Manual II: Administrator's Guide

Edition 1, October 2014

SW Release 6.0.1 and higher

Notice to Users

This document, in whole or in part, may not be reproduced, translated or reduced to any machine-readable form without prior written approval.

Epygi provides no warranty with regard to this document or other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose in regard to this document or such information. In no event shall Epygi be liable for any incidental, consequential or special damages, whether based on tort, contract or otherwise, arising out of or in connection with this document or other information contained herein or the use thereof.

Emergency 911 Calls

YOU EXPRESSLY ACKNOWLEDGE THAT EMERGENCY 911 CALLS MAY NOT FUNCTION WHEN USING QUADRO OR QX AND THAT EPYGI TECHNOLOGIES, LTD. OR ANY AFFILIATES (AGENTS) SUBSIDIARIES, PARTNERS OR EMPLOYEES ARE NOT LIABLE FOR SUCH CALLS.

Limited Warranty

Epygi Technologies, LTD. ('Epygi') warrants to the original end-user purchaser every Quadro and QX to be free from physical defects in material and workmanship under normal use for a period of one (1) year from the date of purchase (proof of purchase required) or two (2) years from the date of purchase (proof of purchase required) for products purchased in the European Union (EU). If Epygi receives notice of such defects, Epygi will, at its discretion, either repair or replace products that prove to be defective.

This warranty shall not apply to defects caused by (i) failure to follow Epygi's installation, operation or maintenance instructions; (ii) external power sources such as a power line, telephone line or connected equipment; (iii) products that have been serviced or modified by a party other than Epygi or an authorized Epygi service center; (iv) products that have had their original manufacturer's serial numbers altered, defaced or deleted; (v) damage due to lightning, fire, flood or other acts of nature.

In no event shall Epygi's liability exceed the price paid for the product from direct, indirect, special, incidental or consequential damages resulting from the use of the product, its accompanying software or its documentation. Epygi offers no refunds for its products. Epygi makes no warranty or representation, expressed, implied or statutory with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability or fitness for any particular purpose.

Return Policy

If the product proves to be defective during this warranty period, please contact the establishment where the unit was purchased. The Integrator will provide guidance on how to return the unit in accordance with its established procedures. Epygi will provide the Return Merchandise Authorization Number to your retailer.

Please provide a copy of your original proof of purchase. Upon receiving the defective unit, Epygi, or its service center, will use commercially reasonable efforts to ship the repaired or a replacement unit within ten business days after receipt of the returned product. Actual delivery times may vary depending on customer location. The Distributor is responsible for shipping and handling charges when shipping to Epygi.

European Limited Warranty

The European Limited Warranty is the same as the Limited Warranty above, except the warranty period is for two years from the date of purchase.

Extended Warranty

Extended Warranty Option

Epygi offers an extended warranty program available for purchase by end users. This option is available at the time of purchase, extending the users original warranty for an additional three (3) years. Combined with the original warranty, the extended warranty would offer a total of five (5) years protection for European end users and four (4) years protection for non-European end users.

Extended Warranty Statement

Epygi Technologies, LTD. extends its Limited Warranty for an additional period of three (3) years from the date of the termination of the original Limited Warranty period (proof of purchase required).

Epygi reserves the right to revise or update its products, pricing, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Epygi Technologies, LTD.

1400 Preston Road, Suite 300, Plano, Texas 75093

Administrative Council for Terminal Attachments (ACTA) Customer Information
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. Located on the equipment is a label that contains, among other information, the ACTA registration number and ringer equivalence number (REN). If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's contact the telephone company to determine the maximum REN for the calling area.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right the file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact EPYGI TECHNOLOGIES, LTD.

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

Electrical Safety Advisory
To reduce the risk of damaging power surges, we recommend you install an AC surge arrestor in the AC outlet from which the Quadro or QX is powered.

Industry Canada Statement
This product meets the applicable Industry Canada technical specifications.

Safety Information
Before using the Quadro or QX, please review and ensure the following safety instructions are adhered to:

- To prevent fire or shock hazard, do not expose your Quadro or QX to rain or moisture.
- To avoid electrical shock, do not open the Quadro or QX. Refer servicing to qualified personnel only.
- Never install wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specified for wet locations.
- Never touch uninsulated telephone wire or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying cable or telephone lines.
- Avoid using your Quadro or QX during an electrical storm.
- Do not use your Quadro, QX or telephone to report a gas leak in the vicinity of the leak.
- An electrical outlet should be as close as possible to the unit and easily accessible.

Emergency Services
The use of VoIP telephony is made available through IP networks such as the Internet and is dependent upon a constant source of electricity, network availability and proper operation of the equipment. If a power outage, network disruption or equipment failure occurs, the VoIP telephony service could be disabled. User understands that in any of those events the Quadro or QX may not be able to support 911 emergency services, and further, such services may only be available via the user's regular telephone line or mobile lines that are not connected to the Quadro or QX. User further acknowledges that any interruption in the supply or delivery of electricity, network availability or equipment failure is beyond Epygi's control and Epygi shall have no responsibility for losses arising from such interruption.

Music on Hold Copyright

The default Music on Hold on the Quadro or QX is a 22 second fragment from Chopin's *Nocturne Op.9 #2* performed by Marina Vardanyan and kindly provided to Epygi Technologies, LTD. The recording is royalty free.

Compliance with Laws

You may not use the Epygi 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.

Table of Contents

Manual I: see Installation Guide

Step-by-step guide to install and configure QX Gateway basically.

Manual II: Administrator's Guide

About this Administrator's Guide **8**
QX Gateway's Graphical Interface **9**
Administrator's Main Page – Dashboard 9
Administrator's Menus **10**
Setup Menu **10**
Basic Setup 11
System (LAN) – System Configuration Wizard 11
Internet (WAN) - Internet Configuration Wizard 12
Needed Bandwidth for IP Calls 14
Date and Time Settings 15
System Mail Settings – Email (SMTP) 16
SMS Settings – Short Text Messaging 16
System Security 17
Language Pack 18
Extensions Menu **19**
Extensions Management 20
Add Extension 21
User Extension Settings 22
Attendant Extension Settings 24
Extension Codecs 27
Upload Universal Extension Recordings 28
Authorized Phones Database 28
Call Back Services 30
Interfaces Menu **31**
General Operation Mode 32
FXS Lines 32
FXS (On-board) Line Settings 32
Diagnostic Loopback 33
FXO Settings 34
E1/T1 Trunk Settings 35
Incoming Interdigit Service 44
ISDN Settings 44
PSTN Lines Sharing 50
PSTN Gateway Operation Mode 50
Telephony Menu **51**
VoIP Carrier Wizard 52
Call Routing Table 53
Call Routing 60
Local AAA Table 60
Global Speed Dial Directory 61
Allowed Characters and Wildcards 62
Best Matching Algorithm 63
Entering SIP Addresses Correctly 65
SIP Tunnel Settings 65
NAT Traversal Settings 67

General Settings 67
SIP Parameters 67
RTP Parameters 68
STUN Parameters 69
NAT Exclusion 69
RTP Settings 70
SIP Settings 71
SIP Aliases 72
TLS Certificates 72
Advanced Settings 72
RTP Streaming Channels 72
Gain Control 73
RADIUS Client Settings 73
Dial Timeout 74
Call Quality Notification 75
Hold Music Settings 75
Firewall Menu 76
Firewall 77
Firewall and NAT 77
Advanced Firewall Settings 77
IDS Log 77
Filtering Rules 78
View All Filtering Rules 78
Incoming Traffic/Port Forwarding 79
Outgoing Traffic 79
Management Access 79
SIP Access 79
Blocked IPs 80
Allowed IPs 80
Custom Services 81
Service Pool Configuration 81
IP Groups 82
IP Pool Configuration 82
SIP IDS Settings 84
Network Menu 85
IP Routing Configuration 86
IP Static Routes 86
IP Policy Routes 86
PPTP/L2TP Routes 87
DHCP Settings 87
DHCP Server 88
DHCP Advanced Settings 89
DHCP Leases 89
DHCP Settings for the VLAN Interface 90
DNS Settings 90
DNS Server Settings 90
Dynamic DNS Settings 91
PPP/ PPTP Settings 92
Advanced PPP Settings 92
SNMP Settings 93
Global SNMP Settings 93
SNMP Trap Settings 94
VLAN Configuration 94
VPN Configuration 95
IPSec Configuration 95
PPTP/L2TP Configuration 98
Status Menu 102

System Status 103
General Information 103
Network Status 103
Lines Status 103
Memory Status 104
Hardware Status 104
SIP Registration Status 104
Events 105
System Events 105
Event Settings 106
Call History 107
Successful, Missed and Unsuccessful Calls 107
CDR Settings 108
Automatic Backup 108
RTP Statistics 110
FAX Statistics 111
LAN/WAN 111
LAN and WAN Interface Statistics 111
Statistics 112
Network Transfer 112
PSTN Channel Usage 113
Maintenance Menu 114
Diagnostics 115
Security Diagnostics 115
Call Capture 116
Ping 116
Traceroute 117
System Logs 117
System Logs Settings 117
Remote Logs Settings 118
User Rights Management 118
Users 118
Roles 119
Backup/Restore 120
Automatic Backup 121
Download Legible Configuration 121
Upload Legible Configuration 122
Firmware Update 122
Upload Firmware 123
Get Firmware From Server 124
Automatic Firmware Update 125
Reboot 125
Registration Form 126
Extension User's Menus 127
Call History 128
PBX Information 129
Account Settings 129
Basic Services 130
Caller ID Based Services 131
Incoming Call Blocking 132
Outgoing Call Blocking 133
Unconditional Call Forwarding 133
Log Out 134
QX's Auto Attendant Services 135
Call Codes Available in Auto Attendant 137
Remote Configuration Menu 137
Call Codes available for QXFXS24 Gateway 138

Appendix: System Default Values **139**
Administrator Settings 139
Extension Settings 143
Appendix: Glossary **145**
Appendix: Software License Agreement **150**

About this Administrator's Guide

The QX Gateway Manual is divided into two parts:

- **Manual I: Installation Guide**
  gives step-by-step instructions to provision the QX Gateway and configure the phone extensions with the Epygi SIP Server. After successfully configuring the QX Gateway, users will be able to make SIP phone calls to remote QX devices, make local calls to the PSTN and access the Internet from devices connected to the LAN.
- **Manual II: Administrator's Guide** explains all QX 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 QX Gateway offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular QX Gateway 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.

QX Gateway's Graphical Interface describes the QX'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 QX 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: Glossary defines some technical terms.

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

QX Gateway's Graphical Interface

Administrator's Main Page – Dashboard

When the administrator logs in, the **Epygi QX Management** page is displayed with a table of active calls (including information about call peers, call duration and start time) at the startup. The number of total active calls is displayed belowthe table.

The button **Terminate** next to each active call is used to terminate the corresponding call.

The following main menus are available on QX Gateway: **Setup**, **Extensions**, **Interfaces**, **Telephony**, **Firewall**, **Network**, **Status** and **Maintenance**. By clicking on menus the administrator may access the settings in each respective category and perform actions specific to each category.

The following menus may additionally occur when pressing to the PBX extensions:

- **Your Extension** (see Extension User's Menus)

  The **Return** link is used to return to the QX Gateway Management page.

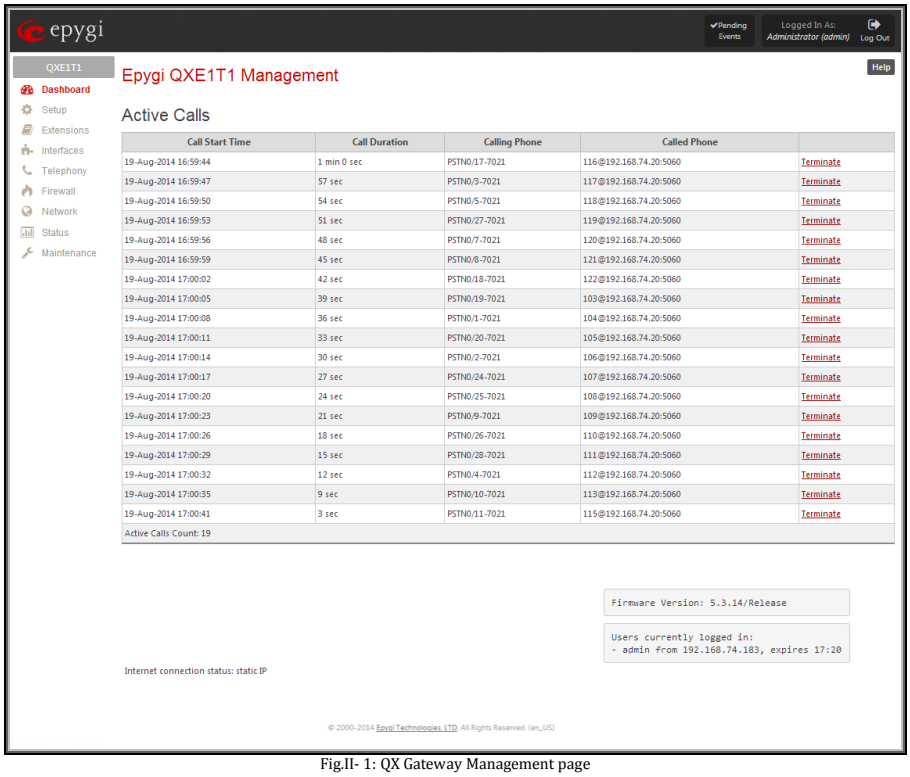


Fig.II- 1: QX Gateway Management page

The functional button **Renew Wan IP Address** appears on the administrator's main **QX Gateway Management** page if the QX Gateway 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 QX Gateway moves to another network.

The button **Pending Events** will be displayed in the upper right corner of the Administrator's Main Menu page. Clicking on the button will lead to the **Events** page that can be also accessed from the Status Menu.

Language selection is available only when the custom Language Pack has been uploaded and it is used to enable custom language for QX GUI or returning back to the default language - English.

The list of **Users currently logged in** is seen in the lower right corner of the Administrator's Main Menu. Information about IP address user accessed QX Gateway GUI from, the username user is logged in and the time until the next automatically logout is provided herein. The current version of the QX Gateway'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.

Log Out is used to close the session between the user PC and QX and to leave the QX Web Management or to enter the management with another login.

Administrator's Menus

Setup Menu

The **Setup Menu** consists of the following sections:

- **Basic Setup**
  - System (LAN)
  - Internet (WAN)
  - Date and Time
  - Email (SMTP)
  - Short Text Messaging (SMS)
- **System Security**
- **Language Pack**

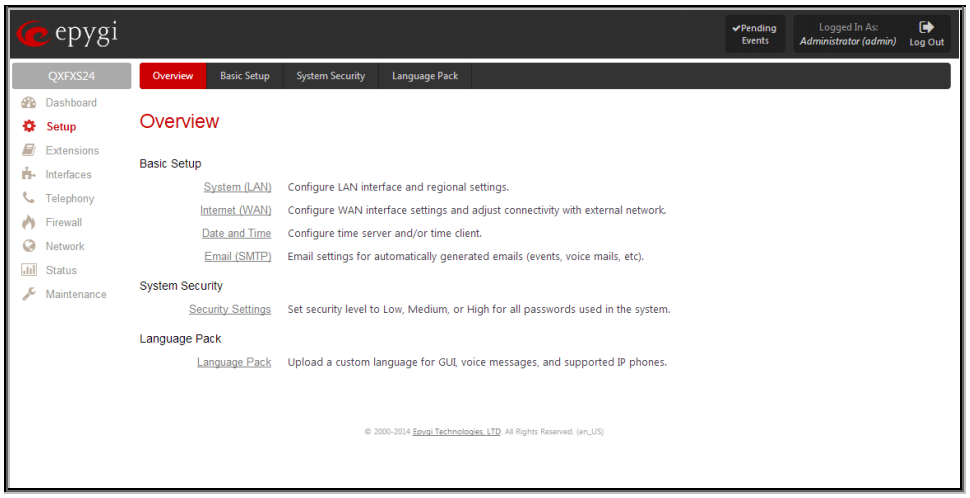


Fig.II- 2: Setup Menu page

Basic Setup

System (LAN) – System Configuration Wizard

The **System Configuration Wizard** allows the administrator to define the QX Gateway's Local Area Network settings and to specify regional configuration settings to make QX Gateway operational in its LAN. The **System Configuration Wizard MUST be run upon QX Gateway'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.

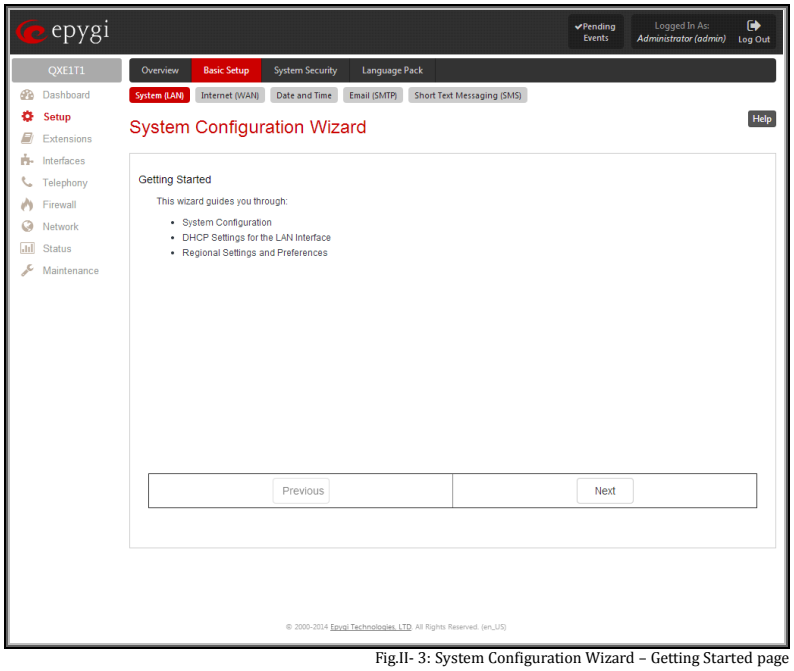


Fig.II- 3: System Configuration Wizard – Getting Started page

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

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

Host Name requires a host name for the QX Gateway device.

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

IP Address requires the QX Gateway host address for the LAN interface.

Subnet Mask requires the QX Gateway hosts' Subnet Mask.

