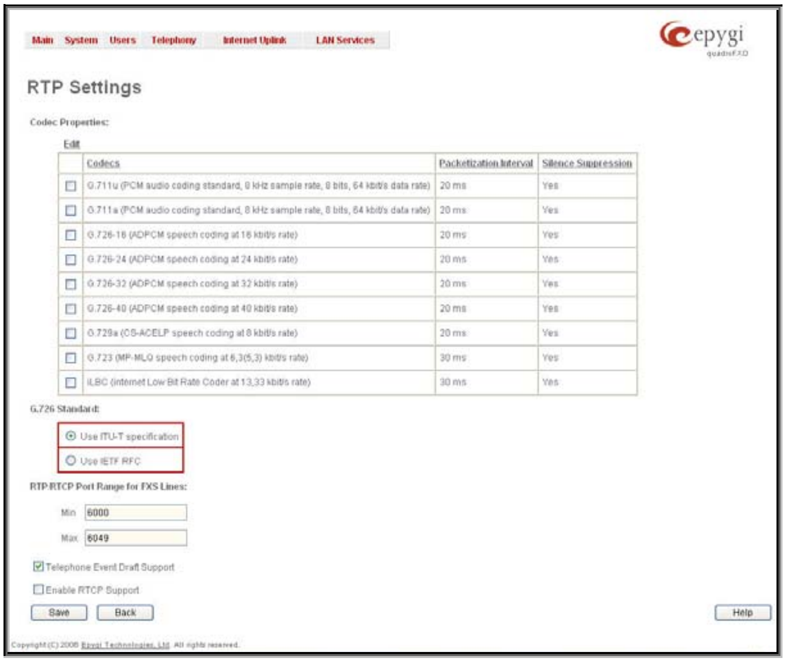
Edit opens the **Edit RTP Settings** page where the codec settings can be modified. To use **Edit**, only one codec may be selected at a time, otherwise the “One record should be selected” error message appears.

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

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

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

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



RTP Settings

Codec Properties:

Edit

	Codecs	Packetization Interval	Silence Suppression
□	G.711u (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)	20 ms	Yes
□	G.711a (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)	20 ms	Yes
□	G.726-16 (ADPCM speech coding at 16 kbit/s rate)	20 ms	Yes
□	G.726-24 (ADPCM speech coding at 24 kbit/s rate)	20 ms	Yes
□	G.726-32 (ADPCM speech coding at 32 kbit/s rate)	20 ms	Yes
□	G.726-40 (ADPCM speech coding at 40 kbit/s rate)	20 ms	Yes
□	G.729a (CS-ACELP speech coding at 8 kbit/s rate)	20 ms	Yes
□	G.723 (MP-MLQ speech coding at 6,3(5,3) kbit/s rate)	30 ms	Yes
□	iLBC (internet Low Bit Rate Coder at 13,33 kbit/s rate)	30 ms	Yes

G.726 Standard:

● Use ITU-T specification
○ Use IETF RFC

RTP/RTCP Port Range for FXS Lines:

Min 6000
Max 6049

☑ Telephone Event Draft Support
□ Enable RTCP Support

Copyright (C) 2008 Epygi Technologies, Ltd. All rights reserved.

Fig. II-75: RTP Settings page

RTP/RTCP Port Range for FXS Lines:

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

Since the specified maximum port has to be higher than the minimum port, the error message “Min port number should be less than max port number” will appear if this condition is not met. The port range must consist of digits only, otherwise the error “Incorrect Port Range: only Integer values allowed” will appear. The difference between Max and Min RTP ports should be 50 ports or less (according to the system’s capabilities) otherwise the corresponding warning appears. RTP/RTCP Port ranges cannot include the defined SIP UDP ports (see SIP Settings) otherwise an error message will appear.

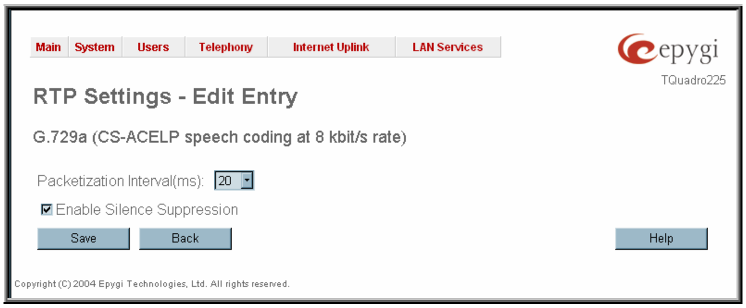
Telephone Event Draft Support enables telephony events transmission according to the draft-ietf-avt-rfc2833bis-04. The checkbox needs to be toggled if the SIP destination party phone or IVR has problems recognizing DTMFs generated by the Quadro.

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

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

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

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



RTP Settings - Edit Entry

G.729a (CS-ACELP speech coding at 8 kbit/s rate)

Packetization Interval(ms): 20

☑ Enable Silence Suppression

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-76: RTP Settings - Edit Entry

To Edit Codec Parameters

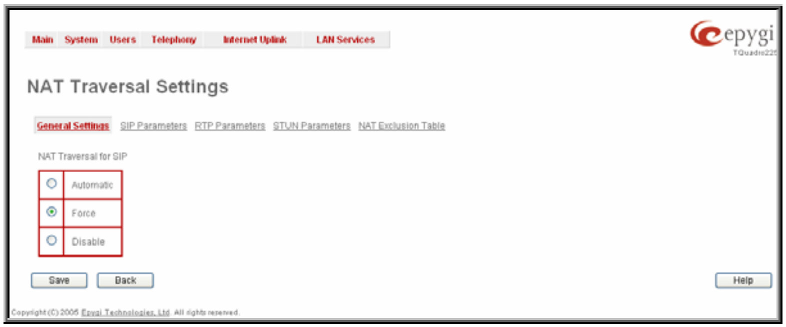
1. Select the codec from the **Codecs Table** that is to be edited.
2. Press the **Edit** button on the **RTP Settings** page. The **Edit Entry** page will appear in the browser window.
3. Change values in **Packetization Interval** and/or enable/disable **Silence Suppression**.
4. To save the codec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

NAT Traversal Settings

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

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

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



NAT Traversal Settings

NAT Traversal for SIP

○ Automatic
● Force
○ Disable

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-77: 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:

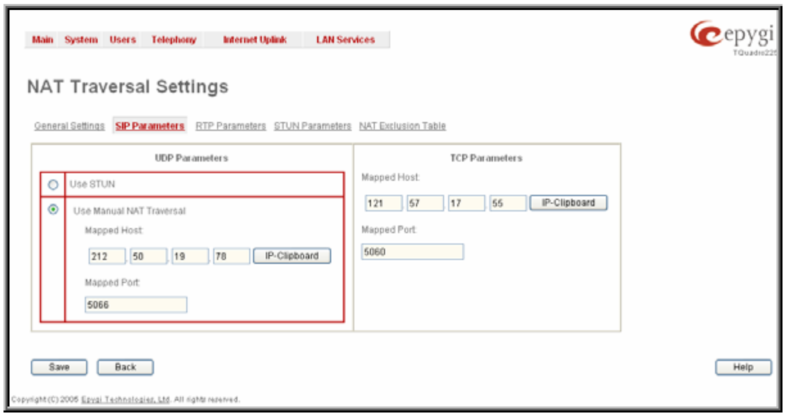
Mapped Host requires the IP address of the mapped host for SIP UDP traffic over NAT.

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.



NAT Traversal Settings

UDP Parameters

○ Use STUN
● Use Manual NAT Traversal

Mapped Host: 212 . 50 . 19 . 78

Mapped Port: 5066

TCP Parameters

Mapped Host: 121 . 57 . 17 . 55

Mapped Port: 5060

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-78: SIP Parameters page

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

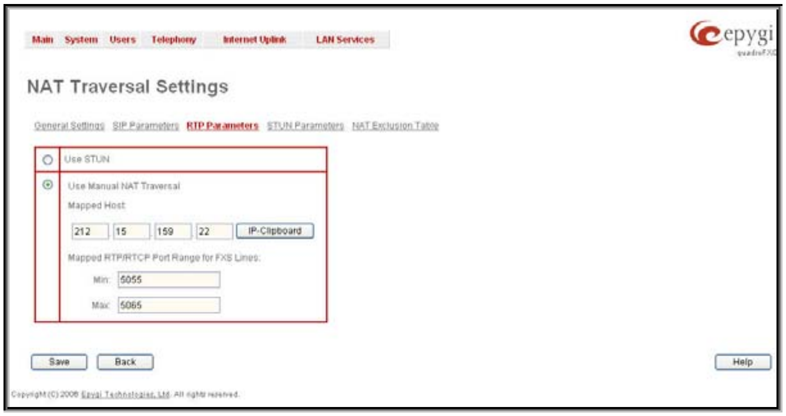
Manipulation radio buttons allow you to select the type of connection over NAT:

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

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

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

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



NAT Traversal Settings

○ Use STUN
● Use Manual NAT Traversal

Mapped Host: 212 . 15 . 159 . 22

Mapped RTP/RTCP Port Range for FXS Lines:

Min: 5055

Max: 5065

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-79: 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:

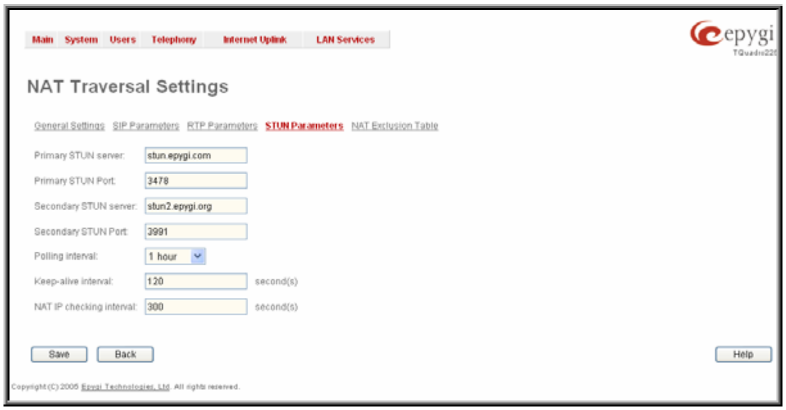
The **STUN Server** text field requires the STUN server’s hostname or IP address. The **STUN Port** text field requires the STUN server port number.

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.



NAT Traversal Settings

Primary STUN server: stun.epygi.com
Primary STUN Port: 3478
Secondary STUN server: stun2.epygi.org
Secondary STUN Port: 3991
Polling interval: 1 hour
Keep-alive interval: 120 second(s)
NAT IP checking interval: 300 second(s)

Fig. II-80: 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.

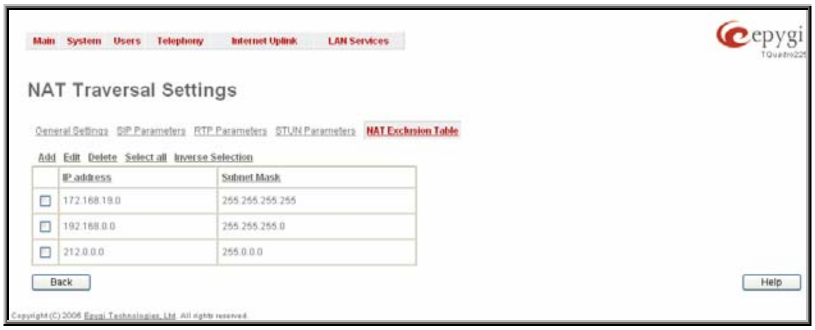
Each column heading in the table is a link. By clicking on the column heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

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.



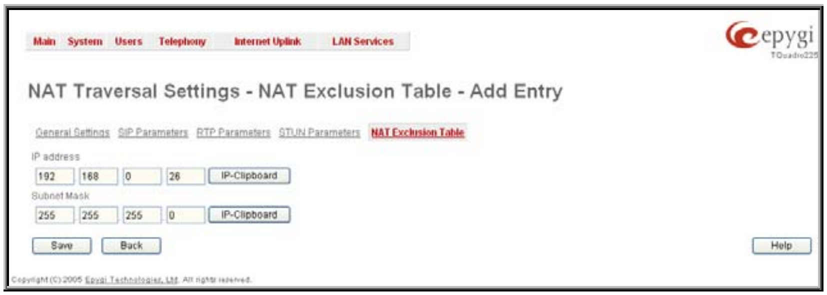
NAT Traversal Settings

	IP address	Subnet Mask
□	172.168.19.0	255.255.255.255
□	192.168.0.0	255.255.255.0
□	212.0.0.0	255.0.0.0

Fig. II-81: 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.



NAT Traversal Settings - NAT Exclusion Table - Add Entry

IP address: 192 168 0 26
Subnet Mask: 255 255 255 0

Fig. II-82: 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**.

ISDN Settings

The **Integrated Services Digital Network** (ISDN) is distinguished by digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. The ISDN Basic Rate Interface (BRI) service offers two B channels (voice transfer) and one D channel (signaling data transfer). The BRI B-channel service operates at 64 kbit/s and is meant to carry user data. The BRI D-channel service operates at 16 kbit/s and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances.

The **ISDN service** allows Quadro act as a user or as a network. If connected to a private PBX, the Quadro should be configured in the network mode. If an ISDN trunk from the CO (Central Office) is connected to the Quadro, it should be configured as a user. Quadro supports the MSN (Multiple Subscriber Number) service, i.e., it can be subscribed to multiple numbers from the CO, and two simultaneous calls can take place at a time.

The **ISDN Trunk Settings** page is used to configure the ISDN trunk and their signaling. There are 4 ISDN trunks available on the Quadro ISDN gateway.

This page offers the following input options:

The **Trunk Settings** table lists the available ISDN trunks on the Quadro and their settings (trunk name and interface types).

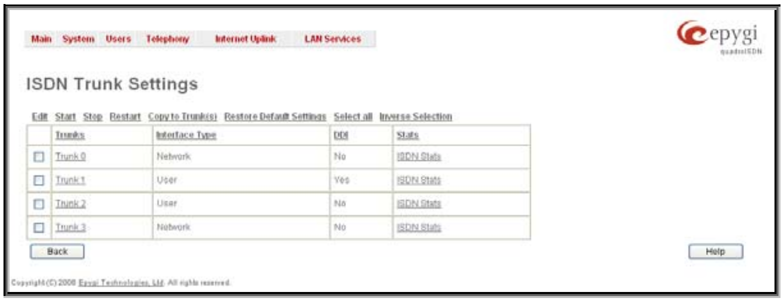
The **Edit** functional button opens the **Edit Entry** page where ISDN Trunk specific settings can be configured (see below).

The **Start** and **Stop** functional links are used to start/shutdown the selected ISDN trunk(s). When an ISDN trunk is in a shutdown state, ISDN calls cannot be placed or received.

The **Restart** functional link is used to bring channel(s) to the initial idle state on both sides. When applying one of these options, any active traffic on the channel(s) will be terminated.

The **Copy to Trunk(s)** functional link displays a page used to choose a trunk to which selected trunk’s settings should be copied to.

The **Restore Default Settings** functional link restores the default signaling settings of the selected ISDN trunk(s).



ISDN Trunk Settings

	Trunks	Interface Type	DDI	Stats
□	Trunk 0	Network	No	ISDN Stats
□	Trunk 1	User	Yes	ISDN Stats
□	Trunk 2	User	No	ISDN Stats
□	Trunk 3	Network	No	ISDN Stats

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-83: ISDN Settings page

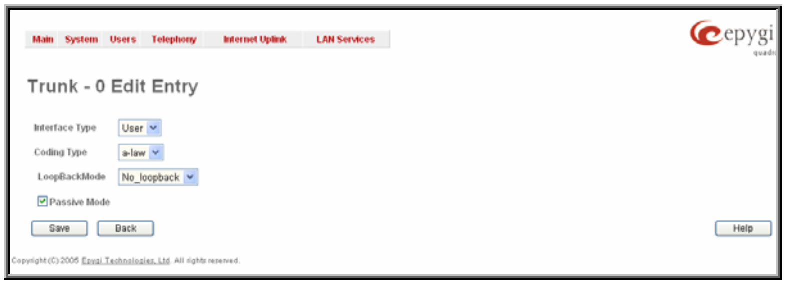
The **Edit Entry** page consists of the following components:

The **Interface Type** drop down list allows you to choose the ISDN trunk interface configuration. At present, only **User** interface is available on the Quadro.

The **Coding Type** drop down list allows you to select between **a-law** and **mu-law** coding types.

The **LoopBackMode** the loopback mode may be selected for trunk diagnostics purposes. When loopback is selected from this list, the B1 and B2 channels will be switched to the loopback mode, the D channels will remain operating normally and any incoming traffic towards the corresponding B1/B2 channels of the ISDN trunk will automatically be sent back to the traffic initiator.

The **Passive Mode** checkbox is used to leave the ISDN Layer1 connection in the Slave mode. When this checkbox is selected, Layer1 remains idle when calls are not available. When this checkbox is not selected, Quadro keeps its Layer1 always active.



Trunk - 0 Edit Entry

Interface Type: User

Coding Type: a-law

LoopBackMode: No_loopback

☑ Passive Mode

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-84: ISDN Settings - Edit page

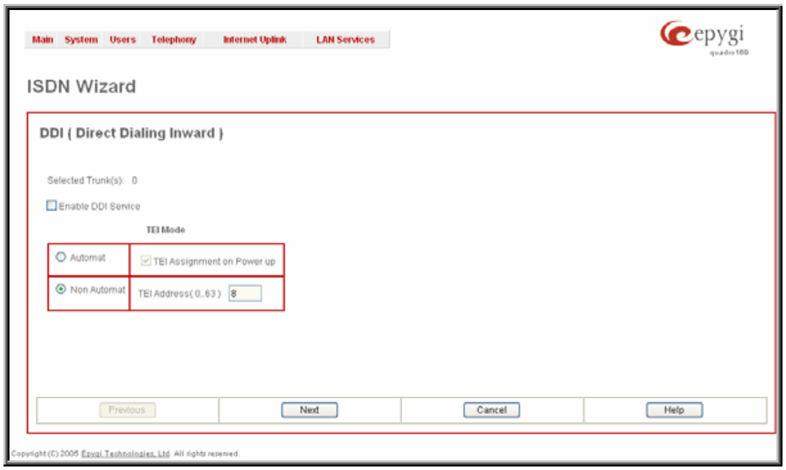
Clicking on the corresponding ISDN trunk will lead to the **ISDN wizard** where ISDN signaling settings can be configured. The **ISDN Wizard** consists of several pages.

The **ISDN Wizard – DDI (Direct Dialing Inward)** page offers the following components:

The **Enable DDI Service** checkbox activates the **DDI (Direct Dialing Inward) Service** on the trunk(s).

The **TEI Mode** manipulation radio buttons are only available when the DDI Service is disabled and they are used to select the TEI selection mode:

- The **Automat** mode requires ISDN connection to be established on the first available channel. If **TEI Assignment on Power up** checkbox is selected Quadro tries to get TEI value after Power UP, otherwise Quadro tries to get TEI value on incoming or outgoing calls.
- The **Non Automat** mode enables the TEI Address text field that requires the channel number (digit values from 0 to 63) for connection establishment between the CO and the ISDN client. In this mode, a private channel may be reserved for the connection. Both call partners need to specify the same channel in their settings.



ISDN Wizard

DDI (Direct Dialing Inward)

Selected Trunk(s): 0

□ Enable DDI Service

TEI Mode

○ Automat	☑ TEI Assignment on Power up
● Non Automat	TEI Address(0..63) 8

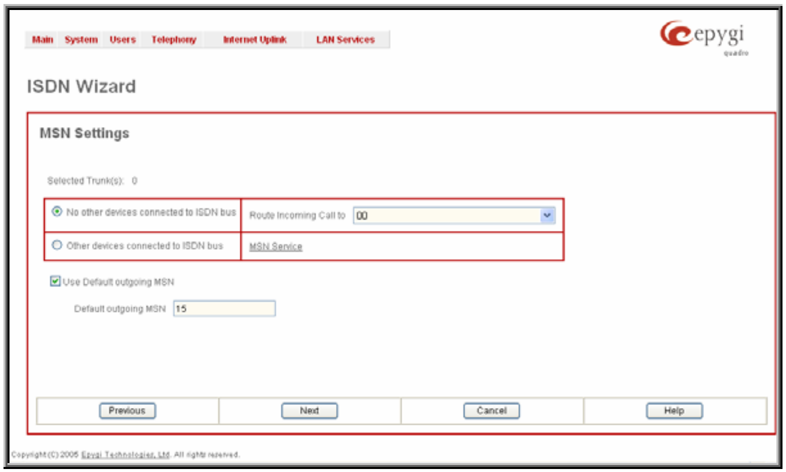
Fig. II-85: ISDN Wizard – DDI (Direct Dialing Inward) page

The **ISDN Wizard – MSN Settings** page offers the following components:

The manipulation radio buttons are present only for ISDN trunk acting in the user mode and when **DDI Service** is disabled from the previous page. This selection is used to choose whether or not other devices are connected to the ISDN bus. It also allows you to switch the MSN (Multiple Subscriber Number) service. This service offers the option of having multiple ISDN numbers provided by the CO (Central Office). It is used to route incoming calls to the Quadro extensions, to the Auto Attendant or routing agent (depending on the subscribed number the call was received on).

Selecting **No other devices are connected to ISDN bus** disables the MSN service on the Quadro and all incoming calls will be routed to the selected destination.

The **Route Incoming call to** drop down list is present only when the ISDN trunk is in the user mode and contains the Attendant, a routing agent with two types of call routing possibilities. It contains all the extensions of Quadro. It allows you to select the destination where the incoming calls should to be routed to. Choosing the **Routing** selection will request the caller to pass the authentication (if enabled) and will invite them to dial the number that will be parsed through the Call Routing Table. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without additional dialing.



ISDN Wizard

MSN Settings

Selected Trunk(s): 0

● No other devices connected to ISDN bus	Route Incoming Call to 00
○ Other devices connected to ISDN bus	MSN Service

☑ Use Default outgoing MSN

Default outgoing MSN 15

Fig. II-86: ISDN Wizard – MSN Settings

The **Other devices are connected to ISDN bus** selection enables the MSN service on the Quadro. It allows you to configure the incoming MSN table. The **MSN Service** link leads to the **MSN Service** pages where MSN numbers can be created and modified.

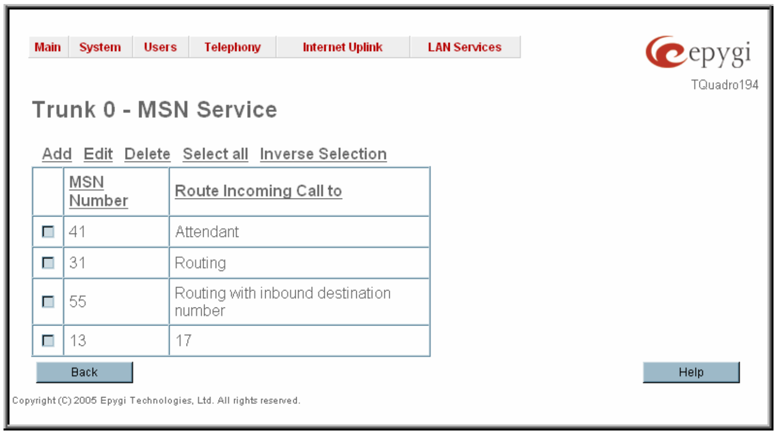
Please Note: It is recommended that you choose **Other devices are connected to ISDN bus** if there are several subscribed numbers and multiple ISDN devices within the network.

The **MSN Service** page lists all existing MSN numbers on the Quadro. It allows you to assign MSNs to the Quadro extensions, to the Auto Attendant, or to the routing client with two kinds of call routing possibilities, where incoming calls will be routed.

The **Add** functional button opens an **Add Entry** page where a new MSN number can be created. The field contains the following components:

The **MSN Number** text field requires the MSN number.

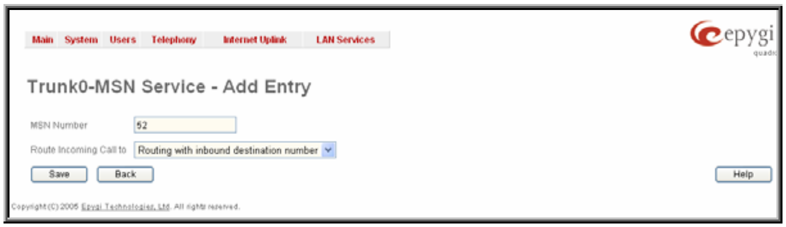
The **Route Incoming Call to** drop down list allows you to select the destination where the incoming call to the certain MSN number will be routed. Choosing the **Routing** selection will request the caller to pass the authentication (if enabled) and will invite them to dial the destination number to connect the user within the Quadro Network. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without any additional dialing.



Trunk 0 - MSN Service

	MSN Number	Route Incoming Call to
□	41	Attendant
□	31	Routing
□	55	Routing with inbound destination number
□	13	17

Fig. II-87: MSN Service page



Trunk0-MSN Service - Add Entry

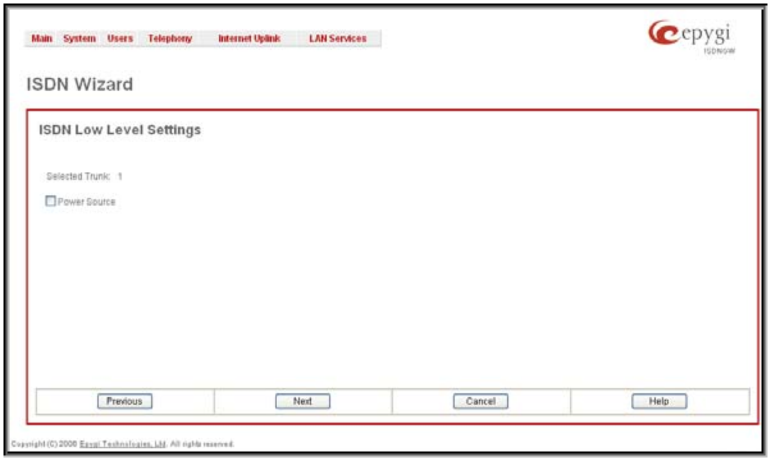
MSN Number: 52

Route Incoming Call to: Routing with inbound destination number

Fig. II-88: MSN Service – Add Entry page

Selecting **Use Default outgoing MSN** allows you to overwrite the source caller information with the one specified in the **Default outgoing MSN** text field when placing outgoing calls toward the CO. The **Default outgoing MSN** text field requires the Quadro identification number that should be registered and recognized at the CO for outgoing calls. If this checkbox is enabled but no value is defined in **Default outgoing MSN**, empty caller information will be sent to the CO. If this checkbox is disabled, the source caller information will be forwarded to the CO.

If the trunk is configured in the Network mode, the next page of the wizard will be the **ISDN Wizard** - **ISDN Low Level Settings** page, otherwise if the trunk is configured in the User mode, this page will be skipped and the next page will be the **ISDN Wizard** - **L2&L3 Settings** page.



ISDN Wizard

ISDN Low Level Settings

Selected Trunk: 1

□ Power Source

Fig. II-89: ISDN Wizard – ISDN Low Level Settings

The **ISDN Wizard - ISDN Low Level Settings** page offers a **Power Source** selection option. When this option is selected, the QuadroISDN device will act as a power supply for the ISDN phones connected to it. Otherwise when this checkbox is not selected, ISDN phones should have their own power supplies.

Please Note: This checkbox should be always disabled when the ISDN gateway has a PBX or Telecom connected.

The **ISDN Wizard - L2&L3 Settings** page offers the following components:

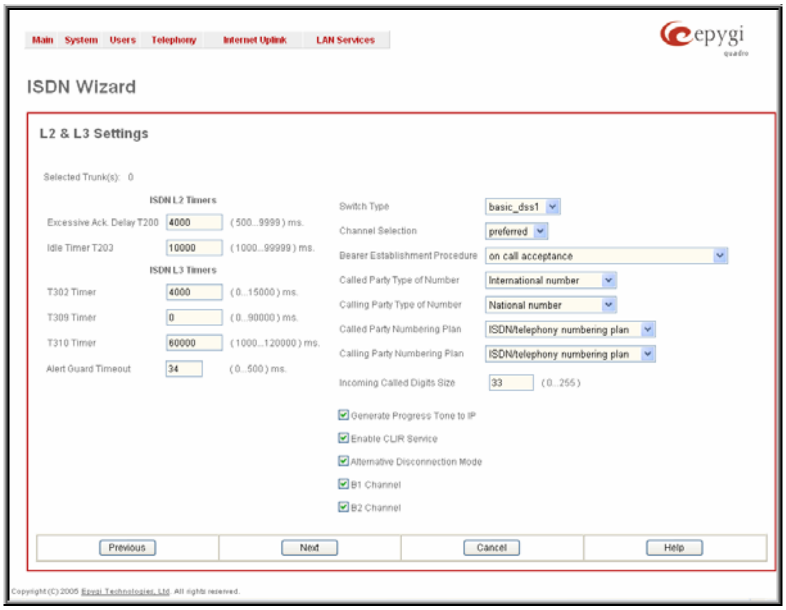
Two groups of timers need to be provided. These settings are adjusted according to the Service Provider requirements.

ISDN L2 Timers:

- **Excessive Ack. Delay T200** configures the period in milliseconds (numeric values from 500 to 9999) between the transmitted signaling packet and its acknowledgement received.
- **Idle Timer T203** configures the period in milliseconds (numeric values from 1000 to 99999) for the ISDN client idle timeout.

ISDN L3 Timers:

- The **T302 Timer** text field requires the value for the T302 timer in milliseconds (digit values from 0 to 15000). It indicates that the time frame system is waiting for a digit to be dialed. When the timer expires, it initiates the call.
- **T309 Timer** requires the value for the T309 timer in milliseconds (numeric values from 0 to 90000). It is responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is zero (0), the T309 timer will be disabled.
- **T310 Timer** requires the value for the T310 timer in milliseconds (numeric values from 1000 to 120000). It is responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) has not yet arrived.
- **Alert Guard Timeout** requires the value for the Alert Guard Timer in milliseconds (numeric values from 0 to 500) between CALL PROC and ALERT messages. Alert Guard Timer it is used when Quadro is connected to a slow ISDN-PBX.



ISDN Wizard

L2 & L3 Settings

Selected Trunk(s): 0

ISDN L2 Timers

Excessive Ack. Delay T200: 4000 (500...9999) ms.

Idle Timer T203: 10000 (1000...99999) ms.

ISDN L3 Timers

T302 Timer: 4000 (0...15000) ms.

T309 Timer: 0 (0...90000) ms.

T310 Timer: 60000 (1000...120000) ms.

Alert Guard Timeout: 34 (0...500) ms.

Switch Type: basic_dss1

Channel Selection: preferred

Bearer Establishment Procedure: on call acceptance

Called Party Type of Number: International number

Calling Party Type of Number: National number

Called Party Numbering Plan: ISDN/telephony numbering plan

Calling Party Numbering Plan: ISDN/telephony numbering plan

Incoming Called Digits Size: 33 (0...255)

☑ Generate Progress Tone to IP

☑ Enable CLIR Service

☑ Alternative Disconnection Mode

☑ B1 Channel

☑ B2 Channel

Fig. II-90: ISDN Wizard – L2&L3 Settings

Recommended values are:
- fast connection (0ms);
- normal (150ms), default;
- slow ISDN-PBX (350ms);
- very slow ISDN-PBX (500ms).

Switch Type is another configuration parameter that depends on the Service Provider.

Channel Selection is used to select between the **Preferred** and **Exclusive** B channel selection methods. For **Preferred** channel selection, the CO answers to the call request by the first available timeslot. With the **Exclusive** channel selection, the CO should feedback only by the timeslot used for the call request.

The **Bearer Establishment Procedure** drop down list allows selecting the session initiation method on the B channel. One of the following options can be selected for the transmission path completion prior to receipt of a call acceptance indication:

- on channel negotiation at the destination interface
- on progress indication with in-band information
- on call acceptance

The **Calling Party Type of Number** drop down list allows you to select the type identifying the origin of call.

The **Called Party Type of Number** drop down list allows you to select the type identifying the sub-address of the called party of the call.

The **Called Party Numbering Plan** and **Calling Party Numbering Plan** drop down lists correspondingly indicate the numbering plan of the called party's and calling party's number.

The **Incoming Called Digits Size** text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When this field has a “0” value, the system uses either the timeout defined in the T302 field or the **Sending Complete Information element** messages to establish a call. Independent on the value in this field, **Sending Complete Information element** and the pound sign always result in call establishment.

The **Generate Progress tone on IP** checkbox selection will generate the progress tone to IP.

Enable CLIR Service checkbox selection enables Calling Line Identification Restriction (CLIR) service which displays the incoming caller ID only if Presentation Indication is allowed on the remote side. Otherwise, if CLIR service is disabled, caller ID will be unconditionally displayed.

When the **Alternative Disconnection Mode** checkbox is not selected, Quadro will disconnect the call as soon as the disconnect message has been received from the peer. When the checkbox is selected, Quadro’s user may hear a busy tone when peer has been disconnected.