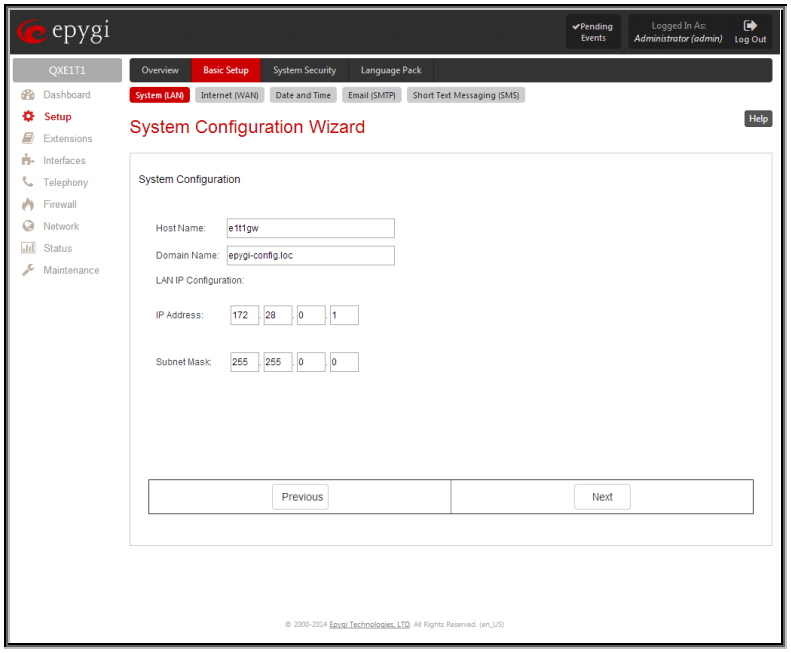


Fig.II- 4: System Configuration Wizard - System Configuration page

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

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

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

- **System Language** – selection is available only when the custom Language Pack has been uploaded and it is used to enable custom language for system voice messages or returning back to the default language English.

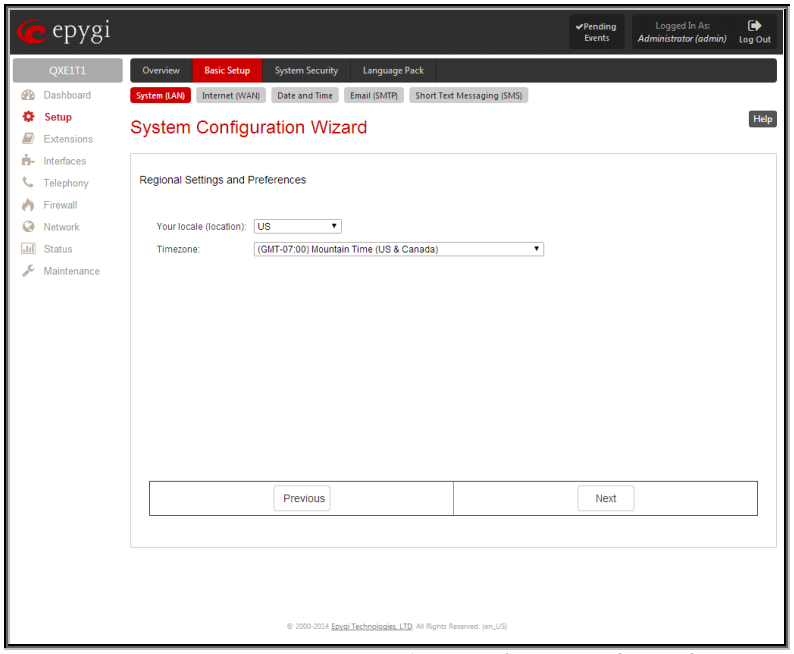


Fig.II- 5: System Configuration Wizard - Regional Settings page

Internet (WAN) - Internet Configuration Wizard

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

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

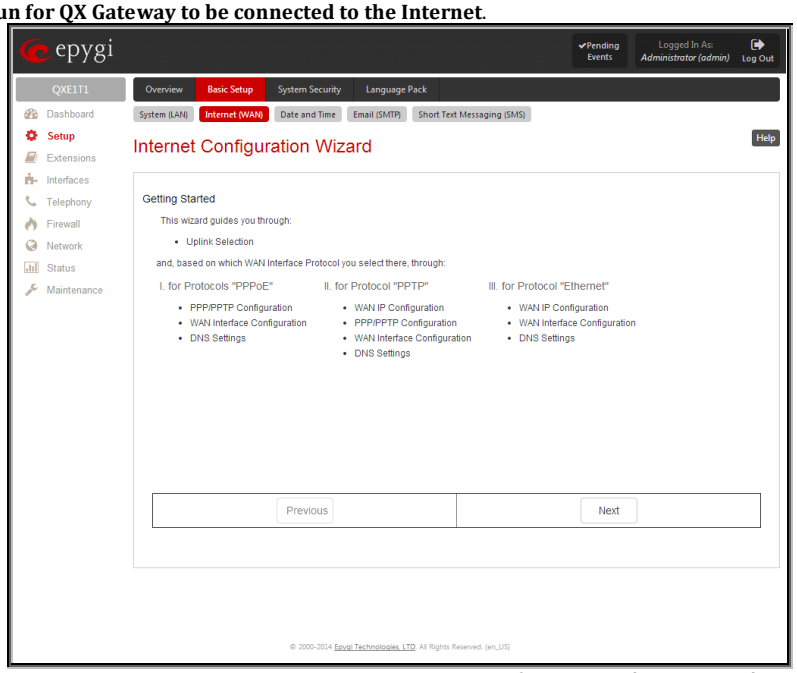


Fig.II- 6: Internet Configuration Wizard – Getting Started page

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

- Uplink configuration (see below)

For Protocols **PPPoE**:

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

For Protocols **PPTP**:

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

For Protocols **Ethernet**:

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

The **Uplink Configuration** page allows you to select the QX Gateway's WAN interface connection type and its bandwidth settings. These settings will make QX Gateway 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):

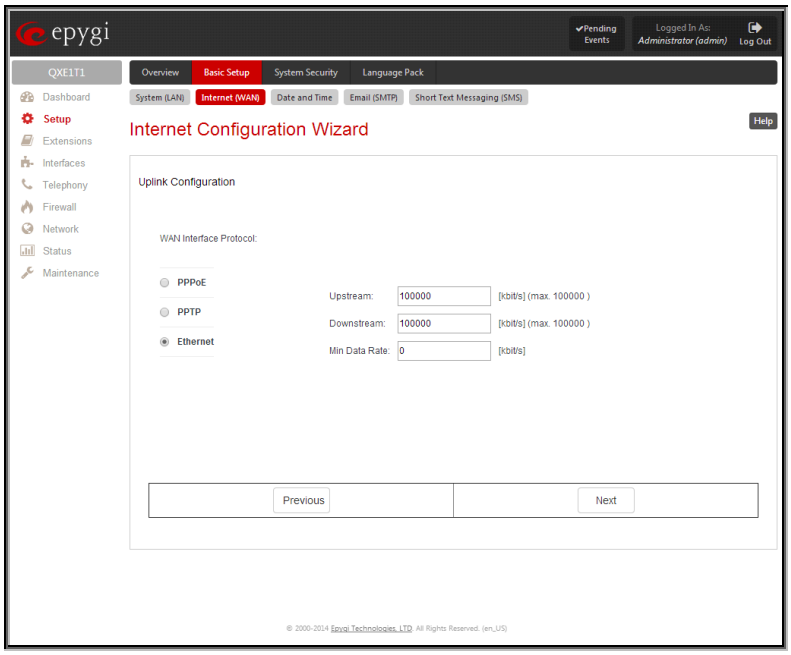


Fig.II- 7: Internet Configuration Wizard - Uplink Configuration page

- **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 QX and ADSL modem. A fixed IP address configuration is needed in this case.
- **Ethernet** - turns on the Ethernet connection.

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 100000, the maximum bandwidth of a 100 Mb Ethernet. You may see the required bandwidth in the chapter Needed Bandwidth for IP Calls.

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 QX Gateway'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 QX Gateway WAN interface.

Subnet Mask requires the subnet mask for the QX Gateway device WAN interface.

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

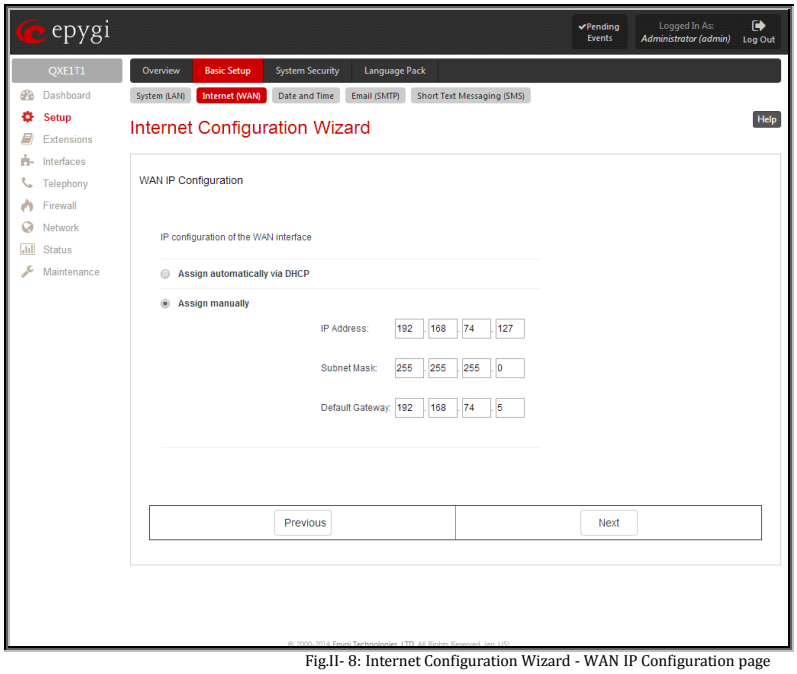


Fig.II- 8: Internet Configuration Wizard - WAN IP Configuration page

The **WAN Interface Configuration** page may be used to modify the MAC address of the QX Gateway. 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 QX.
- **User Defined** requires user defined MAC Address.

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

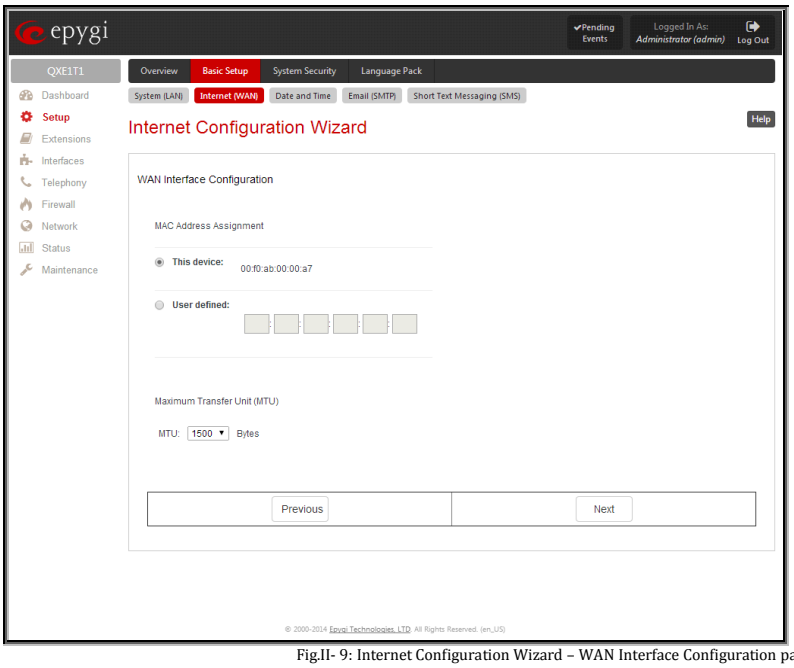


Fig.II- 9: Internet Configuration Wizard – WAN Interface Configuration page

Needed Bandwidth for IP Calls

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

Required Bandwidth for Standard Packets:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:								
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	iLBC-13.33	G.722	G.722.1
10	105	58	66	74	82	50	-	105	74
20	84	37	45	53	61	29	-	84	53
30	76	30	38	45	53	22	27	76	45
40	74	27	34	42	50	19	-	74	42
50	71	25	32	40	48	17	-	71	40
60	67	22	30	37	45	15	20	67	37

Needed Bandwidth for Encrypted Packets when using a SRTP:

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	iLBC-13.33	G.722	G.722.1
10	114	66	74	82	90	58	-	114	82
20	89	41	49	57	65	33	-	89	57
30	81	33	41	49	57	26	31	81	49
40	76	28	36	44	52	20	-	76	44
50	74	26	34	42	50	18	-	74	42
60	72	24	32	40	48	16	22	72	40

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	iLBC-13.33	G.722	G.722.1
10	148	98	105	118	124	92	-	148	118
20	105	59	65	74	81	49	-	105	74
30	90	43	52	60	66	35	41	90	60
40	85	38	45	53	61	30	-	85	53
50	80	34	41	48	56	26	-	80	48
60	74	29	37	45	52	22	26	74	45

Date and Time Settings

The **Date and Time** 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).

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

Enable Simple Network Time Protocol Client enables the SNTP client on the QX Gateway, thus QX Gateway 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.

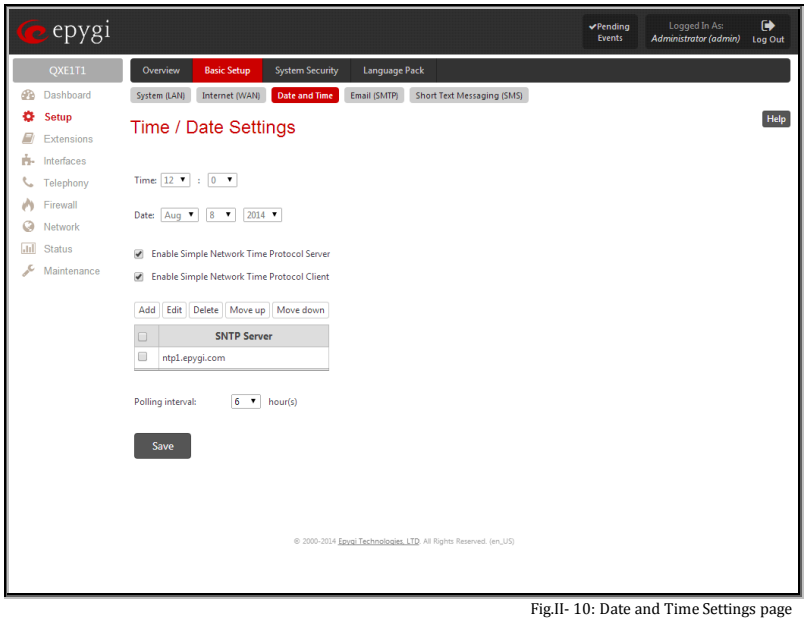


Fig.II- 10: Date and Time Settings page

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, QX's date/time is not being updated automatically).

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

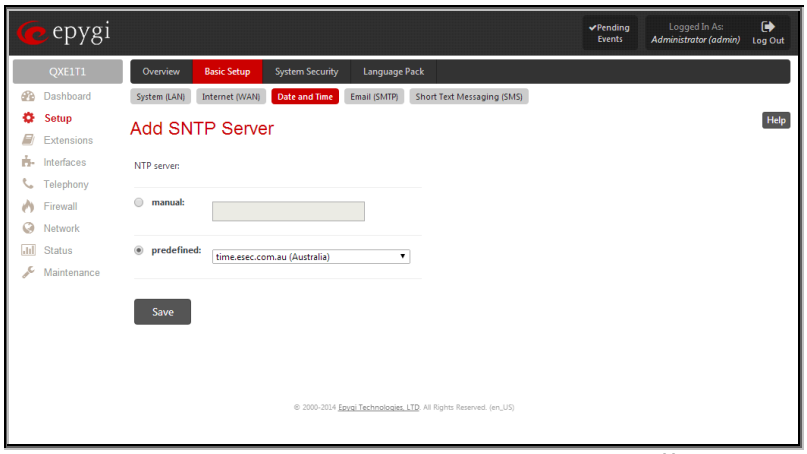


Fig.II- 11: Add NTP Server page

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

System Mail Settings – Email (SMTP)

The **Email (SMTP)** 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 Event Settings 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.

QX Gateway may automatically generate emails to the administrator if events specified in the System Events list occur.

With the **Enable** checkbox system mail sending and voice messages transmission to the extension user's mailbox could be enabled.

SMTP Host requires the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server. This SMTP server is part of your mail server that you normally use to receive and send mails.

SMTP Port requires the SMTP host port number.

Mail Sender Address text field requires the source address for the QX Gateway notification emails. The email address defined here should be an existing valid email 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 email address where system emails will be delivered. The e-mail recipient here can be a QX Gateway 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 e-mails will be delivered.

The server requires a secure connection (TLS) must be selected if the specified SMTP server requires secure connection using TLS. If the specified SMTP server allows using both secure and unsecure connections then this selection forces to establish the secure connection.

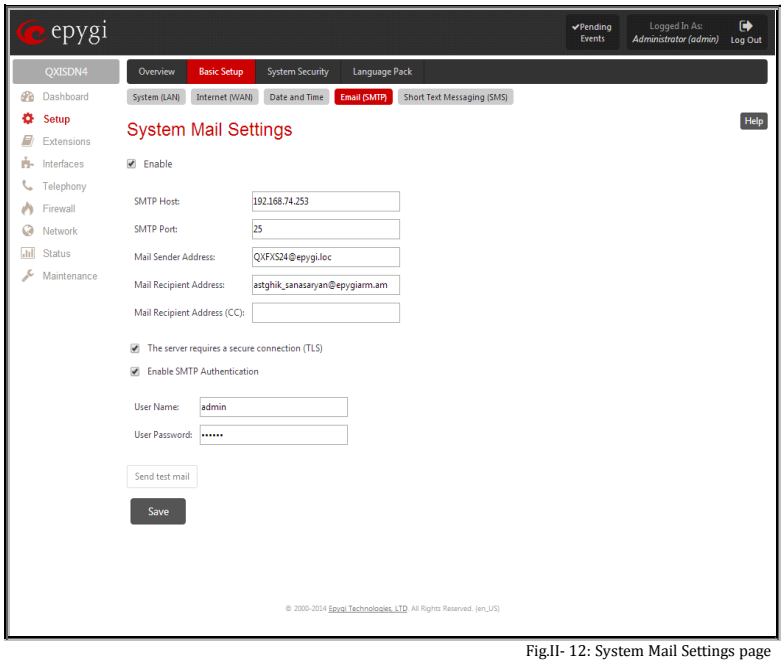


Fig.II- 12: System Mail Settings page

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

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

With the button **Send test mail** a test mail can be sent to the defined email address to verify the settings. 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 the **secure connection (TLS)** if the specified SMTP server requires secure connection.
6. Enable **SMTP Authentication** if it is required on the server.
7. Insert into the corresponding text fields an authentication **User Name** and **User Password** defined by your SMTP server.
8. Press the **Save** button to submit these settings.
9. Use the **Send Test Mail** button to send a test e-mail with the configured settings.