The **B1 Channel** and **B2 Channel** checkboxes enables/disables timeslots for voice transfer. Disabling the timeslot will prevent both incoming and outgoing calls.

Clicking on the **ISDN Stats** link will open the **ISDN Status** page that displays ISDN traffic statistics on the corresponding ISDN trunk. The **ISDN Stats** link is displayed for every active trunk on the board and refers to the page where ISDN trunk and traffic statistics can be viewed.

The **ISDN Trunk Status** page provides the following information about the selected trunk state:

Link displays the ISDN link state: **up** or **down**.

Frame Synchronization displays the signal synchronization state in the trunk: **Yes** or **No**.

HDLC Receive shows the number of packets received in HDLC (High-level Data Link Control) format.

HDLC CRC Error shows the number of packets received with CRC (Cyclical Redundancy Check) errors.

HDLC Packet Abort displays the number of received aborted packets.

HDLC Transmit displays the number of packets transmitted in HDLC format.

HDLC Octet Count displays the number of error packets received in HDLC format.

The following **SDN BRI Layer 2** statistics are displayed for received and transmitted packets:

TEI value shows the actual TEI value.

L2 State shows the actual BRI L2 state.

Information Frame shows the number of signaling packets for call initiation and termination.

Receive Ready displays the number of controlling packets while the ISDN link is up.

Receive Not Ready displays the number of controlling packets in case of inability to accept calls by destination.

SABME shows the number of packets upon connection establishment.

Disconnected Mode shows the number of packets when the connection is being disconnected.

Disconnect shows the number of packets upon connection termination.

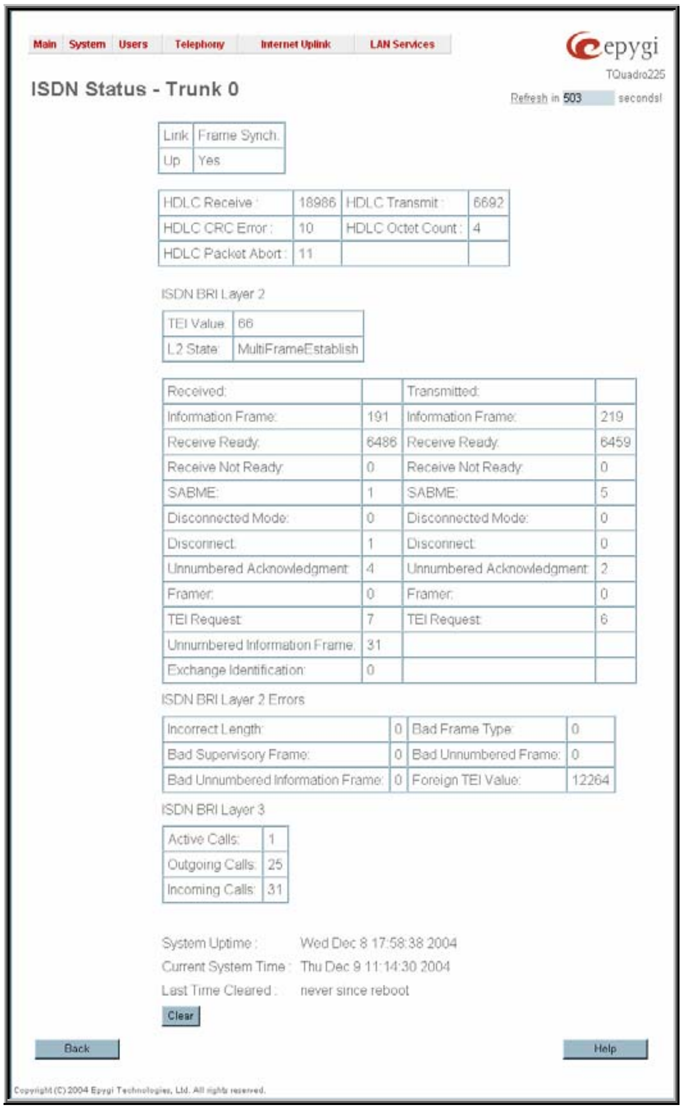
Unnumbered Acknowledgement shows the number of packets upon accepting connection establishment/termination.

Framer shows the number of packets as a result of an error condition.

TEI Request shows the number of packets containing TEI (Terminal Endpoint Identifier) to initiate subscription of the device in the network.

Unnumbered Information Frame shows the number of broadcast signaling packets received for call initiation and termination.

Exchange Identification shows the number of received packets containing connection management settings.



ISDN Status - Trunk 0

Refresh in 503 seconds!

Link	Frame Synch.
Up	Yes

HDLC Receive :	18986	HDLC Transmit :	6692
HDLC CRC Error :	10	HDLC Octet Count :	4
HDLC Packet Abort :	11		

ISDN BRI Layer 2

TEI Value:	66
L2 State:	MultiFrameEstablish

Received:		Transmitted:	
Information Frame:	191	Information Frame:	219
Receive Ready:	6486	Receive Ready:	6459
Receive Not Ready:	0	Receive Not Ready:	0
SABME:	1	SABME:	5
Disconnected Mode:	0	Disconnected Mode:	0
Disconnect:	1	Disconnect:	0
Unnumbered Acknowledgment:	4	Unnumbered Acknowledgment:	2
Framer:	0	Framer:	0
TEI Request:	7	TEI Request:	6
Unnumbered Information Frame:	31		
Exchange Identification:	0		

ISDN BRI Layer 2 Errors

Incorrect Length:	0	Bad Frame Type:	0
Bad Supervisory Frame:	0	Bad Unnumbered Frame:	0
Bad Unnumbered Information Frame:	0	Foreign TEI Value:	12264

ISDN BRI Layer 3

Active Calls:	1
Outgoing Calls:	25
Incoming Calls:	31

System Uptime : Wed Dec 8 17:58:38 2004
Current System Time : Thu Dec 9 11:14:30 2004
Last Time Cleared : never since reboot

Clear

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-91: ISDN Trunk Status page

ISDN BRI Layer 2 Errors statistics:

Incorrect Length shows the number of packets with an incorrect length.

Bad Supervisory Frame shows the number of packets with an incorrect supervisory header.

Bad Unnumbered Information Frame shows the number of packets with an incorrect unnumbered information frame header.

Bad Frame Type shows the number of packets with a bad frame type.

Bad Unnumbered Frame shows the number of packets with an incorrect unnumbered acknowledgement frame header.

Foreign TEI Value shows the number of packets with a bad or foreign TEI (Terminal Endpoint Identifier) value.

ISDN BRI Layer 3 statistics:

Active Calls shows the number of currently active calls in the selected trunk.

Outgoing Calls shows the number of all outgoing calls in the selected trunk.

Incoming Calls shows the number of all incoming calls in the selected trunk.

ISDN trunk statistics are not displayed on this page at first, but the page is automatically refreshed every 10 minutes. Statistics collected from that time, as well as the last resetting of the counter, will be displayed there. **System Uptime**, **Current System Time** and **Last Time Cleared** (last time ISDN statistics has been cleared) are displayed at the bottom of the page.

To reset the statistics counters press the **Clear** button.

PSTN Lines Sharing

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

When sharing mode is enabled, the ISDN Settings page becomes read-only on QuadroISDN and corresponding routing patterns are automatically created in the Call Routing table.

- The configuration of all ISDN trunks on the QuadroISDN will become transparent to Quadro IP PBX upon enabling the sharing mode.
- Independent of the configuration on the QuadroISDN, the incoming calls on all shared ISDN trunk will be automatically routed to the default Auto Attendant (00) once ISDN sharing is activated. Occasionally, routed destinations can be then changed on Quadro IP PBX.
- Any changes applied to the configuration of shared ISDN lines on the Quadro IP PBX will be automatically reflected in the **ISDN Settings** page and **Call Routing** table on the QuadroISDN.

PSTN Lines Sharing page consists of the following components:

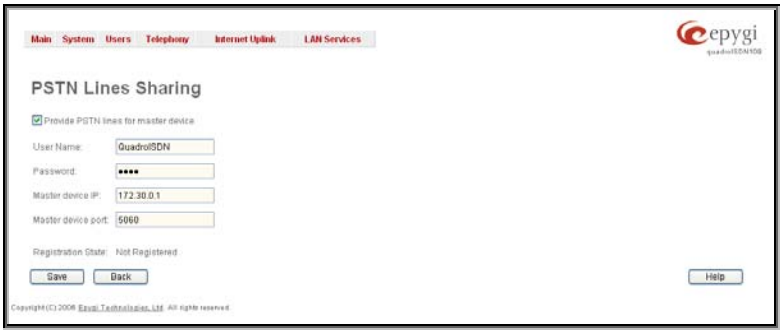
The **Provide PSTN lines for master device** checkbox is used to share the existing ISDN lines to the remote Quadro.

Username and **Password** text fields are used to enter the identification parameters for the authentication on the remote Quadro IP PBX. In its turn, these authentication settings should be added in the **Authorization Parameters** table on the master Quadro IP PBX.

Master device IP text field requires the IP address of the master Quadro current ISDN trunks will be shared for.

Master device port text field requires the port number of the master Quadro current ISDN trunks will be shared for.

Registration State and **Registration Date/Time** fields indicate read-only information about the last successful registration on the master Quadro (i.e. when authentication was successful), its state and the registration date/time.



PSTN Lines Sharing

☑ Provide PSTN lines for master device

User Name: QuadroISDN

Password: ••••

Master device IP: 172.30.0.1

Master device port: 5060

Registration State: Not Registered

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-92: PSTN Lines Sharing page

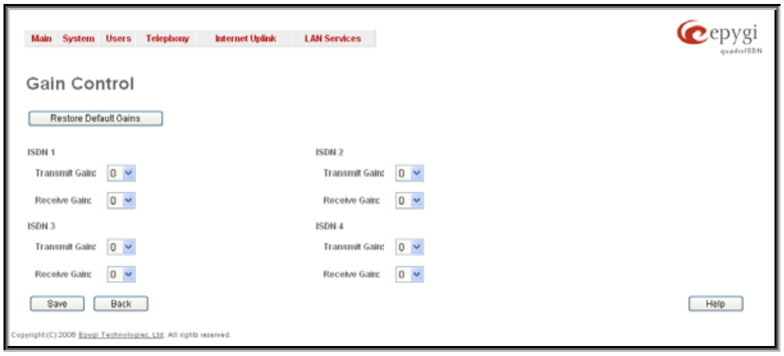
Gain Control

The **Gain Control** settings are used to define transmit and receive gains. For ISDN lines, **Transmit Gain** defines the level of voice transmitted from Quadro to the PSTN network and **Receive Gain** defines the volume of voice received by Quadro from the PSTN network.

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

Please Note: If the gain control has been configured incorrectly, DTMF digits may not be properly recognized. Gain control settings are strictly dependent on the location (country) of Quadro and the phone type.

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



Gain Control

ISDN 1

Transmit Gain: 0

Receive Gain: 0

ISDN 2

Transmit Gain: 0

Receive Gain: 0

ISDN 3

Transmit Gain: 0

Receive Gain: 0

ISDN 4

Transmit Gain: 0

Receive Gain: 0

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

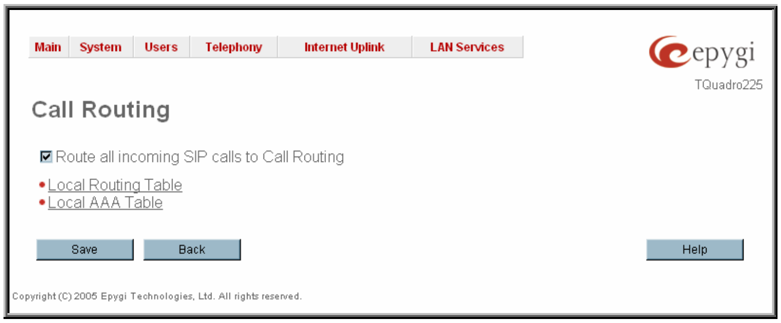
Fig. II-93: Gain Control page

Call Routing

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

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

- The **Route all incoming SIP calls to Call Routing** checkbox is used to route ALL incoming SIP calls (whether or not the pattern matches the extension's SIP registration username) to the Call Routing table. Digits will not be stripped in this case.
- The **Call Routing Table** link leads to the **Call Routing** table where routing patterns may be manually defined.
- The **Local AAA Table** link leads to the page where local AAA (Authentication, Authorization, and Accounting) database can be managed.

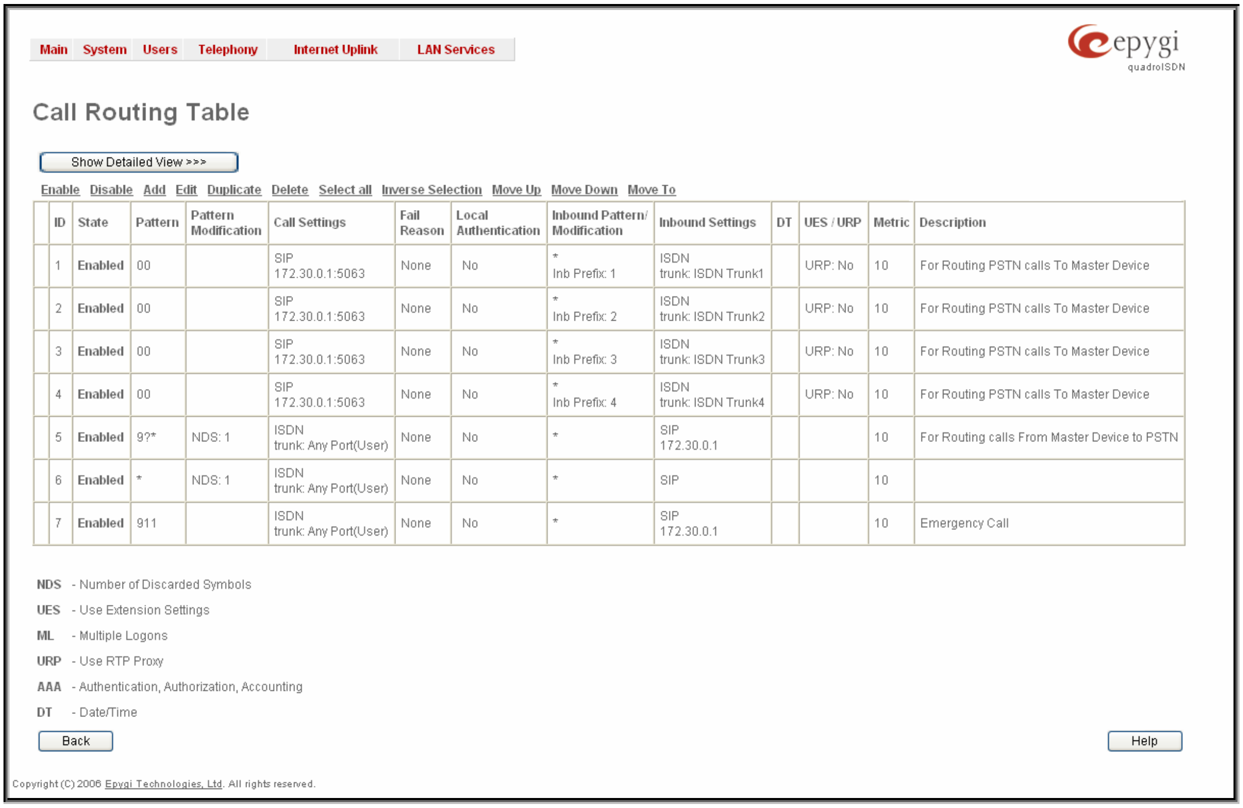


Call Routing

☑ Route all incoming SIP calls to Call Routing

- Local Routing Table
- Local AAA Table

Fig. II-94: Call Routing page



Call Routing Table

	ID	State	Pattern	Pattern Modification	Call Settings	Fail Reason	Local Authentication	Inbound Pattern/ Modification	Inbound Settings	DT	UES / URP	Metric	Description
	1	Enabled	00		SIP 172.30.0.1:5063	None	No	* Inb Prefix: 1	ISDN trunk: ISDN Trunk1		URP: No	10	For Routing PSTN calls To Master Device
	2	Enabled	00		SIP 172.30.0.1:5063	None	No	* Inb Prefix: 2	ISDN trunk: ISDN Trunk2		URP: No	10	For Routing PSTN calls To Master Device
	3	Enabled	00		SIP 172.30.0.1:5063	None	No	* Inb Prefix: 3	ISDN trunk: ISDN Trunk3		URP: No	10	For Routing PSTN calls To Master Device
	4	Enabled	00		SIP 172.30.0.1:5063	None	No	* Inb Prefix: 4	ISDN trunk: ISDN Trunk4		URP: No	10	For Routing PSTN calls To Master Device
	5	Enabled	9?*	NDS: 1	ISDN trunk: Any Port(User)	None	No	*	SIP 172.30.0.1			10	For Routing calls From Master Device to PSTN
	6	Enabled	*	NDS: 1	ISDN trunk: Any Port(User)	None	No	*	SIP			10	
	7	Enabled	911		ISDN trunk: Any Port(User)	None	No	*	SIP 172.30.0.1			10	Emergency Call

NDS - Number of Discarded Symbols
UES - Use Extension Settings
ML - Multiple Logons
URP - Use RTP Proxy
AAA - Authentication, Authorization, Accounting
DT - Date/Time

Fig. II-95: Call Routing table

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

The **Call Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and inbound caller settings, RTP Proxy and Date/Time period settings, metric and description), as well as automatically created and undeletable patterns created from the System Configuration Wizard. If the ISDN trunk settings (ISDN interface type, signaling type, etc.) have been changed after defining the corresponding route, **invalid** is displayed next to the ISDN routing pattern. Invalid ISDN patterns will not be allowed.

The alternating **See Detailed View** and **Show Brief View** buttons are used to display entries in the Call Routing table in detailed and brief views correspondingly. The brief view displays the most important settings of the routing rules. The detailed view displays all settings of the routing rules as they are configured in the Call Routing Wizard (see below).

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

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

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

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

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

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

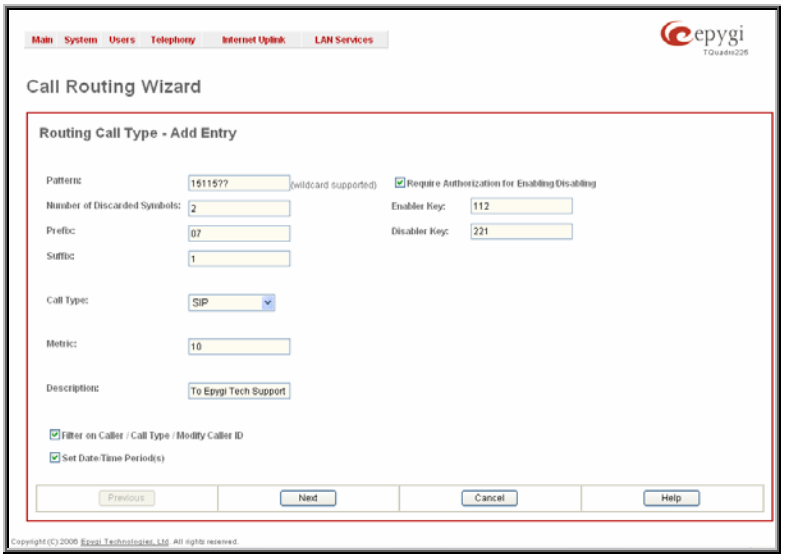
Pattern requires entering the routing pattern's identification. To make a specified call, the appropriate routing pattern should be dialed. Wildcards are allowed here (see chapter Entering a SIP Addresses correctly). '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers, '!' 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. The following tags can be used for this field:

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



Call Routing Wizard

Routing Call Type - Add Entry

Pattern: 151157? (wildcard supported)
☑ Require Authorization for Enabling/Disabling
Number of Discarded Symbols: 2
Enabler Key: 112
Prefix: 07
Disabler Key: 221
Suffix: 1
Call Type: SIP
Metric: 10
Description: To Epygi Tech Support
☑ Filter on Caller / Call Type / Modify Caller ID
☑ Set Date/Time Period(s)

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-96: Call Routing Wizard - page 1

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

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

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

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

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

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

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

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

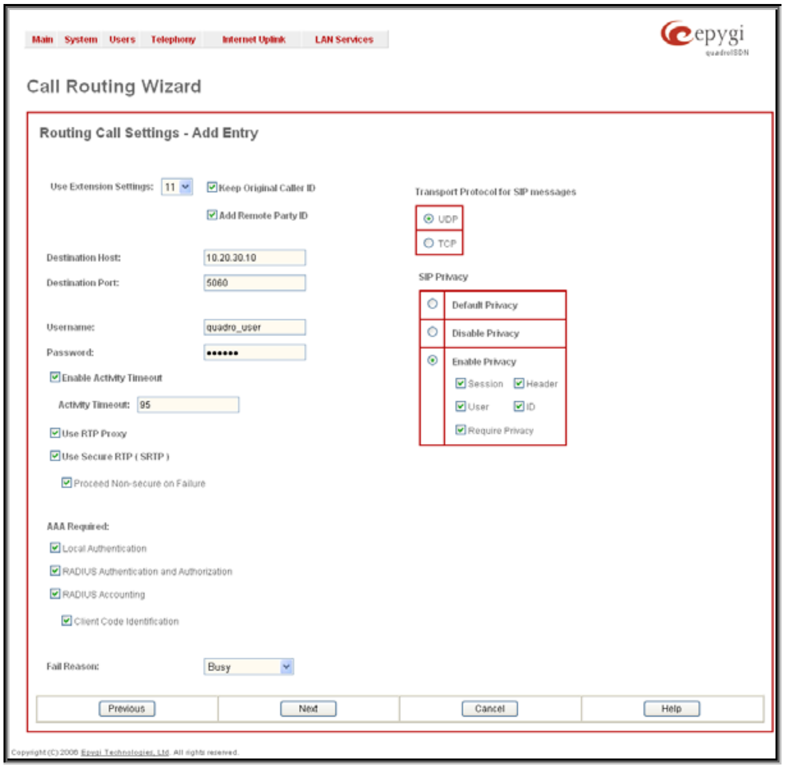
Destination Host requires the IP address or the host name of the destination (for a direct call) or the SIP server (for calls through the SIP server).

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.

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

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



Call Routing Wizard

Routing Call Settings - Add Entry

Use Extension Settings: 11 ☑ Keep Original Caller ID

☑ Add Remote Party ID

Destination Host: 10.20.30.10

Destination Port: 5060

Username: quadro_user

Password: ••••••

☑ Enable Activity Timeout

Activity Timeout: 95

☑ Use RTP Proxy

☑ Use Secure RTP (SRTP)

☑ Proceed Non-secure on Failure

AAA Required:

☑ Local Authentication

☑ RADIUS Authentication and Authorization

☑ RADIUS Accounting

☑ Client Code Identification

Fail Reason: Busy

Transport Protocol for SIP messages

● UDP

○ TCP

SIP Privacy

○ Default Privacy

○ Disable Privacy

● Enable Privacy

☑ Session ☑ Header

☑ User ☑ ID

☑ Require Privacy

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-97: Call Routing Wizard - page 2

The **Multiple Logons (ML)** checkbox is only available for the IP-PSTN call type and allows/denies multiple logon to the public SIP server with the same username at the same time.

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

Use Secure RTP (SRTP) checkbox is available for **SIP** and **IP-PSTN** call types and is used to encrypt RTP streams outgoing from the Quadro. This selection enables **Proceed Non-secure on Failure** checkbox. When the **Proceed Non-secure on Failure** checkbox is also selected, the non-secure RTP streams transmission will be allowed even when **Use Secure RTP (SRTP)** checkbox is selected but the peer side does not support the SRTP. Otherwise, when **Proceed Non-secure on Failure** checkbox is not selected and the peer side does not support SRTP, the call will not be established.

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

- **Local Authentication** – with this checkbox selected, callers will need to pass authentication through the Local AAA table (see below) when dialing the current pattern.
- **RADIUS Authentication and Authorization** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, callers will need to pass the authentication through RADIUS server (see above) when dialing the current pattern.
- **RADIUS Accounting** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, authentication will not take place, but a caller identifying a CDR (call detail report) will be sent to the RADIUS server. This checkbox selection enables accounting on the RADIUS for a certain call. This selection enables the **Client Code Identification** checkbox which is used to activate/deactivate the code identification on the RADIUS server. When the **Client Code Identification** checkbox is selected, caller may optionally dial an identity code at the end of the corresponding route. To make an identified call, caller should dial **Routing Number + * + Identity Code**. Here, **Identity Code** is an arbitrary digit combination used to identify the corresponding routing rule. Identity Code can be used to identify certain called destinations. This will allow to search the calls by the certain identity code criteria on the RADIUS server (for example, for further billing calculation purposes).

  If the authentication is configured based on the caller’s address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.

The **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:

- **Cannot Establish Connection** – this failure reason is only available for ISDN calls and indicates cases when a connection cannot be established.

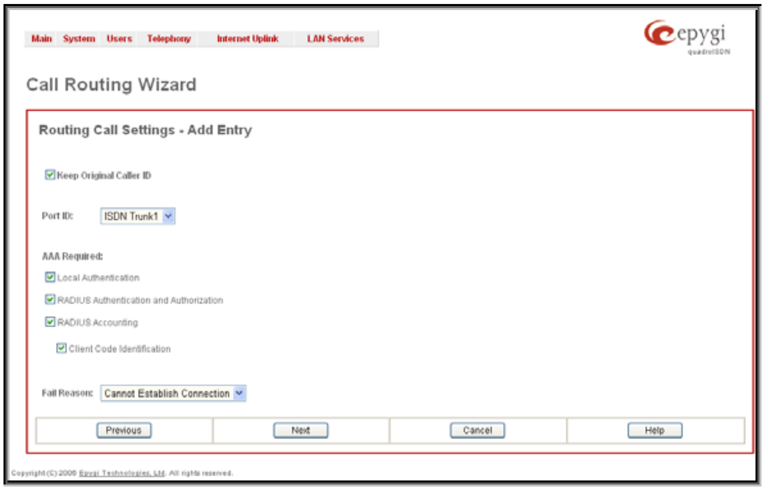
- **Wrong Number** – available for PBX, SIP and IP-PSTN call types and indicates cases when the dialed number is wrong.
- **Busy** - available for PBX, SIP and IP-PSTN call types and indicates cases when the dialed destination is busy.
- **Network Failure** - available for SIP and IP-PSTN call types and indicates cases of system overload, network failure or a timeout expiration occurred.
- **Other** - available for SIP and IP-PSTN call types and indicates cases of authorization, negotiation, not supported, request rejected or other unknown errors occur.
- **System Failure** - available for SIP and IP-PSTN call types and 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.



Call Routing Wizard

Routing Call Settings - Add Entry

☑ Keep Original Caller ID

Port ID: ISDN Trunk1

AAA Required:

☑ Local Authentication

☑ RADIUS Authentication and Authorization

☑ RADIUS Accounting

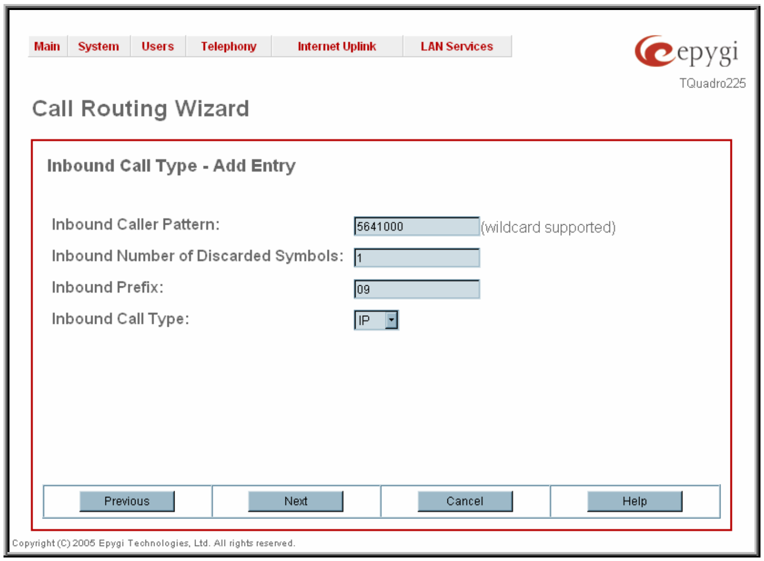
☑ Client Code Identification

Fail Reason: Cannot Establish Connection

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-98: Call Routing Wizard - page 3 for ISDN call type

The **Port ID** drop down list is present for ISDN call types and contains ISDN trunks. **Any Port** selection allows to route calls via the first available ISDN trunk.



Call Routing Wizard

Inbound Call Type - Add Entry

Inbound Caller Pattern: 5641000 (wildcard supported)

Inbound Number of Discarded Symbols: 1

Inbound Prefix: 09

Inbound Call Type: IP

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-99: Call Routing Wizard - page 3

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

The **Inbound Caller Pattern** field requires the caller’s address where the current route will be applied. Alphanumerics and any characters supported in the SIP username are allowed for this field. Wildcards are allowed here (see chapter Entering a SIP Addresses correctly). '[' , ']' , ',', '-', ‘{‘, ‘}’ are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified pattern; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified pattern.

The **Number of Discarded Symbols (NDS)** text field requires the number of digits that should be discarded from the beginning of the **Inbound Caller Pattern**. The field should be empty if digits do not need to be discarded. Only numerics are allowed for this field, otherwise the error message “Error: Number of Discarded Symbols is incorrect - digits allowed only” will appear.

The **Inbound Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Inbound Caller Pattern** instead of the discarded digits. (For example, if the routing pattern is 12345, the Number of Discarded Symbols is two, and the prefix digits are 909, the final phone number will be 909345.) Wildcards are allowed here (see chapter Entering a SIP Addresses correctly).
The **Inbound Call Type** drop down list gives you the option to select the call type (PBX, SIP, ISDN, Any) used by the inbound caller to reach the Quadro.

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

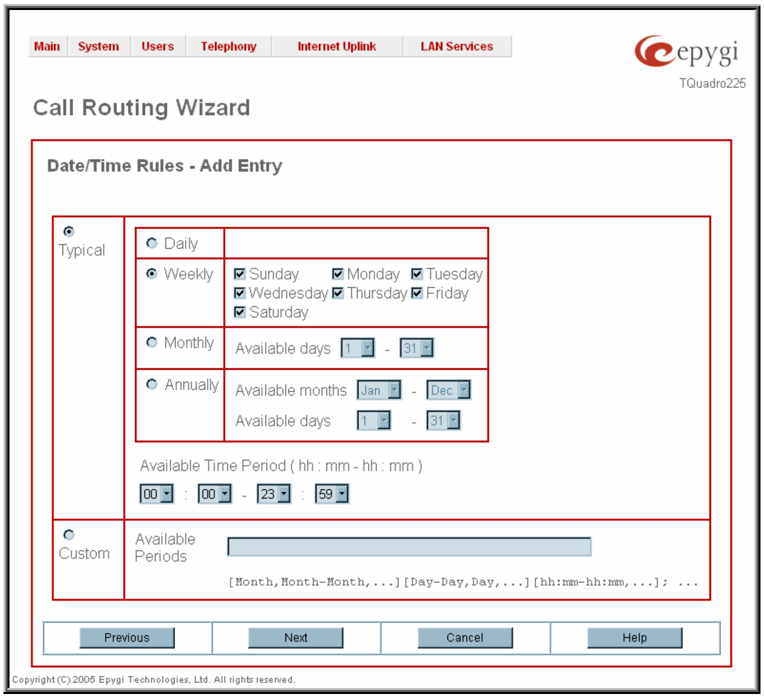
The **Call Routing Wizard** - Page 5 appears if the **Set Date / Time Period(s)** checkbox previously had been enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the pattern validity period(s).
This page provides selection between **Typical** and **Custom** date/time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

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

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

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

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



Call Routing Wizard

Date/Time Rules - Add Entry

● Typical
- ○ Daily
- ● Weekly: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday
- ○ Monthly: Available days 1 - 31
- ○ Annually: Available months Jan - Dec; Available days 1 - 31

Available Time Period (hh : mm - hh : mm)
00 : 00 - 23 : 59

○ Custom
Available Periods
[Month,Month-Month,...][Day-Day,Day,...][hh:mm-hh:mm,...]; ...

Previous
Next
Cancel
Help
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-100: Call Routing Wizard - page 5

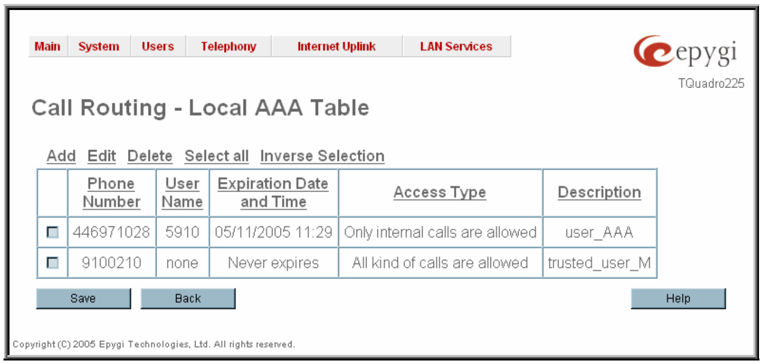
The **Duplicate** functional button is used to create a routing pattern with the settings of an exiting one. This is to avoid configuring a new routing entry completely by duplicating an existing entry with different settings. To use the **Duplicate** button only one record may be selected, otherwise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

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

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

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

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


Main
System
Users
Telephony
Internet Uplink
LAN Services
epygi
TQuadro225

Call Routing - Local AAA Table

Add Edit Delete Select all Inverse Selection

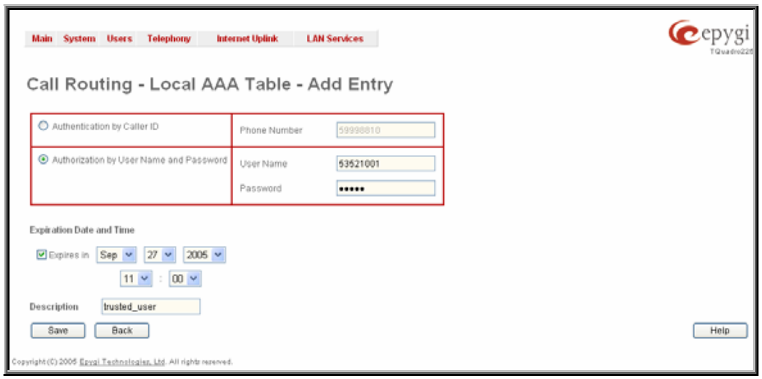
	Phone Number	User Name	Expiration Date and Time	Access Type	Description
□	446971028	5910	05/11/2005 11:29	Only internal calls are allowed	user_AAA
□	9100210	none	Never expires	All kind of calls are allowed	trusted_user_M

Save
Back
Help
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-101: PSTN User Registration page

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the type of authorization and the following other parameters:

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller’s phone number (which is considered to be automatically detected). The **Phone Number** text field requires the caller’s phone number. Only numeric and wildcard characters (see chapter Entering a SIP Addresses correctly) are allowed for this field. '[' , ']' , ',', '-', ‘{‘, ‘}’ are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number.
- **Authorization by Username and Password – this** selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication username. Only numeric values are allowed for this field, otherwise the error message “Incorrect Username - digits allowed only” will appear. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the error message “Incorrect Password - digits allowed only” will appear.



Call Routing - Local AAA Table - Add Entry

○ Authentication by Caller ID	Phone Number	59998810
● Authorization by User Name and Password	User Name	53521001
	Password	•••••

Expiration Date and Time

☑ Expires in Sep 27 2005
11 : 00

Description trusted_user

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-102: PSTN User Registration - Add Entry page

The **Expiration Date and Time** drop down-lists are used to set the date and time when the registration will expire.
The **Expires in** checkbox is used to enable the **Expiration Date and Time** feature.
The **Description** text field requires an optional description about the calling party.

To create a new Call Routing rule

1. Click on the **Call Routing Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Call Type** from the drop down list.
6. Define the **Metric** or leave the default.
7. Enter a **Description** if needed.
8. Enable the **Filter on Caller / Call Type / Modify Caller ID** checkbox, if the route functionality should be limited. This is dependent on the inbound caller information.
9. Enable the **Set Date/Time Period(s)** checkbox if a route should be functional within certain time/date intervals.
10. Press **Next**.
11. Select the user or attendant extension from the **Use Extension Settings** drop down list that the call will be placed on.
12. Specify the **Destination Host** and **Port Number**, **Username** and **Password** if an **IP** or **IP-PSTN** call type has been selected. For the **IP-PSTN** call type, enable **Multiple Logons** if necessary. Enable the **Use RTP Proxy, Use Secure RTP (SRTP)** and **Proceed Non-secure on Failure** checkboxes if needed.
13. Choose the Authentication and Accounting method from the **AAA Required** drop down list.
14. Choose a **Fail Reason** from the corresponding drop down list.
15. Configure **Transport Protocol for SIP messages** and **SIP Privacy** parameters as needed.
16. Press the **Next** button.
17. If the **Filter on Caller / Call Type / Modify Caller ID** checkbox has been previously enabled, fill in the **Inbound Caller Pattern** into the corresponding text field. Choose the needed value from the **Inbound Call Type** drop down list, as well as the **Inbound Number of Discarded Symbols** and **Inbound Prefix** values.
18. Press the **Next** button.
19. If **IP** has been selected on the previous step in the **Inbound Call Type** drop down list, then **Inbound Host** should be inserted in the current page. If **ISDN** has been selected in the **Inbound Call Type** drop down list, then the ISDN trunk should be selected here.
20. If the **Set Date/Time Period(s)** checkbox has been selected on the first page, pressing **Next** will open the **Date/Time Rules** page where route validity should be defined.
21. Press the **Finish** button to establish a local route with the inserted settings.

To create a local AAA entry

1. Click on the **Local AAA Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Local AAA Table** page.
3. Choose the Authentication type.
4. Enter the **Phone Number** or the **Username** and **Password** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

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: that is 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*
?2?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).

Table 1 The list split into two subgroups
?2?1 123? [1-3]??? {100-150, asd, *\?}1 1[1-3]3[0-8] 1231
1 123* {11-15}3* [1-3]* 12*31 *2*1 *

Step 2: The two groups of patterns are 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.

Table 2

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

Table 3

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

Table 4

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

Table 5

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

VoIP Carrier Wizard

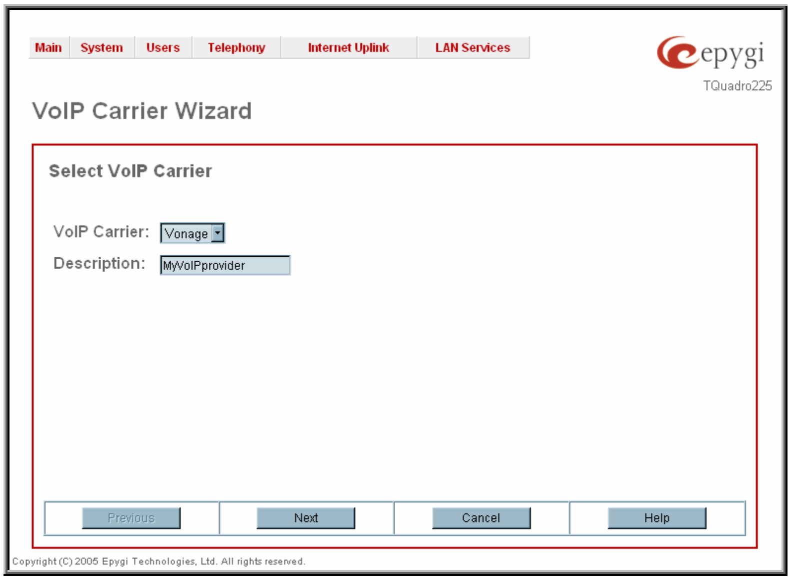
The **VoIP Carrier Wizard** is used to define access codes for available VoIP Carrier accounts which will particularly allow you to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

For each configured VoIP carrier, the wizard creates a specific IP-PSTN routing rule in the Call Routing table. Additionally, a virtual extension automatically generated in Extensions Management will be registered on the defined VoIP Carrier’s SIP server. The settings of that extension will be used to make calls from Quadro’s users towards the created VoIP Carrier will be placed.

VoIP Carrier Wizard – Page 1 provides a following option of describing the VoIP carrier:

When predefined carrier is selected in the **VoIP Carrier** drop down list, the SIP Server and Port will be already predefined in the next page. **Manual** selection allows you to manually set up the VoIP Carrier settings.

The **Description** field allows you to insert an optional description of the VoIP Carrier.



VoIP Carrier Wizard

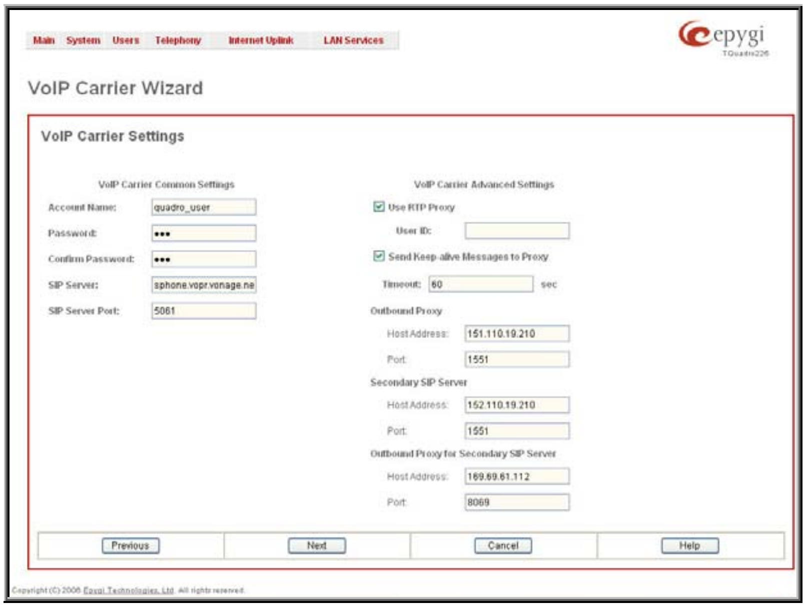
Select VoIP Carrier

VoIP Carrier: Vonage

Description: MyVoIPprovider

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-103: VoIP Carrier Wizard page



VoIP Carrier Wizard

VoIP Carrier Settings

VoIP Carrier Common Settings

Account Name: quadro_user

Password: •••

Confirm Password: •••

SIP Server: sphone.vopr.vonage.ne

SIP Server Port: 5061

VoIP Carrier Advanced Settings

☑ Use RTP Proxy

User ID:

☑ Send Keep-alive Messages to Proxy

Timeout: 60 sec

Outbound Proxy

Host Address: 151.110.19.210

Port: 1551

Secondary SIP Server

Host Address: 152.110.19.210

Port: 1551

Outbound Proxy for Secondary SIP Server

Host Address: 169.69.61.112

Port: 8069

VoIP Carrier Wizard – Page 2 is used to define VoIP Carrier Settings. The page contains following components:

1. VoIP Carrier Common Settings

The **Account Name** text field requires a username for authentication on the defined SIP server.

The **Password** text field requires a password for authentication on the defined SIP server.

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

The **SIP Server** text field requires an IP address or the hostname of the SIP server destination party it is registered on.

The **SIP Server Port** text field requires the port number of the SIP server destination party it is registered on.

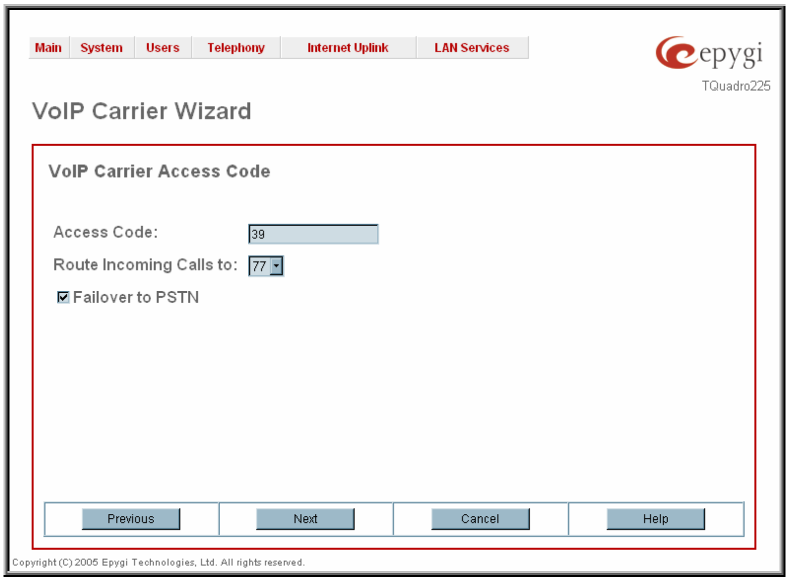
2. VoIP Carrier Advanced Settings

The **Use RTP Proxy** checkbox is applicable only when a route is used for calls towards a configured VoIP Carrier from a peer located outside the Quadro. When this checkbox is selected, the RTP streams between external users will be routed through Quadro. When the checkbox is not selected, RTP packets will move directly between peers.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested only for certain SIP servers. For others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If a reply is not received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will continue to be sent to the server.

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



VoIP Carrier Wizard

VoIP Carrier Access Code

Access Code: 39

Route Incoming Calls to: 77

☑ Failover to PSTN

VoIP Carrier Wizard – Page 3 contains the following VoIP Carrier access code selection components:

The **Access Code** text field requires a digit combination by dialing, which the corresponding VoIP Carrier will be reached.

The **Route Incoming Calls To** drop down list allows you to select an extension (or Auto Attendant) on the Quadro where incoming calls from the configured VoIP Carrier should be routed to.

The **Failover to PSTN** checkbox selection will route the call to the PSTN through local ISDN line in case if the VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the Call Routing table. This maintains digit transmission to the local PSTN when an IP call towards the configured VoIP Carrier cannot be established.

Please Note: A warning message will appear when the defined **Access Code** already exists in the Call Routing table or causes a conflict with entries already in the Call Routing table. In this case, when continuing through the **VoIP Carrier Wizard**, the existing entry in the Call Routing table will automatically be overwritten by the new settings.

RADIUS Client Settings

RADIUS (Remote Authentication Dial In User Service) specifies the RADIUS protocol used for authentication, authorization and accounting, to differentiate, to secure and to account for the users. The RADIUS Server provides the option for a caller from/through Quadro to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the Quadro, and according to the configuration of **AAA Required** option (see Call Routing table), the RADIUS server will be used to authenticate user and/or to account for the call. This can be accomplished by automatic detection of the caller’s number or a customized login prompt where the caller is expected to enter a username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, user passwords are encrypted when sent between the client and RADIUS server to eliminate the possibility of a party viewing an unsecured network where they could determine a user's password. If no response from the RADIUS Server is returned after the Receive Timeout expires, the request is resent numerous times as defined in the Retry Count list. The client can also forward requests to an alternate server(s) if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not recognize must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the Quadro Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the Quadro.

Please Note: The RADIUS Client cannot be disabled if there is at least one route with **RADIUS Authentication and Authorization** or **RADIUS Accounting** values configured in the **AAA Required** drop down list at the Call Routing table. In order to be able to disable the RADIUS Client on the Quadro, appropriate routes should be removed first.

The other RADIUS Client settings are divided into three groups:

1. Registration Settings

The **Primary Server** requires the IP address of the primary Radius Server.

The **Secondary Server** requires the IP address of the secondary Radius Server.

NAT Station IP text fields require the NAT PC WAN IP address. If no NAT Station is specified here, Quadro's IP address will be sent to the RADIUS server.

Secret Key is used to insert the secret key between the Radius client and the server. Contact the Radius server administrator to get the secret key for your Quadro.

The **Confirm Secret Key** field is used to verify the secret key. If the entered **Secret Key** does not correspond to the one in the **Confirm Secret Key** field, the error message "The Secret Key does not match. Please try again" will appear.

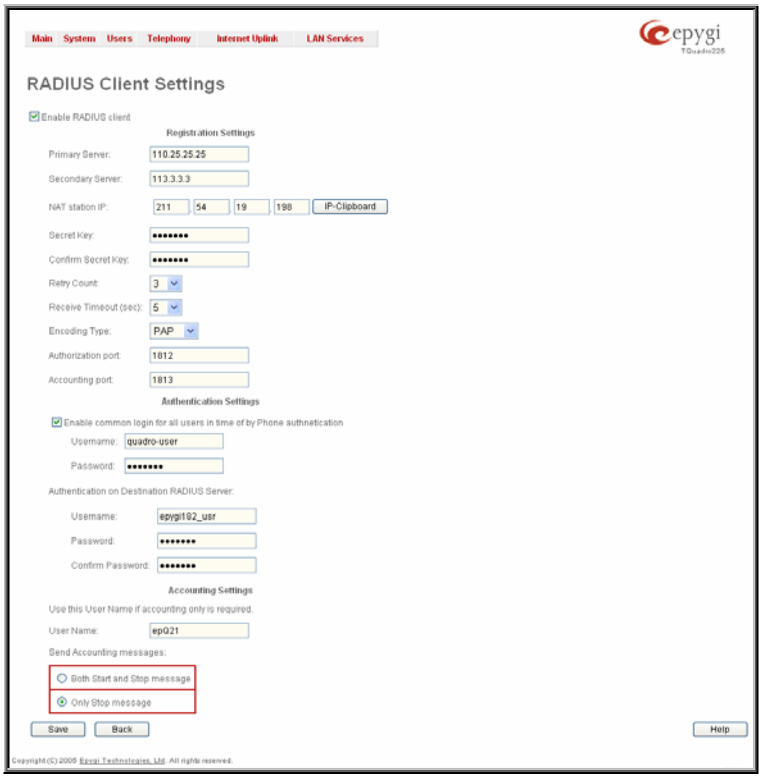
Retry Count allows you to select the number of attempts authorized before canceling the registration.

Receive Timeout allows you to select the timeout (in seconds) between two attempts to register.

Encoding Type allows you to select the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type should also be requested from the Radius Server administrator.

The **Authorization Port** text field requires the port number on the RADIUS server where Quadro is to send the authentication requests.

The **Accounting Port** text field requires the port number on the RADIUS server where Quadro is to send the accounting messages.



RADIUS Client Settings

☑ Enable RADIUS client

Registration Settings

Primary Server: 110.25.25.25

Secondary Server: 113.3.3.3

NAT station IP: 211 . 54 . 19 . 198

Secret Key: •••••••

Confirm Secret Key: •••••••

Retry Count: 3

Receive Timeout (sec): 5

Encoding Type: PAP

Authorization port: 1812

Accounting port: 1813

Authentication Settings

☑ Enable common login for all users in time of by Phone authnetication

Username: quadro-user

Password: •••••••

Authentication on Destination RADIUS Server:

Username: epygi182_usr

Password: •••••••

Confirm Password: •••••••

Accounting Settings

Use this User Name if accounting only is required.

User Name: epQ21

Send Accounting messages:

○ Both Start and Stop message

● Only Stop message

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-104: Radius Client Settings page

2. Authentication Settings

The **Enable common login for all users in time of by Phone authentication** checkbox enables custom settings for the callers who passed an authorization by phone on the Quadro. This checkbox enables **Username** and **Password** text fields to insert the custom settings that will stand instead of the source caller's settings when being delivered to the RADIUS server.

The **Authentication on Destination RADIUS Server** parameters group is used to insert a **Username** and a **Password** (followed by the password confirmation) to pass authentication on the RADIUS Server of the destination Quadro. If these fields are left empty, the original authentication settings that users enter for authentication will be used.

3. Accounting Settings

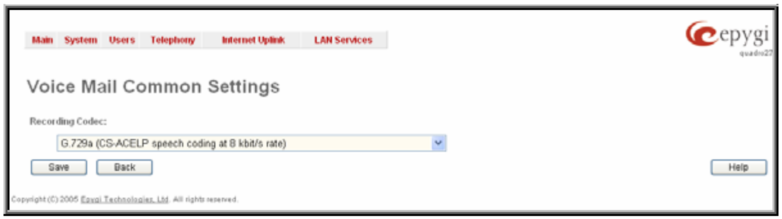
The **Username** field is dedicated for accounting services only. It is used to insert an identification username for accounting purposes. When no username is specified in this field, the source username will be used for accounting.

The **Send Accounting messages** manipulation radio buttons group is used to select sending both **Start** and **Stop** accounting messages or only **Stop** accounting message.

Voice Mail Common Settings

The **Voice Mail Common Settings** page is used to configure the Voice Mail recording codec.

The page consists of the **Recording Codec** drop down list contains the existing codecs for voice mail compression. Changing the Voice Mail recording codec will directly affect the allocated memory size for users.



Voice Mail Common Settings

Recording Codec: G.729a (CS-ACELP speech coding at 8 kbit/s rate)

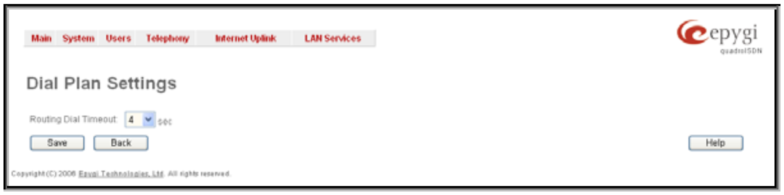
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-105: Voice Mail Coming Settings page

Dial Plan Settings

The **Dial Plan Settings** page is used to adjust the dialing timeouts for the routing calls over Quadro.

This page consists of the only drop down list used to configure the dialing timeout for the Routing calls. Values selected in the lists indicate the interval between the dialed number and it being applied to the network.



Dial Plan Settings

Routing Dial Timeout: 4 sec

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-106: Dial Plan Settings page

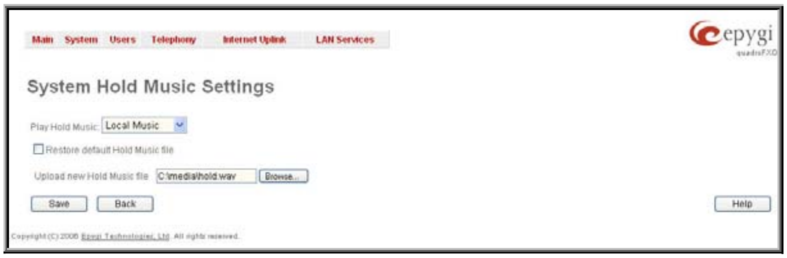
Hold Music Settings

The **System Hold Music Settings** allows you to define the hold music played to the PSTN party when it is held by the IP user. This page also allows you to define the percentage of system memory dedicated to the uploaded hold music file. This page contains following components:

The **Play Hold Music** drop down list specifies the music played to the PSTN party when it is held by remote IP user. It offers the following options:

- **Off** - no music will be played.
- **Local Music** – the hold music configured on the Quadro will be sent to the remote PSTN party while it is on hold.
- **Remote Music** – music sent by the IP party will be transparently passed to the PSTN user while it is held by the IP party.

Restore Default Hold Music File enables the default hold music. If the checkbox is selected, the text field **Upload New Hold Music File** will be disabled.



System Hold Music Settings

Play Hold Music: Local Music

☐ Restore default Hold Music file

Upload new Hold Music file C:\media\hold.wav

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

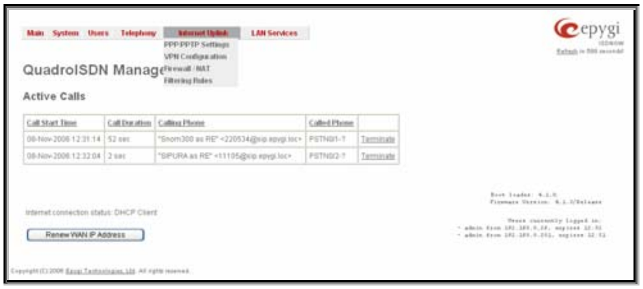
Fig. III-107 Basic Services - Hold Music Settings page

The **Upload New Hold Music File** text field can be used to enter the path where the custom hold music file is located. If the hold music file is browsed with the help of file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the hold music file.

The music file needs to be in PCMU wave format, otherwise the system will prevent uploading the file and will display the warning message "Invalid audio file or format is not supported". Additionally, the system will refuse uploading if insufficient memory is available for the Quadro and will then announce "You do not have enough space".

The **Download Hold Music File** link appears only if a file has been uploaded recently. It downloads the audio file to the PC and opens a window where the saving location can be specified.

Internet Uplink Menu



QuadroISDN Manage

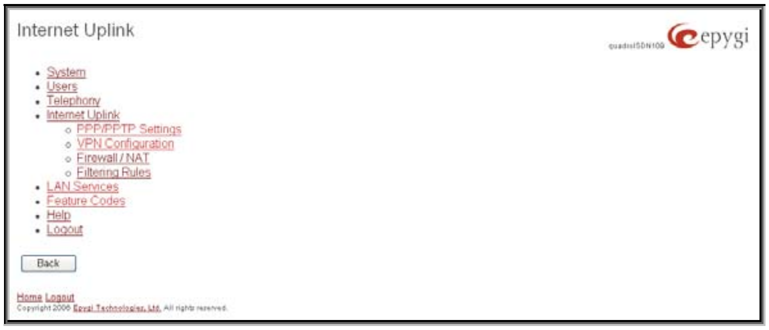
Active Calls

Call Start Time	Call Duration	Calling Phone	Called Phone	
08-Nov-2006 12:31:14	52 sec	"Snom300 as RE" <220534@sip.epygi.loc>	PSTN0/1-1	Terminate
08-Nov-2006 12:32:04	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	PSTN0/2-1	Terminate

Internet connection status: DHCP Client

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-108: Internet Uplink menu in Dynamo theme



Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-109: Internet Uplink menu in Plain theme

PPP/ PPTP Settings

The **PPP/PPTP Settings** page is used to establish a connection over the DSL link, or any other type of uplink, to the ISP. A connection is needed to set up and make or receive calls through PPP over Ethernet. The connection may be configured for manual setup or always up. Once a connection has been established between the Quadro and the provider, Quadro users will be able to make and receive calls at any time.

The **PPP/PPTP Settings** page offers the following components:

The Advanced PPP Settings link refers to the same named page where certain parts of the negotiation process during connection establishment can be adjusted. This link is not available when accessing this page through the Internet Configuration Wizard.

The **PPTP Server** text fields are only enabled when Quadro is running with the PPTP interface and require the IP address of the PPTP server.

The **Encryption** drop down list is only enabled when Quadro is running with the PPTP interface and it is used to select the encryption for the traffic over the PPTP interface.

Authentication Settings require the Username and Password used for the authentication on the ISP server.

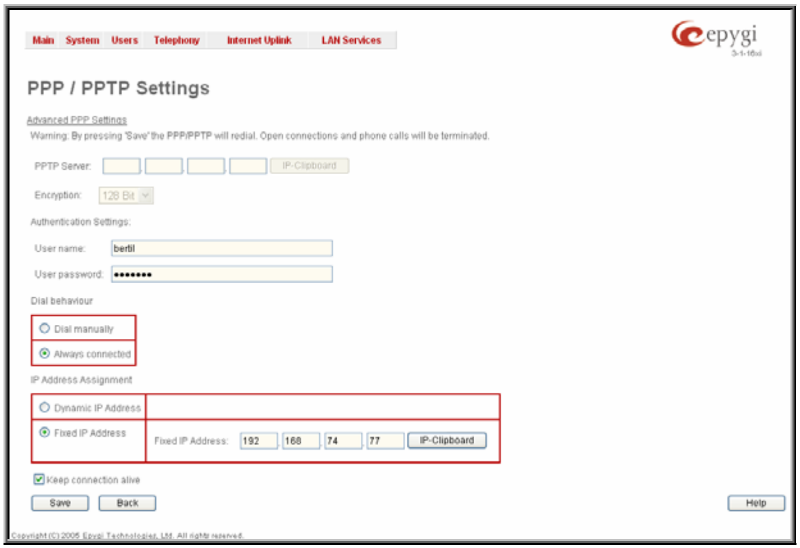
Dial Behavior radio buttons enables the following selections:

- **Dial Manually** - if this radio button is activated, a button will be displayed in the main management window that serves to switch the Internet connection on/off. When accessing the Internet, every station of the connected LAN has to connect to Quadro first.
- **Always connected** - Quadro stays in the always connected mode. This will allow always being online in the network.

IP Address Assignment radio buttons are used to define the IP address assignment for the PPP interface with the following options:

- **Dynamic IP Address** – the IP address to the PPP interface will be assigned dynamically by the DHCP server.
- **Fixed IP Address** – the fixed user defined IP address will be assigned to the PPP interface.

The **Keep Connection alive** checkbox enables keeping the connection alive by sending control packets dedicated for the link state verification.



PPP / PPTP Settings

Advanced PPP Settings

Warning: By pressing 'Save' the PPP/PPTP will redial. Open connections and phone calls will be terminated.

PPTP Server: ___ . ___ . ___ . ___

Encryption: 128 Bit

Authentication Settings:

User name: bertil

User password: •••••••

Dial behaviour

○ Dial manually

● Always connected

IP Address Assignment

○ Dynamic IP Address

● Fixed IP Address — Fixed IP Address: 192 . 168 . 74 . 77

☑ Keep connection alive

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-110: 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.

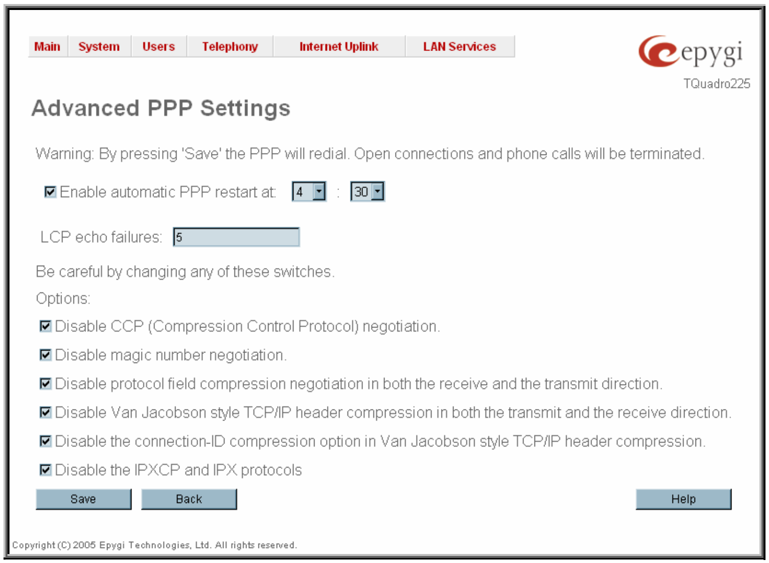
Disable magic number negotiation - with this option, PPPD cannot detect a looped-back line. This option should only be selected if the peer is not working properly.

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.



Advanced PPP Settings

Warning: By pressing 'Save' the PPP will redial. Open connections and phone calls will be terminated.

☑ Enable automatic PPP restart at: 4 : 30

LCP echo failures: 5

Be careful by changing any of these switches.

Options:

☑ Disable CCP (Compression Control Protocol) negotiation.

☑ Disable magic number negotiation.

☑ Disable protocol field compression negotiation in both the receive and the transmit direction.

☑ Disable Van Jacobson style TCP/IP header compression in both the transmit and the receive direction.

☑ Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression.

☑ Disable the IPXCP and IPX protocols

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-111: Advanced PPP Settings page

VPN Configuration

A **VPN (Virtual Private Network)** is established to connect two local networks (intranets) securely over the Internet securely. The VPN routers manage authentication between servers and clients and handle data encryption for the connection. Only authorized users may access the network and the data exchange cannot be intercepted.

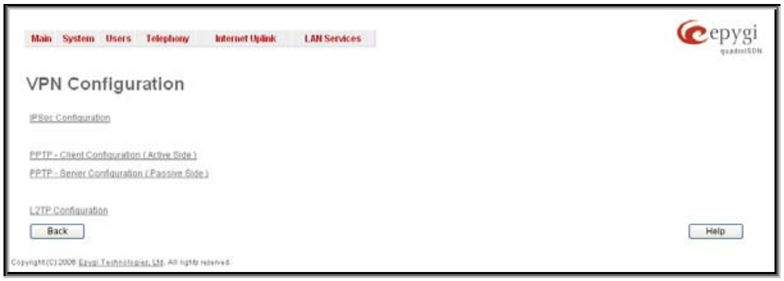
VPN connections are, in many ways, like every Internet connection, they are based on IP addresses, which means, the concerned VPN gateways must authenticate the IP addresses of their respective partner’s VPN gateways. Each time a specific VPN is to be established, usually the same IP addresses are expected. This will not create problems if both VPN partners have fixed WAN IP addresses. There may be circumstances reasons to prefer dynamically allocated IP addresses. To enable devices that use a variable IP address as part of a VPN, they are turned into “Road Warriors”. For example, at this point they are able to reach their corporate network via authentication at the company's VPN gateway device. This VPN gateway device must have a fixed IP address for Internet access. Every VPN needs at least one VPN gateway with a fixed IP address.

The partner devices of a VPN must have different WAN IP addresses, and if they are connected to local area networks, these LAN’s must have different IP addresses. As all Quadro devices have the same default IP addresses on delivery, at least one of them must be reconfigured in order to set a new IP address.

Quadro supports several kinds of VPN connections such as **IPSec**, **L2TP** and **PPTP**.

The **VPN Configuration** page offers four links (IPSec Configuration, PPTP Client Configuration, PPTP Server Configuration and L2TP Configuration), which leads to the corresponding feature settings pages.

Attention: It is strongly recommended not to run different types of VPN tunnels between the same endpoints simultaneously.