SMS Settings – Short Text Messaging

The **SMS Settings** (available only for QXFXO4, QXISDN4 and QXE1T1 Gateways) are used to configure the SMS parameters that will allow QX Gateway to send the event notifications via SMS to the extension user's mobile phone. However, for QX Gateway to deliver SMS notifications, the SMS service should be enabled and SMS settings should be configured from this page.

Enable SMS Service enables the SMS service on the QX Gateway.

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

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

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

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

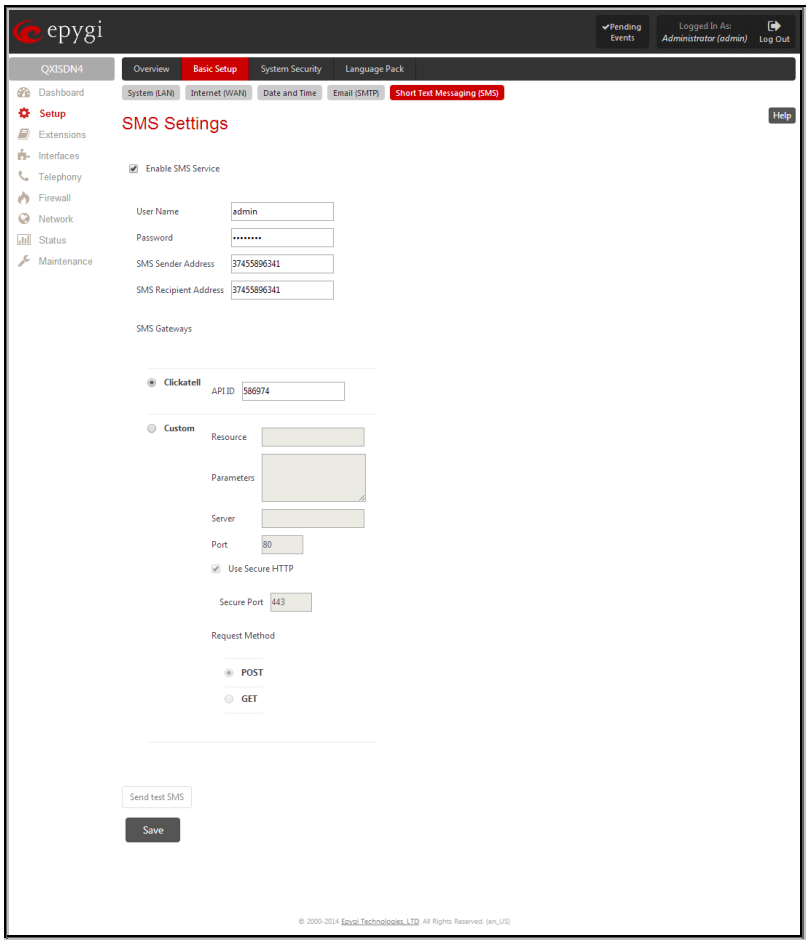


Fig.II- 13: SMS Settings page

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

  Resource text field requires the HTTP resource name on the SMS gateway, for example: /http/sms.cgi.

  Parameters text field requires the parameters to be submitted to the resource address. The value of this field represents a string with tokens (separated by percent (%) symbols) inside. Each token indicates a value of the certain field on this page. The value is dependent on the SMS gateway requirements. For example:

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

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

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

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

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

System Security

The **System Security Management** offers a possibility of managing the global security levels.

The **System Security Management** page includes the following components:

The **Security Level table** - allows selecting the Security Level defining requirements to the IP Lines' password strength and the Security Report granularity. The security levels are as follows:

- **Low** - There are no specific restrictions on the strength of the saved password. Only the critical warnings on the Call Routing Rules to PSTN and IP-PSTN, disabled Firewall and IDS will be generated in Security Report.
- **Medium** - The minimum strength of the IP Line passwords should be "good". The Security Report will generate warnings on all unsecured Call Routing rules, IP Line passwords, Firewall level (if it is set to lower than "Medium") and disabled IDS.
- **High** - The minimum strength of the IP Line passwords should be "strong". The Security Report will generate warnings on the IP Line passwords, disabled IDS, unsecured SIP, and unsecured Routing Rules to SIP, PSTN and IP-PSTN and also regarding the Firewall level if it is set to lower than "High".

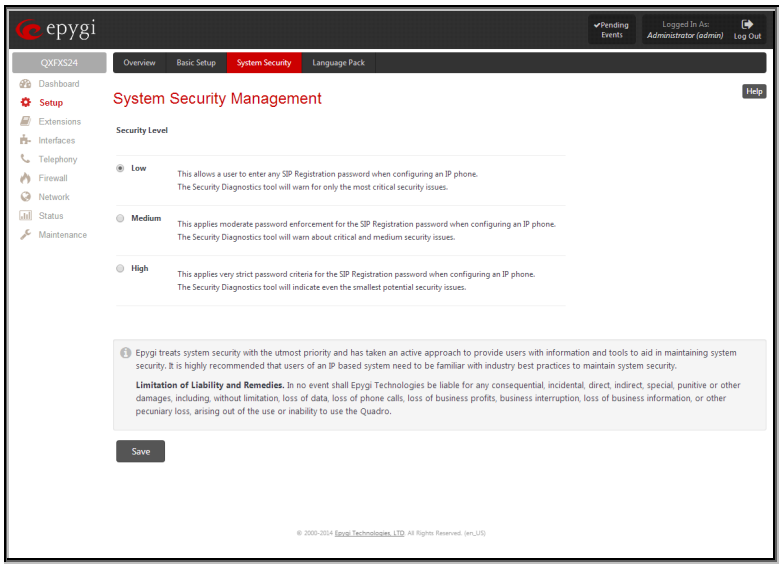


Fig.II- 14: System Security Management page

Language Pack

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

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

- All voice mails and custom voice messages (only when embedded memory storage is used)
- Call History (only when embedded memory storage is used)
- Pending events (only when embedded memory storage is used)
- Transfer statistics

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

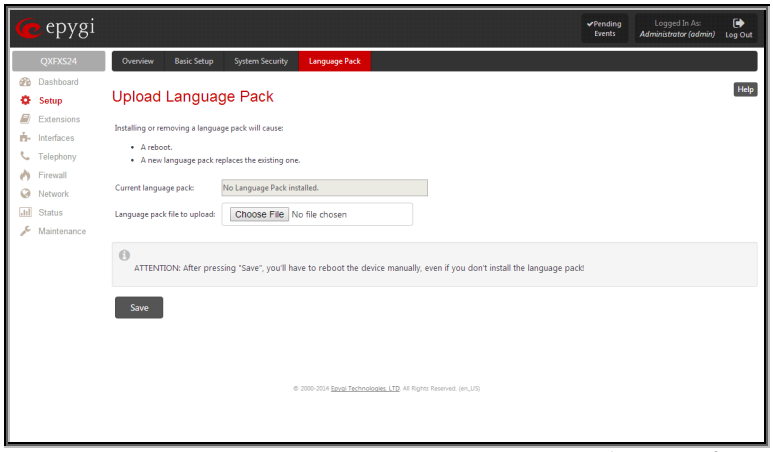


Fig.II- 15: Language Pack page

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

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

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

Pressing **Save** will start uploading the custom language pack to the board.

Attention: Pressing the **Save** button will stop some vital processes on the QX Gateway, therefore you will need to reboot your device manually even if you have cancelled the language pack update procedure on the following steps.

The next page displayed will show verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if applicable). After final confirmation, the system will upload the selected custom Language Pack and it will reboot.

Extensions Menu

The **Extensions** menu allows you to configure the following settings:

- **Extensions**
  - Add Extension
- **Recordings**
- **Authorized Phones**

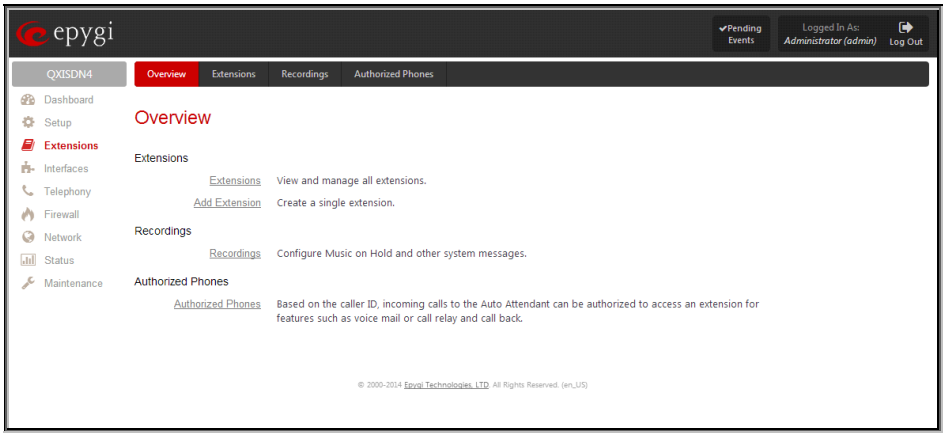


Fig.II- 16: Extensions Menu page

Extensions Management

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

When this page is accessed for the first time after the QX Gateway'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 QX Gateway. This page disappears once being saved.

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

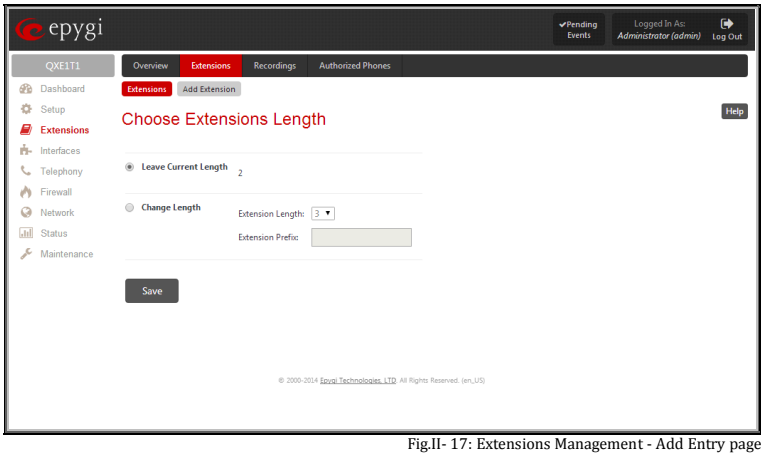


Fig.II- 17: Extensions Management - Add Entry page

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

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

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

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

Two types of user extensions, **active** and **inactive**, can be created on the QX Gateway. 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.

Attendant extensions (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) are dedicated to the IVR system on the QX Gateway. These extensions are used by callers to reach QX's users and use the remote access and call relay services. It is possible to create Auto Attendants with the custom scenarios. By default, QXFXO4, QXISDN4 and QXE1T1 Gateways have one Auto Attendant extension (00) which is undeletable.

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

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

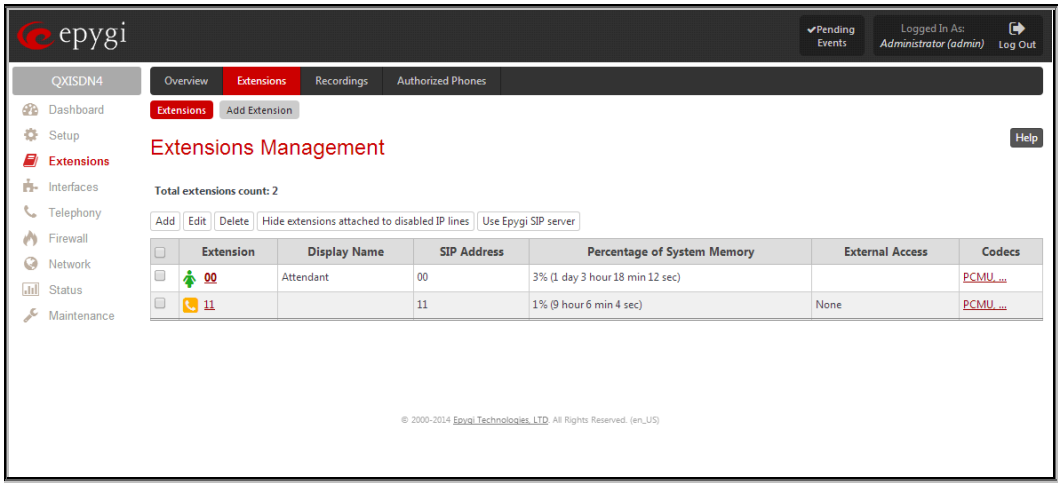


Fig.II- 18: Extensions Management page

The following columns are present in the table:

- **Extension** - lists user or attendant extensions on the QX. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **Percentage of System Memory** - indicates the user space (in percentages) configured for each extension. The actual available duration (in minutes) for the extension voice mails, uploaded/recorded greetings and blocking messages is also displayed here.
- **External Access** - indicates whether the GUI Login or Call Relay options are 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 **Your Extension** menu.

To add an extension click on the **Add** button or use the Add Extension tab (see below).

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

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

Please Note: Save changes before moving among settings groups.

The **Edit** functional button also 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.

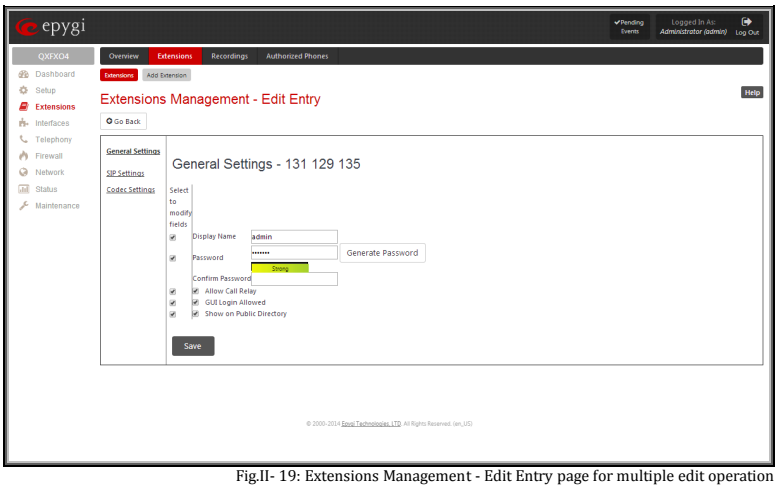


Fig.II- 19: Extensions Management - Edit Entry page for multiple edit operation

Add Extension

Add Extension menu opens the **Extensions Management - 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. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" will appear. If an extension with the same number already exists in the Extensions Management table, the error "Extension already exists" will appear.

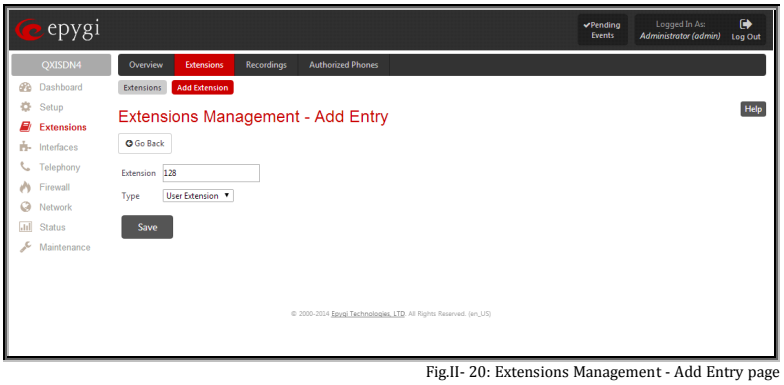


Fig.II- 20: Extensions Management - Add Entry page

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

The **Type** drop down list is used to select the type of the extension to be created (for details see below). The following values are available in this list:

- Attendant
- User Extension

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.

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 creating the extension.

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords. The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

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.

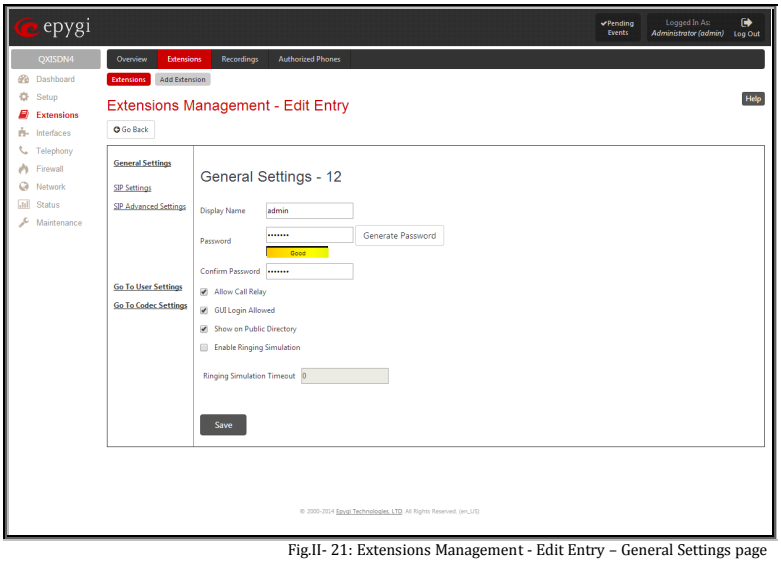


Fig.II- 21: Extensions Management - Edit Entry – General Settings page

Attached Line (available only for QXFXS24 gateways) lists all free lines to where an extension may be attached.

Allow Call Relay (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) enables the current extension to be used to access the Call Relay service in the QX'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.

GUI Login Allowed (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) checkbox enables the current extension to be used to access the QX via WEB interface by extension name and password.

With the **Show on Public Directory** (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) checkbox enabled, the details of the corresponding extension will be displayed in the PBX Information page.

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

2. SIP Settings

This page provides two functions. It allows an extension on the QX to register to an external SIP server. The registration to the external SIP server (e.g. ITSP) is usually required before the server will allow the call to be received. This page also allows for incoming SIP calls to ring an extension. Upon receiving a SIP Invite from an external SIP server, the QX will look to match the called number with the settings in the **User Name/DID Number** field.

User Name/DID Number is the registration user name on the external SIP server or the DID number from the ITSP. The user name needs to be unique on the external SIP server. This field length is limited to 32 symbols.