VPN Configuration

IPSec Configuration

PPTP - Client Configuration (Active Side)

PPTP - Server Configuration (Passive Side)

L2TP Configuration

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-112: VPN Configuration page

An IPSec connection includes authentication and encryption to protect data integrity and confidentiality. VPNs are “virtual” in the sense that individuals can use the public Internet as a means of securely accessing an internal network. Once the IPSec connection is established, users have access to the same network resources, addresses, and so forth as if they were connected locally. VPNs are “private” because the data is encrypted between two VPN gateways. Encryption makes it very difficult for anyone to intercept data and capture sensitive information such as passwords. The Quadro can be set up to act as a VPN router when connected to the Internet with a fixed IP address or as an IPSec connection Road Warrior when using dynamic IP addresses.

Establishing an IPSec connection normally requires the functionality of a VPN gateway on each side of the communication line. An intelligent Internet access router, for example Quadro, delivers this function but also PCs or workstations may also be equipped with VPN gateway functionality. Home offices typically prefer dynamically allocated IP addresses.

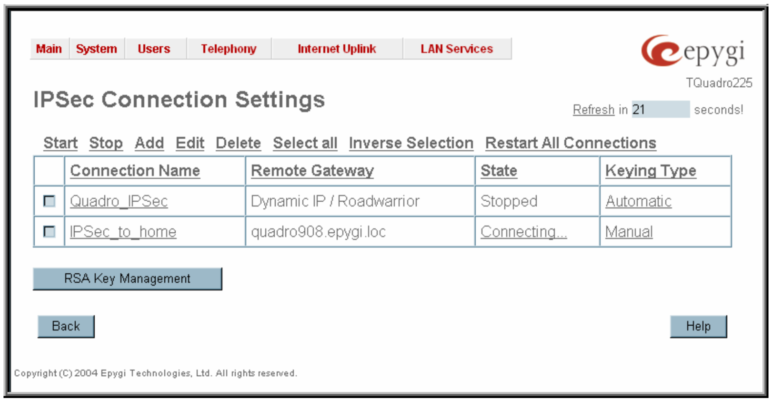
When Quadro is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. Quadro is then prepared to establish an IPSec connection with another VPN gateway device, but also allows access to Road Warriors. A notebook /laptop used by a traveling employee could also be a Road Warrior. Access to their company’s intranet via an IPSec connection can be obtained regardless of their location.

Quadro can also be set up to act as a Road Warrior. If a home office is connected to the Internet via Quadro with PPPoE (Point-to-Point Protocol) and dynamic IP addressing, setting up Quadro as a Road Warrior will allow an IPSec connection to the corporate network.

For the encryption and decryption of the data transmitted via the IPSec connection, a key is used. **RSA** used by Quadro is an asymmetric key system. It has to be available on both sides of the IPSec connection and will generate a different pair of keys on each side, a private key and a public key. During the connection establishment, some data is encrypted with the remote party’s public key. They can be decrypting the data with their private key and the data encrypted there with Quadro’s public key can be decrypted with Quadro’s private key. Since the private key is never transmitted, it stays completely unknown to everyone, thus the system remains safe. Even if someone gets the public key, decryption cannot be possible without the private key. Quadro generates such a pair of keys automatically when it is set up. The user cannot see the private key, but must know the public key because their IPSec connection partner will need it.

Please Note: A pair of keys will always be generated, a public one and a private one. The previously generated pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

The **IPSec Configuration** link refers to the **IPSec Connection Settings** page. This page provides an overview of all existing IPSec connections characterized by their **Connection Name**, the **Remote Gateway** (the IP address or the hostname of the IPSec connection partner), the **State** of the IPSec connection (Stopped, Connecting, Activated, Waiting or Connected) and the dedicated **Keying Type** (the encryption type). The content of the table can be sorted in ascending or descending order by clicking on the header of the respective column. There is a checkbox for every IPSec connection to select it for further editing.



IPSec Connection Settings

TQuadro225

Refresh in 21 seconds!

Start Stop Add Edit Delete Select all Inverse Selection Restart All Connections

	Connection Name	Remote Gateway	State	Keying Type
□	Quadro_IPSec	Dynamic IP / Roadwarrior	Stopped	Automatic
□	IPSec_to_home	quadro908.epygi.loc	Connecting...	Manual

RSA Key Management

Back

Help

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-113: IPSec Connection Settings page

Start activates the connection establishment of the selected IPSec connection. The **State** of the IPSec connection will change into “Connected” or “Activated” depending on the IPSec connection type. If no record is selected, the error message “One Record should be selected” appears.

Attention: It is not recommended to simultaneously start a static and a dynamic connection configured to use the same secret key. A dynamic connection may capture the static connection peer and vice versa, depending on which connection established first.

Stop disconnects the selected IPSec connection. The state of the IPSec connection will change into “Stopped”. If no record is selected, the error message “One Record should be selected” will appear. More than one record may be selected at a time to be stopped.

Add leads to the **Add IPSec Connection** wizard where a new IPSec connection can be defined and specified. The wizard provides several pages.

Edit leads to a set of **IPSec Connection Properties** pages to modify the parameters of the selected IPSec connection. The page includes the same components as the **Add IPSec Connection** page. To operate with **Edit**, only one record may be selected, otherwise an error message “One row must be selected” appears.

Restart all Connections restarts all active IPSec connections. The **State** of these IPSec connections will turn into **Connected** or **Activated** if the restart procedure has been successfully completed.

RSA Key Management leads to the **RSA Key Management** page to see the current RSA key, to generate a new one and to send it to the peer via e-mail.

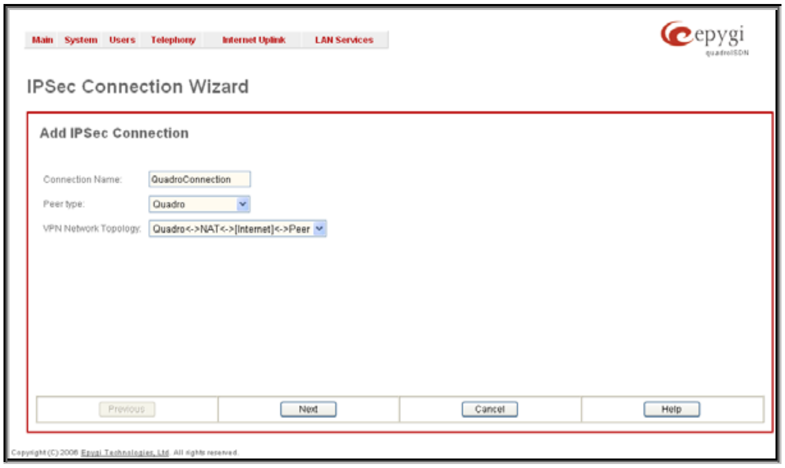
The first IPSec Connection Wizard page **Add IPSec Connection** has the **Connection Name** text field that requires a new mandatory IPSec connection name. If the text field is not filled in, the error message otherwise an error will occur “Error: Incorrect connection name” will appear.

Please Note: The input in the **Connection Name** field should only be in Latin characters, otherwise an error occurs and IPSec connection cannot be created.

The **Peer type** drop down list is used to choose the remote machine type for the IPSec Connection to be established. If the list does not include the required type of machine, choose **Other**.

The **VPN Network Topology** drop down list allows you to select the location of the peers participating to the VPN connection. The following options are present in the list:

- Quadro<>Peer – direct connection between Quadro and a peer.
- Quadro<>[Internet]<>Peer – connection between Quadro and peer over Internet.
- Quadro<>NAT<>[Internet]<>Peer – connection between Quadro and peer over Internet through Quadro provider’s NAT.
- Quadro<>[Internet]<>NAT<>Peer – connection between Quadro and peer over Internet through peer provider’s NAT.



IPSec Connection Wizard

Add IPSec Connection

Connection Name: QuadroConnection

Peer type: Quadro

VPN Network Topology: Quadro<->NAT<->[Internet]<->Peer

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-114: IPSec Connection Wizard - Add IPSec Connection

The second page of the IPSec Connection Wizard, **IPSec Connection Properties** serves to specify the members of the IPSec Connection and to set the basic parameters for encryption.

A group of radio buttons are used with **Dynamic IP/Road Warrior** and **Static IP/ Remote Gateway** to select if the remote Quadro (or another VPN gateway device) is connected to the Internet with a dynamic IP address and is acting as a **Road Warrior**, or is connected to the Internet with a fixed IP address and is acting as a **VPN Gateway**.

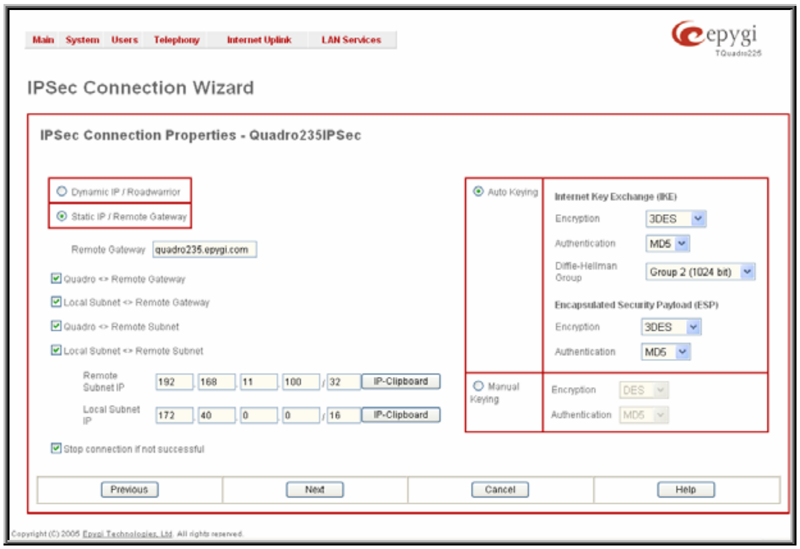
If **Dynamic IP / RoadWarrior** is selected, the **Remote Gateway IP Address** text field will automatically generate the value “any”, to allow access independent from the sending IP address.

Selecting **Static IP / Remote Gateway** requires entering the IP address or the hostname of the remote Quadro (or another VPN gateway device) in the **Remote Gateway** text field.

Please Note: The **Static IP/ Remote Gateway** selection is not possible if this Gateway is positioned behind NAT, since the IP-address of the remote gateway is not reachable directly in this case.

Quadro <> Remote Gateway allows access from the local Quadro to the remote VPN gateway (local subnet and remote subnet are not included). This includes management access. The checkbox is disabled when “Quadro<>NAT<>[Internet]<>Peer” or “Quadro<>[Internet]<>NAT<>Peer” the is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

Local Subnet <> Remote Gateway allows access from all stations connected to the local network to the remote VPN gateway device (local Quadro and remote subnet are not included). The checkbox is disabled when “Quadro<>[Internet]<>NAT<>Peer” is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.



IPSec Connection Wizard

IPSec Connection Properties - Quadro235IPSec

○ Dynamic IP / Roadwarrior
● Static IP / Remote Gateway

Remote Gateway: quadro235.epygi.com

☑ Quadro <> Remote Gateway
☑ Local Subnet <> Remote Gateway
☑ Quadro <> Remote Subnet
☑ Local Subnet <> Remote Subnet

Remote Subnet IP: 192 . 168 . 11 . 100 / 32 [IP-Clipboard]
Local Subnet IP: 172 . 40 . 0 . 0 / 16 [IP-Clipboard]

☑ Stop connection if not successful

● Auto Keying

Internet Key Exchange (IKE)
Encryption: 3DES
Authentication: MD5
Diffie-Hellman Group: Group 2 (1024 bit)

Encapsulated Security Payload (ESP)
Encryption: 3DES
Authentication: MD5

○ Manual Keying
Encryption: DES
Authentication: MD5

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-115: IPSec Connection Wizard -IPSec Connection Properties

Quadro <> Remote Subnet allows access from the local Quadro to all stations of the remote LAN (local subnet and remote VPN gateway devices are not included). The checkbox is disabled when “Quadro<>NAT<>[Internet]<>Peer” is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

Local Subnet <> Remote Subnet allows access from all stations of the local network to all stations of the remote LAN (VPN gateway devices are not included). In this case, the local and remote subnet IP addresses and subnet masks have to be entered in the corresponding text fields **Local Subnet IP** and **Remote Subnet IP**.

More than one of the above checkboxes may be selected to specify the desired communication relations.

The **Stop Connection if not successful** checkbox allows you to stop the IPSec connection attempts if the partner is still unreachable after the timeout period. If the checkbox is not selected, the system will continue to try to reach the IPSec connection partner.

The right side of the page offers the following security settings for key exchange, data encryption and authentication:

The area **Keying Type** offers the choice between automatic and manual keying. To use manual keying, the **Static IP / Remote Gateway** needs to be selected.

Auto Keying requires the **ESP** (Encapsulated Security payload) and **IKE** (Internet Key Exchange) settings (in addition to **Diffie-Helman Group** settings) to be selected for the automatic keying exchange. **Encryption** and **Authentication** parameters should be defined for each of these standards, as well as for the **Manual Keying**.

The **Encryption** drop down list offers the following standards for selection:

DES (Data Encryption Standard) is a block cipher algorithm with 64-bit blocks and a 56-bit key. This algorithm is considered to be unsecure for sensitive information.

3DES (Triple DES) uses three DES encryptions on a single data block with three different keys to achieve a higher security than is available from a single DES pass.

AES (Advanced Encryption Standard) is a computer security standard, which became effective on May 26, 2002 by NIST to replace DES. The cryptography scheme is a symmetric block cipher, which encrypts and decrypts 128-bit blocks of data. Lengths of 128, 192, and 256 bits are standard key lengths used by AES.

The area **Authentication** offers the following parameters to be selected:

SHA (Secure Hash Algorithm) is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPSEC.

SHA1 is an enhanced version of SHA. It works with checksums like MD5 does, but it makes a longer hash.

MD5 (Message Digest) is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.

The **Diffie-Hellman** parameter is used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group, which is based upon the prime numbers.

Group 2048 (high) is stronger (more secure) than Group 2 (medium), which is stronger than Group 1 (low). Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, and Group 2048 provides 2048 bits. If mismatched groups are specified on each peer, negotiation fails.

Depending on whether the automatic keying type or the manual one has been selected, the button **Next** will lead you to the **Automatic Keying** or **Manual Keying** page.

The third page of the IPSec Connection wizard, **Automatic Keying**, is used to setup a type of password (**Shared Secret**) or the **RSA** public key to secure your IPSec Connection. The functionality of **Perfect Forward Secrecy** (PFS) can be added to both. Following ways of automatic keying are available.

- **Shared Secret** is a type of password consisting of any characters that both of the IPSec Connection partners must know. The authentication will be done with this shared secret. All encryption functions below will remain concealed.

  Please Note: It is also not recommended to start multiple road warrior connections with the **Shared Secret** automatic keying selected. For multiple road warriors to be started at the same time, it is recommended to use RSA keying with **Local ID** and **Remote ID** fields configured.

- **RSA** requires the public RSA key of your IPSec Connection partner.

Please Note: System prevents to start a connection with Shared Secret automatic keying selected if there is already a connection with RSA automatic keying started, and vice versa.

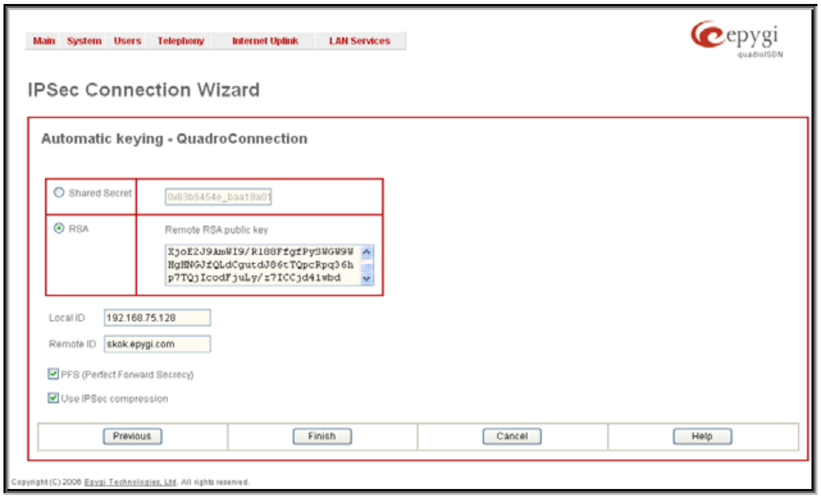
The **Local ID** requires an IP address, Quadro FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

Remote ID also requires an IP address, the IPSec Connection partner’s FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

The **Local ID** and **Remote ID** text fields may have the values in one of the formats presented below:

- **IP address** – example: 10.1.19.32.
- **Host name** – example: vpn.epygi.com. This form requires additional resources to resolve the host name, therefore it is not recommended to use this format.
- **@FQDN** – example: @vpn.epygi.com. This form is considered as a string, and is not being resolved. It is recommended to use this form for most applications.
- **user@FQDN** - example: quadro@vpn.epygi.com. This form is also considered as a string, and is not being resolved. It has no advantages over the previous form.

Please Note: If **Shared Secret** is defined, the **Local ID** and **Remote ID** may be undefined. Exceptions are cases when NAT Traversal is enabled and/or the partner device is a road warrior; in this case at least one of the IDs need to be defined.



IPSec Connection Wizard

Automatic keying - QuadroConnection

○ Shared Secret 0x63b5454e_baa19a01

● RSA Remote RSA public key
XjoE2J9AmWI9/R188FfgfPySWGW9W
HgMNGJfQLdCgutdJ86tTQpcRpq36h
p7TQjIcodFjuLy/z7ICCjd41wbd

Local ID 192.168.75.128

Remote ID skok.epygi.com

☑ PFS (Perfect Forward Secrecy)

☑ Use IPSec compression

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-116: IPSec Connection Wizard - Automatic Keying Settings page

PFS (Perfect Forward Secrecy) is a procedure of system key exchange, which uses a long-term key and generates short-term keys as is required. Thus, an attacker who acquires the long-term key can neither read previous messages that they may have captured nor read future ones.

Use IPSec Compression enables IPSec data compression. This option is displayed only if the IPSec-VPN partner supports it.

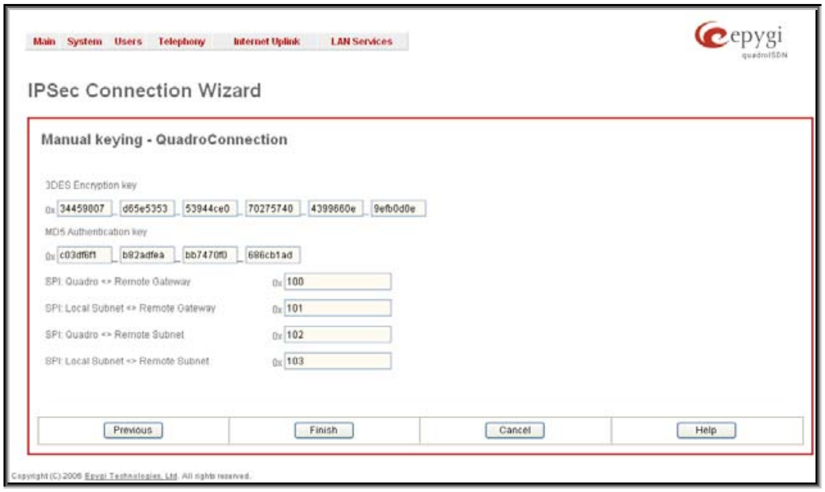
The **Manual Keying** page offers the following components:

Depending on the selected encryption and authentication services of the prior page (IPSec Connection Properties) you will get some of the following text fields:

- **DES Encryption Key**
- **3DES Encryption Key**
- **SHA1 Authentication Key**
- **MD5 Authentication Key**

Manual keys must be entered in the hexadecimal format, otherwise the error message “Incorrect Encryption Key” will appear.

The **SPIs** (Security Parameter Index) are indices to keep the IPSec Connection tunnels distinct. A security association (SA) is defined by destination, protocol and SPI. Without the SPI, connections to the same gateway using the same protocol cannot be distinguished.



IPSec Connection Wizard

Manual keying - QuadroConnection

3DES Encryption key

0x 34459807 _ d65e5353 _ 53944ce0 _ 70275740 _ 4399860e _ 9efb0d0e

MD5 Authentication key

0x c03df6f1 _ b82adfea _ bb7470f0 _ 686cb1ad

SPI: Quadro <> Remote Gateway 0x 100

SPI: Local Subnet <> Remote Gateway 0x 101

SPI: Quadro <> Remote Subnet 0x 102

SPI: Local Subnet <> Remote Subnet 0x 103

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-117: IPSec Connection Wizard - Manual Keying Settings page

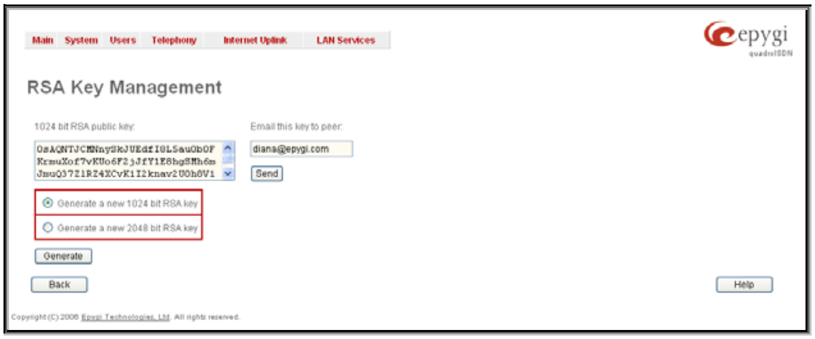
The public key is displayed in the **RSA Public Key** text field so that the user may inform their IPSec connection partner about it, for example, via fax.

The user has the option of generating a new pair of keys by specifying the key length with the corresponding radio buttons **Generate a new 1024bit RSA Key** and **Generate a new 2048bit RSA Key** and then clicking the **Generate** Button.

A valid RSA key should fit to following requirements:

- RSA key doesn't start with "0s"
- RSA key doesn't end with "=="
- RSA key contains symbols other than Alphanum, +, /, =

The **Email this to the peer** text field requires the mailing address of the IPSec connection partner. The **Send** button will insert Quadro’s public RSA key into an e-mail and send it to the IPSec connection partner.



RSA Key Management

1024 bit RSA public key:

```
0sAQNTJCMNnySkJUEdfI0LSauObOF
KrmuXof7vKUo6F2jJfY1E8hgSMh6m
JmuQ37Z1RZ4XCvK1I2knav2U0h8V1
```

Email this key to peer: diana@epygi.com

● Generate a new 1024 bit RSA key

○ Generate a new 2048 bit RSA key

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-118: IPSec Connection Wizard - IPSec Connection RSA Key Settings page

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) is used to establish a virtual private network (VPN) over the Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers. PPTP encapsulates any type of network protocol (IP, IPX, etc.) and transports it over IP. Therefore, if IP is the original protocol, IP packets ride as encrypted messages inside PPTP packets running over IP. PPTP is based on point-to-point protocol (PPP) and the Generic Routing Encapsulation (GRE) protocol. Encryption is performed by Microsoft's Point-to-Point Encryption (MPPE), which is based on RC4.

L2TP (Layer **2 T**unneling **P**rotocol) is a protocol from the IETF, which allows a PPP session to run over the Internet, an ATM, or frame relay network. L2TP does not include encryption (as does PPTP), but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP network server (LNS) at the corporate side. Large carriers also may use L2TP to offer remote POPs to smaller ISPs. Users at the remote locations dial into the modem pool of an L2TP access concentrator, which forwards the L2TP traffic over the Internet or private network to the L2TP servers at the ISP side, which then sends them on to the Internet.

For **PPTP and L2TP Connections**, two parties are required: a **Client** and a **Server**. The client is responsible for establishing the connection, hence active. The server is waiting for clients; it is not able to initiate the connection itself, hence passive.

Attention: L2TP tunnels have no data encryption mechanism.

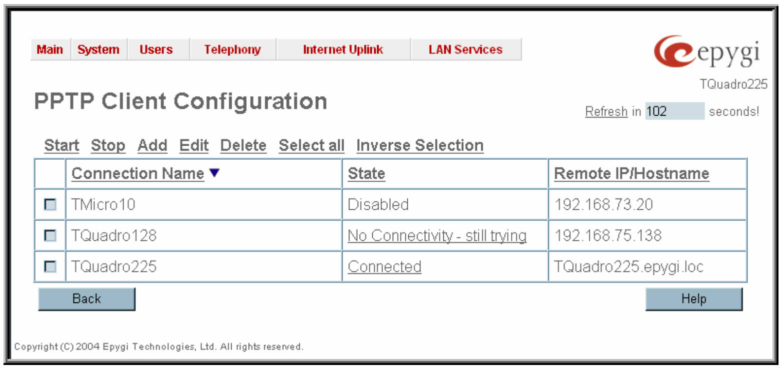
The **Host Name** and a **Password** specify each side. The client should know the server’s name and password (the Quadro server has no password) and the server should set the client’s host name and a password. The client and server settings have to match on both sides for successful connection establishment.

Clients and Servers are identified by their hostnames, which means that only one client can be connected to the server in the same network. Servers also define the range of IP addresses that are assigned to the Server and Client hosts participating in a connection.

The **PPTP Client Configuration** link displays a page where all existing PPTP client connections are listed, characterized by their **Connection Name**, the **State** of the PPTP connection (Pending, Disabled, Trying…, Authentication Failure, No Connectivity - still trying, Unknown, Broken, or Connected) and the **Remote IP/Hostname** (the IP address or the hostname of the PPTP server). The state of the PPTP Connections, except for the “Disabled” state, is established as a link that refers to the page where logout information about the PPTP connection status is displayed. Logs can be useful to determine problems on PPTP connections failure.

Start initiates the PPTP client(s) activity (reaching the server). Several client connections may be selected at the same time.

The **Stop** button is used to stop the selected PPTP client(s) activity. Several client connections may be selected at the same time using this function.



PPTP Client Configuration

Refresh in 102 seconds!

	Connection Name ▼	State	Remote IP/Hostname
□	TMicro10	Disabled	192.168.73.20
□	TQuadro128	No Connectivity - still trying	192.168.75.138
□	TQuadro225	Connected	TQuadro225.epygi.loc

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-119: PPTP Client Configuration page

Add leads to the **PPTP Client Connection - Add Entry** page where a new PPTP client connection can be established. This page contains the following components:

Server Host Name requires the server’s hostname.

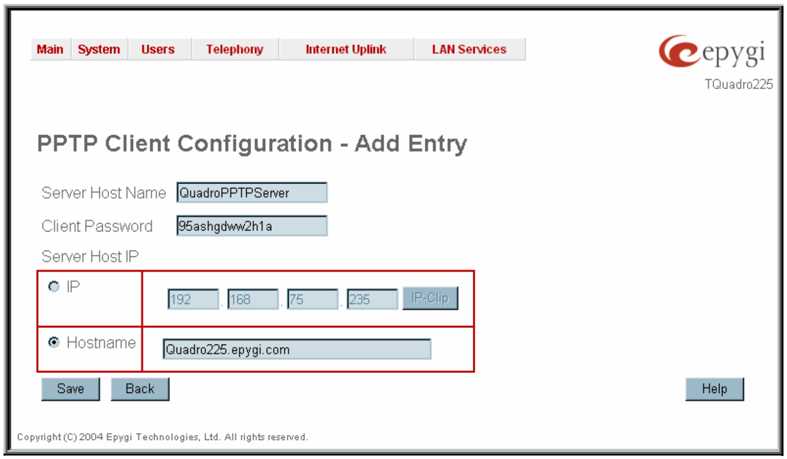
Please Note: The input in the **Server Host Name** field should only be in Latin characters, otherwise an error occurs and no PPTP connection can be created.

Client Host Password requires the local peer password.

The **Server Host IP** radio buttons allow selecting the PPTP server.

IP requires the IP address of the PPTP server.
Hostname requires the FQDN (Full Qualified Domain Name) of the PPTP server.

Please Note: All settings should be configured the same way on both the PPTP client and server hosts. In other words, for successful PPTP tunnel establishment; all settings should match each other.



PPTP Client Configuration - Add Entry

Server Host Name: QuadroPPTPServer

Client Password: 95ashgdww2h1a

Server Host IP

○ IP: 192 . 168 . 75 . 235

● Hostname: Quadro225.epygi.com

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-120: PPTP Client Configuration - Add Entry page

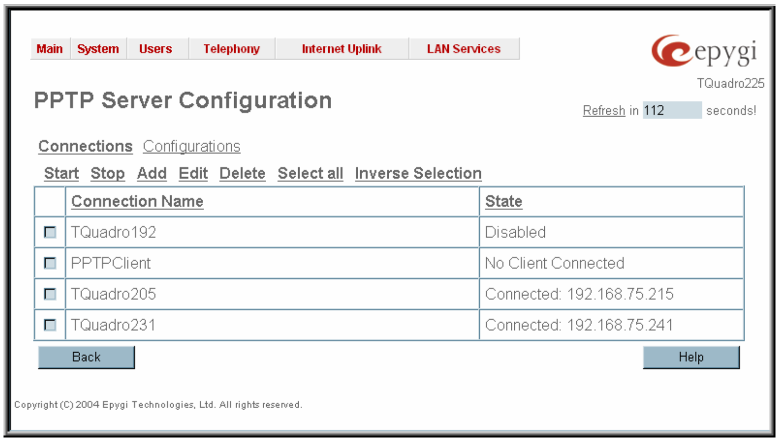
The **PPTP Server Configuration** link displays a page to configure the PPTP server connections. It is divided into two pages with a table of the existing PPTP server connections on one page and the PPTP server settings on the other.

The page **PPTP Server Connections** offers the following input options:

The table **PPTP Server Connections** lists all the PPTP connections, characterized by their **Connection Name** and the **State** of the PPTP connection (Disabled, No Client Connected or Connected: IP address). Each PPTP Server connection can hold only one PPTP tunnel.

Start is used to activate the selected PPTP connection(s). Several server connections may be selected at the same time.

Stop is used to deactivate the selected PPTP connection(s). Disabling the connection will disconnect all connected clients and close the PPTP tunnel. Several server connections can be selected at the same time to operate with this function.



PPTP Server Configuration

Refresh in 112 seconds!

	Connection Name	State
□	TQuadro192	Disabled
□	PPTPClient	No Client Connected
□	TQuadro205	Connected: 192.168.75.215
□	TQuadro231	Connected: 192.168.75.241

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-121: PPTP Server Configuration page

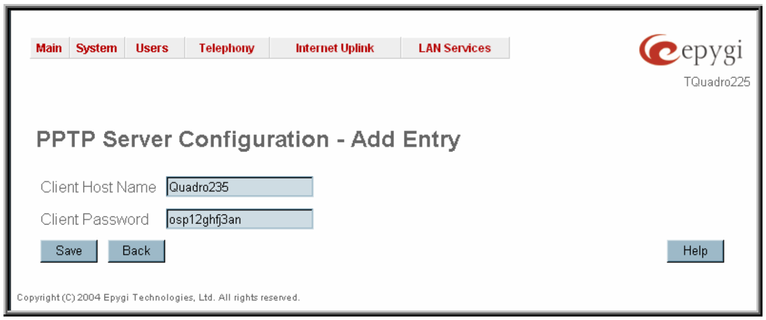
Add leads to the **PPTP Server Connection - Add Entry** page where a new PPTP Server connection can be made.

Client Host Name and **Client Password** require the corresponding client’s host name and password.

Please Note: The input in the **Client Host Name** field should only be in Latin characters, otherwise an error occurs and no PPTP connection can be created.

In certain cases, **Client Host Name** can be a conditional username defined by the client and used for PPTP connection establishment.

Please Note: All settings should be configured the same way on both the PPTP client and server. In other words, for successful PPTP tunnel establishment, all settings should match.



PPTP Server Configuration - Add Entry

Client Host Name: Quadro235

Client Password: osp12ghfj3an

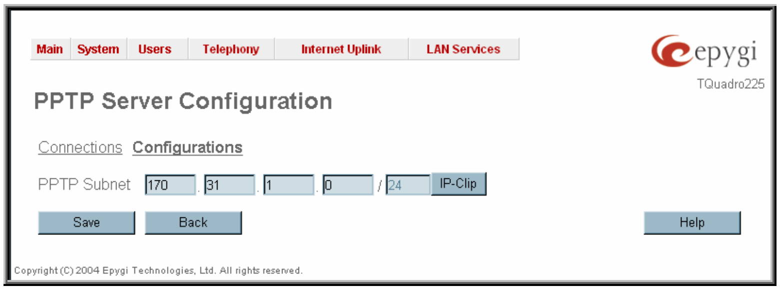
Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-122: PPTP Server Configuration - Add Entry page

The **PPTP Server Configuration** page is used to configure the PPTP server settings and offers the following components:

The **PPTP Subnet** text fields are used to enter the IP address range for the PPTP server and clients within the PPTP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the PPTP connection.

Please Note: The first address specified in the PPTP Subnet will be assigned to the PPTP server; others will be assigned to the clients. The PPTP server subnet should be different from the L2TP server subnet, otherwise a corresponding error message will appear.



PPTP Server Configuration

PPTP Subnet: 170 . 31 . 1 . 0 / 24

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-123: PPTP Server Configuration page

The **L2TP Configuration** link displays a page to configure the L2TP connections.