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

Confirm 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.

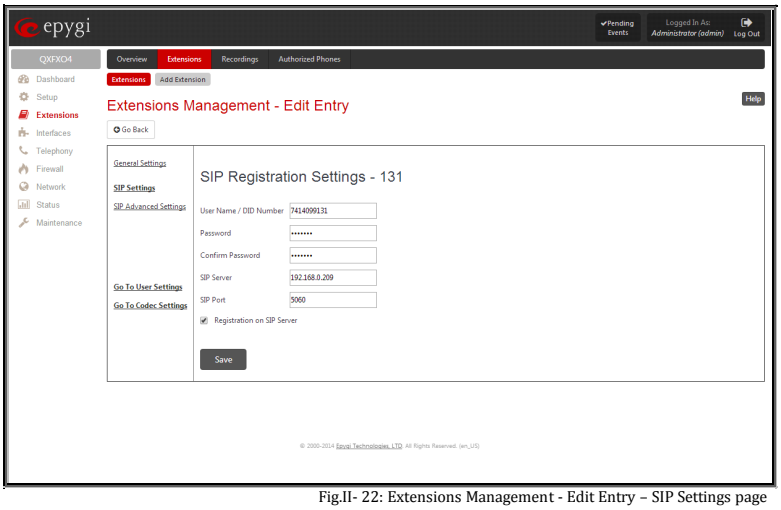


Fig.II- 22: Extensions Management - Edit Entry – SIP Settings page

SIP Server indicates the 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.

SIP Port indicates the 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, QX 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.

Please Note: If the ITSP does not require each DID to uniquely register to the external SIP server, then only enter the DID number in the **User Name/DID Number** field. The other fields are not required.

3. SIP Advanced Settings

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

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

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

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

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

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

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

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 QX to reach the selected SIP servers.

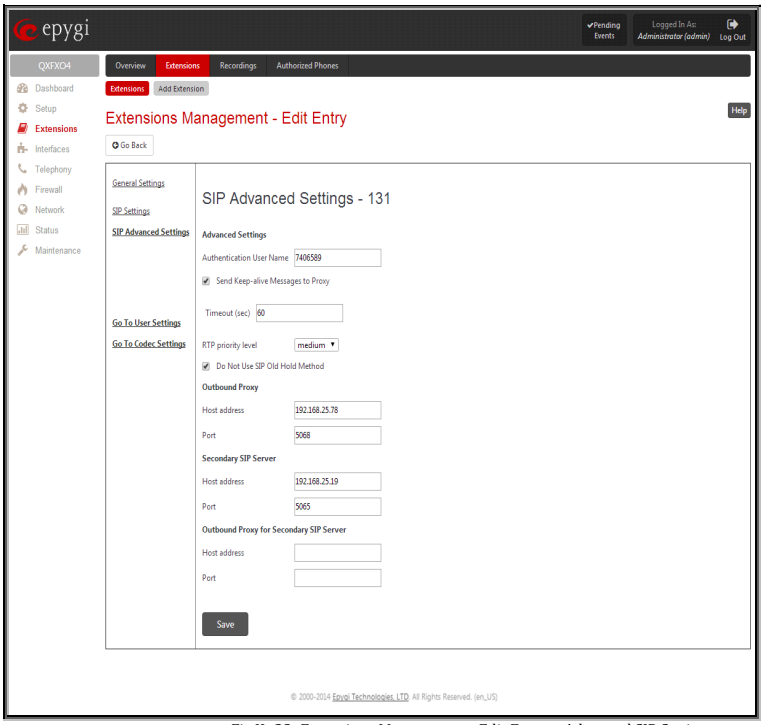


Fig.II- 23: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Voice Mailbox Settings

The **Voice Mailbox Settings** (available only for QXFXS24 Gateways) are used to manage Voice Mail service for the corresponding extension and to define the location where voice mails will be collected.

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 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, QX 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.

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

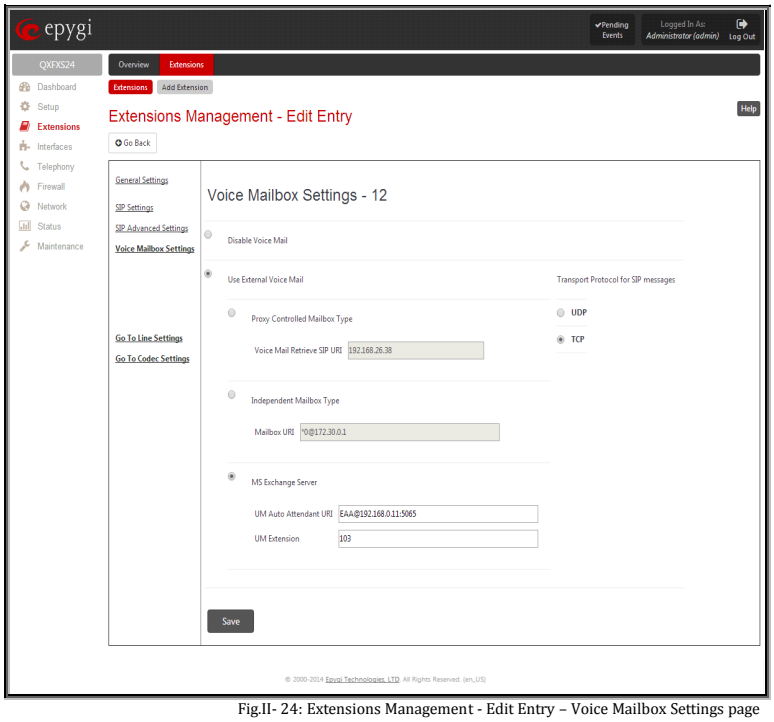


Fig.II- 24: Extensions Management - Edit Entry – Voice Mailbox Settings page

- With **MS Exchange Server** you can keep recorded voice messages into one universal inbox.

  - **UM Auto Attendant URI** text field requires the SIP URI of the MS Exchange Server. When extension accesses his mailbox by dialing ***0**, the call will be redirected to the voice mailbox on the MS Exchange Server.

  - **UM Extension** text field requires an extension number that Unified Messaging will use when voice mail is submitted to the user's MS Exchange Server mailbox.

Please Note: When the **MS Exchange Server** option is selected as an external voice mail server, the transport protocol **TCP** is automatically used regardless of the **Transport Protocol for SIP messages** radio button selection.

Attendant Extension Settings

For **Attendant** extensions (available only for QXFXO4, QXISDN4 and QXE1T1 gateways), 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 AA 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 QX'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.

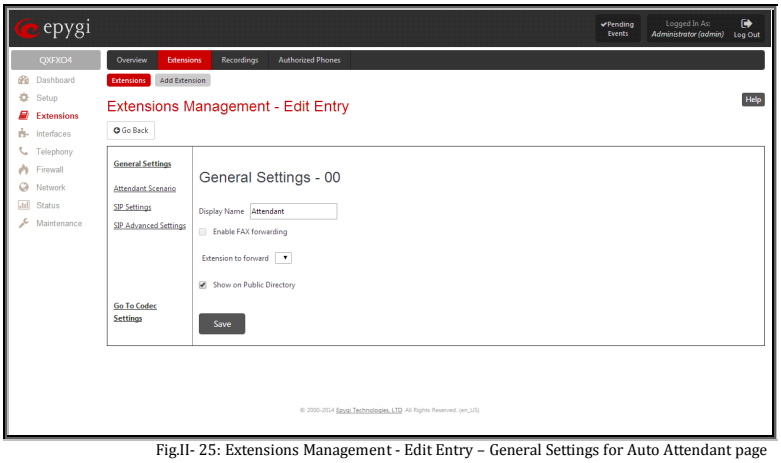


Fig.II- 25: Extensions Management - Edit Entry – General Settings for Auto Attendant page

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding auto attendant extension will be displayed in the PBX Information page.

2. Attendant Scenario

This group is used to select between default and custom attendant functionality scenarios.

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

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

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

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

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

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

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

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

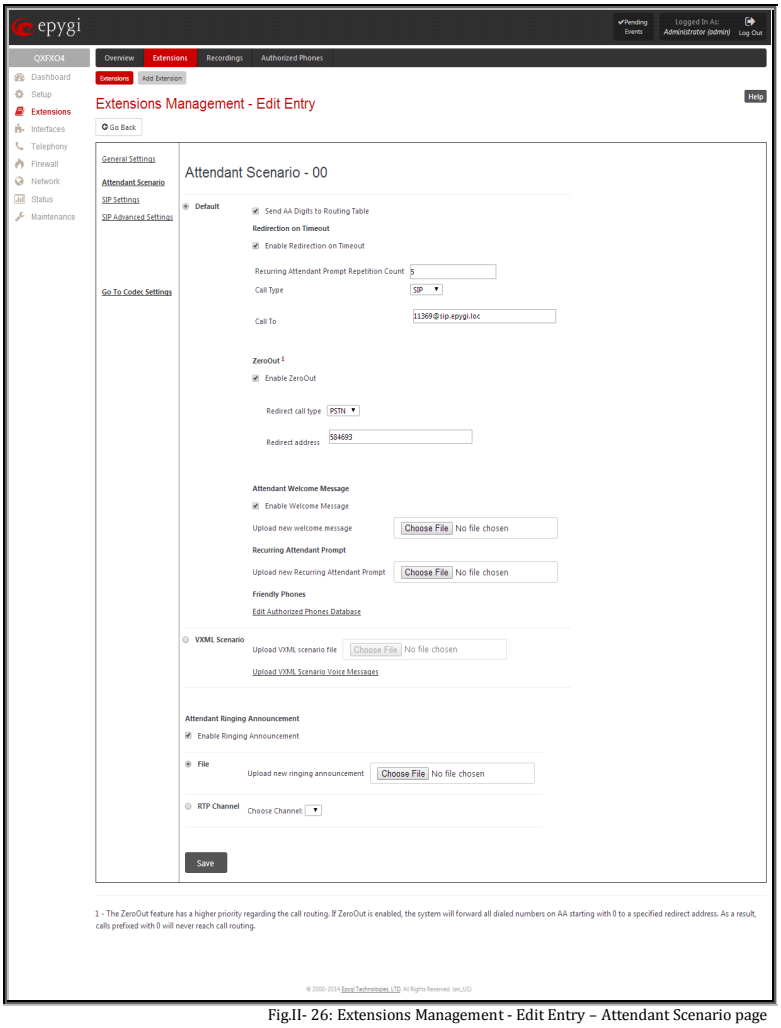


Fig.II- 26: Extensions Management - Edit Entry – Attendant Scenario page

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

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

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

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

  Enable Welcome Message checkbox is used to enable/disable the Auto Attendant welcome message (the default one or the custom one uploaded from this page or recorded from the handset being played when callers enter QX'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 (CCITT u-law, 8 kHz, 8 bit Mono) 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.

Choose File 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 (CCITT u-law, 8 kHz, 8 bit Mono) 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.

  Choose File 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.

- **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 QX Authorized Phones database, they are free to access the Auto Attendant Services without passing the authentication or to use the Call Back services.

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

- The **Upload VXML 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. **Choose File** opens the file chooser window to browse for a custom scenario file.

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

- The **View/Download VXML 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 VXML 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.

Choose File opens a file chooser window to browse for a custom voice message for an archive file with the "tar.gz" extension containing the custom attendant scenario and the voice prompt recordings.

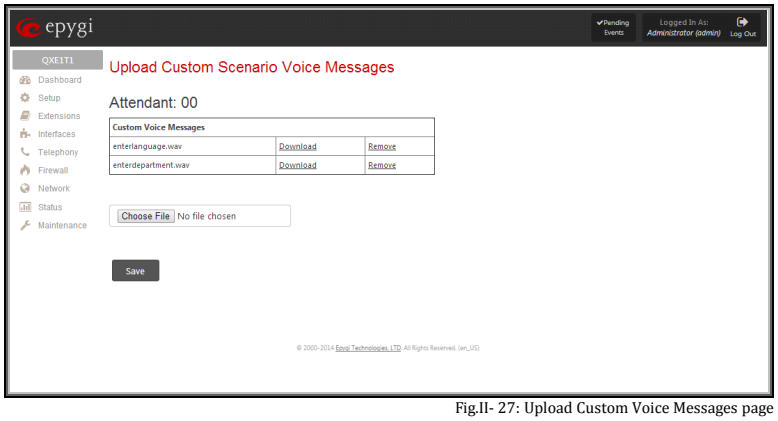


Fig.II- 27: Upload Custom Voice Messages page

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

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

The group offers the following components:

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

- **File** selection is used to upload the ringing announcement file. The following option is available under this selection:

  Upload new ringing announcement indicates the file name used to upload an announcement. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) 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.

Choose File 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.

- **RTP Channel** selection is used to define the channel for the broadcast streaming. The RTP channels are created by the system administrator. Therefore if you are experiencing problems with using the RTP channels as ringing announcement, or no RTP channels are available to select on this page, turn to your system administrator for clarification.

Extension Codecs

To establish an IP voice communication, call participants have to use the same codec. When establishing a communication line, this codec is negotiated. If the caller does not find an appropriate codec, the communication does not take place. To allow communication with all IP callers, it is helpful to support as many codecs as possible. In this case, all codecs that the system offers should be enabled in the **Codecs** table. On the other hand, some codecs require quite a high transfer rate of up to 64 kBit/s. If you definitely do not want to use these codecs, make sure they are disabled in the **Codecs** table.

The **Codecs** table lists the voice and video codecs supported by the QX. Each table entry is assigned a checkbox that is used to manipulate the entry, for example to disable, to move it up or down, etc.
The table entries in bold type indicate codecs enabled for the selected extension/attendant. The enabled codecs participate in codec negotiation at the call setup. The order of the enabled codecs is very important. Each codec in the table has a higher priority than the codecs below it, and a lower priority than the codecs above it. A codec placed at the top of the table is used as the preferred codec. When establishing a call, the system will try this codec first. If the remote party does not support the preferred codec, the following codecs will be tried out strictly in the order given in the **Codecs** table.

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

Enable/Disable enables or disables the selected codec. Disabled codecs do not participate in codec negotiation, i.e. they will never be used to for call setup. At least one codec must be enabled; otherwise voice communication with an extension/attendant will be impossible.

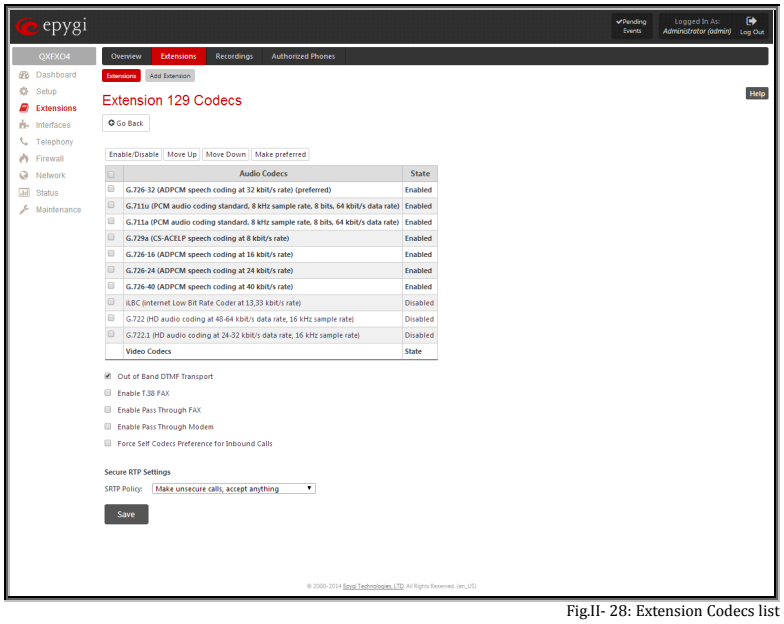


Fig.II- 28: Extension Codecs list

Move up moves the selected codec one level up, increasing the codec's priority.

Move down moves the selected codec one level down, decreasing the codec's priority.

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

The following settings are available for user extensions and attendants only:

Out of Band DTMF Transport enables the DTMF code transmission in parallel with the voice stream. Destination received the DTMF code will play it locally if it supports the feature too. This helps avoid DTMFs loss in case of heavy traffic. The feature is valuable for all codecs but it is especially recommended for low bit rate codecs, such as G.729, G.726/16, etc.

Enable T.38 FAX enables the T.38 codec support of FAX transmission for incoming unified FAX messages (fax to mailbox) and remote IP devices connected to Epygi unit via routing rules which using the target extension user settings (UES).

Enable Pass Through FAX enables the G.711 codec support for incoming unified FAX messages and IP devices connected to the attached IP line.

If both of the above checkboxes are enabled, the T.38 codec will be used as a preferred codec for FAX transmission. If it is not supported by the peer, the G.711 codec will be used instead.

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

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

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

Secure RTP Settings are used to configure secure voice over IP communication on the QX. The **SRTP Policy** drop down list is used to select the secure IP connection policy. For IP phones, the following options are available:

- **Make and accept only secure calls** - only the secure calls will be generated and accepted.
- **Make and accept only unsecure calls** - only the unsecure calls will be generated and accepted.
- **Try to establish secure calls, accept anything** - system will try first to establish secure call, but will fallback to unsecure call if party doesn't accept secure calls; both secure and unsecure incoming calls will be accepted, as requested by remote party, with the preference given to establishing secure call.
- **Make unsecure calls, accept anything** - system will establish unsecure outgoing calls, but both secure and unsecure incoming calls will be accepted as requested by remote party.

For bandwidth used by secure calls, see Needed Bandwidth for IP Calls.

Upload Universal Extension Recordings

The **Upload Universal Extension Recordings** (available only for QXISDN4, QXFXO4 and QXE1T1 Gateways) are to be defined by the QX administrator and will be present instead of the default voice messages for all extensions on the QX. 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 QX.

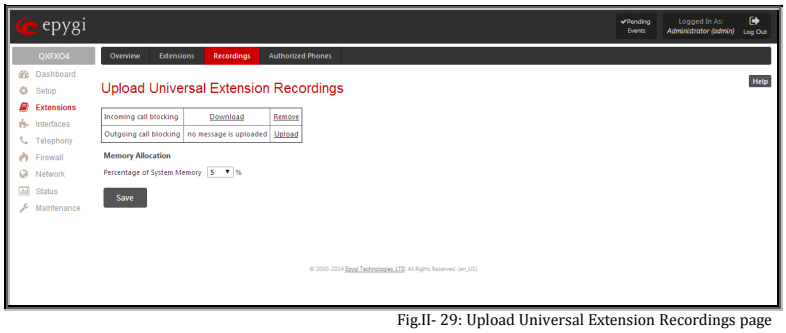


Fig.II- 29: Upload Universal Extension Recordings page

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

Authorized Phones Database

The **Authorized Phones Database** page (available only for QXISDN4, QXFXO4 and QXE1T1 gateways) is used to create a list of trusted external phones. If they are part of the QX Authorized Phones database, external SIP or PSTN, then users are free to access the QX 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 QX Auto Attendant. A direct connection to the **Call Relay** menu can be optionally provided.

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

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

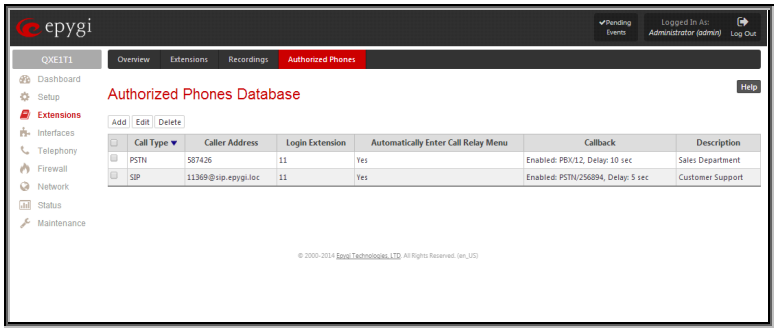


Fig.II- 30: Authorized Phones Database

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

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

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

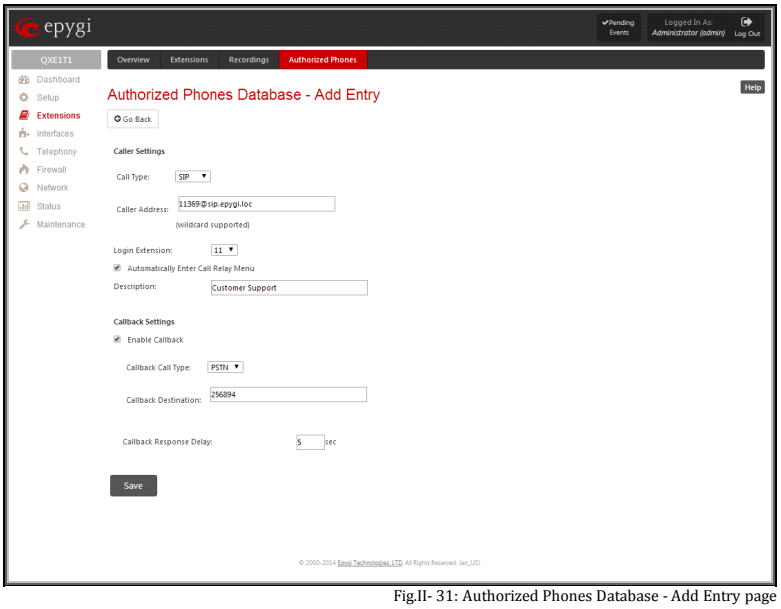


Fig.II- 31: Authorized Phones Database - Add Entry page

Caller Settings

The **Call Type** drop down list includes possible incoming call types (PSTN, SIP or Auto). In **SIP**, the caller connects QX 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 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.

The **Login Extension** drop down list provides all existing extensions on the QX. When calling the QX 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 QX system. The trusted user will directly access the QX 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 QX 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 and Call Relay services with no authentication.

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

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

Callback Settings

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

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

The **Callback Destination** text field requires the destination number where QX should instantly call back to. The value inserted in this field is dependent on the selected callback call type: for **PBX**, extension number 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.

The **Callback Response Delay** text field requires the delay (in seconds) after which the call back will be performed.

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

Pre-Configured Call Back

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

To use **Pre-configured Call Back**, the caller registered in the Authorized Phones Database should simply call to the QX's Auto Attendant through SIP or PSTN, let the call to ring twice and then hang up. Call Back will be instantly activated, and QX will call back to the defined Call Back destination. By answering the incoming call caller will be connected to the Auto Attendant menu.

Please Note: Depending on the call back destination, make sure that there is at least one PSTN line (FXO, E1T1 or ISDN) routed to the Auto Attendant (from the FXO Settings, E1/T1 Trunk Settings or ISDN Settings page) or Auto Attendant has a proper SIP registration (see Attendant Extension Settings).

Remote Call Back

The **Remote Call Back Configuration** service is used by authorized callers to configure or reconfigure existing call back configuration on the QX. Remote Call Back Configuration is divided into two modes accessible from the QX'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 callers registered in the Authorized Phones Database to create a new trusted caller with Call Back enabled. They can also modify the Call Back destination of existing callers in the Authorized Phones Database. By calling QX's Auto Attendant and entering the Auto Attendant menu, the caller can use the * 6 code to create a new trusted caller as well as to modify the Call Back destination for the already registered callers in the Authorized Phones Database.

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

When system accepts the inserted settings, the corresponding entry will be logged to the Authorized Phones Database. The caller will then be disconnected from the QX's Auto Attendant and the defined Call Back destination will receive a call from the QX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX's Auto Attendant.

Please Note: The detected caller number must correspond to the one applied by the caller. In case of PSTN call back at least one PSTN line must be available on the QX. There must be network connectivity and the destination must be reachable.

Non-Permanent Call Back configuration service allows trusted caller to organize one-time Call Back to the defined destination. In this situation, no entry will be logged to the Authorized Phones Database. By calling QX's Auto Attendant and entering the Auto Attendant menu, the caller can use * 5 menu (see Call Codes Available in Auto Attendant) to modify the Call Back destination for already registered callers in the Authorized Phones Database.

The system will ask to login by dialing the number and an appropriate password for the QX's extension that is used as login extension in the Call Back settings. After login, caller should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database. The caller will then be disconnected from the QX's Auto Attendant and the defined Call Back destination will receive a call from the QX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX's Auto Attendant.

Please Note: For both **Permanent Call Back** and **Non-Permanent Call Back**, the detected caller number must correspond to the one configured for trusted caller. In case of PSTN call back at least one PSTN line must be available on the QX. There must be network connectivity and the destination must be reachable.

Interfaces Menu

The **Interfaces** menu allows you to configure the following settings:

For QXFXS24 Gateways:

- **General Operation Mode**
- **FXS Lines**
  - FXS (On-board) Line Settings
  - Diagnostic Loopback

For QXFXO4, QXE1T1 and QXISDN4 Gateways:

- **FXO Settings**
- E1/T1 Trunk Settings
- **ISDN Settings**
- **PSTN Lines Sharing**
  - PSTN Gateway Operation Mode

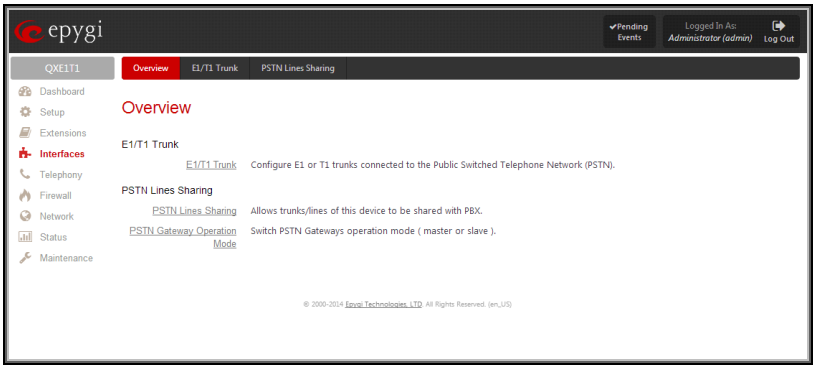


Fig.II- 32: Interfaces Menu page

General Operation Mode

The **General Operation Mode** page provides the option of setting up a corresponding mode for the QXFXS24 gateway.

The **General Operation Mode** radio buttons are as follows:

- The **Stand-alone mode** selection configured the device manually from its own GUI. In this mode the device is used as a standalone gateway.
- The **PNP Mode** selection getting the device configuration from another QX IP PBX unit. Some configuration values could be altered manually if needed.

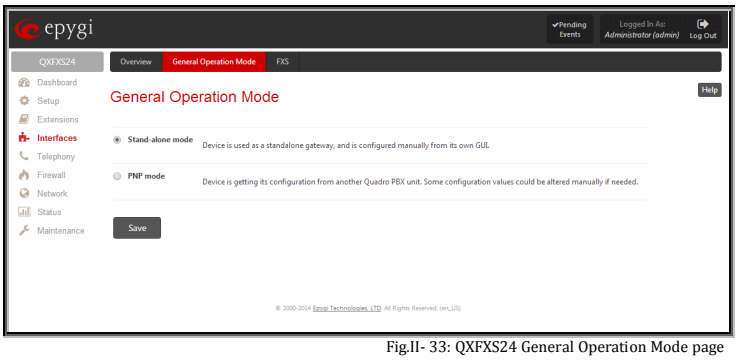


Fig.II- 33: QXFXS24 General Operation Mode page

FXS Lines

FXS (On-board) Line Settings

The **FXS (On-board) Line Settings** page is used to configure QX lines and to define the caller ID detection type, configure remote party disconnect indication and select the ringer type on each of them. Additionally this page provides an option to enable Loopback diagnostics on the lines.

The **Onboard Line Settings** page shows the table **Available Lines** where all active lines of QX are listed (QXFXS24 has 24 active lines) with their **Attached Extension**. If the line is attached to an extension, the corresponding extension number is displayed in this column; otherwise "none" is displayed if the extension is not attached to the line. By clicking on the extension number, the Extensions Management - General Settings page will appear, where the line attached to the extension can be reconfigured. Additionally, the table provides information about the selected **Ringer Type** and **Caller ID** detection method that is configured for the selected line. The caller ID detection method is different for various types of phones and can be found in the phone manual.

When pressing on the line number under the **Available Lines** column, the **FXS On-board Line Settings** page specific for the current line is opened and offers the following input options:

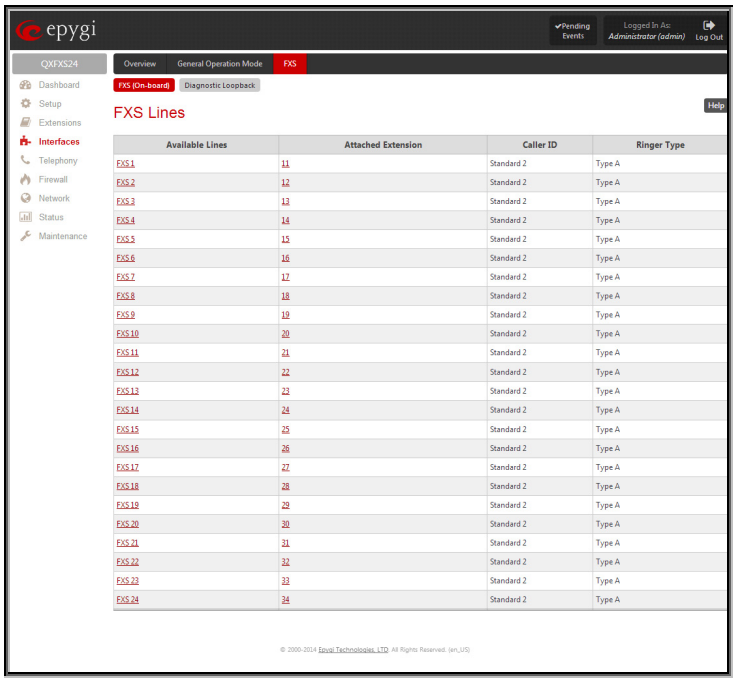


Fig.II- 34: FXS Line page

The **Caller ID** drop down list contains various standards of Caller ID transmissions. It is used to send the calling party's information to the phone attached to the selected line:

- No Caller ID.
- FSK, send prior to the first ring.
- FSK, send between the first and second ring.
- FSK, send both prior to a ring and between the first and second ring.
- DTMF, send prior to the first ring.
- DTMF, send between the first and the second ring.
- Combined, send both DTMF prior to the first ring and FSK between the first and the second rings.

The QX sends the current time/date to the called phone together with the caller's information.

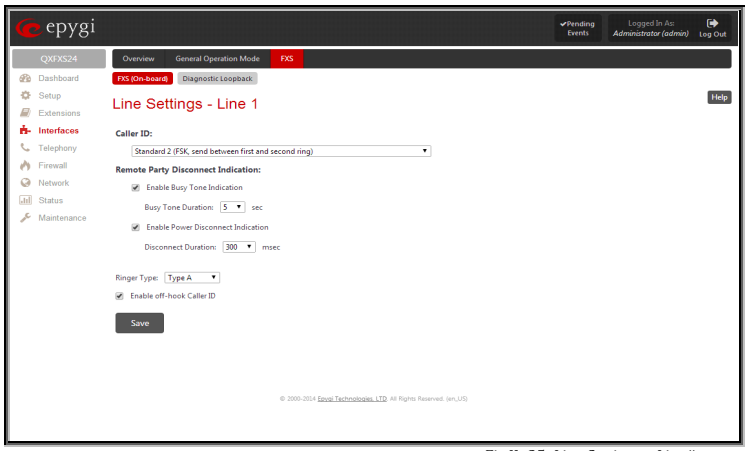


Fig.II- 35: Line Settings – Line# page

A group of **Remote Party Disconnect Indication** parameters are used to configure the private PBX attached to the QXFXS24 FXS port.

- The **Enable Busy Tone Indication** checkbox enables a busy tone transmission to the FXS port when the remote party being called is disconnected. The **Busy Tone Duration** drop down list is used to select the period (in seconds) when a busy tone will be transmitted to the FXS port.
- The **Enable Power Disconnect Indication** checkbox enables the power cycling on the FXS line when the remote party being called is disconnected. Power Disconnect is applied after the busy tone transmission on the FXS line. The **Disconnect Duration** drop down list is used to select the period (in milliseconds) when the FXS line power will be down.

The **Ringer Type** drop down list allows you to select the frequency of the ringer supported by the phone attached to the line. Information can be found on the phone enclosure or in the phone's manual. Problems with the ringer might occur if the ringer type selected here does not correspond to the one supported by the phone.

Please Note: The supported ringer type can be found on the bottom of the phone, in the "**Ren:x.xN**" value where **N** is the ringer type supported by the phone. For example, if N=A, the TypeA ringer type should be selected, if N=B, the TypeB&Z ringer type should be selected.

The **Enable off-hook Caller ID** checkbox enables Caller ID transmission to the phone in the off-hook state attached to a certain line. Service is applicable to the phones supporting the Call Waiting Caller ID feature.

Information on the Caller ID system:

Caller ID is a service identifying the caller (when performing a call or sending a voice mail) and notifying the called party about the identity of the caller. The Caller ID service is available only for phones with a display to show that information. Two types of Caller ID notification are available on QX: **FSK** and **DTMF**.

FSK Standard:

The FSK standard supports caller ID indication either with the phone handset on-hook or if the called party is already busy with another call or operation (handset is off-hook). For internal calls, caller ID notification in FSK can show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's extension number. The second line shows the caller's nickname (if indicated in the configuration). For external IP calls, caller ID notification in FSK can also show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's user name. The second line shows the caller's nickname (if indicated in configuration). If the nickname is not available and there is a display name, provided by the caller party, the second line will display it, otherwise the URL, in the format: username@host will be displayed. For calls from the PSTN network, the entire caller ID message will be shown.

DTMF Standard:

The DTMF standard supports caller ID indication only if the phone handset is on-hook (phone is free and ready to accept calls). This standard also has caller ID notification conditions but they are non-configurable. Caller ID notification in DTMF can show only one line of identifiable parameters on the called phone's display. For internal calls, it is the caller's extension number. For external IP calls, it is the caller's user name. For calls from the PSTN network, caller ID will only display the caller's phone number.

Please Note: DTMF supports only parameters consisting of digits. If any letter symbol has been used in the external caller user name, DTMF will not display caller ID.

To Configure the FXS Line Settings

1. Click on the line number link in the **FXS Lines** table. The **Line Settings - Line#** page will appear in the browser window.
2. Use the **Caller ID** drop down list to select the caller ID detection system mode corresponding to the phone type.
3. Enable the **Dialing Prefix With Caller ID** checkbox if needed.
4. Configure the **Remote Party Disconnect Indication** parameters by selecting the corresponding checkboxes.
5. Define a **Ringer Type** from the corresponding drop down list.
6. Enable **Off-hook Caller ID** if needed.
7. Press the **Save** button on the **Line Settings - Line#** page to save the caller ID system and other line specific configuration settings.

Diagnostic Loopback

The **FXS Lines Loopback Settings** page is used to configure the lines for voice loopback diagnostics. When loopback is enabled on the line, any incoming calls to the corresponding line will automatically pick up on the first ring and any voice towards the line will automatically be sent back to the caller (the caller will hear themselves in the handset). **Loopback Timeout** provides the option of limiting the voice loopback diagnostics duration, i.e. the caller will be disconnected from the QX when the **Loopback Timeout** expires.

The **FXS Lines Loopback Settings** page shows the only table where all FXS lines of the QX are listed. On this page, the loopback diagnostics may be enabled/disabled and the Loopback Timeout can be adjusted for FXS lines.

The **FXS Lines Loopback** table lists all the FXS lines on the QX along with their loopback parameters (**Loopback State** and **Loopback Timeout**).

The **Edit** functional link leads to the **FXS Lines Loopback Settings - Edit Entry** page where **Loopback Timeout** (in seconds) may be configured for one or more selected FXS line(s).

The **Enable/Disable Loopback** functional link is used to enable/disable the Loopback service on the selected FXS line(s).

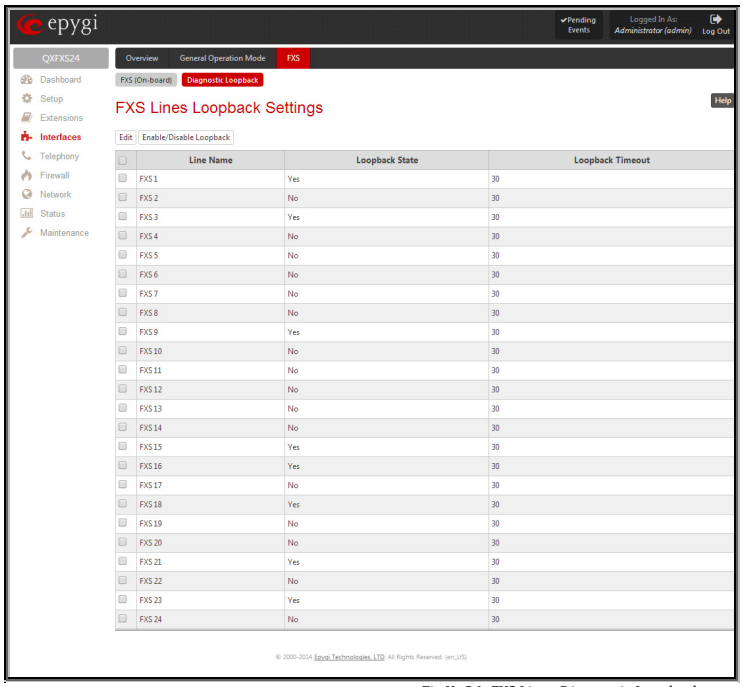


Fig.II- 36: FXS Lines Diagnostic Loopback page

FXO Settings

The **FXO Settings** are used to configure the FXO support that allows QXFXO4 to connect to other PBXs or analog telephone lines.