Attention: L2TP tunnels have no data encryption mechanism.

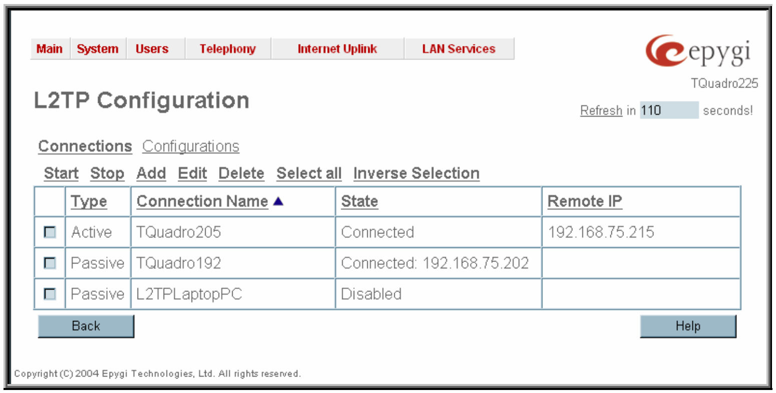
The **L2TP Configuration** page has two pages with the table of existing L2TP connections on one page and the L2TP server settings on the other page.

The **L2TP Connections** page has the following components:

The **L2TP Connections** table lists all the L2TP connections characterized by their **Connection Name**, connection **Type** (active or passive), the **State** of the L2TP connection (Waiting, Connected, Trying, Disabled or Down) and the **Remote IP** address (the IP address or the hostname of the L2TP partner if connection is active). Each L2TP passive connection can hold only one L2TP tunnel.

Start is used to enable the selected L2TP server or client connection(s). Several records may be selected at the same time with this function.

Stop is used to disable the selected L2TP server or client connection(s). Stopping the server will disconnect all connected clients and close the L2TP tunnel. Several records may be selected at the same time with this function.



L2TP Configuration

	Type	Connection Name ▲	State	Remote IP
□	Active	TQuadro205	Connected	192.168.75.215
□	Passive	TQuadro192	Connected: 192.168.75.202	
□	Passive	L2TPLaptopPC	Disabled	

Fig. II-124: L2TP Configuration page

Add leads to a page where the connection type (active or passive) must be selected. Afterwards, the appropriate **Add L2TP Connection** page will be displayed where a new L2TP connection can be established.

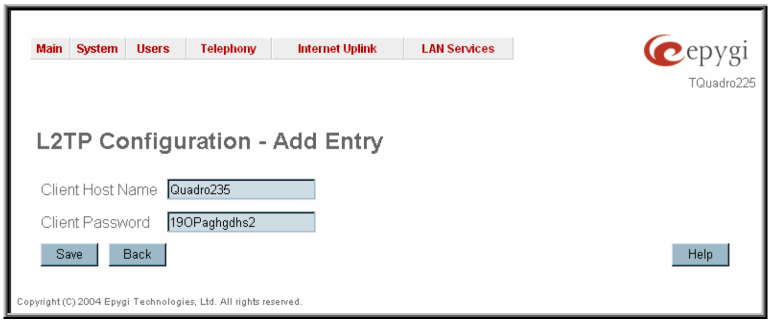
The **Passive L2TP Connection - Add Entry** page is used to specify passive L2TP server connections.

Client Host Name and **Client Password** text fields require the corresponding client’s host name and password.

Please Note: The input in the **Client Host Name** field should only be in Latin characters, otherwise an error occurs and no L2TP connection can be created.

In certain cases, **Client Host Name** can be a conditional username defined by the client and used for L2TP connection establishment.

Please Note: All settings on this page should be configured in the same way on both the L2TP client and server. In other words, for successful L2TP tunnel establishment, all settings should match.



L2TP Configuration - Add Entry

Client Host Name: Quadro235

Client Password: 19OPaghgdhs2

Fig. II-125: L2TP Configuration - Add Passive Connection page

The **Active L2TP Connection - Add Entry** page is used to specify L2TP client connections and offers the following components:

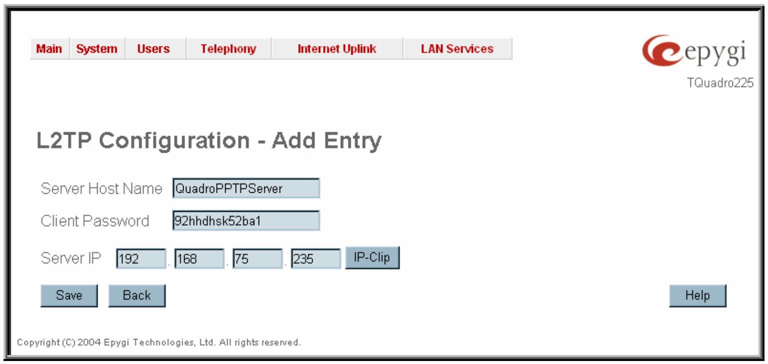
The **Server Host Name** text field requires the L2TP server’s name.

Please Note: The input in the **Server Host Name** field should only be in Latin characters, otherwise an error occurs and no L2TP connection can be created.

The **Client Host Password** text field requires the local peer password.

The **Server IP** text field requires the IP address of the L2TP server.

Please Note: All settings must be configured the same way both on the L2TP client and the server hosts. For successful L2TP tunnel establishment, all settings should match each other.



L2TP Configuration - Add Entry

Server Host Name: QuadroPPTPServer

Client Password: 92hhdhsk52ba1

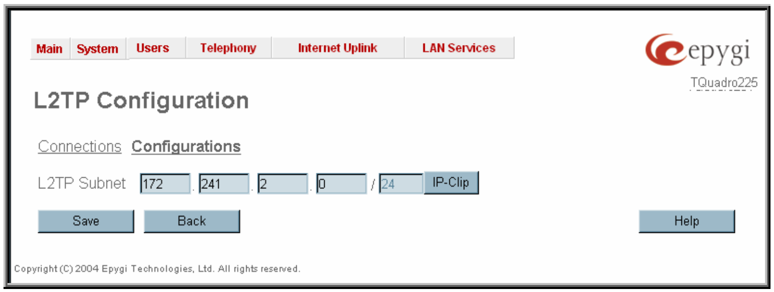
Server IP: 192 . 168 . 75 . 235

Fig. II-126: L2TP Configuration - Add Active Connection page

The **Configuration** page is used to configure the L2TP server settings and provides the following input options:

The **L2TP Subnet** text fields are used to enter the IP address range for the L2TP server and clients within the L2TP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the L2TP connection.

Please Note: The first address specified in the L2TP Subnet will be assigned to the L2TP server; others will be assigned to the clients. The L2TP server subnet should be different from the PPTP server subnet, otherwise a corresponding error message will appear.



L2TP Configuration

L2TP Subnet 172 . 241 . 2 . 0 / 24

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-127: L2TPServer Configuration page

To Specify an IPSec Connection

1. Press the **Add** button on the **IPSec Connection Settings** page. The **IPSec Connection Wizard** will appear in the browser window.
2. Select a VPN **Peer Type** and assign a name to the **IPSec Connection**. Press **Next** to go to the next page of the IPSec Connection wizard.
3. Enter the remote side IP parameters, check subnets/gateways for the connection, select the NAT traversal option (if needed), and the desired keying type. Press **Next** to go to the next page of the IPSec Connection wizard.
4. If the **Automatic Keying** type has been selected, enter the automatic keying parameters and select the PFS and IPSec compression options (if needed). If the **Manual Keying** type has been selected enter the encryption and authentication keys and SPI(s).
5. To specify an IPSec connection with these parameters, press **Finish**. Press **Cancel** to abort the operation.

To Manage an RSA key for the IPSec Connection

1. Press the **RSA Key Management** button on the **IPSec Connection Settings** page. The **IPSec Connection RSA Key** will appear in the browser window.
2. Select the RSA key length and press **Generate** to generate a new RSA public key. This may take several seconds.
3. Enter a destination e-mail address in the **Email this key to peer** text field, then press **Send** to send the new RSA public key.

To Specify a PPTP Client Connection

1. Press the **Add** button on the **PPTP Client Configuration** page.
2. Enter the server host name in the **Server Host Name** text field.
3. Specify the PPTP client password in the **Client Password** text field.
4. Using the radio buttons on the page, select the server address representation (IP address or hostname) and provide the corresponding information in the **Server Host IP** fields.
5. Press **Save** to add a PPTP connection with these settings.

To Add a PPTP Server Connection

1. Press the **Add** button on the **PPTP Server Configuration** page.
2. Enter the client host name and the password in the **Client Host Name** and **Client Password** text fields.
3. Press **Save** to add a PPTP connection with these settings.

To Add an Active L2TP Connection

1. Press the **Add** button on the **L2TP Configuration** page.
2. Select the **Active Connection** link.
3. Enter the server host name in the **Server Host Name** text field.
4. Specify the L2TP client password in the **Client Password** text field.
5. Specify the server’s IP address in the **Server IP** text field.
6. Press **Save** to add an active L2TP connection with these settings.

To Add a Passive L2TP Connection

1. Press the **Add** button on the **L2TP Configuration** page.
2. Select the **Passive Connection** link.
3. Enter the client host name and the password in the **Client Host Name** and **Client Password** text fields.
4. Press **Save** to add a passive L2TP connection with these settings.

To Delete/Stop/Start/Enable/Disable a VPN Connection

1. Select one or more checkboxes of the corresponding connections that should to be deleted/stopped/started from the **Connection** tables. Press **Select all** to delete/stop/start all connections.
2. Click on the Delete/Stop/ Start button from the table’s menu to perform the corresponding operation for the selected VPN connection(s).
3. If deleting, confirm it with pressing on **Yes**. The VPN connection will be deleted. To abort the deletion and keep the VPN connection in the list, click **No**.

Firewall and NAT

The **Firewall Configuration** page allows setting up a firewall, configuring the security level and enabling the NAT and IDS services of Quadro.

A **Firewall** is a security service configured by the Quadro administrator based on various criteria. The firewall allows or blocks traffic based on policies, services and/or IP addresses. The firewall has several levels of security policies (low, medium or high). The administrator may add additional service-based rules. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level.

NAT (Network Address Translation) is used to allow Quadro LAN members to connect to the Internet using Quadro's WAN IP address. The Quadro/NAT also handles forwarding incoming packets from the WAN to the PCs or devices on Quadro’s LAN.

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

The **Enable NAT** checkbox selection enables Network Address Translation.

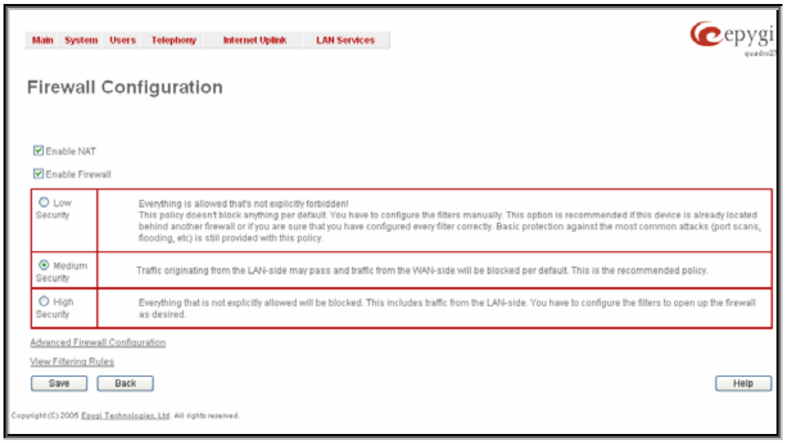
The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are the following:

- **Low Security** - Everything that is not explicitly forbidden will be allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

The Advanced Firewall Settings link refers to the page where Quadro’s privacy can be configured.

The **View Filter Rules** link opens the Filtering Rules page.



Firewall Configuration

☑ Enable NAT

☑ Enable Firewall

○ Low Security	Everything is allowed that's not explicitly forbidden! This policy doesn't block anything per default. You have to configure the filters manually. This option is recommended if this device is already located behind another firewall or if you are sure that you have configured every filter correctly. Basic protection against the most common attacks (port scans, flooding, etc) is still provided with this policy.
● Medium Security	Traffic originating from the LAN-side may pass and traffic from the WAN-side will be blocked per default. This is the recommended policy.
○ High Security	Everything that is not explicitly allowed will be blocked. This includes traffic from the LAN-side. You have to configure the filters to open up the firewall as desired.

Advanced Firewall Configuration

View Filtering Rules

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-128: Firewall and NAT Settings page

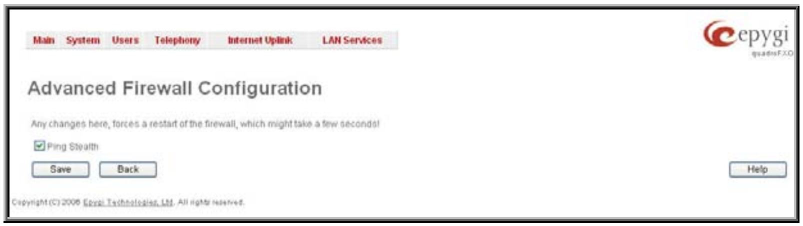
Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and operation addressed towards the device. With this feature enabled, Quadro will answer with inscrutable messages to the Ping operation.

Please Note: Operations are available only when the firewall is enabled from the Firewall and NAT page.

This page offers the following components:

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



Advanced Firewall Configuration

Any changes here, forces a restart of the firewall, which might take a few seconds!

☑ Ping Stealth

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

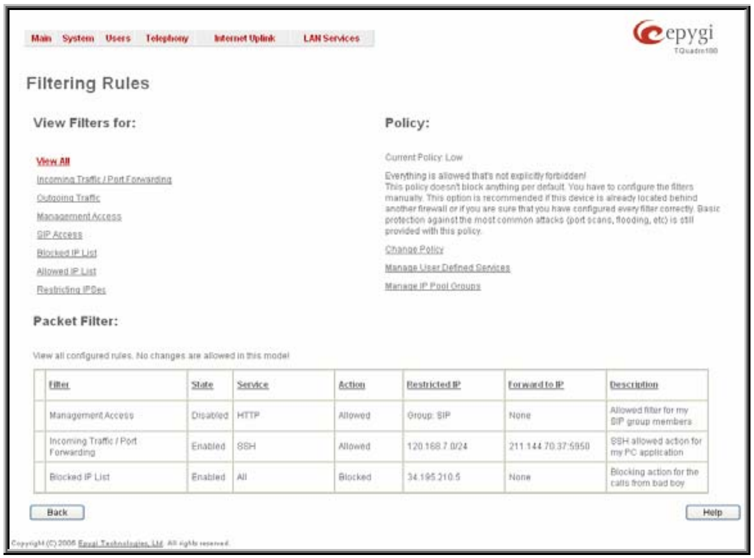
Fig. II-129: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows you to configure the filters for incoming and outgoing traffic.

To prevent inaccurate configuration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. Since the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled (additionally NAT should be enabled to use the **Port Forwarding** function in the **Incoming Traffic / Port Forwarding** filtering rules). The filtering rules are independent from the security level, so they will work if enabled, no matter what security level has been selected.

Please Note: Applying firewall rules will prevent the establishment of new connections that violate the rules. Applying rules does not kill existing connections that violate the rule.



Filtering Rules

View Filters for:

View All
Incoming Traffic / Port Forwarding
Outgoing Traffic
Management Access
SIP Access
Blocked IP List
Allowed IP List
Restricting IPSec

Policy:

Current Policy: Low

Everything is allowed that's not explicitly forbidden!
This policy doesn't block anything per default. You have to configure the filters manually. This option is recommended if this device is already located behind another firewall or if you are sure that you have configured every filter correctly. Basic protection against the most common attacks (port scans, flooding, etc) is still provided with this policy.

Change Policy

Manage User Defined Services

Manage IP Pool Groups

Packet Filter:

View all configured rules. No changes are allowed in this model

Filter	State	Service	Action	Restricted IP	Forward to IP	Description
Management Access	Disabled	HTTP	Allowed	Group: SIP	None	Allowed filter for my SIP group members
Incoming Traffic / Port Forwarding	Enabled	SSH	Allowed	120.168.7.0/24	211.144.70.37:5950	SSH allowed action for my PC application
Blocked IP List	Enabled	All	Blocked	34.195.210.5	None	Blocking action for the calls from bad boy

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-130: Filtering Rules page

View All displays all configured filters specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). Since it is read-only, no modifications are allowed and no functional buttons are available.

The **Incoming Traffic/Port Forwarding** filter is for incoming traffic. The rules here allow or deny systems on the Internet to reach the services of Quadro's LAN. The NAT service should be enabled on the Quadro to provide the possibility of **Port Forwarding** in the **Incoming Traffic/Port Forwarding** filtering rules. The **Port Forwarding** function will be unavailable if NAT is disabled on the Quadro.

The **Outgoing Traffic** filter is for outgoing traffic. The rules here allow or deny Quadro's LAN users to reach external services.

Management Access is used to enable management access to the Quadro from the Internet. A host on the Internet can be allowed to reach the Quadro.

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.

Restricted IPSec - Generally hosts in a VPN are allowed to have access to any service, i.e., no traffic will be blocked. They are treated as if they were part of the Quadro LAN. However, this service can be manually denied here.

The **Filtering Rules** page provides several links. Each link opens its specific parameters on the same page. Only **Change Policy** (see chapter Firewall and NAT), **Manage user Defined Services** (see chapter Service Pool) and **Manage IP Pool Groups** (see chapter IP Pool) lead to separate pages. The **Filtering Rules** page also includes the currently selected firewall security (**Policy**) level and its description.

The table displayed on the bottom of this page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Disable** is used to disable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action,** a **Restriction** to certain IP address(es) or IP groups, and if adding a rule for **Incoming Traffic/Port Forwarding**, the destination IP address for **Forwarding**.

The page to add a rule for **Incoming Traffic/Port Forwarding** offers the following input options:

Service includes a list of possible services to be configured. All user-defined services also will be displayed in this list.

Action includes possible actions to setup the rule.

Forward to IP requires the destination IP address where traffic should be transferred to if it comes from the restricted host. The IP address defined in this field will be ignored for blocked action of the **Incoming Traffic/Port Forwarding** rule.

Note: It is not allowed to forward incoming packets when the NAT service is disabled on the Quadro.

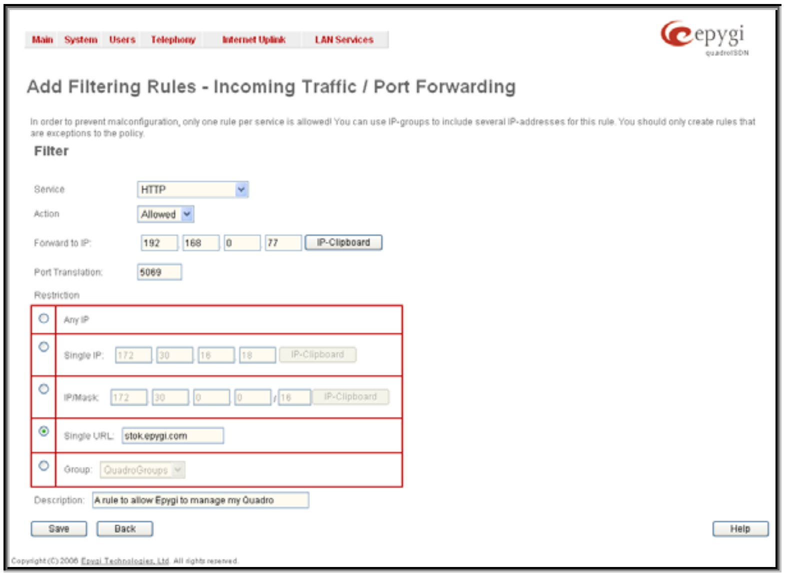
Port Translation text field is available for “Allowed” action only and optionally requires the port number that will stand instead of the original port number when incoming packet is being forwarded. If this field is left empty, the original port number will be used when forwarding the packet.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.
- Selecting **Single IP** requires the IP address of the allowed or blocked host.
- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. The following are **Maskbit** examples:

  255.0.0.0= /8,
  255.255.0.0 = /16,
  255.255.255.0 = /24,
  255.255.255.255= /32
- **Single URL** requires the hostname of the allowed or blocked host.
- **Group** indicates the user-defined groups that include IP addresses that should to be allowed or blocked.

The **Description** field is used to insert an optional description of the filtering rule.



Add Filtering Rules - Incoming Traffic / Port Forwarding

In order to prevent malconfiguration, only one rule per service is allowed! You can use IP-groups to include several IP-addresses for this rule. You should only create rules that are exceptions to the policy.

Filter

Service: HTTP

Action: Allowed

Forward to IP: 192 . 168 . 0 . 77

Port Translation: 5069

Restriction

○ Any IP

○ Single IP: 172 . 30 . 16 . 18

○ IP/Mask: 172 . 30 . 0 . 0 / 16

● Single URL: stok.epygi.com

○ Group: QuadroGroups

Description: A rule to allow Epygi to manage my Quadro

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-131: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filter** link (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List, Allowed IP List or Restricting IPSec) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the **Filtering Rules** page. A page where a new rule may be added will appear in the browser window. The page will be named corresponding to the selected filter.
3. Select a service name from the **Service** list to configure a rule for it. If the list has a default value, do not change the default values.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, do not change the default values.
5. Enter the IP address in the **Forward to IP** field if an **Incoming Traffic Rule** is to be added.
6. Choose the restriction type by selecting **Any**, **Single IP**, **IP/Mask** or **Single URL** and enter the required information in the text fields or select a group.
7. Insert a **Description**, if needed.
8. To add a rule with these parameters, press **Save**.

To Delete Filtering Rules

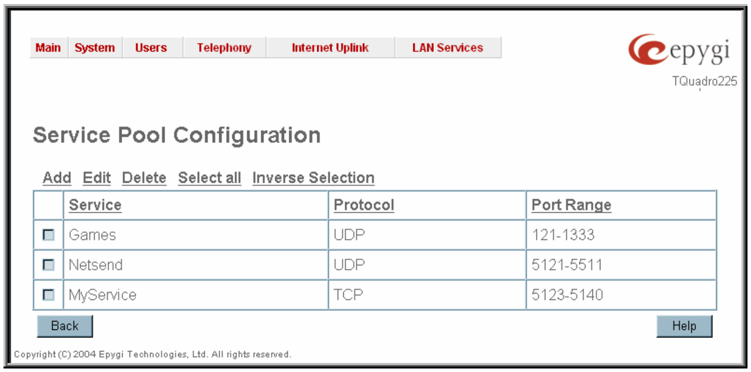
1. Select the **Filter** link to delete a rule from its table. The appropriate **Filter** table will appear in the same window.
2. Check one or more checkboxes of the corresponding rules that should be deleted from the rules table. Press **Select all** if all rules should to be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

Service Pool

The **Service Pool** table is a list of all created services and their parameters. It is used to add new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or permission by defining a new filtering rule with the following:

Add opens the **Add New Service** page where new services may be added.

Edit opens the **Edit Service** page where the service parameters (except for the service name) can be modified. This page includes the same components as the **Add New Service** page. To operate with **Edit** only one record may be selected, otherwise the error message “One row must be selected” will appear.

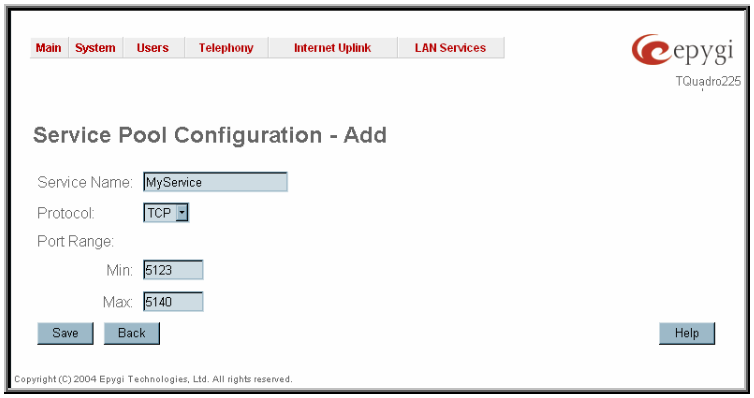


Service Pool Configuration

	Service	Protocol	Port Range
□	Games	UDP	121-1333
□	Netsend	UDP	5121-5511
□	MyService	TCP	5123-5140

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-132: Service Pool page



Service Pool Configuration - Add

Service Name: MyService

Protocol: TCP

Port Range:

Min: 5123

Max: 5140

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-133: Service Pool - Page to add a new Service

The **Add** page is used to add new services and includes the following text fields and buttons:

Service Name requires a name for the service that should be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.

To Add a new Service

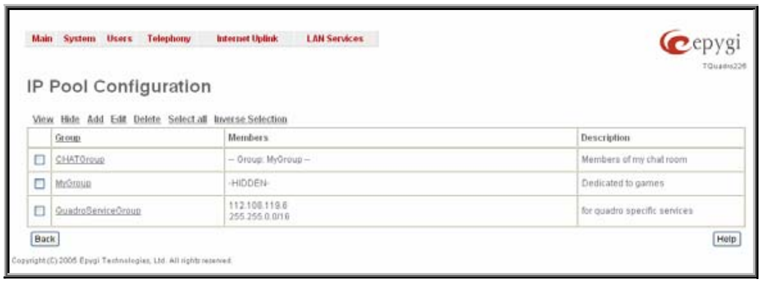
1. Select the **Manage User Defined Services** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **Service Pool Configuration** page. A page where a new service may be added will appear in the browser window.
3. Define a service name in the **Service Name** text field.
4. Select the protocol type for the service from the **Protocol** drop down list.
5. Enter the port range in the **Port Range** text fields or leave one of them empty to define a particular port for the service.
6. To add a service with these parameters, click on **Save**.

To Delete a Service

1. Select the **Manage User Defined Services** link. The **Service Pool Configuration** page appears with the table of services (if any).
2. Check one or more checkboxes of the corresponding services that should be deleted from the **Service Pool** table. Press **Select all** if all services should be deleted.
3. Click on the **Delete** button on the **Service Pool Configuration** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

IP Pool

The **Manage IP Pool Groups** link opens the **IP Pool Configuration** page.



IP Pool Configuration

	Group	Members	Description
□	CHATGroup	-- Group: MyGroup --	Members of my chat room
□	MyGroup	-HIDDEN-	Dedicated to games
□	QuadroServiceGroup	112.108.119.6 255.255.0.0/16	for quadro specific services

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-134: IP Pool Configuration page

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.

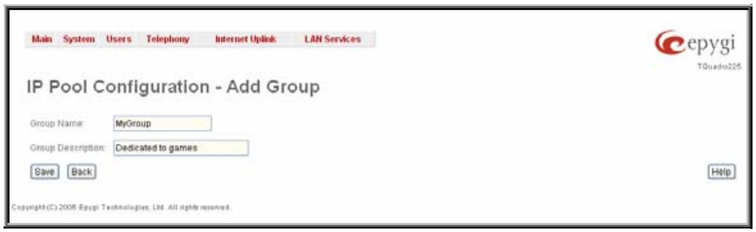
Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise the error message “One row must be selected” will appear.

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains).

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



IP Pool Configuration - Add Group

Group Name: MyGroup

Group Description: Dedicated to games

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

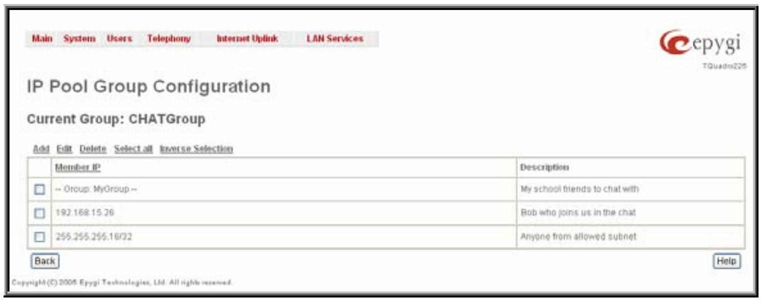
Fig. II-135: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise the error message “One row must be selected” will appear.



IP Pool Group Configuration

Current Group: CHATGroup

	Member IP	Description
□	-- Group: MyGroup --	My school friends to chat with
□	192.168.15.26	Bob who joins us in the chat
□	255.255.255.16/32	Anyone from allowed subnet

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-136: IP Pool Group Configuration page

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

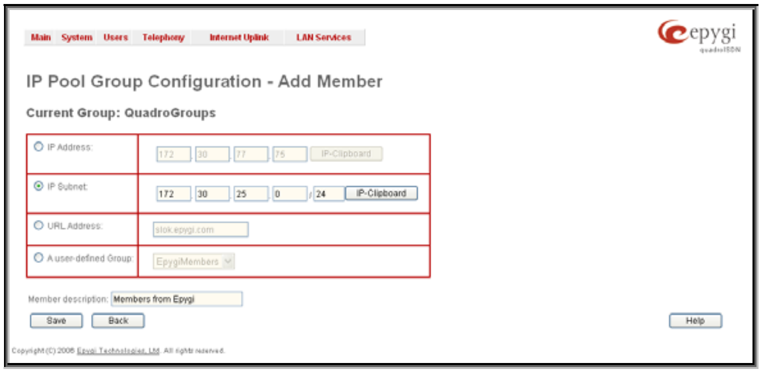
IP Address requires the member IP address to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

URL Address requires the member hostname to be added to the group.

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

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



IP Pool Group Configuration - Add Member

Current Group: QuadroGroups

○ IP Address:	172 . 30 . 77 . 75 IP-Clipboard
● IP Subnet:	172 . 30 . 25 . 0 / 24 IP-Clipboard
○ URL Address:	slok.epygi.com
○ A user-defined Group:	EpygiMembers

Member description: Members from Epygi

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. II-137: 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** or **URL Address** text field, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
8. Enter a **Member Description** in the corresponding text field, if needed.
9. To add a member with these parameters to the selected group press **Save**.

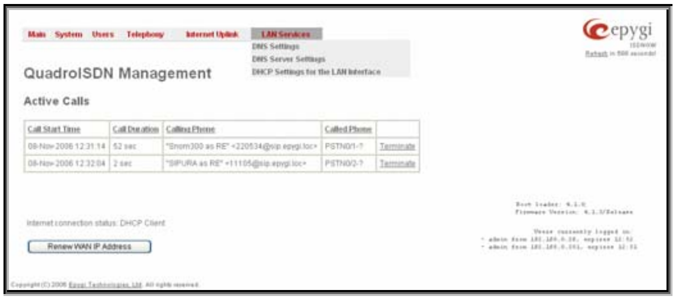
To Delete a Member

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Click on the desired members that should be deleted. The **IP Pool Group Configuration** list will appear.
3. Check one or more checkboxes of the corresponding members that should be deleted from the **Members** table. Press **Select all** if all members should be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.
5. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

To Delete a Group

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Check the one or more checkboxes of the corresponding groups that should be deleted from the groups table. Press **Select all** if all groups should be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

LAN Services Menu


Main System Users Telephony Internet Uplink LAN Services
DNS Settings
DNS Server Settings
DHCP Settings for the LAN Interface
epygi
Renew WAN IP Address
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

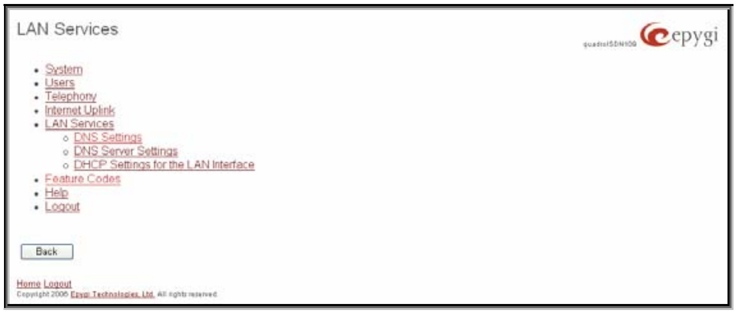
QuadroISDN Management

Active Calls

Call Start Time	Call Duration	Calling Phone	Called Phone	
08-Nov-2006 12:31:14	52 sec	"Snom300 as RE" <220534@sip.epygi.loc>	PSTN0/1-?	Terminate
08-Nov-2006 12:32:04	2 sec	"SIPURA as RE" <11105@sip.epygi.loc>	PSTN0/2-?	Terminate

Internet connection status: DHCP Client

Fig. II-138: LAN Services menu in Dynamo theme


quadroISDN100
epygi
Back
Home Logout
Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

LAN Services

- System
- Users
- Telephony
- Internet Uplink
- LAN Services
  - DNS Settings
  - DNS Server Settings
  - DHCP Settings for the LAN Interface
- Feature Codes
- Help
- Logout

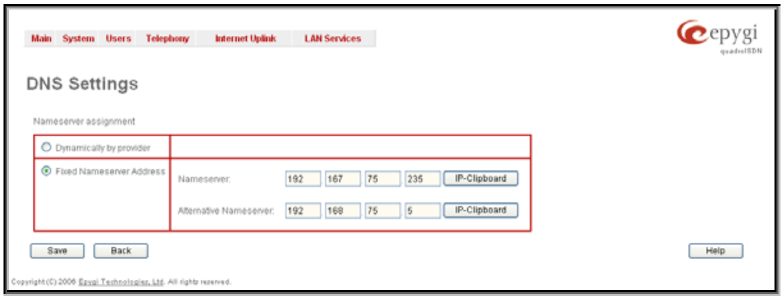
Fig. II-139: LAN Services menu in Plain theme

DNS Settings

The **DNS Settings** page provides the option of setting up a name server for the Quadro. It offers the following components:

The **Nameserver Assignment** radio buttons are as follows:

- The **Dynamically by provider** selection automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** is a manually selected name server. The **Nameserver** text field requires the IP address of an external name server. The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.