The QXFXO4 has 4 FXO lines. The **FXO Settings** allows you to limit incoming or outgoing calls for the selected FXO line if required. Depending on configuration of the FXO gateways, multiple shared FXO ports from one or more FXO gateways may be available on the QXs, thus giving you the option to use them simultaneously.

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

If the FXO service is disabled, the **Allowed Call Type**, **Route Incoming Call to** and **PSTN number** columns are set to "N/A".

Clicking on the FXO line number will open the **FXO Settings - FXO#** page where the FXO line settings may be modified. The **FXO Settings - FXO#** page consists of the following components:

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

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

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

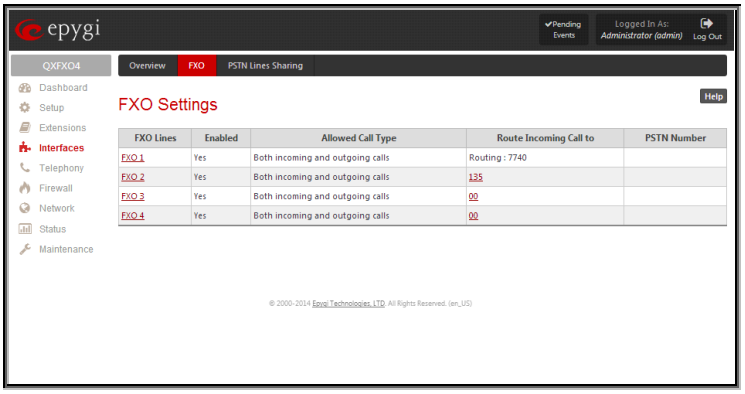


Fig.II- 37: FXO Settings page

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

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

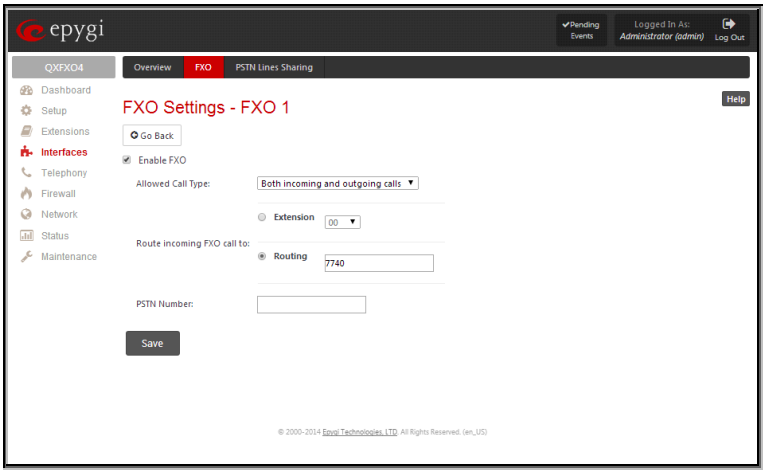


Fig.II- 38: FXO Settings – FXO# page

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

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

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

To modify the FXO Settings

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

E1/T1 Trunk Settings

The **E1/T1 Trunk Settings** allows QXE1T1 to be connected to a PBX or to a CO (Central Office) via E1/T1 lines, using E1/T1 CAS/CCS signaling. QXE1T1 may act as a user or as network. If connected to a private PBX, the QXE1T1 should be configured in the network mode. If an E1/T1 trunk from the CO is connected to the QXE1T1, it should be configured as a user.

QXE1T1 has one E1/T1 trunk available.

The **E1/T1 Trunk Settings** page is used to configure the E1/T1 trunk and the timeslots settings. The page consists of the following components:

The **Trunk Settings** table lists the available E1/T1 trunks on the QX and their settings (Trunk name, E1/T1 mode, interface, signaling types). Clicking on the trunk will open its **Signaling Settings** page (**Trunk CAS Signaling Settings** or **Trunk CCS Signaling Settings** page depending on the selected signaling type) while selecting the corresponding trunk's checkbox and pressing **Edit** will open the **Trunk – Edit Entry** page. **E1/T1 Stats** link is displayed for every active trunk on the board and refers to the page where E1/T1 trunk and traffic statistics can be viewed.

Start and **Stop** functional links are used to start/shutdown the selected E1/T1 trunk(s). When E1/T1 trunk is shutdown state, no E1/T1 calls could be placed and received.

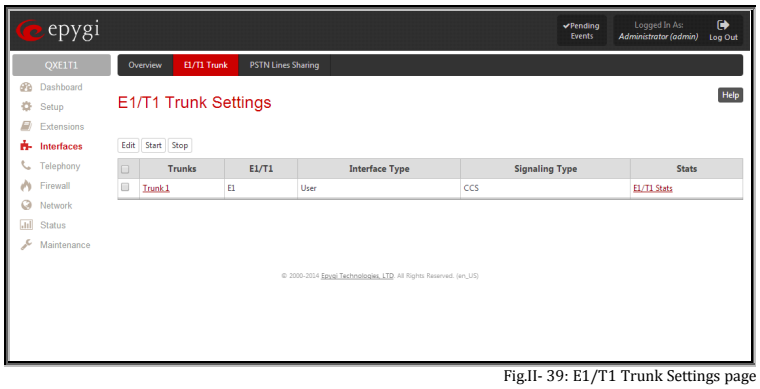


Fig.II- 39: E1/T1 Trunk Settings page

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

The **Interface Type** drop down list gives an option to choose between E1/T1 **User** and **Network** interface configuration.

The **Signaling Type** drop down list allows selection of **CAS** (Channel Associated Signaling) or **CCS** (Common Channel Signaling) signaling types. The same timeslot is used both for voice and data transmission in case of CAS signaling. In the case of CCS signaling a single timeslot is used for signaling data transmission on the entire trunk. All other timeslots are used for voice transmission.

The **E1** and **T1** radio buttons are used to select between E1 and T1 modes. The T1 mode enables 24 timeslots, and the E1 mode enables 32 timeslots to be used. The selection of E1 or T1 enables the **Line Code**, **Frame mode**, **Line Build Out**, **Coding Type, LoopBackMode** and **Clock Mode** settings. These settings are configured to match the E1/T1 settings from the service provider.

Attention: See the Call Routing Table chapter to ensure that modifications to the E1/T1 trunk settings do not lead to broken routes in the Call Routing Table.

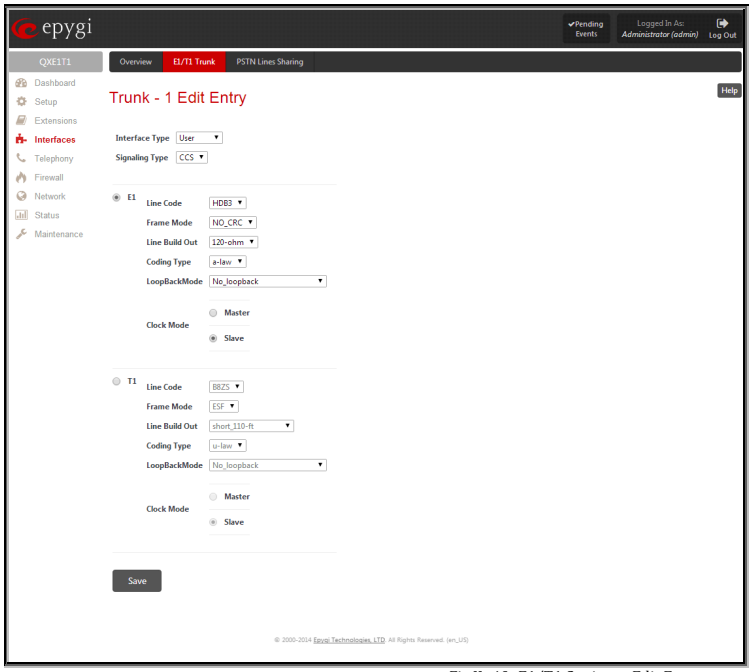


Fig.II- 40: E1/T1 Settings –Edit Entry page

The **Trunk CAS Signaling Settings** page lists the available timeslots of the trunk with CAS signaling and their settings.

The Incoming Interdigit Service link leads to the page where the dial plan for incoming E1/T1 calls from CO/PBX to the QX can be configured.

Incoming Digits Timeout text field requires a value between 0 and 20000 (in milliseconds) and is used to define the timeout during which incoming digits from the destination party calling QX will be collected before being applied as an incoming called number.

Signaling Standard drop down list is available only in E1 mode and is used to select the connection signaling standard.

Force Update functional button is used to apply immediately the new settings on the selected timeslot(s). This will force the timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.

Enable/Disable functional buttons are used to enable/disable the selected timeslot(s).

Select one or more timeslots and click on **Edit** to open the **CAS Signaling Wizard** that guides through the key configuration parameters specific to the timeslot.

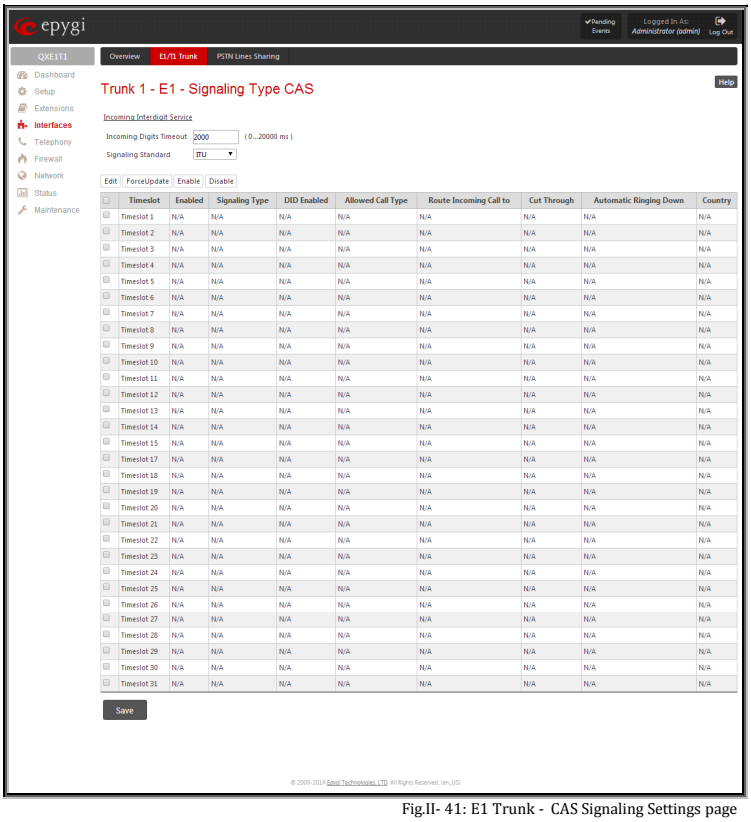


Fig.II- 41: E1 Trunk - CAS Signaling Settings page

The **CAS Signaling Wizard** offers a possibility to configure the selected timeslot(s) and provides a variable group of parameters depending on the E1/T1 trunk configuration.

CAS Signaling Wizard – Page 1 allows to configure signaling type settings and consists of following components:

Allowed Call Type is used to select the allowed call directions: incoming, outgoing or both.

Signaling Type allows selecting the CAS signaling type.

Please Note: R2 signaling (compelled and non-compelled) can be used with an E1 interface both in User and Network modes. QX with E1 interface in the CAS mode detects the busy tone only in case of R2 compelled and non-compelled (both with and without ANI) signaling types.

Force Update Timeslots checkbox can be optionally selected in order to apply new settings immediately. This will force the timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.

Please Note: QX does not support the **Forward Digit** selected on the CO when acting in the **User** mode with **CAS Loop Start** signaling type.

Get PSTN/PBX Error Message checkbox enables notification message in case of outgoing calls to unreachable, incorrect or non existent destination.

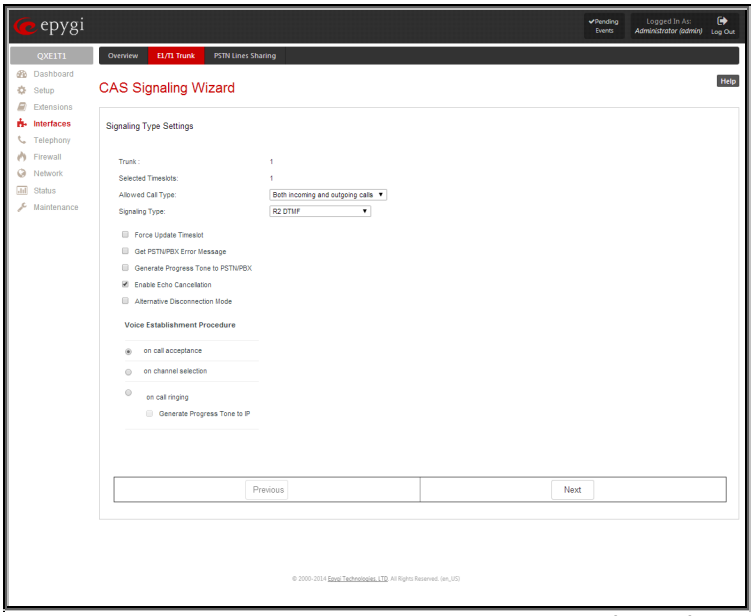


Fig.II- 42: CAS Signaling Wizard – Page 1

When **Generate Progress Tone to PSTN/PBX** checkbox is selected, QX generates ring tones to incoming callers during E1/T1 call dialing. This feature is mainly applicable to 2-stage dialing mode.

Enable Echo Cancellation checkbox enables the echo cancellation mechanism on the selected timeslot(s).

When **Alternative Disconnection Mode** checkbox is selected, the QX will play a busy tone towards the PBX/CO if the call has been failed. After 60 second timeout, the QX will disconnect the call from PBX/CO and will stop playing the busy tone.

Voice Establishment Procedure manipulation radio buttons group is used to select a method of voice establishment on the trunk:

- **On call acceptance** – with this selection, voice will be established after call is being accepted.
- **On channel selection** - with this selection, call will be accepted during channel selection. This selection is not allowed for R2 signaling.
- **On call ringing** - with this selection, voice will be established after call is being ringing. Selection enables **Generate Progress Tone** checkbox which is used to enable the progress tone generation upon voice establishment.

CAS Signaling Wizard - Page 2 appears if the **Signaling Type** on the previous page is set to any of the **E&M** types or to **R2 DTMF**. The page provides the possibility of enabling the DID Service on the timeslot(s) and contains the following component:

The **Enable DID Service** checkbox is used to enable/disable **DID** (Direct Inward Dialing) service for the selected timeslot(s).

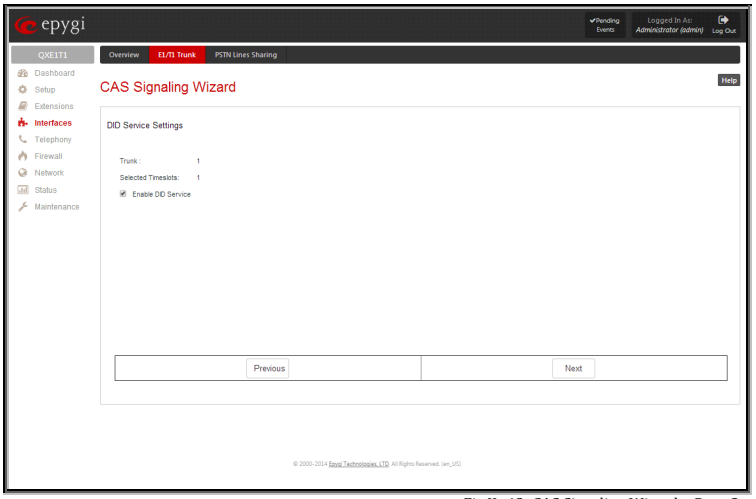


Fig.II- 43: CAS Signaling Wizard – Page 2

CAS Signaling Wizard – Page 3 allows to set the destination for incoming calls to be routed to and to enable **Cut Through** and **Automat Ringing Down** services for signaling different from R2 (all types).

Route Incoming Call to drop down appears when **Both incoming and outgoing calls** or **Incoming calls only** is selected from the **Allowed Call Type** list and allows selecting the destination where incoming calls should be routed. The list contains all extensions of the QX, Attendant and Routing agent. The routing agent gives two kinds of call routing possibilities in user mode and one in network mode. Choosing the **Routing** selection (available in User mode only) will request the caller to pass the authentication (if enabled) and will invite the caller to dial the destination number to connect the user within the QX Network. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without any additional dialing.

When **DID service** is enabled (in User mode only), incoming calls can be only routed to the Routing agent with simple **Routing** and **Routing with inbound destination number** call routing possibilities.

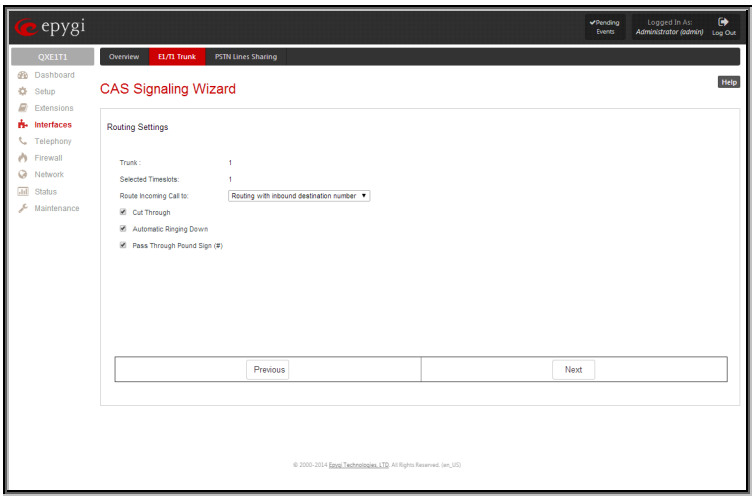


Fig.II- 44: CAS Signaling Wizard – Page 3

Attention: When QX acts in the Network mode with the Attendant as a destination to route the incoming calls, digit forwarding should be disabled on the PBX side. Otherwise, incoming digits may be mistaken as special calling codes on the QX's Attendant.