Main System Users Telephony Internet Uplink LAN Services
epygi
quadroISDN
IP-Clipboard
IP-Clipboard
Save
Back
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

DNS Settings

Nameserver assignment

○ Dynamically by provider

● Fixed Nameserver Address

Nameserver: 192 . 167 . 75 . 235

Alternative Nameserver: 192 . 168 . 75 . 5

Fig. II-140: DNS Settings page

DNS Server Settings

The **DNS Server** on the Quadro provides the services to the hosts in the Quadro’s LAN. With this service, Quadro returns the correct IP address to the requested domain name, so that any device in the LAN can be accessed by its hostname or alternative alias name.

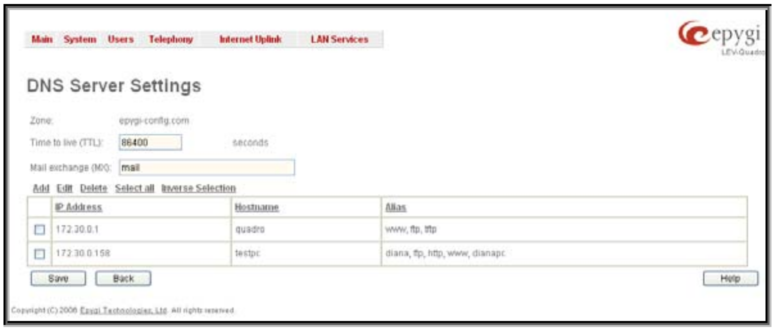
The **DNS Server Settings** page is used to configure DNS server settings on the Quadro and to define a list of aliases for the devices in the Quadro’s LAN. This page contains the following components:

Zone field displays the Quadro’s host domain name as it is configured in the System Configuration Wizard.

Time to live (TTL) text field indicates the time (in seconds) during which the DNS server will keep the resolved names in its cache. During this time the same address will be resolved from the cache of the DNS server. When this timeout expires, the requested address will be resolved newly.

Mail Exchange (MX) text field indicates the mail server’s hostname. When resolving the email address, the reference will go to the mail server defined in this field, before being sent out to the external network. The value in this field will be used in the MX record in the DNS server on the Quadro.

The table on this page lists aliases for each of the device in the Quadro’s LAN to be resolves through the DNS server.


Main System Users Telephony Internet Uplink LAN Services
epygi
LEV-Quadro
Add Edit Delete Select all Inverse Selection
Save
Back
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

DNS Server Settings

Zone: epygi-config.com

Time to live (TTL): 86400 seconds

Mail exchange (MX): mail

	IP Address	Hostname	Alias
□	172.30.0.1	quadro	www, ftp, tftp
□	172.30.0.158	testpc	diana, ftp, http, www, dianapc

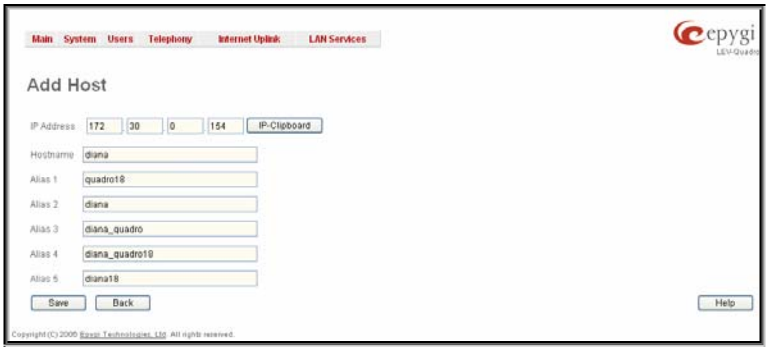
Fig. II-141: DNS Server Settings page

Add functional link opens the page **Add Host** where a list of aliased can be defined for the certain device in the Quadro’s LAN. The page contains the following components:

IP Address text fields require the IP address of the device in the Quadro’s LAN.

Hostname text field requires the hostname of the device in the Quadro’s LAN.

Alias text fields are used to enter up to 5 alias names by which the device in the Quadro’s LAN will be resolved.


Main System Users Telephony Internet Uplink LAN Services
epygi
LEV-Quadro
IP-Clipboard
Save
Back
Help
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Add Host

IP Address 172 . 30 . 0 . 154

Hostname diana

Alias 1 quadro18

Alias 2 diana

Alias 3 diana_quadro

Alias 4 diana_quadro19

Alias 5 diana18

Fig. II-142: DNS Server Settings – Add Host page

DHCP Settings for the LAN Interface

The **DHCP Settings** page provides the option of enabling a DHCP server and controlling the Quadro user’s LAN settings. Therefore, Quadro LAN users will automatically be provided with the following settings using the configured parameters:

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

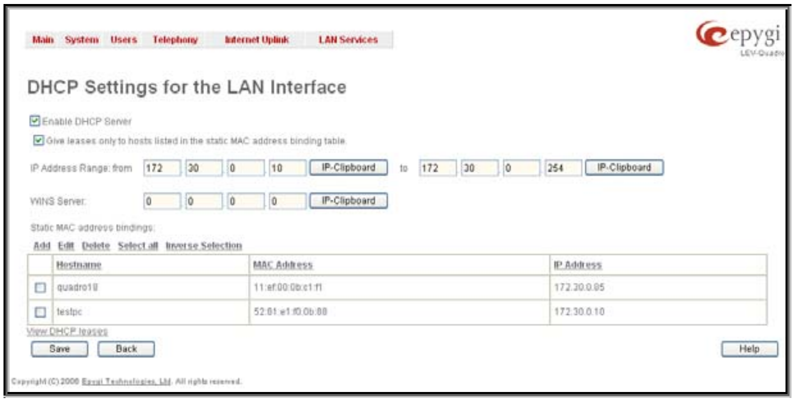
The **DHCP Settings** page offers the following input options:

Enable DHCP Server checkbox activates the DHCP server on Quadro. With this checkbox enabled, Quadro will be able to assign dynamic IP addresses to the devices in its LAN.

Give leases only to hosts listed in the static MAC address binding table checkbox enables the DHCP services only for the devices listed in the table below. With this checkbox selected, no DHCP services will be provided to the other devices.

IP Address Range defines a range of IP addresses that will be assigned to the Quadro LAN users. The IP range must be at least 6, otherwise the error message “Address Range too small” will prevent it from being saved. The error message “Address Range too large” will appear if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the Quadro LAN users.



DHCP Settings for the LAN Interface

☑ Enable DHCP Server

☑ Give leases only to hosts listed in the static MAC address binding table

IP Address Range: from 172 . 30 . 0 . 10 to 172 . 30 . 0 . 254

WINS Server: 0 . 0 . 0 . 0

Static MAC address bindings:

	Hostname	MAC Address	IP Address
□	quadro18	11:ef:00:0b:c1:f1	172.30.0.85
□	testpc	52:01:e1:f0:0b:88	172.30.0.10

Fig. II-143: DHCP Settings page for LAN interface

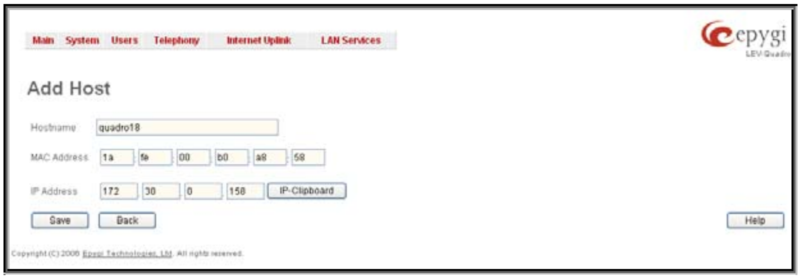
The table on this page allows you to set a static IP address binding on the MAC address of the device in the Quadro’s LAN. When this table is configured, the devices with defined hostnames and MAC addresses will always get the same LAN IP address from the DHCP server. Otherwise, devices not listed in this table will get dynamic LAN IP addresses.

Add functional button opens an **Add Host** page where a new static MAC address binding can be defined. The page consists of the following components:

IP Address text fields require the IP address of the device in the Quadro’s LAN.

MAC Address text fields require the MAC address of the device in the Quadro’s LAN.

Hostname text field requires the hostname of the device in the Quadro’s LAN.



Add Host

Hostname: quadro18

MAC Address: 1a : fe : 00 : b0 : a8 : 58

IP Address: 172 . 30 . 0 . 158

Fig. II-144: Static MAC address binding – Add Host page

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

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

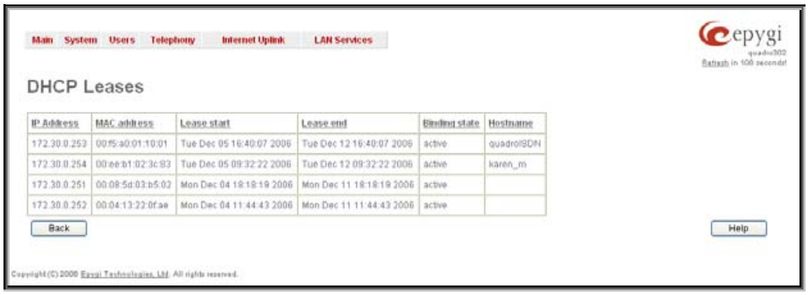
IP address - host IP address, assigned by Quadro.

MAC address - host MAC address, provided by the host itself.

Lease Start - date and time when the leased IP address has been activated.

Lease End - date and time when the leased IP address has been or will be deactivated.

Hostname - hostname, provided by the host itself.



DHCP Leases

IP Address	MAC address	Lease start	Lease end	Binding state	Hostname
172.30.0.253	00:f5:a0:01:10:01	Tue Dec 05 16:40:07 2006	Tue Dec 12 16:40:07 2006	active	quadroISDN
172.30.0.254	00:ee:b1:02:3c:83	Tue Dec 05 09:32:22 2006	Tue Dec 12 09:32:22 2006	active	karen_m
172.30.0.251	00:08:5d:03:b5:02	Mon Dec 04 18:18:19 2006	Mon Dec 11 18:18:19 2006	active	
172.30.0.252	00:04:13:22:0f:ae	Mon Dec 04 11:44:43 2006	Mon Dec 11 11:44:43 2006	active	

Fig. II-145: DHCP Leases page for LAN interface

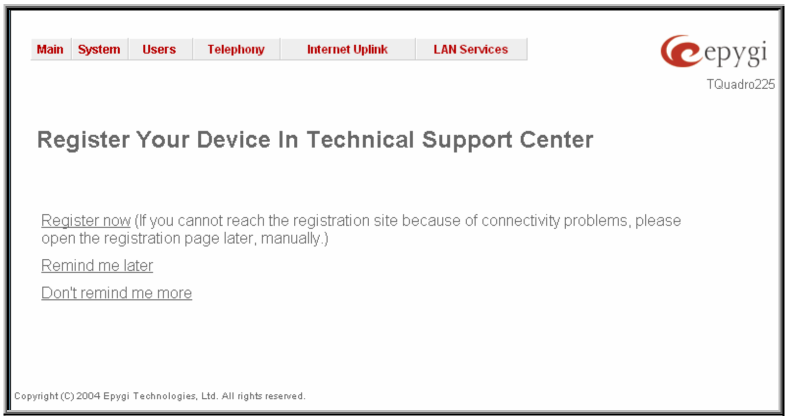
Registration Form

The **Registration Form** page appears when administrating an unregistered Quadro, and it has been created for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It provides several links offering the following registration options:

Register now leads to the Epygi Technical Support System Registration page and requires customer’s information to submit the Quadro registration form.

Remind me later hides the registration notification in the Quadro through System Configuration Wizard or Internet Configuration Wizard until the next administrating activities..

Don’t remind me more hides the registration notification forever.



Register Your Device In Technical Support Center

Register now (If you cannot reach the registration site because of connectivity problems, please open the registration page later, manually.)

Remind me later

Don't remind me more

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-146: Device Registration page

Logout

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

Extension User's Menus

When logging in as an extension user the page **Main Menu** is displayed with the Extensions Management table as a startup (see below).

Voice Mail

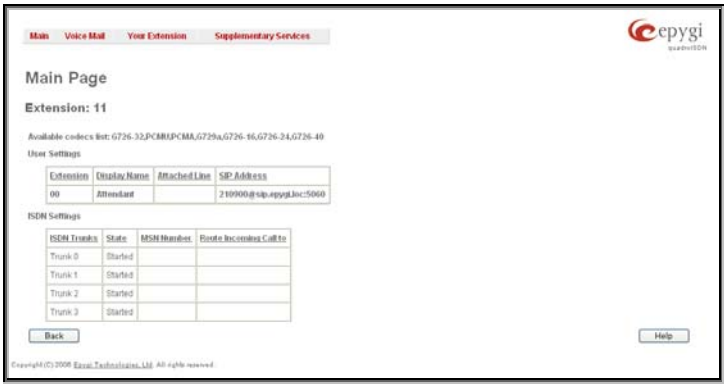
- Voice Mailbox
- Voice Mail Settings
- Group List

Your Extension

- Call Statistics
- Account Settings

Supplementary Services

- Caller ID Based Services
  - Incoming Call Blocking
  - Outgoing Call Blocking
  - Call Hunting
  - Unconditional Call Forwarding



Main Page

Extension: 11

Available codecs list: G726-32,PCMU,PCMA,G729a,G726-16,G726-24,G726-40

User Settings

Extension	Display Name	Attached Line	SIP Address
00	Attendant		210900@sip.epygi.loc:5060

ISDN Settings

ISDN Trunks	State	MSN Number	Route Incoming Call to
Trunk 0	Started		
Trunk 1	Started		
Trunk 2	Started		
Trunk 3	Started		

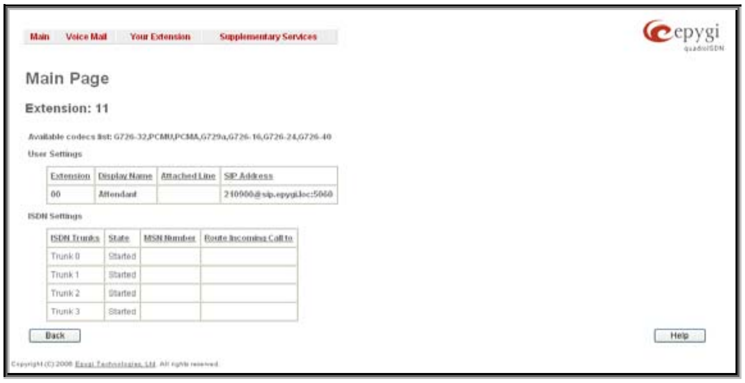
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-1: Quadro Extension User’s page

Main Page

The **Main Page** provides read only information about the extension codecs, other extensions and available ISDN trunks on the Quadro depending on the active interface.

The **Main Page** displays a list of available codecs for the corresponding extension, the list of other extensions on the Quadro, their Display names and the SIP registration username. It also displays the ISDN trunks state and the destination to route incoming calls. For ISDN trunks, trunk specific MSN numbers are displayed here.



Main Page

Extension: 11

Available codecs list: G726-32,PCMU,PCMA,G729a,G726-16,G726-24,G726-40

User Settings

Extension	Display Name	Attached Line	SIP Address
00	Attendant		210900@sip.epygi.loc:5060

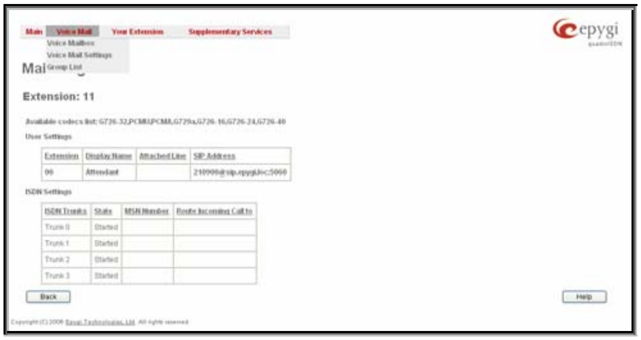
ISDN Settings

ISDN Trunks	State	MSN Number	Route Incoming Call to
Trunk 0	Started		
Trunk 1	Started		
Trunk 2	Started		
Trunk 3	Started		

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-2 Extension’s Main Page

Voice Mail



Extension: 11

Available codecs list: G726-32,PCMU,PCMA,G729a,G726-16,G726-24,G726-40

User Settings

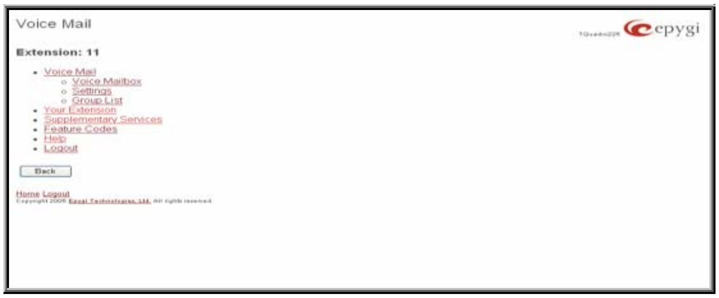
Extension	Display Name	Attached Line	SIP Address
00	Attendant		210900@sip.epygi.loc:5060

ISDN Settings

ISDN Trunks	State	MSN Number	Route Incoming Call to
Trunk 0	Started		
Trunk 1	Started		
Trunk 2	Started		
Trunk 3	Started		

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-3 Voice Mail menu in Dynamo Theme



Voice Mail

Extension: 11

- Voice Mail
  - Voice Mailbox
  - Settings
  - Group List
- Your Extension
- Supplementary Services
- Feature Codes
- Help
- Logout

Home Logout
Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-4 Voice Mail menu in Plain Theme

The **Voice Mail Service** provides a possibility to leave brief voice messages on the mailbox of an unavailable or busy Quadro extension. The caller hears a greeting message (configurable by the extension user) and a signal initiating the Voice Mail recording. The extension user may configure the maximum duration of the voice message, as well as the Voice Mail system activation timeout (see chapter Voice Mail Settings).

Received voice messages are stored in the Voice Mailbox. They can be accessed by the * 0 key combination from the phone handset and via Quadro management. Voice messages can to be played, marked (from GUI only), deleted, replied to (from handset only) or forwarded by the user. Messages with a facsimile (FAX) attached will be displayed in a special way in the Voice Mailbox on web management access and will be indicated by a special voice signal when accessing the message from the handset. The Incoming FAX message can be viewed and downloaded to the PC from the Voice Mailbox at Web management access as a *.tif picture file.

Quadro’s Voice Mail service also allows reviewing system messages used for telephony services functionality. The voice mail greeting, incoming and outgoing blocking messages, user’s name and out of office greeting can be played, recorded and restored. Greeting messages are played to the caller announcing that the called extension is unavailable and asking to leave a voice mail. Blocking messages are played when receiving or making incoming/outgoing calls from/to the restricted destination. User’s name is played when surfing the Extensions Directory. The personal out of office greeting is played instead of the main greeting message, when out of office option is selected on the extension.

Voice Mailbox

Quadro provides caller the possibility of leaving voice messages when called extension is busy or unavailable. A voice mail greeting message, and a voice signal indicating voice mail recording initiation, are played back to the caller.

All voice mail functionality settings, such as enabling the greeting message, adjusting the maximal voice mail duration, voice mail system activation timeout, etc, are configurable by the user through the extension’s Voice Mail Settings.

Received voice mails are stored and are accessible in the extension’s Voice Mailbox. Quadro supports two ways of accessing the extension’s Voice Mailbox: through the phone handset and through Quadro Web Management. With both options, the user is free to manipulate with voice mails located in the Voice Mailbox, such as playing, deleting, forwarding, etc.

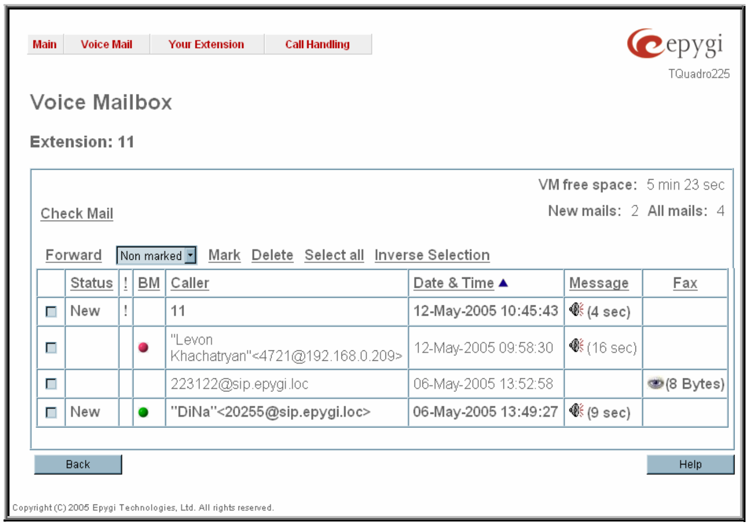
When accessing the Voice Mailbox through the phone handset, additional settings to manipulate the user defined system messages are provided. The user can define their own Voice Mail Greeting, Incoming and Outgoing Blocking messages as well as the User’s recorded name. Each of these system messages can be played, recorded and restored. Voice Mail Greeting messages are played back to the caller announcing that the called extension is unavailable and asking to leave a voice mail. Blocking messages are played back to the caller when receiving or making incoming/outgoing calls from/to the restricted destination. User’s recorded Name is used in the Extensions Directory when the spelled name matches the entry in the directory table.

Instructions on accessing and navigating within the voice messages and Voice Mailbox Services via the phone handset are described in the Feature Codes.

Please Note: When playing newly received voice mails (via a phone handset or with the use of the **Play** button in this page) will deprive the “New” state of the voice mail.

The **Voice Mailbox** can hold **New** (not yet played) and **Old** (already played) voice mails. The **Status** column in the Voice Mailbox table indicates the current state of the voice mails. All new mails in the table are displayed in bold font. Playing a voice mail cancels both the **New** status and bold font.

Voice mails can be selected to be played, deleted, marked as important or book-marked, etc. Additionally they can be forwarded to desired email addresses.



Voice Mailbox

Extension: 11

VM free space: 5 min 23 sec

New mails: 2 All mails: 4

	Status	!	BM	Caller	Date & Time ▲	Message	Fax
□	**New**	**!**		**11**	**12-May-2005 10:45:43**	**(4 sec)**	
□			●	"Levon Khachatryan"<4721@192.168.0.209>	12-May-2005 09:58:30	(16 sec)	
□				223122@sip.epygi.loc	06-May-2005 13:52:58		(8 Bytes)
□	**New**		●	**"DiNa"<20255@sip.epygi.loc>**	**06-May-2005 13:49:27**	**(9 sec)**	

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-5 Extension Voice Mailbox

VM free space provides information on the number of minutes/seconds of free voice mailbox space.

The following functional buttons and fields are available:

Check Mail refreshes the mailbox and updates the number of newly arrived mails (if any).

New Mails shows the number of newly arrived mails since the user's last access to the voice mailbox.

All Mails shows the number of all mails existing in the mailbox.

The **Voice Mailbox** tables display all voice mails in the mailbox:

Status - indicates whether the voice mail is **New** and not yet played. New mails are displayed in bold font.

! - indicates whether message has an urgent priority or not.

BM (bookmark) - shows marked records. The fields can include some indications (image signs) depending on the type of being marked.

Caller – is the address of the caller who left the voice mail.

Date & Time – is the voice mail receipt date and time.

Message – indicates voice mail duration (in minutes/seconds) and a speaker sign used to play (using any available media player supported by your Operation System) the received voice mail or to download the audio file to the PC.

FAX (facsimile) – indicates whether a FAX message is attached to the voice mail, and if so, displays the size of the FAX message (in KBs) and an icon used to view the incoming FAX message or download the graphical file to PC.

The column headings of the voice mail tables are created as a link. By clicking on the column heading the table will be sorted by the selected column. Upon sorting (ascending, descending) arrows will be displayed next to the column heading. Each row in the Voice Mailbox tables can be selected by a checkbox for editing, deleting or marking.

The following functional buttons serve to modify the table entries:
Forward link allows forwarding a selected voice mail to one or more email addresses with some enclosed message in the email body. The link refers to the page where email addresses should be defined (use a space or a comma to separate the mailing addresses in the text field), email subject and some message can be inserted. Voice mails will get automatically converted to the G.711 codec before being attached to the email. The Voice Mail forwarding feature is active only when Mail Service is enabled otherwise the “Mail Service is disabled” error appears.

Mark submits the values chosen out of the drop down list aside (Important or Bookmark) to the selected records.
Delete removes the selected voice mail record(s).
Select All checks all existing entries in the table.
Inverse Selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

To Play a Voice Mail

1. Click on the speaker icon of the corresponding voice message.
2. Depending on you browser’s settings the .wav file will be played directly or an application will ask you to save the .wav file on the local PC. In the second option, please specify the path and run the media file from the specified location to play it.

To Mark a Voice Mail Record

1. Select the checkbox of the corresponding record in the **Voice Mailbox** table that should to be marked. Press **Select all** if all extensions should to be marked.
2. Select the desired marking type from the **Mark** drop down list.
3. Select the **Mark** button to initiate the marking operation. Depending on the selected marking type the record(s) will show an image sign in the corresponding **BM** field.

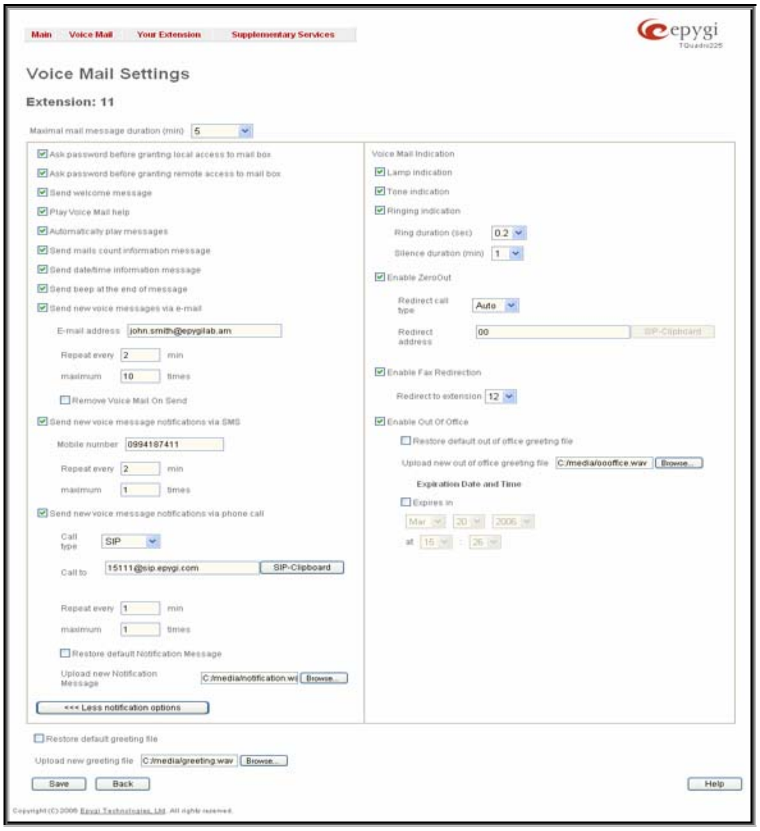
To Delete a Voice Mail Record

1. Select the checkbox of the corresponding record(s) in the **Voice Mailbox** table that should to be deleted. Click on **Select all** if all records should to be deleted.
2. Select the **Delete** button.
3. Confirm the deletion with **Yes**. The selected voice messages will be deleted. To abort the deletion and keep the messages in the inbox, select **No**.

Voice Mail Settings

The **Voice Mail Settings** permits enabling the **Voice Mail Service** for the callers if the called extension is not available or does not answer. The voice mail system will be activated allowing the caller to leave a voice message. This page also provides information on the voice mailbox settings such as maximal mail message duration, voice mail indication method when a new voice mail arrives, various settings for the voice mailbox as well as a possibility to send voice mails via e-mail.

Please Note: Voice Mail Settings are only available when the Voice Mailbox is enabled on the extension. If you find Voice Mail Settings are unavailable please refer to your system administrator.



Voice Mail Settings

Extension: 11

Maximal mail message duration (min) 5

☑ Ask password before granting local access to mail box
☑ Ask password before granting remote access to mail box
☑ Send welcome message
☑ Play Voice Mail help
☑ Automatically play messages
☑ Send mails count information message
☑ Send date/time information message
☑ Send beep at the end of message
☑ Send new voice messages via e-mail

E-mail address john.smith@epygilab.am
Repeat every 2 min
maximum 10 times
☐ Remove Voice Mail On Send

☑ Send new voice message notifications via SMS
Mobile number 0994187411
Repeat every 2 min
maximum 1 times

☑ Send new voice message notifications via phone call
Call type SIP
Call to 15111@sip.epygi.com
Repeat every 1 min
maximum 1 times
☐ Restore default Notification Message
Upload new Notification Message C:/media/notification.wa

Voice Mail Indication
☑ Lamp indication
☑ Tone indication
☑ Ringing indication
Ring duration (sec) 0.2
Silence duration (min) 1
☑ Enable ZeroOut
Redirect call type Auto
Redirect address 00
☑ Enable Fax Redirection
Redirect to extension 12
☑ Enable Out Of Office
☐ Restore default out of office greeting file
Upload new out of office greeting file C:/media/oooffice.wav
Expiration Date and Time
☐ Expires in
Mar 20 2006
at 15 : 26

☐ Restore default greeting file
Upload new greeting file C:/media/greeting.wav

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-6 Voice Mail Settings page

The **Voice Mail Settings** page offers the following input options:

Maximal mail message duration lists the possible values for the maximal mail duration (counted in minutes) during which a voice mail will be recorded. The **Unlimited** selection allows voice message recording as long as the user's space remains.

Ask password before granting local access to mailbox protects local access of the user's voice mailbox. If the checkbox is checked a user password will be required to access the voice mailbox via * 0 digit combination.

Ask password before granting remote access to mailbox protects remote access of the user's voice mailbox. If the checkbox is checked a user password will be required to access the voice mailbox when reaching it through the Auto Attendant.

Send welcome message enables a welcome message to be played to the user when accessing the mailbox locally.

Play Voice Mail Help is an optional setting that plays voice mail help instructions to the user when entering the Voice Mailbox. This option guides the user through the mailbox, explaining how to play and delete the voice mails as well as modifying system messages.

Automatically play messages will auto play of all voice mails. Whenever entering the voice mailbox, the system will sequentially play the date/time when the message was received followed by the voice mail itself in the order sorted by the priority level (starting with the message in highest priority) or. If no priority is specified, they will be played in the order in which messages were received, i.e. starting with first (oldest) message. When the last message is played, the Voice Mail help will be replayed.

Send mails count information message announces the number of **New** (unread) voice messages in the mailbox when entering the mailbox.

Send date/time information message announces the time and date a voice message was received and is played before every voice message.

Send beep at the end of message enables an optional parameter that activates a "beep" sound after each played voice message.

Send new voice message via email is an option to send new voice mail files via e-mail to the defined recipients. Mails will be automatically converted to the Windows wave (PCMU) format before being attached to the e-mail. Checkbox activates the following input options:

> **Email Address** requires the e-mail address(es) of the person(s) that should to receive the newly arrived voice mails on their e-mail account(s). Use a space or a comma to separate the mailing addresses in the text field.
>
> The next two fields are used for retransmission of email notifications. Number of times text field requires the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If notification is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field.
>
> **Remove Voice Mail on send** removes the voice mail from the user mailbox after sending it to the e-mail recipient(s).
>
> **Please Note:** This service will work only when **System Mail** is enabled on the Quadro. Contact your system administrator if you have problems with voice mail delivery via email.

Send new voice message notification via SMS allows the voice mail notification delivery via SMS to the defined mobile number. Checkbox activates the following input options:

> **Mobile Number** text field requires the destination's mobile number.
>
> The next two fields are used for retransmission of SMS notifications. The number of times text field requires the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the notification is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field.
>
> **Please Note:** This service will work only when **SMS Service** is enabled on the Quadro. Contact your system administrator if you have problems with voice mail notifications delivery via SMS.

Send new voice message notification via phone call enables the voice mail notification delivery via a phone call to the defined phone number. The checkbox activates the following input options:

> **Call Type** drop down list includes the available call types:
>
> - PBX - local calls to Quadro extensions;

- SIP – calls through a SIP server;
- Auto – for undefined call types. The destination (independent on whether it is a PBX number or SIP address) will be reached through Routing;
- Callback – automatic call to the voice mail author. This can be used as a notification that the recipient has received the voice mail but has not yet played it.

Call To text field requires the destination’s phone number depending on the selected call type. For **Callback** call type, no destination’s phone number is required.

The next two fields are used for retransmission of phone notifications. Number of times text field indicates the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the notification is specified to be sent only once, insert “1” in **Repeat every** text field and “0” in the Number of times text field. For **Callback** call type, the first notification is sent to the voice mail author after the first expiration of the interval defined in the **Repeat every** text field. For calls with call type different from Callback, the first notification will be sent immediately.

Restore default Notification Message restores the default notification message. If the checkbox is selected, the file upload will be disabled.

Upload new Notification Message will show the attached notification file selected by the current extension. Please note that a different notification message can be uploaded in case this service serves as a notification to the extension user (to inform about the new voice mail received) or if it serves as a notification for the voice mail author to be informed that the message has been received by the Quadro but is not yet played by the extension user. The uploaded file needs to be in the PCMU wave format, otherwise the system will prevent uploading with the “Invalid audio file, or format is not supported” warning message. The system also prevents uploading in case insufficient space is available on Quadro for the corresponding extension and gives a “You do not have enough space” warning.

Browse browses for the notification file that must be in PCMU wave format.

Download Notification Message appears only if a file has been uploaded previously. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

Voice Mail indication enables user notifications for new voice messages in the mailbox. The checkbox offers the following three types of voice mail indications:

Lamp indication– depending on the type of phone a visual blinking signal will announce a new voice mail.

Tone indication – the user will hear a specific tone when lifting the handset.

Ringing indication – the user will be able to create a specific ring pattern when new voice mail has arrived. The checkbox enables the following ringing pattern configuration parameters:

- **Ring duration** – the available ring durations (counted in seconds).
- **Silence duration** – the available silence durations (counted in minutes).

The **ZeroOut** voice mail feature allows a caller that has reached the called extension’s voice mailbox to accelerate the automatic redirection feature instead of leaving a message in the extension’s Voice Mailbox. To activate this feature, the caller should dial 0 digit (see Feature Codes) during the voice mail greeting which invites the caller to leave a message. The caller will then be automatically transferred to the destination specified in this page.

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

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

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

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

The **Enable FAX Redirection** checkbox is used to redirect the incoming FAX (facsimile) when the FAX tone is detected after Voice Mail has been activated. The checkbox selection enables the **Redirect to extension** drop down list where extensions with enabled FAX Support are listed and is used to select the extension where the incoming FAX should be forwarded.

The **Enable Out of Office** checkbox allows activation of the Out of Office message which acts as an optional Voice Mail Greeting message in the period while the user is out of office, on vacations, etc. When this checkbox is selected, a user-defined Out of Office message will be played (if uploaded or recorded from the phone handset, otherwise a default Out of Office message will be used) to the caller which reached the called extension’s Voice Mailbox.

Restore default Out of Office file restores the default Out of Office message file. If the checkbox is selected, the file upload will be disabled.

Upload new Out of Office Greeting file will show the attached Out of Office message file selected by the current user. The Out of Office message file will be played to a caller when entering the voice mail system. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent its uploading and will give the “Invalid audio file, or format is not supported” warning message. The system also prevents uploading when insufficient space is available on Quadro for the corresponding extension. In this situation, the “You do not have enough space” warning will be received. Optionally, the Out of Office message can be recorded from the phone handset (see Feature Codes).

Browse browses for the Out of Office message file that must be in PCMU wave format.

Download Out of Office Greeting file appears only if some file has been uploaded previously. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

Expiration Date and Time selection is used to set the expiration date and time of the Out of Office message validity. When the expiration date/time expires, the Out of Office message automatically gets disabled and Voice Mail regular greeting gets activated again.

Restore default Greeting file will restore the default greeting file. If the checkbox is selected, the file upload will be disabled.

Upload new greeting file will show the attached greeting file selected by the current user. The greeting file will be played to a caller when entering the voice mail system. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading and the “Invalid audio file, or format is not supported” warning message will be received. The system also prevents uploading in case insufficient space is available on Quadro for the corresponding extension. In this situation, the “You do not have enough space” warning will be received. Optionally, a greeting file can be recorded from the phone handset (see Feature Codes).

Browse browses for the greeting file that must be in PCMU wave format.

Download Greeting File appears only if a file has been previously uploaded. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

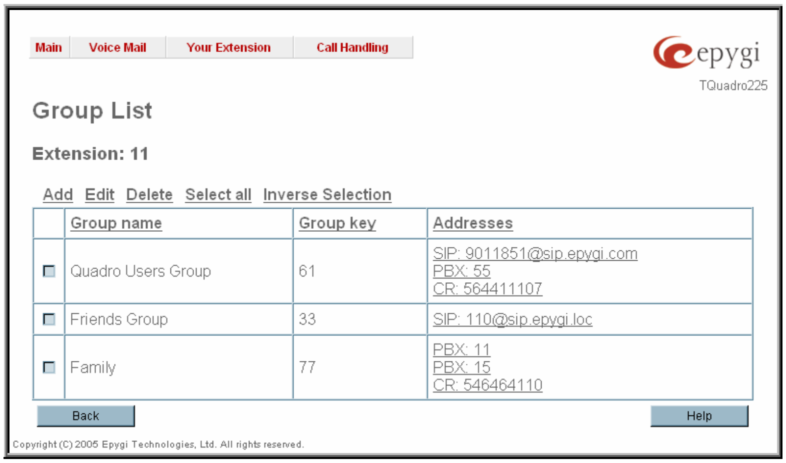
Group List

Group List allows you to define Groups with the specified addresses inside. The **Group List** is used to send or forward voice messages (see Feature Codes) to the number of addresses simultaneously. Groups may consist of a variety of PBX and SIP addresses.

The **Group List** page consists of a table where all defined Group Keys and the corresponding addresses are listed.

Press on a link in the **Addresses** column to access the **Address List for the Group** page and to modify the addresses of the corresponding group. If Group doesn’t include addresses, “no address is available” will be displayed in the **Addresses** column.

The **Add** functional button opens the **Group List - Add Entry** page where a new Group Key can be defined.



Group List

Extension: 11

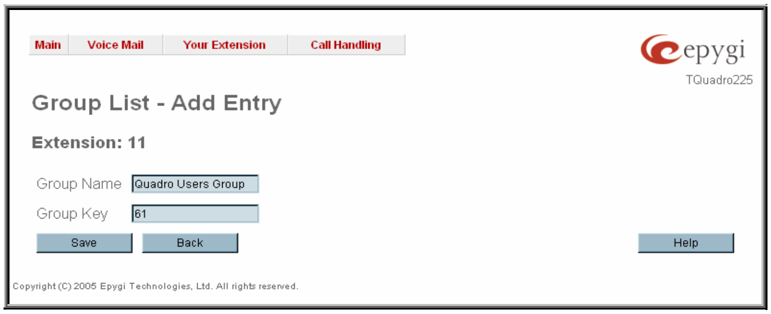
	Group name	Group key	Addresses
□	Quadro Users Group	61	SIP: 9011851@sip.epygi.com PBX: 55 CR: 564411107
□	Friends Group	33	SIP: 110@sip.epygi.loc
□	Family	77	PBX: 11 PBX: 15 CR: 546464110

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. III-7 Group List page

The **Group List - Add Entry** page consists of two text fields used to insert the **Group Key** and the **Group Name** (optionally). The **Group Key** should include numeric characters only and should be unique in the Group List table.

Please Note: Groups with keys equal to extension numbers on Quadro have a higher priority and will be applied when sending or forwarding a voice message to the corresponding destination.



Group List - Add Entry

Extension: 11

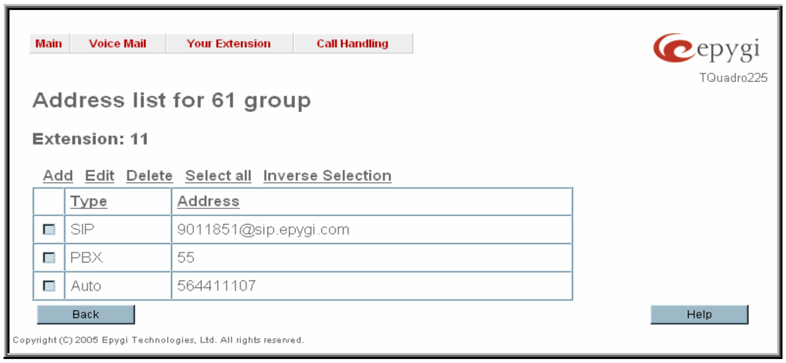
Group Name	Quadro Users Group
Group Key	61

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. III-8 Add Group page

The **Address List for the Group** page contains a table of addresses where new address may be added to the group and existing ones may be edited or deleted.

The **Add** functional link moves to the **Address List for the Group – Add Entry** page where new address may be defined.



Address list for 61 group

Extension: 11

	Type	Address
□	SIP	9011851@sip.epygi.com
□	PBX	55
□	Auto	564411107

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

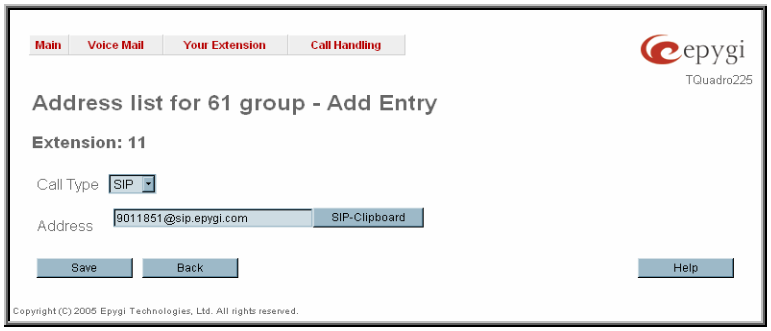
Fig. III-9 Addresses List page

Address List for the Group – Add Entry page consists of he following components:

Call Type lists the available call types:

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

The **Address** text field is used to define the address that ought to be included in the group. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the Quadro extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined.



Address list for 61 group - Add Entry

Extension: 11

Call Type: SIP

Address: 9011851@sip.epygi.com

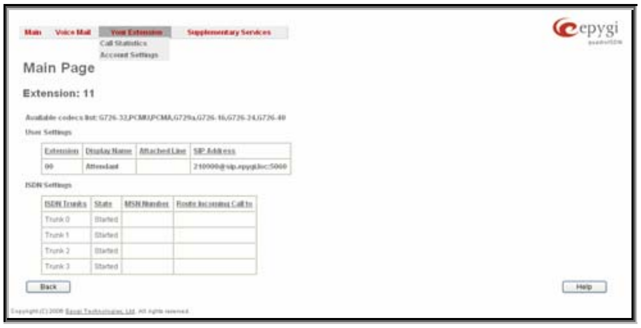
Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. III-10 Add Address page

To Configure a Group

1. Press Add in the Group List page. **Group List - Add Entry** page will be displayed in the browser window.
2. Fill in the **Group Key** and **Group Name** (optionally) in the same named field.
3. Press **Save**.
4. Click on the link in the row corresponding to the newly created Group.
5. Press Add in the **Address List for the Group** page. **Address List for the Group – Add Entry** page appears.
6. Choose a **Call Type** from the corresponding drop down list.
7. Define the group member address in the **Address** text field.
8. Press **Save**.

Your Extension



Main Page

Extension: 11

Available codecs list: G726-32,PCMU,PCMA,G729a,G726-16,G726-24,G726-40

User Settings

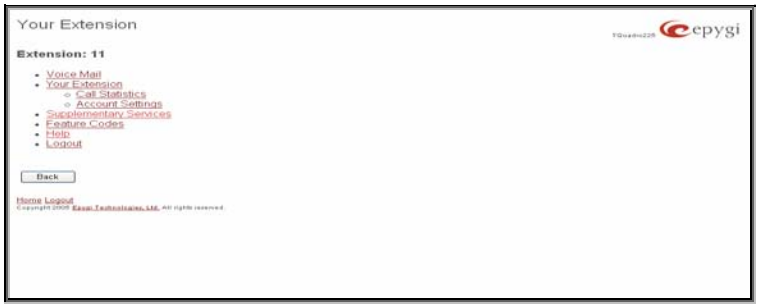
Extension	Display Name	Attached Line	SIP Address
00	Attendant		210000@sip.epygi.loc:5000

ISDN Settings

ISDN Trunks	State	MSN Number	Route Incoming Call to
Trunk 0	Started		
Trunk 1	Started		
Trunk 2	Started		
Trunk 3	Started		

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig.III-11 Your Extension menu in Dynamo theme



Your Extension

Extension: 11

- Voice Mail
- Your Extension
  - Call Statistics
  - Account Settings
- Supplementary Services
- Feature Codes
- Help
- Logout

Home Logout

Copyright 2006 Epygi Technologies, Ltd. All rights reserved

Fig. III-12 Your Extension menu in Plain Theme

Call Statistics

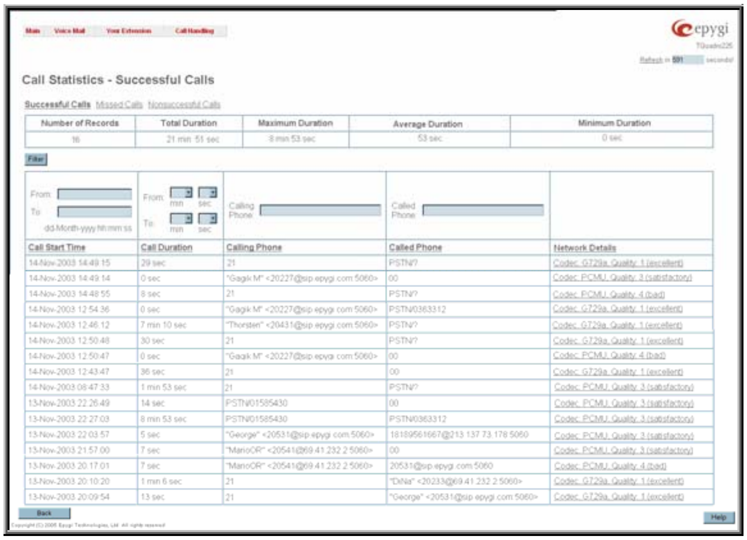
The **Call Statistics** page collects the call events and their parameters over the Quadro, i.e. incoming and outgoing calls reporting. It contains three tables and provides reports on successful, not successful and missed incoming and outgoing calls for the current extension only. This page also allows you to filter the collected **Call Statistics** based on various criteria. The search components are as follows:

The **From** and **To** text fields are used to search by date and time. The data must be inserted in the following format: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The **From** field must indicate an earlier date and time from that which is indicated in the **To** field. If the entered data is not an earlier date and time, the “Minimal date should be less than maximal date” error message prevents statistics from filtering.

The **From** and **To** drop down lists are used to search by duration. The duration needs to be specified from the listed values. The **From** field must indicate a shorter duration than the **To** field. If the entered data is a larger duration, the “Minimal duration should be less than maximal duration” error message prevents statistics from filtering.

Called Phone requires the called party’s SIP address, extension or PSTN number as a search criteria.

Calling Phone requires the caller party’s SIP address, extension or PSTN number as a search criteria. For both **Called** and **Calling Phone** wildcards are available (see chapter Entering a SIP Addresses correctly). If the defined caller or called addresses are inserted incorrectly the “Calling (Called) address is incorrect” error message will prevent filtering.



Refresh in 591 seconds!

Call Statistics - Successful Calls

Successful Calls Missed Calls Nonsuccessful Calls

Number of Records	Total Duration	Maximum Duration	Average Duration	Minimum Duration
16	21 min 51 sec	8 min 53 sec	53 sec	0 sec

Call Start Time	Call Duration	Calling Phone	Called Phone	Network Details
14-Nov-2003 14:49:15	29 sec	21	PSTN/?	Codec: G729a, Quality: 1 (excellent)
14-Nov-2003 14:49:14	0 sec	"Gagik M" <20227@sip.epygi.com:5060>	00	Codec: PCMU, Quality: 3 (satisfactory)
14-Nov-2003 14:48:55	8 sec	21	PSTN/?	Codec: PCMU, Quality: 4 (bad)
14-Nov-2003 12:54:36	0 sec	"Gagik M" <20227@sip.epygi.com:5060>	PSTN/0363312	Codec: G729a, Quality: 1 (excellent)
14-Nov-2003 12:46:12	7 min 10 sec	"Thorsten" <20431@sip.epygi.com:5060>	PSTN/?	Codec: G729a, Quality: 1 (excellent)
14-Nov-2003 12:50:48	30 sec	21	PSTN/?	Codec: G729a, Quality: 1 (excellent)
14-Nov-2003 12:50:47	0 sec	"Gagik M" <20227@sip.epygi.com:5060>	00	Codec: PCMU, Quality: 4 (bad)
14-Nov-2003 12:43:47	36 sec	21	00	Codec: G729a, Quality: 1 (excellent)
14-Nov-2003 08:47:33	1 min 53 sec	21	PSTN/?	Codec: PCMU, Quality: 3 (satisfactory)
13-Nov-2003 22:26:49	14 sec	PSTN/01585430	00	Codec: PCMU, Quality: 3 (satisfactory)
13-Nov-2003 22:27:03	8 min 53 sec	PSTN/01585430	PSTN/0363312	Codec: PCMU, Quality: 3 (satisfactory)
13-Nov-2003 22:03:57	5 sec	"George" <20531@sip.epygi.com:5060>	18189561667@213.137.73.178:5060	Codec: PCMU, Quality: 3 (satisfactory)
13-Nov-2003 21:57:00	7 sec	"MarioOR" <20541@69.41.232.2:5060>	00	Codec: PCMU, Quality: 3 (satisfactory)
13-Nov-2003 20:17:01	7 sec	"MarioOR" <20541@69.41.232.2:5060>	20531@sip.epygi.com:5060	Codec: PCMU, Quality: 4 (bad)
13-Nov-2003 20:10:20	1 min 6 sec	21	"DiNa" <20233@69.41.232.2:5060>	Codec: G729a, Quality: 1 (excellent)
13-Nov-2003 20:09:54	13 sec	21	"George" <20531@sip.epygi.com:5060>	Codec: G729a, Quality: 1 (excellent)

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-13 Extension’s Call Statistics page

The **Call Statistics - Successful Calls, Call Statistics - Missed Calls** and **Call Statistics - NonSuccessful Calls** tables list the successful, missed and not successful incoming and outgoing calls and their parameters (Call Start Time, Call durations, Calling and Called phones) for each corresponding extension. Each column heading in the tables are created as links. By clicking on a column heading, the table will be sorted by the selected column. After the sorting (ascending or descending) arrows will be displayed next to the column heading.

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

The **Network Details** column is available in the **Successful Calls** table only and provides brief information about the call quality and the codecs used to transmit and receive packets. Clicking on the successful call details will open **RTP Statistics** page where detailed information (Call Quality, Receive and Transmit Codecs, Number of Packets and Packet Sizes, Number of Received Lost Packets, Receive Jitter and Receive Maximum Delay) about the established call is provided. The **Call Detail** column is available in the **Non Successful Calls** table only and indicates the reason why the call was unsuccessful.

Filter performs a search procedure according to the selected criteria. The search may be conducted with several criteria at the same time.

To Filter the Statistics

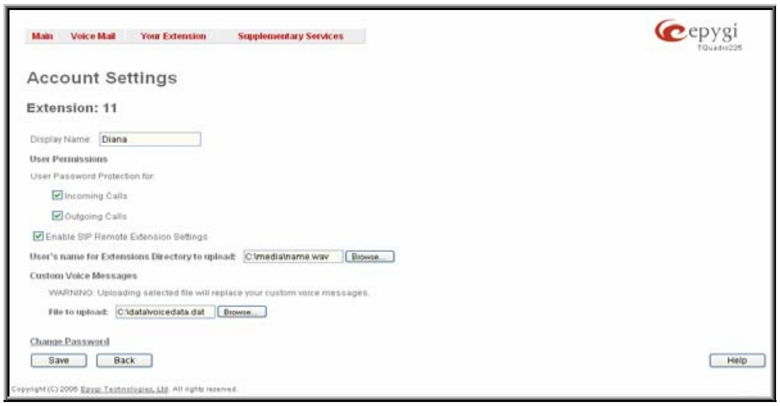
1. Enter the desired search criteria.

2. Click on the **Filter** button to search call reports within the **Call Statistics** table.

Please Note: To return to the complete statistics table clear all search criteria and press **Filter**.

Account Settings

The **Account Settings** page provides information on the extension display name, allows changing the user password, enabling user password protection for incoming/outgoing calls and downloading/uploading of a file with the user-defined voice greetings. All parameters listed on this page may be modified and submitted. This page consists of the following components:



Account Settings

Extension: 11

Display Name: Diana

User Permissions

User Password Protection for:

☑ Incoming Calls

☑ Outgoing Calls

☑ Enable SIP Remote Extension Settings

User's name for Extensions Directory to upload: C:\media\name.wav

Custom Voice Messages

WARNING: Uploading selected file will replace your custom voice messages.

File to upload: C:\data\voicedata.dat

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. III-14 Extension Account Settings page

Extension shows a non-editable parameter providing information about the current user extension number.

Display Name defines an optional parameter used to identify the caller. Usually the display name appears on the phone display if a call is placed or a voice mail is sent. The field is not limited regarding symbol usage but its length is limited to twenty characters.

Password Protection for:

- **Incoming Calls** enables password protection for incoming calls. If the service is enabled a user password is required to be able to accept the incoming calls.
- **Outgoing Calls** enables password protection for outgoing calls. If the service is enabled a user password is required to be able to make calls.

Enable SIP Remote Extension Settings checkbox is only visible when the system administrator has activated the **SIP Remote Extension** service for the corresponding extension at least one time. With this checkbox, the extension user may enable/disable the **SIP Remote Extensions** functionality. The administrator defines all settings of the SIP Remote Extension feature.

Please Note: If you find the **Enable SIP Remote Extension Settings** checkbox missing on this page, please consult with your system administrator for the first-time activation of the **SIP Remote Extension** service on the corresponding extension.

The **User's name for Extensions Directory to upload** text field is used to enter the path where the file with the user's name is located. If the file with the user's name is browsed with the help of file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the file with the user's name. The user's name also can be modified from the handset and will be played when the spelled name matches the name configured for the corresponding user.

Please Note: A user cannot be reached through the Extensions Directory until their name is recorded/uploaded into the Extensions Directory.

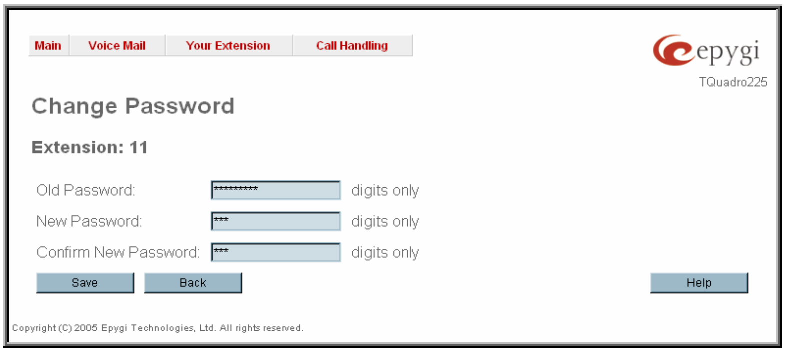
The **Download User's name** link is used to download the user-defined wave file with the user's name.

The **File to upload** text field is used to type in the path where the backed up file with voice messages is located. If voice greetings are browsed with the help of a file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the previously downloaded file with custom voice messages.

Attention: Uploading the selected file will replace your custom voice messages. Uploading custom messages downloaded from the other Quadro will overwrite messages that have not been configured by the user with the current device defaults. This means that if some default messages were used on one Quadro, they may be completely different on another Quadro after uploading of the voice data.

The link **Download custom voice messages** appears only when there are user-defined custom greetings recorded. It is used to download a compressed file with all user specified voice messages. The link opens the file-chooser window to specify the saving location.

The link **Change Password** refers to the page where the user password can be changed.



Change Password

Extension: 11

Old Password: ********* digits only

New Password: *** digits only

Confirm New Password: *** digits only

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-15 Change Password page for extension access

The **Change Password** page requests the following information:

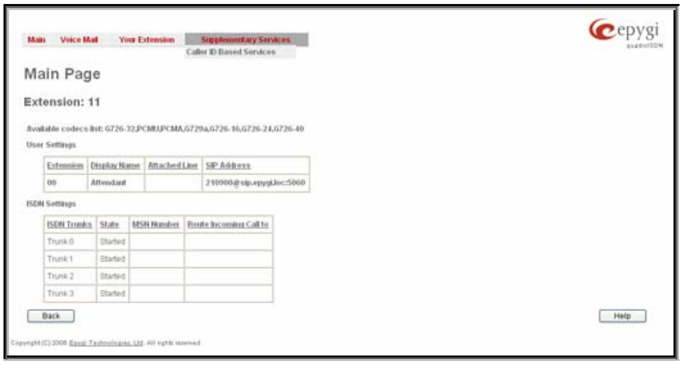
Old Password requires the existing password for the extension access (this field is not displayed when the administrator updates the user's password from the User specific configuration page).

New Password is used to change the existing one. The password should only consist of digits with a length of zero to twenty (0-20) digits.

Confirm New Password is used to confirm the new password. If the entered **New Password** does not match to the new one entered in the **Confirm Password** field the "The passwords do not match. Please try again" error warning will appear.

Please Note: It is highly recommended to define a proper and non-empty password on this page if the extension is being used for the Call Relay service from the Quadro's Auto Attendant.

Supplementary Services



Main Page

Extension: 11

Available codecs list: G726-32,PCMU,PCMA,G729a,G726-16,G726-24,G726-40

User Settings

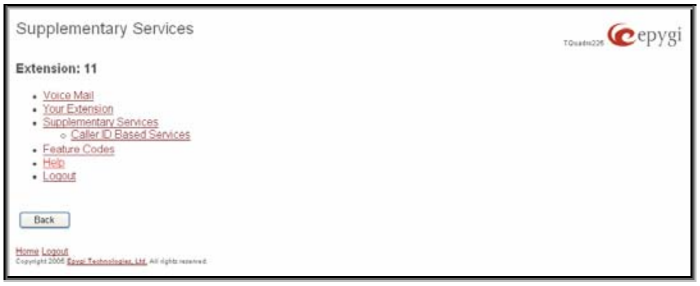
Extension	Display Name	Attached Line	SIP Address
00	Attendant		210900@sip.epygi.loc:5060

ISDN Settings

ISDN Trunks	State	MSN Number	Route Incoming Call to
Trunk 0	Started		
Trunk 1	Started		
Trunk 2	Started		
Trunk 3	Started		

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. III-16 Supplementary Services menu in Dynamo Theme



Supplementary Services

Extension: 11

- Voice Mail
- Your Extension
- Supplementary Services
  - Caller ID Based Services
- Feature Codes
- Help
- Logout

Copyright 2006 Epygi Technologies, Ltd. All rights reserved.

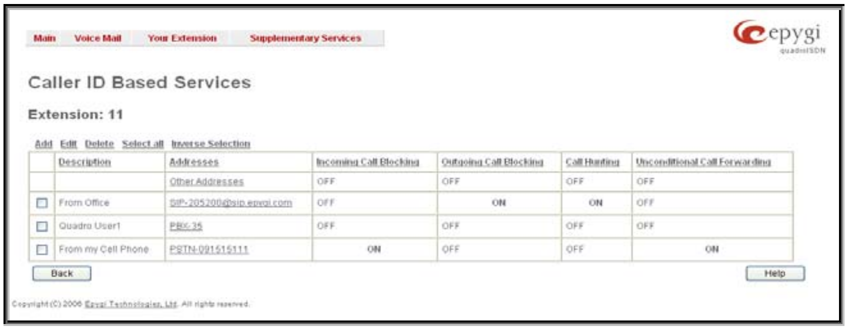
Fig. III-17 Supplementary Services menu in Plain Theme

Caller ID Based Services

The **Caller ID Based Services** page provides options to configure a set of telephony settings from the same page. Call Forwarding, Incoming and Outgoing Call Blocking and Call Hunting are configurable from this page.

The **Caller ID Based Services** page contains a table listing all caller or called destinations and the ON/OFF status of the caller ID based services. The caller or called destination numbers are used to configure caller ID based services based. The column headings in the table are designed as links. By clicking on a column heading, the table will be sorted by the selected column. After sorting, (ascending or descending) arrows will be displayed next to the column heading.

The table also has **Any Address** entry that is undeletable. It is used to configure caller ID based services for all addressed. When adding a new caller address **Any Address** is changed to **Other Addresses**. Now there could be different configurations for the specified addresses and for all others.



Caller ID Based Services

Extension: 11

	Description	Addresses	Incoming Call Blocking	Outgoing Call Blocking	Call Hunting	Unconditional Call Forwarding
		Other Addresses	OFF	OFF	OFF	OFF
□	From Office	SIP-205200@sip.epygi.com	OFF	ON	ON	OFF
□	Quadro User1	PBX-35	OFF	OFF	OFF	OFF
□	From my Cell Phone	PSTN-091515111	ON	OFF	OFF	ON

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-18 Caller ID Based Services page

Add opens the **Caller ID Based Services** - **Add Entry** page where a new address can be defined. This page consists of the following components:

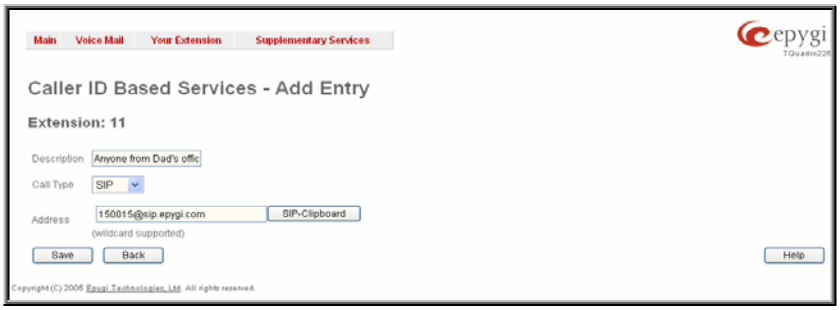
The **Description** text field requires optional information about the address owner.

Call Type lists the available call types:

- PBX - local Quadro extensions and Auto Attendant
- SIP – caller or called destinations reached through a SIP server
- PSTN – caller or called destination dialed from or to PSTN
- Auto – used for undefined call types. In this case, for incoming calls from specific address, configuration of caller ID based services will apply either to PBX, SIP or PSTN callers. For outgoing calls, the called destination will be reached through Routing.

Address requires a SIP address (see chapter Entering a SIP Addresses correctly), an extension or a PSTN number, for whom supplementary services should be applied. If the address already exists in the table, selecting **Save** will give the error "Caller address already exists". A wildcard is allowed in this field (see chapter Entering a SIP Addresses correctly). Entering "*" as PBX or PSTN addresses will apply configuration of supplementary services to all extensions or PSTN users.

Two digits should be inserted in the **Address** text field for the PBX call type. The PSTN number length depends on the area code and phone number.



Caller ID Based Services - Add Entry

Extension: 11

Description: Anyone from Dad's offic

Call Type: SIP

Address: 150015@sip.epygi.com

(wildcard supported)

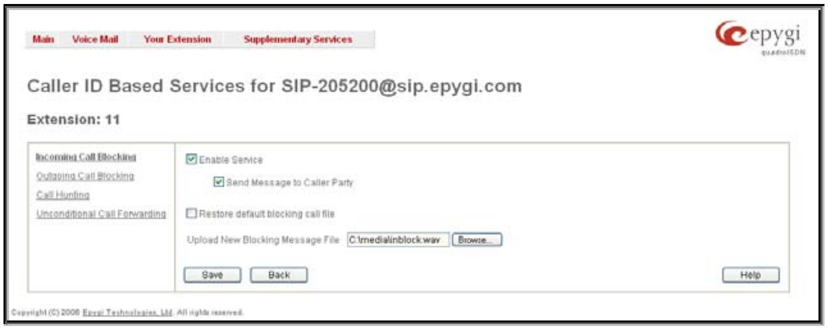
Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-19 Caller ID Based Services – Add Entry page

When clicking on the **Address** in the **Caller ID Based Services** table, the caller ID based services configuration pages for the corresponding extension will be displayed.

The **Caller ID Based Services for Address** page consists of two frames. In the left frame all caller ID based services are listed. Clicking on the corresponding caller ID based service, its settings will be displayed in the right frame.

Please Note: Remember to save changes before moving between the caller ID based services configuration pages.



Caller ID Based Services for SIP-205200@sip.epygi.com

Extension: 11

☑ Enable Service

☑ Send Message to Caller Party

□ Restore default blocking call file

Upload New Blocking Message File C:\media\inblock.wav

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-20 Caller ID Based Services for Address page

Below are the instructions to configure each caller ID based service available to the user.