Cut Through checkbox is available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from R2 (all types) and is used to reconnect the call (terminated by some reason, e.g. user error, network problems, etc.) by going on-hook and off-hook again even if the call partner is off-hook and not involved in the call.

Automat Ringing Down checkbox is available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from R2 (all types) and allows an E1/T1 device connected to the QX to establish a hot-line call (automatic call without any digits dialed).

Pass Through Pound Sign (#) checkbox is only available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from E&M FGD or R2 (except for R2-DTMF). When this checkbox is selected, the pound sign (#) detected in the dialed number will be passed through and will be considered as a part of the dialed number. When this checkbox is not selected, the detected pound sign (#) will be considered as a call acceleration digit.

CAS Signaling Wizard – Page 4 appears only in E1 User mode when signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is R2 (all types) and is used to configure country settings. Page consists of the following components:

Country drop down list is used to set the location where QX is located to support the correct functionality of R2 signaling. For countries absent in this list, use **ITU** selection.

Use Default Country Settings checkbox restores default advanced settings for the selected country. When this checkbox is not selected, next page will provide a possibility to manually configure advanced country settings.

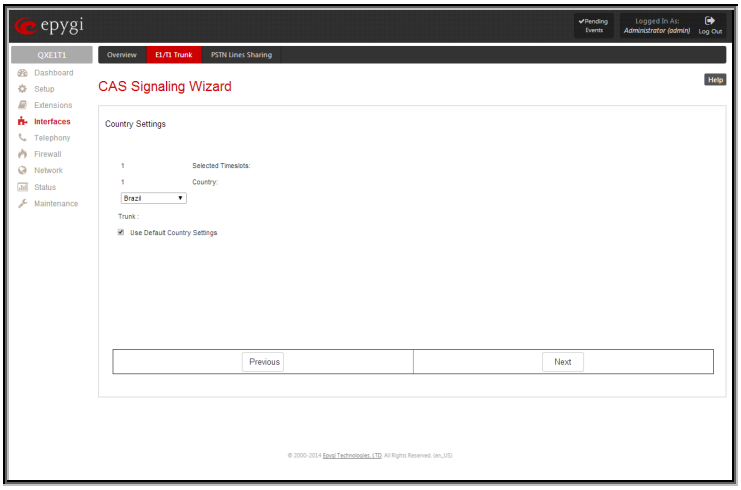


Fig.II- 45: CAS Signaling Wizard – Page 4

CAS Signaling Wizard – Page 5 appears only in E1 User mode when signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is R2 (all types) and when **Use Default Country Settings** checkbox is not selected on the previous page. This page is used to configure advanced country settings. Page consists of the following components:

ANI Category drop down list appears only when R2 signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard - Page 2** is different from **R2 DTMF** is used to select the calling party priority depending on the call originator's location specifics.

ANI Request Transmit and **ANI Request Receive** drop down lists allow you to select the Caller ID request R2 tones for transmit and receive.

Seize Acknowledge Timeout text field is used to define a timeout (in a range from 2 to 2000 milliseconds) between incoming seize signal and the corresponding feedback.

Answer Guard Timeout text field is used to define a wait timeout (in a range from 0 to 1000 milliseconds) Group-B Answer Signal and Line Answer.

Release Guard Timeout text field is used to define an idle timeout (in a range from 0 to 120000 milliseconds) between the disconnect signal receipt and call disconnection.

Dialing Delay Timeout text field is used to define a timeout (in a range from 0 to 2000 milliseconds) before injecting dialed digits. Timeout specially refers to R2 DTMF signaling.

Incoming DNIS Size text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When field has 0 value, system uses either timeout defined in the **Incoming digits timeout** field or the **End of Address** messages to establish a call. Independent on the value in this field, the message **End of Address** always causes the call establishment.

Unused A:B:C:D text fields require to configure unused C and D bits of E1/T1 CAS signaling (A and B bits are predefined). Fields may have either 0 or 1 values.

Invert A:B:C:D text fields are used to invert the ABCD status bits in time-slot 16 before TX and after RX. If bit is set to 1, the router inverts it before transmission and after the receipt.

End of DNIS (I-15) checkbox is used to enable End of DNIS service.

Collect Call checkbox is only available when **Brazil** is selected in the **Country** drop down list on the previous page of the wizard and when the PBX attached to the QX supports this feature. When this checkbox is selected and in case of incoming calls, always the called destination will pay for the call. Option is particularly applicable when calling from the mobile phone. Checkbox should be selected when the appropriate feature is enabled on the PBX.

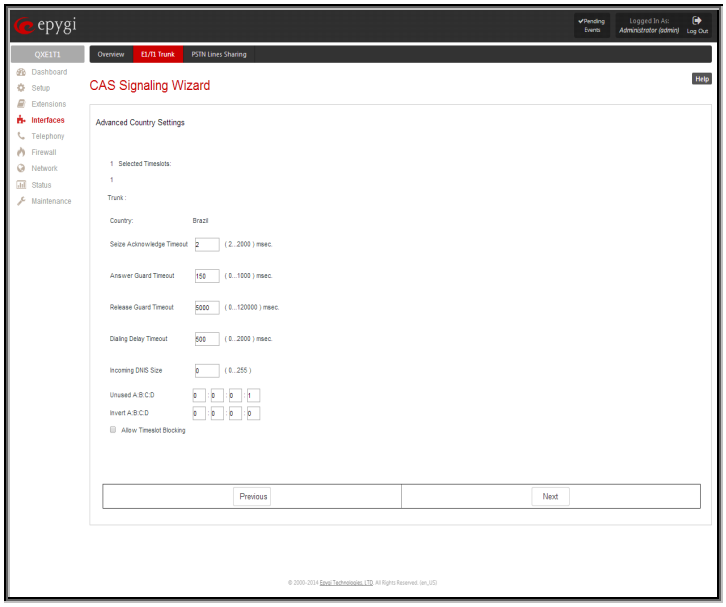


Fig.II- 46: CAS Signaling Wizard – Page 5

The **Allow Timeslot Blocking** checkbox indicates whether the system should use blocked timeslots to make outgoing PSTN calls. If this checkbox is selected, the system will NOT use timeslots blocked by the carrier. If the checkbox is clear, the system will try to unblock the timeslots and will make outgoing calls if succeeded.

Group B Support manipulation radio button group is present only when **R2** signaling selected from **Signaling Type** drop down list on the previous page is different from **R2 DTMF** and is used to enable/disable the **Group B Support**. The **Group B Support** manipulation radio button group offers following selections:

- **Enable** – this selection enables **Group B Support** both for answer and busy recognitions of transmit and receive signals. This selection requires you to define transmit and receive signals. The **Transmit Answer Signal** and **Transmit Busy Signal** parameters are defined from the drop down lists on this page. When transmit signals are selected, press **Next** on this page to access the **R2 Receive Signal Settings** page where **Receive Answer Signal** and **Receive Busy Signal** should be defined. Use the checkboxes to select the **Receive Answer Signal** and **Receive Busy Signal** values. Multiple values are allowed for each signal.
  Please Note: Warning appears if you have selected the same signal type both for receive answer and receive busy recognitions.
- **Partial Enable** – selection partially enables **Group B Support** with for answer recognition only. This selection requires you to define transmit and receive signals. The **Transmit Answer Signal** parameter is defined from the drop down list on this page. When transmit signal is selected, press **Next** on this page to access the **R2 Receive Signal Settings** page where **Receive Answer Signal** should be defined. Use the checkboxes to select the **Receive Answer Signal** value. Multiple values are allowed for each signal.
- **Disable** – selection disables **Group B Support** and requires defining the **Answer Signal** parameter.

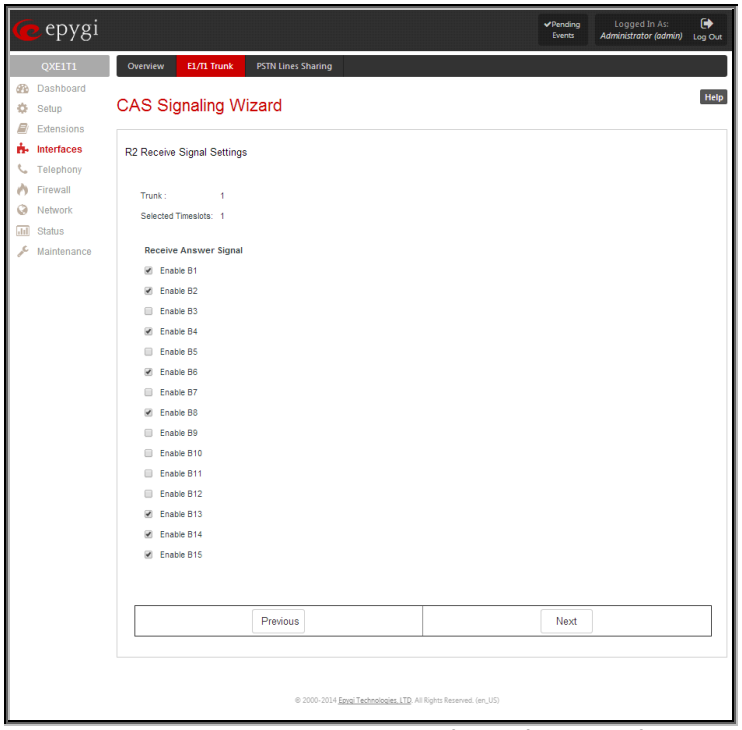


Fig.II- 47: CAS Signaling Wizard – Receive Signal Settings page

The **Trunk CCS Signaling Settings** page allows configuring CCS signaling settings and gives a possibility to select timeslots for signaling data transfer/receive and voice transfer. The page consists of the following components:

The **Non Automat** checkbox switches to non-automatic Terminal Endpoint Identifier (TEI) searching and enables the **TEI Address** text field that requires a TEI number (digit values from 0 to 63) for connection establishment between CO and E1/T1 client. In automatic mode, an E1/T1 connection will be established on the first available TEI, while in non-automatic mode a specific TEI may be reserved for the connection. In this case both call partners need to specify the same TEI in their settings.

The **SAPI Value** text field requires an additional Service Access Point Identifier (SAPI) value (digit values from 1 to 62) that is used to support additional interface between ISDN Layer 2 and Layer 3. Leaving this field empty (default value), only Call Control and Layer 2 management procedures will be activated.

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

In the **Network Mode** (PBX connected):

- If **Non Automat** mode is selected, the same **TEI address** should be specified on both sides- QX and PBX.
- If **Automat** mode is selected the user on PBX side will have the opportunity to set any mode related to TEI assignment in PBX configuration. This will allow PBX connection to the QX without providing the TEI address from QX.

In the **User Mode** (CO connected) the TEI assignment is dependent on CO settings:

- Select **Non Automat** mode and insert the same **TEI address** provided by CO.
- Select any mode related to TEI assignment if automat TEI searching mode is selected on CO side.

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

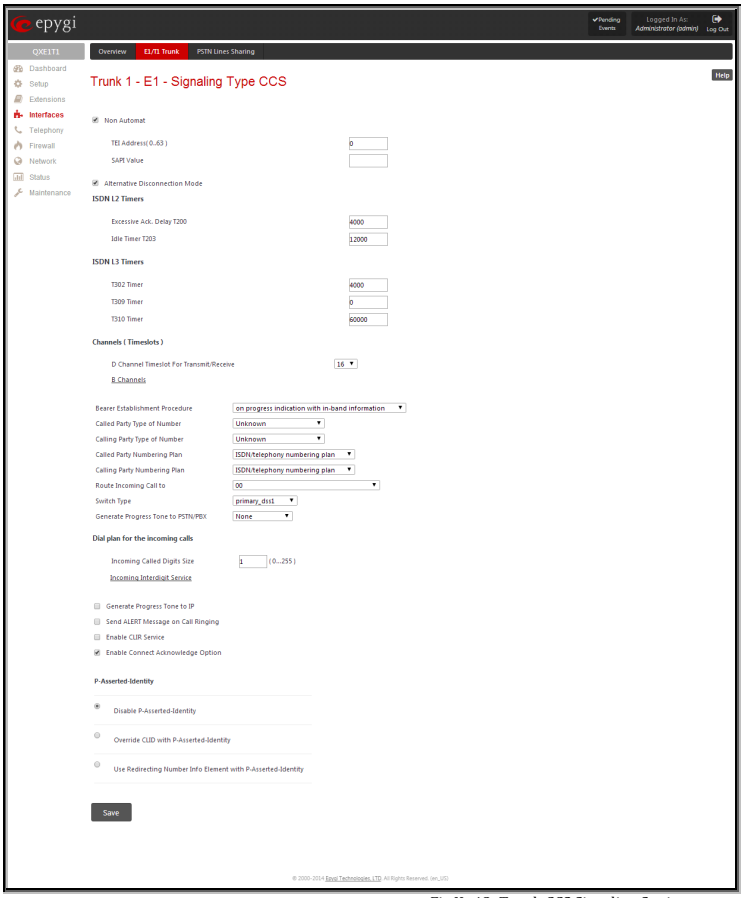


Fig.II- 48: Trunk CCS Signaling Settings page

ISDN L2 Timers:

- The **Excessive Ack. Delay T200** text field configures the period in milliseconds (digit values from 500 to 9999) between transmitted signaling packet and its acknowledgement received.
- The Idle Timer T203 text field configures the period in milliseconds (digit values from 1000 to 99999) for E1/T1 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) and indicates the time frame system is waiting for digit to be dialed and when timer expires, it initiates the call. Timer is not applicable for DMS-100 switch types.
- The **T309 Timer** text field requires the value for the T309 timer in milliseconds (digit values from 0 to 90000) responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is 0, T309 timer will be disabled.
- The **T310 Timer** text field requires the value for the T310 timer in milliseconds (digit values from 1000 to 120000) responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) is not yet arrived.

The **D Channel Timeslot For Transmit/Receive** drop down list contains the timeslots to be selected for signaling data transmit/receive.

The **B Channel** link leads to the **Signaling Type CCS – B Channel Settings** page where available timeslots may be enabled/disabled for the voice transfer and echo cancellation feature may be configured.

The **Force Update** option can be optionally used to apply new settings immediately. The **Restart** option is used to bring timeslot(s) to the initial idle state on the both sides. When applying one of these options, any active traffic on the timeslot(s) will be terminated.

Channel Selection drop down list 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, while for **Exclusive** channel selection CO should feedback only by the timeslot used for the call request.

Channel Selection Ordering drop down list is used to choose the B channels selection (Ascending or Descending). When **Ascending** selection is configured, B channels will be defined starting from B1 to B23/B30. For **Descending** selection, B channels will be defined from B23/30 to B1. If your CO/PBX has **Ascending** B channels selection configured, it is recommended to use **Descending** B channels selection and vice versa.

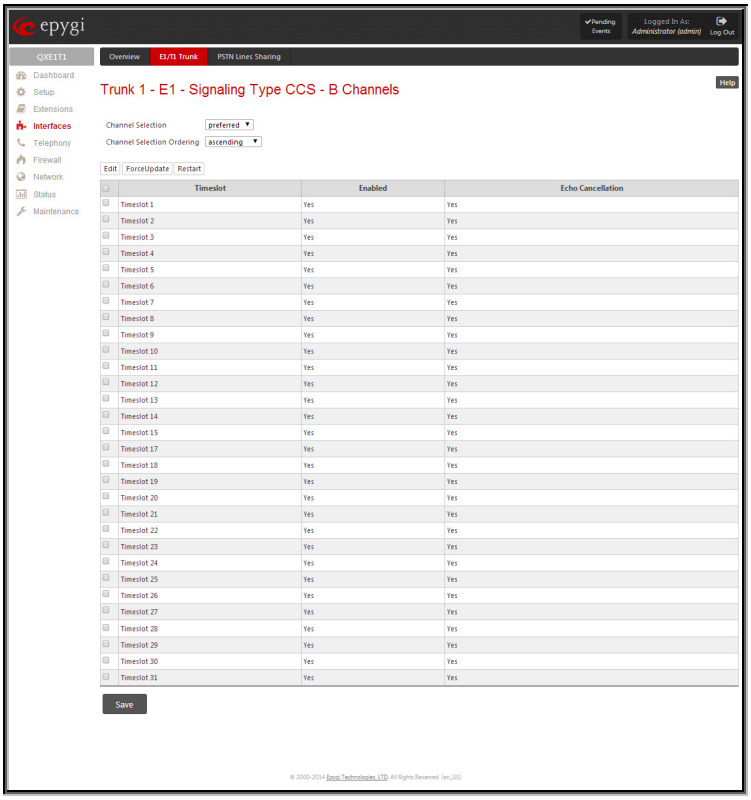


Fig.II- 49: Trunk CCS Signaling Settings – B Channels page

Edit functional button opens **B channels – Edit Entry** page, which contains 3 checkboxes:

- **Enable Timeslot** – used to enable/disable the selected timeslot(s);
- **Force Update Timeslot** – used to apply new settings immediately by restarting the timeslot(s);
- **Enable Echo Cancellation** – used to enable/disable the echo cancellation feature on the selected timeslot(s).

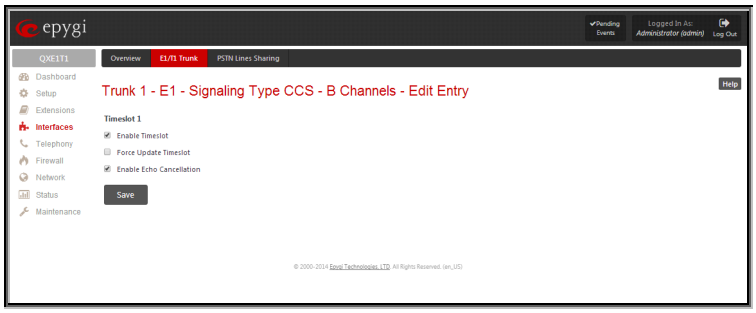


Fig.II- 50: E1 Trunk - CCS Signaling Settings – B Channels – Edit Entry page

Please Note: A timeslot can be used either for voice or data transfer. Timeslot selected for the D Channel receive/transmit is missing in the list of B channels.