To Configure Caller ID Based Services

1. Press the **Add** button on the **Caller ID Based Services** page. The **Caller ID Based Services - Add Entry** page, where new addresses can be defined, will appear in the browser window.
2. Define an optional **Description** of the address.
3. Select the call type from the **Call Type** drop down list.
4. Enter the SIP address, extension or PSTN number (dependant on the chosen call type) in the **Address** text field according to the entering rules.
5. To add an address to the **Caller ID Based Services** table, click **Save**.
6. Click on the newly created **Address** in the **Caller ID Based Services** table to open the **Caller ID Based Services for Address** page.
7. From the left frame, choose a Caller ID Based Services. From the right frame, enable, configure and adjust the corresponding service. Do this for each service. Remember to **Save** the configurations each time moving between the Caller ID Based Services configuration pages.

To Edit Caller ID Based Services

1. Select the checkbox of the corresponding address that has to be edited in the **Caller ID Based Services** table. The **Caller ID Based Services - Edit Entry** page will appear in the browser window.
2. Change the **Description** of the address, if needed.
3. Change the **Call Type** and the **Address** defined in the corresponding fields.
4. **Save** changes.
5. If the reconfiguration of **Caller ID Based Services** is needed, click on the corresponding **Address** in the **Caller ID Based Services** table to open the **Caller ID Based Services for Address** page.
6. From the left frame, choose a Caller ID Based Services. From the right frame, change the corresponding service settings, if required. Remember to **Save** the configurations each time moving between the Caller ID Based Services configuration pages.

Incoming Call Blocking

Incoming Call Blocking allows blocking unwanted incoming calls for a Quadro extension. This page provides the necessary settings for incoming call blocking. It indicates if the service is enabled for the particular caller and whether or not the custom message will be used to inform the caller about the call being blocked. If the service for the particular caller has been enabled by the administrator and has been stated as protected, the user cannot disable it.

Please Note: The administrator can protect the service from being disabled by you. Contact the administrator if callers complain that they cannot reach you.

The **Enable Service** checkbox selection blocks all calls to the current extension using the corresponding **Address** listed in the Caller ID Based Services table where the Incoming Call Blocking service is configured.

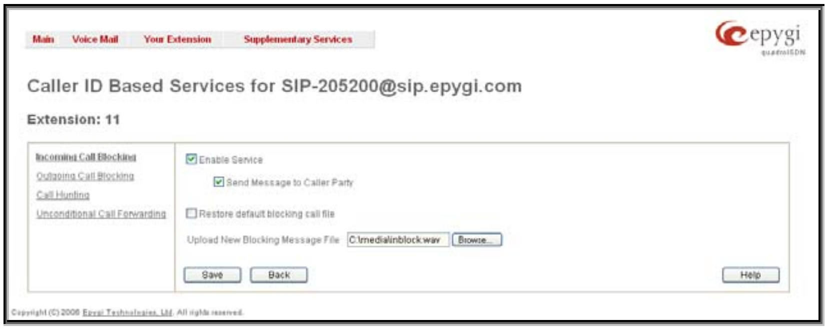
The **Send Message to Caller Party** checkbox is available when the service is enabled and initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without notification.

The **Restore Default Blocking Call File** restores the default incoming call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Call File** requires the name of the desired voice message file. The file needs to be in PCMU wave format, otherwise the system will prevent uploading it and the “Invalid audio file, or format is not supported” warning message will be received. The system also prevents uploading if there is not enough space available for the corresponding extension. You will then receive the “You do not have enough space” warning.

Browse is used to browse custom voice message used for incoming call blocking.

The **Download Voice Message File** link only appears if a file has been previously uploaded. The link is used to download the audio file to the PC and opens a window where the saving location can be specified.



Caller ID Based Services for SIP-205200@sip.epygi.com

Extension: 11

☑ Enable Service

☑ Send Message to Caller Party

□ Restore default blocking call file

Upload New Blocking Message File C:\media\inblock.wav

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-21 Incoming Call Blocking page

Outgoing Call Blocking

Outgoing Call Blocking allows blocking unwanted outgoing calls for a Quadro extension where the destination **Address** service is configured. This page provides the necessary settings for the outgoing call blocking service. It indicates whether service is enabled for the particular caller and whether or not a custom message will be used to inform caller about the call being blocked. If the service a particular caller has been enabled by administrator and has been stated as protected, the user cannot disable it.

Please Note: The administrator can protect the service from being disabled by you. Contact the administrator if you have problems establishing a certain call.

The **Enable Service** checkbox selection blocks all calls to the corresponding **Address** listed in the Caller ID Based Services table associated to the corresponding extension.

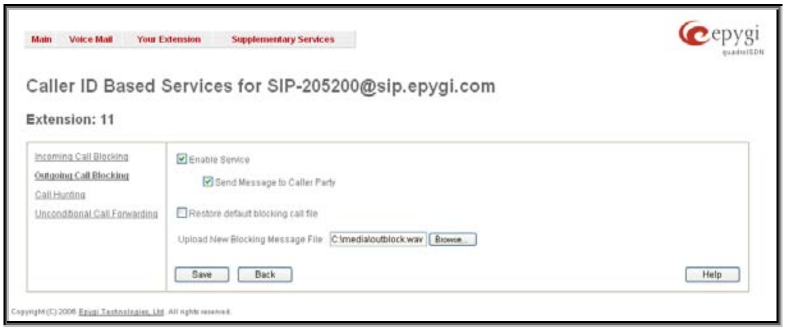
The **Send Message to Caller Party** checkbox is available when service is enabled and it initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without a warning.

The **Restore Default Blocking Call File** restores the default outgoing call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Call File** requires the name of the desired voice message file. The file needs to be in PCMU wave format, otherwise the system will prevent uploading it and "Invalid audio file, or format is not supported" warning message will be received. The system also prevents uploading if there is not enough space available for the corresponding extension. The "You do not have enough space" warning will then be received.

Browse is used to browse custom voice message used for outgoing call blocking.

The **Download Voice Message File** link appears only if a file has been previously uploaded. This link is used to download the audio file to the PC and opens a window where the saving location can be specified.



Caller ID Based Services for SIP-205200@sip.epygi.com

Extension: 11

☑ Enable Service

☑ Send Message to Caller Party

☐ Restore default blocking call file

Upload New Blocking Message File: C:\media\outblock.wav

Fig. 3-22 Outgoing Call Blocking page

Call Hunting

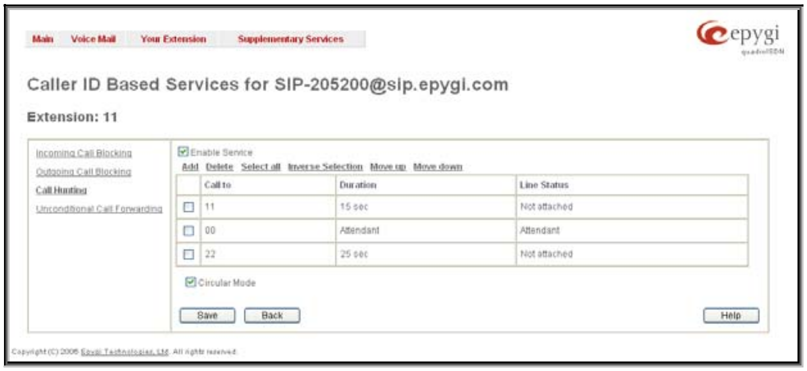
The **Call Hunting** service provides the possibility of an incoming call consecutively ringing on several extensions depending on the calling party. The **Call Hunting** page contains a table where all the participants in the call hunting group for the corresponding extension should be defined.

Attention: By configuring the **Call Hunting**, the **Forwarding** service will automatically be disabled on the current extension.

Selecting **Enable Service** activates the Call Hunting service on the current extension.

The table displayed here lists the extensions where the call must be consecutively duplicated in case of a call from the corresponding caller. **Line Status** indicates if the extension is **Attached**, **Not Attached** or Attendant. An extension cannot ring if it is **Not Attached**. The administrator must attach it to the line from the **Extensions Management** page.

When the order of entries in the **Call To** table is defined in the consecutive ringing order, the **Move Up/ Move Down** becomes available. This will move the checked **Call To** extension either one level up or down.



Caller ID Based Services for SIP-205200@sip.epygi.com

Extension: 11

☑ Enable Service

	Call to	Duration	Line Status
☐	11	15 sec	Not attached
☐	00	Attendant	Attendant
☐	22	25 sec	Not attached

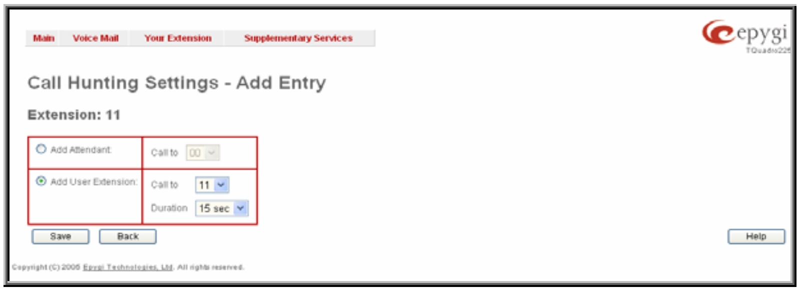
☑ Circular Mode

Fig. 3-23 Call Hunting page

Add opens the **Add Entry** page to add called extensions (an attendant or a user extension). It has manipulation radio buttons to select the type of extension to be added to Call Hunting. It contains the following components:

- The **Call To** drop down list contains Quadro's attendant or user extensions, depending on the radio button selected. It is possible to add the same extension more than once to the **Call To** table. The extension will ring, depending on the order, as often as configured.
- The **Duration** drop down list is only available for user extensions only. It is used to select the period (in seconds) for which the corresponding user's extension should ring.

When saving the call hunting configuration, a message will notify the user that the Many Extensions Ringing and the Call Forwarding services have been disabled.



Call Hunting Settings - Add Entry

Extension: 11

○ Add Attendant:	Call to: 00
● Add User Extension:	Call to: 11 Duration: 15 sec

Fig. 3-24 Call Hunting – Add Entry page

The **Circular Mode** checkbox enables the call hunting start over when the last extension in the Call Hunting table has been called and there is still with no answer. When this checkbox is not selected, call hunting will terminate once the last extension in the Call Hunting table does not answer the call, the incoming call will then be redirected to the Voice Mailbox of the extension call it originally called (if enabled) or it will be disconnected.

Note: The Voice Mail Service will be activated on the extension initiating the Call Hunting only after all extensions in the Call Hunting table are called at least once, regardless the **No Answer Timeout** configured from the **Error! Reference source not found.** page.

Unconditional Call Forwarding

Unconditional Call Forwarding is a service of Quadro that allows the automatic unconditional transfer of incoming calls to a variety of other destinations.

Please Note: By setting up the unconditional forwarding service, **Many Extension Ringing** and **Call Hunting** services will be automatically disabled.

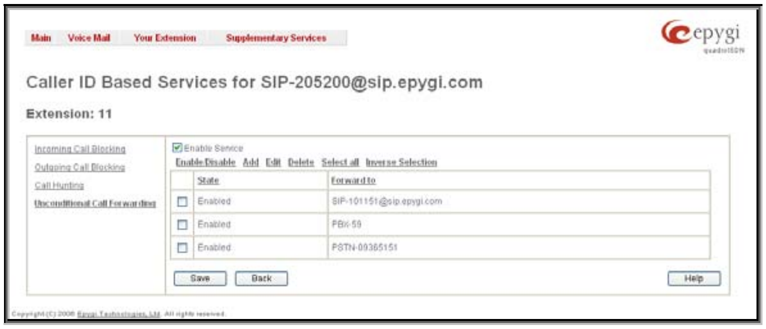
The **Enable Service** checkbox selection activates the unconditional call forwarding service on the current extension.

The table displayed here lists the destinations where the incoming call from a particular caller should be unconditionally forwarded.
Enable/Disable functional button is used to enable/disable the corresponding forwarding destinations. This is helpful to avoid removing forwarding destination(s) if they are not applicable at the moment.
Add opens the **Add Entry** page to add forwarding destinations. It consists of the following components:

Call Type lists the available call types:

- PBX - forwarding destination is a local Quadro extensions or Auto Attendant
- SIP – forwarding destination is reached through a SIP server
- PSTN – forwarding destination is a PSTN user
- Auto – used for undefined call types. In this case, the routing pattern will be considered and parsed through the Local Routing Table.

The **Forward To** text field requires the SIP address (see chapter Entering a SIP Addresses correctly), extension or PSTN number, where an incoming call from a certain caller should be unconditionally forwarded. If the address already exists in the table, selecting **Save** will display the error “Caller address already exists”. A wildcard is allowed in this field (see chapter Entering a SIP Addresses correctly). Entering “*” as PBX or PSTN addresses will apply the configuration of Caller ID Based services to all extensions or PSTN users.



Caller ID Based Services for SIP-205200@sip.epygi.com

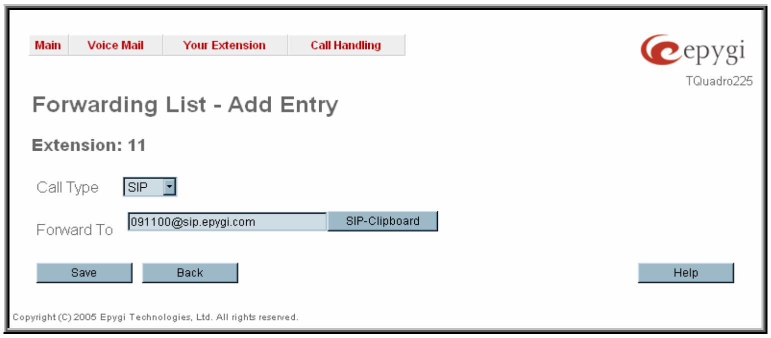
Extension: 11

☑ Enable Service

	State	Forward to
□	Enabled	SIP-101151@sip.epygi.com
□	Enabled	PBX-59
□	Enabled	PSTN-09365151

Copyright (C) 2006 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-25 Unconditional Call Forwarding page



Forwarding List - Add Entry

Extension: 11

Call Type: SIP

Forward To: 091100@sip.epygi.com

Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. 3-26 Call Forwarding – Add Entry page

Two digits should be inserted in the **Forward To** text field for the PBX call type. The PSTN number length depends on the area code and phone number.

When saving the unconditional call forwarding configuration, a message will notify the user that Many Extension Ringing and Call Hunting services have been disabled.

Logout

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

.

Quadro’s Feature Codes

This chapter describes how Quadro’s feature codes allow the user to navigate through Quadro’s services with the help of a phone handset. These services are **Establishing a Call** and **Voice Mail Services**.

Establishing a call

To make a call, dial the **Routing Number**.

Routing Numbers and available routes to, from and through Quadro are listed in the **Call Routing Table**. The **Call Routing Table** is configured and managed by Quadro’s Administrator. To receive information about dialing rules, please contact the administrator.

Please Note: You may accelerate establishing a connection by entering a pound (#) sign dialed at the end of the routing number.

Voice Mail Services

Please Note: This service is only available from Auto Attendant.

The **Voice Mail Services** are divided into two main parts (**Voice Mailbox** and **Review System Messages**). Each of these parts has a hierarchy that is described below.

*0 **Enter Voice Mail Services**		
*0 Exit Voice Mail Services	*1 Go to the top of the Voice Mail Services Tree	*2 Go one level up in the Voice Mail Services Tree

Voice Mailbox

Please Note: This service is only available from Auto Attendant.

After entering the voice mail services (using the keys *0) press the key 1 to enter the Voice Mailbox menu. The following key combinations are available to navigate within the new messages:

*0 **Enter Voice Mail Services**		
1 Voice Mailbox Menu		
1 Send a Message or Leave a Reminder	2 Play First Message	3 Get Date/Time Info
4 Play Previous Message	5 Play Current Message	6 Play Next Message
7 Print the attached FAX (and press START button on the FAX machine)	8 Play Last Message	9 Delete Current Message
*	0 Reply or Forward a Message	#

The **Voice Mailbox** menu has the following sub-hierarchy in the **Reply or Forward a Message** and the **Send a Message or Leave a Reminder** menus:

<table>
<tr><th colspan="4">0
Reply or Forward a Message</th></tr>
<tr><td>0
Call Back
immediately</td><td>1
Reply by Voice Mail</td><td colspan="2">2
Forward a Message
(any FAX attached to the message will be also forwarded)</td></tr>
<tr><td rowspan="4"></td><td>Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.</td><td colspan="2">Dial
Destination Number</td></tr>
<tr><td>#
Record a Message</td><td rowspan="2">#
Record a Message</td><td>Dial additional
Destination Number</td></tr>
<tr><td rowspan="2"></td><td>#
Record a Message</td></tr>
<tr><td colspan="2">Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.</td></tr>
</table>

1 **Send a Message or Leave a Reminder**		
Dial **Destination Number**		# Leave a reminder
# Record a Message	Dial additional **Destination Number**	Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.
	# Record a Message	
Dial 1 to mark the message as Urgent, or press pound to assign the Normal priority.		

Please Note: This service is restricted regarding sending a message to PSTN destinations. A message will be successfully received by the destination if all of the following criteria are met:

- The connection to the destination is successful;
- The voice mail service is enabled on the destination;
- There is enough space in the voice mailbox of the destination;
- The duration of the forwarded/replied message is less than the maximum voice mail duration set up at the destination.

Review System Messages

Please Note: This service is only available from Auto Attendant.

Use the digit 3 to enter the area where the personal system messages can be modified. A voice notification will play the list of available system messages that may be modified so the user can select the desired system message by the corresponding buttons:

* 0 **Enter Voice Mail Services**				
3 **Review System Messages**				
1 Greeting Message	3 Incoming Blocking Message	4 Outgoing Blocking Message	5 Your Name	6 Out of Office Message
1 Listen to Current Greeting Message	1 Listen to Current Incoming Blocking Message	1 Listen to Current Outgoing Blocking Message	1 Listen to Current Name recorded	1 Listen to Current Out of Office Message
2 Record a New Greeting Message	2 Record a New Incoming Blocking Message	2 Record a New Outgoing Blocking Message	2 Record a New Name	2 Record a New Out of Office Message
3 Restore Default Greeting Message	3 Restore Default Incoming Blocking Message	3 Restore Default Outgoing Blocking Message	3 Restore Default Name	3 Restore Default Out of Office Message
# Stop Recording or Playback Greeting Message	# Stop Recording or Playback Incoming Blocking Message	# Stop Recording or Playback Outgoing Blocking Message	# Stop Recording or Playback Name Message	# Stop Recording or Playback Out of Office Message

Services for Incoming Calls

Please Note: This service is only available from Auto Attendant.

Calling to the extension's Voice Mailbox		
1 Skip the ring tones and start Voice Mail recording	0 (during the greeting message) Calling to the Zero Out destination	# Skip the greeting message and start Voice Mail recording

Quadro’s Auto Attendant Services

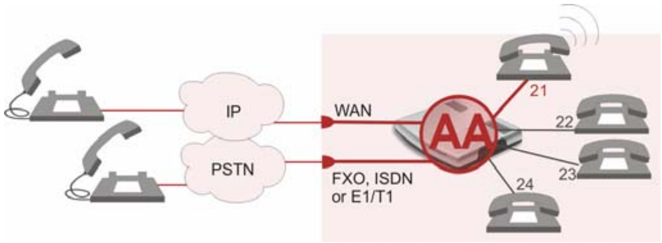
Quadro’s Auto Attendant is addressed to provide remote access to the Quadro voice connectivity services. Specifically it supports remote connection to Quadro extensions, their mailboxes and making pass-through calls to other destinations. Remote access to the Quadro auto attendant is possible through IP and PSTN calls.

Quadro’s Auto Attendant can be accessed locally, remotely from the IP network (by dialing Auto Attendant’s SIP address) and from the PSTN network (by dialing Quadro’s PSTN number) if the calls addressed to the Quadro’s PSTN number are routed to the Auto Attendant.

Attention: If the Auto Attendant authentication attempts have been failed for the five times, Quadro’s Auto Attendant will become unavailable for the next 5 minutes.

The automated attendant services are divided into the feature groups listed below. The **Connection Service** is supported by the voice messages help which helps caller to navigate within area using the handset buttons. Other feature groups are available using the appropriate call code, but are not supported by voice messages. Thus, they are hidden for external callers.

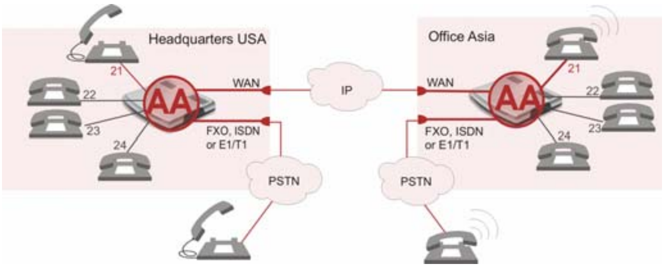
Connection Service provides access to all extensions of the Quadro device without restrictions: All Quadro extensions may call each other dialing the extension number. And all external callers (using PSTN or IP calling) can reach every Quadro extension dialing Quadro’s phone number and using the Auto Attendant’s voice menu to be connected to the desired extension by entering the extension number.



Call Relay

As the Quadro Auto Attendant is registered at Epygi’s SIP server by default, it may be used as a kind of private switching center, if the Auto Attendant is routed to the particular ISDN trunk line as a “default user”. Then it allows e.g. establishing cost-saving long-distance calls: Via PSTN to the Quadro Auto Attendant (e.g. USA headquarters), via IP to the remote Quadro Auto Attendant (e.g. Office Asia) and via PSTN to the desired destination (see call codes below).

Access to **Call Relay** needs authorization.

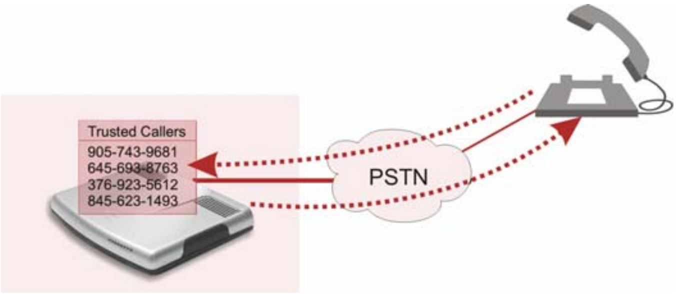


Remote Configuration Menu

This menu allows extension owners to remotely enable/disable the Unconditional Call Forwarding Service for all callers on the corresponding extension. The menu requires extension authorization.

Call Back

With the Quadro's Call Back service the PSTN callers can save the call charge when calling to/through the Quadro to the third party IP or PSTN destinations. The Quadro allows you to configure a list of those trusted PSTN callers that are allowed to make free of charge calls through Quadro. Two types of Call Back configurations are available on the Quadro: **Pre-configured Call Back** and **Remote Call Back Configuration**.



Pre-configured Call Back

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

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

Remote Call Back Configuration

Call Back settings may be configured/reconfigured by authorized PSTN caller over a phone by calling to the Quadro's Auto Attendant. There are two options for configuring Call Back remotely:

- Permanent Call Back
- Non-Permanent (Instant) Call Back

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

Permanent Call Back

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

Entering the Permanent Call Back reconfiguration menu, the system will ask to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in Call Back settings.

After passing the login successfully the PSTN callers should follow the voice instructions for configuring a new entry or reconfiguring the existing entry in Authorized Phone database.

When the system accepts the settings, the corresponding entry will be logged to the Authorized Phones Database. The PSTN caller will be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds if the detected PSTN caller address corresponds to the one applied by the caller (and if ISDN trunk is available on the Quadro, network connectivity is fine and destination is reachable). Answering the incoming call, the PSTN caller will be connected to the Quadro's Auto Attendant.

Non-Permanent Call Back

Non-Permanent Call Back configuration service allows the trusted caller to organize one-time Call Back to the defined PSTN destination. No entry will be logged to the Authorized Phones Database in this case.

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

The system will ask to login by dialing the number and an appropriate password for the Quadro's extension that is used as login extension in Call Back settings.

After passing the login successfully the PSTN callers should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database.

The PSTN caller will be disconnected from the Quadro's Auto Attendant and the defined Call Back destination will receive a call from the Quadro within the next 45 seconds if the detected PSTN caller address corresponds to the one applied by the caller (and if ISDN line is available on the Quadro, network connectivity is fine and destination is reachable). Answering the incoming call, the PSTN caller will be connected to the Quadro's Auto Attendant.

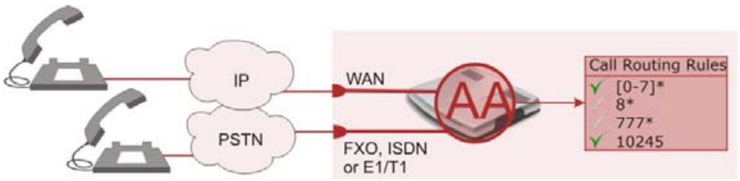
Call Routing Management Menu

This menu is used to manage the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry.

Dialing *7 at the Auto Attendant welcome message, will ask for an enabler/disabler key used to enable or disable the routing rule(s) correspondingly. Since multiple routing rules may have the same enabler/disabler key combinations (the same key may be used as enabler for one routing rule, and as disabler for another one), dialing the certain key will affect all pre-configured routing rules.

If the routing record has an authorization enabled on the enabler/disabler key, administrator's password will be required to be inserted after the key. Once the administrator's password is dialed, system plays a confirmation about the accepted configuration and the state of the certain routing rule(s) is getting modified.

If administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.



Call Codes Available in Auto Attendant

For external IP calls addressed to the Auto Attendant or incoming calls from mainline routed to the Auto Attendant or local by dialing the 2-digit attendant extension, following key combinations are available to access and manipulate within Auto Attendant services:

Incoming call to Auto Attendant Services or dial locally	**Keys**
Extensions Menu - establishing a connection to an extension on the called Quadro	- (already in)
Call Relay Menu - mainly for external calls (IP/ISDN), local calls are allowed, too. Service allows you to avoid hanging up and redo the entire dialing, if Quadro detects an error in the dialed number or the user decides to cancel the call and start a new one: Entering the combination * * the call will be interrupted and the user will get an invitation to make a new one. This is applicable during dialing, after the ring tone has started, and after the call has been established.	* 2
“* *” digit combination is applicable: ● During the dialing, ● After ring tones start, ● After call establishment. **Under the following restrictions:** ● This feature can be used when accessing the AA from the PSTN line to make IP or local calls ● This feature can be used when calling to PSTN through the AA ● This feature is not available on the second Quadro Auto Attendant (calling from one Auto Attendant to another)	
Remote Configuration Menu – allows remote enabling/disabling of Unconditional Call Forwarding service for All Callers on the extension.	* 4
Non-Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to change the callback destination for a one-time callback. After the caller hangs up, Quadro will call back to the newly specified number, but this change will not be logged into Authorized Phones Database.	* 5
Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to reconfigure Authorized Phones Database entries by modifying the caller’s and/or callback numbers. As a result, the caller will be able to initiate a callback, only by calling from the newly specified caller number.	* 6
Call Routing Management Menu – allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry.	* 7
Quits the Auto Attendant and starts a dial tone.	Flash 4

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name -admin Password - 19
Quadro Hostname	quadroISDN
Domain Name	epygi-config.com
LAN IP Address	172.28.0.1 Subnet Mask - 255.255.0.0
DHCP Server	Enabled, IP Range - 172.28.0.100-172.28.0.254, WINS - 0.0.0.0.
Regional Settings and Preferences	Locale – US, TimerZone – Central Time (US & Canada), 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 Settings	Dynamically by provider
DNS Server Settings	Time to live (TTL) – 86400 seconds, Mail exchange (MX) – undefined, No DNS aliases defined.
Wake on LAN	No entries.
IP Routing Configuration	No Routes
Event Settings	”Display notification” for all except System Login Success event, which 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
SNMP Settings	SNMP - Enabled, System Location and System Contact - undefined, SNMP v1 / 2c – enabled SNMP v1 / v2c Read-Only Community – public SNMP v1 / 2c Read-Write Access – disabled No SNMP traps defined
Language Pack	Default - English Custom Language Pack - none
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Extension (all accessible pages for extension), Local Administrators (all accessible pages for localadmin).
Extension Length	2, Prefix – undefined.
Extensions Management	00 extension exists
Attendant 00 Settings – General	Display name – Attendant, FAX forwarding – disabled, Show on public directory – enabled, Percentage of System Memory – 3%.
Attendant 00 Settings – Attendant Scenario	Scenario – default, Send AA digits to Routing Table – enabled,

Parameter	System Default Value
	Redirection on Timeout – disabled, Enable welcome message – enabled, Welcome message, Recurring Attendant Prompt and Attendant Ringing Announcement – default, Authorized Phones Database – undefined.
Attendant 00 Settings – SIP	Registration username and password - automatically generated, SIP server - sip.epygi.com, SIP Server port – 5060, SIP Server Registration – disabled.
Attendant 00 Settings – SIP Advanced	Authentication User Name – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined.
Attendant 00 Settings - Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, G723, iLBC Codec state – all Codecs in the list enabled, Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Universal Extension Recordings	Default, Percentage of System Memory – 3%.
Call Statistics	Enabled 100 entries for all type of calls
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 RTP/RTCP port range for FXS lines - 6000-6099 G276 Standard - ITU-T specification 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
ISDN Settings	ISDN Trunks - Trunk 1, Trunk 2, Trunk 3 and Trunk 4 exist. Settings for all Trunks: State – started, Interface – User, Coding Type - a-law, Loopback mode - no loopback, Passive Mode – disabled, Signaling settings for all Trunks: DID Service – disabled, TEI Mode – Automat, TEI Assignment on Power up – enabled, MSN Settings - No other devices connected to ISDN bus, Route Incoming Call to - 00, Use Default outgoing MSN – enabled,

Parameter	System Default Value
	Default outgoing MSN – undefined, Excessive Ack. delay T200 – 4000, Idle timer T203 – 10000, T302 timer – 4000 T309 timer – 0, T310 timer – 60000, After Guard Timeout -150, Switch type - basic_dss1, Channel Selection – preferred, Bearer Establishment Procedure - on progress indication with in-band information, Called Party Type of Number – unknown, Calling Party Type of Number – unknown, Called Party Numbering Plan – ISDN/telephony numbering plan, Calling Party Numbering Plan – ISDN/telephony numbering plan, Incoming Called Digits Size – 0, Generate Progress Tone to IP – disabled, Enable CLIR Service – disabled, Alternative Disconnection Mode – enabled, B1 and B2 channels – enabled.
PSTN Lines Sharing	Disabled.
Gain Control Settings	ISDN Trunks: Transmit Gain: 0 Receive Gain: 0
Call Routing	Route all incoming SIP calls to Call Routing – enabled. Local Routing table – no entries. Local AAA Table - no entries.
RADIUS Client Settings	Disabled
Voice Mail Common Settings	Voice Mail Recording - G729a
Dial Timeouts	4 seconds
Hold Music Settings	Play Hold Music – Local Music, Hold Music file – default.
IPSec, PPTP and L2TP	No connections
Firewall	Firewall – disabled, Ping Stealth – enabled.
NAT	Enabled
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all), SIP Access (Allowed for all), No user defined services and IP pool groups

Extension Settings

Parameter	System Default Value
Voice Mail Settings	Maximal mail message duration - 5 min, Ask password before granting local access to mail box – disabled, Ask password before granting remote access to mail box – enabled, Send welcome message – disabled, Play Voice Mail help – enabled, Automatically play messages - enabled, Send mails count information message – disabled, Send date/time information message – enabled, Send beep at the end of message – enabled, Send new voice messages via e-mail – disabled, Send new voice message notifications via SMS – disabled, Send new voice message notifications via phone call – disabled, Voice Mail Indication - Tone indication, Zero Out – enabled, to 00 default Attendant, FAX Redirection – disabled, Out of Office – disabled, Greeting message – default.
Group List	No entries
Account Settings	Display Name – undefined, User Password Protection – disabled both for incoming and outgoing calls, Custom Voice Messages – default.
Caller ID Based Services	No entries in the table. For Any Callers – all services are disabled. Blocking Voice Messages – default.

Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD.
Software License Agreement

THIS IS A CONTRACT. CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, SIMPLY DO NOT USE THE HARDWARE OR SOFTWARE.

- **License.** Epygi Technologies, Ltd. (the "Licensor"), hereby grants to you a non-exclusive right to use the Quadro Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may only use the Licensed Materials in connection with your operation of the Quadro or any Quadro SIP Gateway product. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.

- **Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or transfer of the Licensed Materials is subject to the terms of this Agreement.

- **Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.

- **No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language.

- **Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro or any Quadro SIP Gateway product. If you sell your license rights in the Licensed Materials you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

- **Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.

- **Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

  EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

- **LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR EXCEED THE LICENSE FEE

PAID FOR THE LICENSE MATERIALS.
The foregoing limitation, exclusion and disclaimers apply to the maximum extent permitted by applicable law.

- **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

- **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227-19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.

- **Entire Agreement.** It is understood that this Agreement, along with the Quadro Installation Guide and User's Manual, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.

- **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.

- **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.

- **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.

If you have any questions about this Agreement, please write to Epygi at 6900 North Dallas Parkway, Suite 850, Plano, Texas 75024 or call Epygi at 972.692.1166.