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

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

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

The **Route Incoming Call to** drop down list contains Attendant, routing agent with two kinds of call routing possibilities, and all extensions of QX and allows selecting the destination where incoming calls will be routed to. Choosing the "**Routing with inbound destination number**" selection will request the authentication (if enabled) and then will automatically use the initially dialed number to connect the destination without any additional dialing.

Attention: When QX acts in the Network mode with the Attendant as a destination to route the incoming calls to, digit forwarding should be disabled on the private PBX side otherwise incoming digits may be mistaken as a special calling codes on the QX's Attendant.

Switch Type is another configuration parameter that depends on the Service Provider when acting in the User mode and the private PBX capabilities when acting in the Network mode.

The **Generate Progress Tone to PSTN/PBX** drop-down list contains the options for sending progress (ring-back) tone to callers from the PSTN/PBX. The following options are available in the list:

- **None** configures the system to send ALERT messages without the Progress Indicator information element (IE).
- **Unconditional** configures the system to send ALERT/PROGRESS messages with the Progress Indicator IE. With this option, the system will send its own progress tone.
- **Conditional** configures the system to send ALERT/PROGRESS messages with Progress Indicator IE. With this option, the system will send its own progress tone only if there is no early media (180/183 with SDP) from the called party.

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 field has 0 value, system uses either 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 pound sign always cause the call establishment.

P-Asserted-Identity:

The **Disable P-Asserted-Identity** radio button disables the P-Asserted-Identity feature for both incoming and outgoing calls.

The **Override CLID with P-Asserted-Identity** radio button selection enables the SIP P-Asserted-Identity support.

For the calls from SIP to E1/T1 if the Invite SIP message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on E1/T1 is sent with the original Caller ID which comes from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field.

For the calls from E1/T1 to SIP with restricted Caller ID, the SIP Invite message contains P-Asserted-Identity field with the value from the Caller ID on E1/T1. The SIP From field contains anonymous.

The **Use Redirecting Number Info Element with P-Asserted-Identity** radio button selection enables full support of the SIP P-Asserted-Identity.

For the calls from SIP to E1/T1, if the SIP Invite message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on E1/T1 contains the number from the user name field and the Redirecting Number IE contains the original number from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field.
For the calls from E1/T1 to SIP with Caller ID, the SIP Invite message contains P-Asserted-Identity field with the original number value from the Redirecting Number IE on E1/T1. The SIP From field contains the value from the user name.

The **E1/T1 Trunk Status** page provides information about the selected trunk state. Following information is displayed on this page:

- **E1/T1 mode** - displays which mode is selected: E1 or T1.
- **Interface Type** - displays selected interface type: User or Network.
- **Signaling Type** - displays selected signaling type: CAS or CCS.
- **Clock Mode** - displays the selected clock mode: Master or Slave.
- **Framing mode** - displays selected framing mode.
- **Link** - displays E1/T1 link state: up or down.
- **Frame Synchronization** - displays the signal synchronization state in the trunk: Yes or No.
- **Red Alarm** - indicates that the receive frame alignment for the line has been lost and the data cannot be properly extracted. The red alarm is indicated by the loss of frame condition for the various framing formats.
- **Out of Frame** - number of Out of Frame errors.
- **Line Code Violation** - number of Line Code Violation errors.
- **Frame Synchronization** - number of Frame Synchronization errors.
- **Link Synchronization** - number of Link Synchronization errors.

The following statistics are available, if **CAS Signaling** is selected:

- **Active Calls** - currently active calls in the selected trunk.
- **Outgoing Calls** - total outgoing calls in the selected trunk.
- **Incoming Calls** - total incoming calls in the selected trunk.

Following statistics is available when **CCS Signaling** is selected:

ISDN PRI Layer statistics:

- **Received Packets** - number of received packets.
- **Received Errors** - number of received errorneous packets.
- **Transmitted Packets** - number of transmitted packets.
- **Transmitted Errors** - number of transmitted errorneous packets.

ISDN PRI Layer 2 statistics is displayed for actual TEI value and the received and transmitted packets:

- **TEI Value** – the actual TEI assigned.
- **L2 State** – the state of the TEI assignment.
- **Information Frame** - signaling packets for call initiation and termination.
- **Receive Ready** - controlling packets during E1/T1 link is up.
- **Receive Not Ready** - controlling packets in case of inability to accept calls by destination.
- **SABME** - packets upon connection establishment.
- **Disconnected Mode** - packets when connection is being disconnected.
- **Disconnect** - packets upon connection termination.
- **Unnumbered Acknowledgement** - packets upon accepting connection establishment/termination.
- **Framer** - packets as a report of an error condition.
- **TEI** - packets containing TEI (Terminal Endpoint Identifier) to initiate subscription of the device in the network.
- **Unnumbered Information Frame** - broadcast signaling packets received for call initiation and termination.
- **Exchange Identification** - received packets containing connection management settings.

ISDN PRI Layer 2 Errors statistics:

- **Incorrect Length** - packets with incorrect length.
- **Bad Supervisory Frame** - packets with incorrect supervisory header.
- **Bad Unnumbered Information Frame** - packets with incorrect unnumbered information frame header.
- **Bad Frame Type** - packets with bad frame type.
- **Bad Unnumbered Frame** - packets incorrect unnumbered acknowledgement frame header.
- **Bad TEI Value** - packets with bad TEI (Terminal Endpoint Identifier) value.

ISDN PRI Layer 3 statistics shows the same information as for CAS signaling.

No E1/T1 trunk statistics is displayed in this page at first, but page is getting automatically refreshed every 10 minutes. Statistics collected since that time and the last resetting of the counter will be displayed here.

The **Blocked Timeslots** text field lists the timeslots blocked by the carrier. The field is present for E1/T1 CAS R2 signaling type only.
Current System Time displays the actual time on the QX and the **Last Time Cleared** displays the exact date and time when the E1/T1 Stats has been manually cleared last time. **System Uptime** displays the period QX is on since last reboot.
To reset the statistics counters press the **Clear** button.

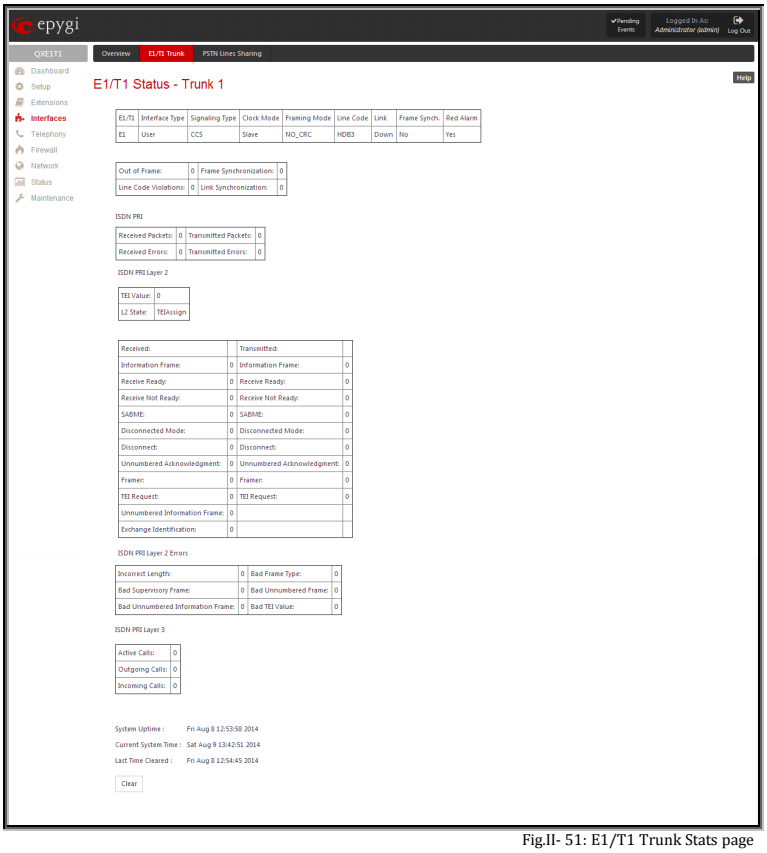


Fig.II- 51: E1/T1 Trunk Stats page

Incoming Interdigit Service

The **Incoming Interdigit Service** is used to configure E1/T1 dial plan for the incoming calls from CO/PBX to the QX. This service allows you to speed up the call establishment procedure by detecting the prefix. The calls will be speed up by the timeout defined in the **Incoming Digits Timeout** text field.

When the system detects incoming dialed number starting with any of the prefixes listed in the **Incoming Interdigit Service** table, it will wait for the rest of the digits, as specified for the corresponding prefix in the **Incoming DNIS Size** text field (see below). Once all digits are received, the system will route the call to the destination.

The **Incoming Interdigit Service** page lists a table with existing E1/T1 dial plan entries and allows you to manage them.

By default, the table on the **Incoming Interdigit Service** page lists the locale specific (selected from the System Configuration Wizard) E1/T1 dial plan settings. For some countries, this table may however be empty.

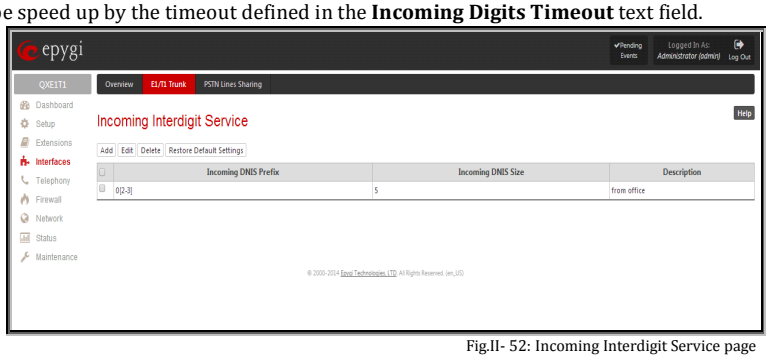


Fig.II- 52: Incoming Interdigit Service page

Add functional button leads to the **Add Entry** page where a new E1/T1 dial plan entry can be configured.

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

The **Incoming DNIS Prefix** text field requires the prefix of the incoming dialed number. '[' , ']' , ',', '-', are used to define a range or a quantity of prefixes. For example, 2[5-9] means that the prefix of the dialed number may be 25, 26, 27, 28, or 29. 3[4,7,0] means that the prefix of the dialed number may be 34, 37 or 30. Only one range of prefixes can be defined in the **Incoming DNIS Prefix** text field.

Fig.II- 53: Incoming Interdigit Service – Add Entry page

The **Incoming DNIS Size** text field requires the total length of the dialed number, including the prefix digits. The number defined in this field should be greater than the longest prefix defined in the **Incoming DNIS Prefix** text field, otherwise the error message will appear.

The **Description** text field requires an optional description for an E1/T1 dial plan entry.

The **Restore Default Settings** functional button is used to restore the locale specific E1/T1 dial plan entries

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 QXISDN4 gateway act as a user or as a network. If connected to a private PBX, the QXISDN4 should be configured in the network mode. If an ISDN trunk from the CO (Central Office) is connected to the QXISDN4, it should be configured as a user. QXISDN4 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 QXISDN4 gateway.

The **Trunk Settings** table lists the available ISDN trunks on the QXISDN4 and their settings (trunk name and interface types).

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).

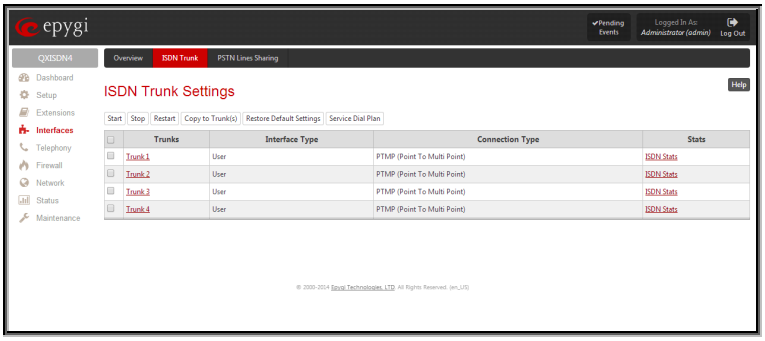


Fig.II- 54: ISDN Trunk Settings page

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

The **ISDN Wizard – ISDN Settings** allows you to choose the interface type and the connection type of the selected trunk(s).

The **Interface Type** drop down list allows you to select between the User and the Network interfaces. If the ISDN port of the QX is connected to the CO then **User** interface type should be selected. If the ISDN port of the QX is connected to the PBX then **Network** interface type should be selected (in that case QX acts as a CO for that PBX).

The **Connection Type** manipulation radio button group allows you to choose the connection type for the selected trunk(s):

- **PTP (Point to Point)**
  In case of connection to the CO (**User** interface type is selected on QX) choose this option if only QX is connected to the ISDN trunk from CO (no other ISDN devices are connected to the particular ISDN trunk from CO besides the QX).
  In case of connection to the PBX (**Network** interface type is selected on QX) choose this option if only the PBX is connected to the ISDN trunk from the QX (no other ISDN devices are connected to the particular ISDN trunk from the QX).
  In both cases, with this selection, QX sets the TEI to manually mode assigning the default value of 0. If needed, that value can be changed later in the **Advanced Settings** page of ISDN Wizard.

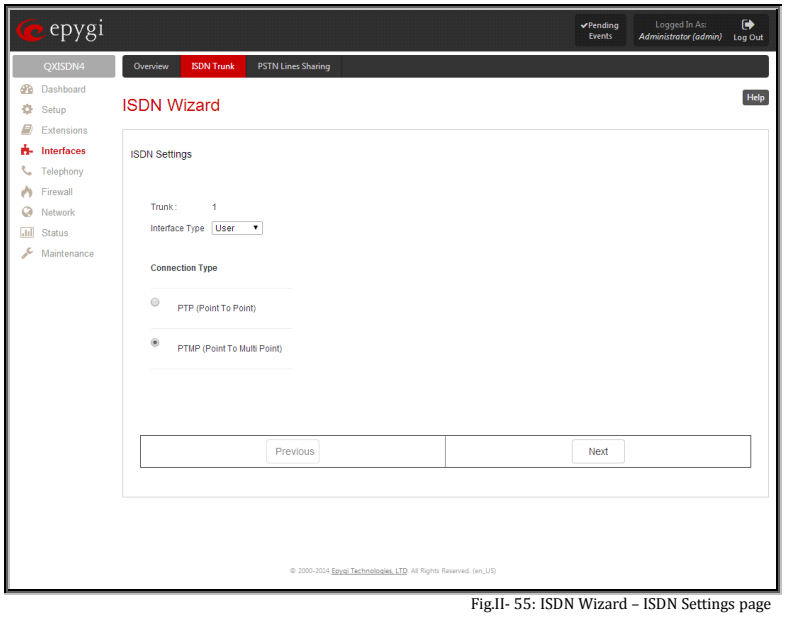


Fig.II- 55: ISDN Wizard – ISDN Settings page

- **PTMP (Point to Multi Point)**
  In case of connection to the CO (**User** interface type is selected on the QX) choose this option if there can be other devices connected to the same ISDN trunk from CO except the QX.
  In case of connection to PBX (**Network** interface type is selected on the QX) choose this option if there can be other devices connected to the same ISDN trunk from QX except for the PBX.
  In both cases, with this selection QX sets the TEI to automatic mode.

Please Note: Consult with your CO operator or network administrator before configuring the ISDN connection type.

The **ISDN Wizard - Page 2** content is dependent on the connection type selected on the previous page of **ISDN Wizard**:

The next page is **ISDN Wizard – MSN Settings** page which is used to turn on the MSN configuration. It is recommended to enable the MSN when there are multiple ISDN devices connected to the same ISDN bus. If the MSN is enabled on this page, the next page will require the MSN table configuration.

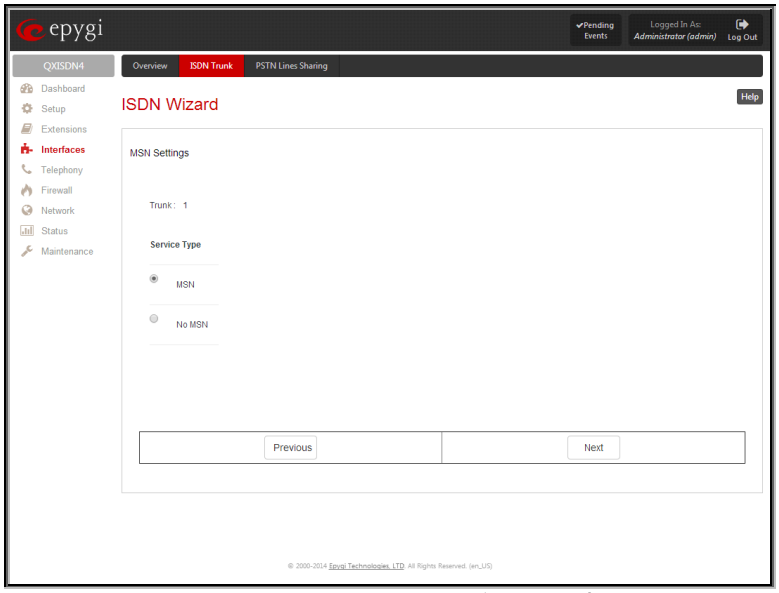


Fig.II- 56: ISDN Wizard – ISDN MSN Settings page

For MSN service enabled, the **Routing Settings** page is used to assign MSN numbers to the certain destinations on the QX. The MSN number can be assigned to the QX's extensions, to the Auto Attendant, or to the routing agent. The destination selected from this page will ring upon incoming call to the corresponding MSN number comes in.

The fields in the **MSN Number** column require the MSN numbers allocated to the QX.

Please Note: At least one MSN number should be defined in this page. The system displays an error message if the same MSN number is used twice in this page.

The **Route Incoming Call to** drop-down lists is used to select the destination where the incoming call addressed to the certain MSN number will be routed. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without any additional dialing. If MSN is disabled on the **ISDN Wizard - MSN Settings** page, the **ISDN Wizard - Routing Settings** page contains only one **Route Incoming Call to** drop-down list.

Selecting the **Use Default outgoing Caller ID** allows you to overwrite the source caller information with the one specified in the **Default outgoing Caller ID** field when placing outgoing calls toward the CO. The **Default outgoing Caller ID** field requires the caller ID for the outgoing calls from the QX through the ISDN trunk. That number should be registered at the CO and can be one of the MSNs provided by the CO. If this checkbox is enabled but no value is defined in the **Default outgoing Caller ID**, empty caller information will be sent to the CO. If this checkbox is disabled, the source caller information will be forwarded to the CO.

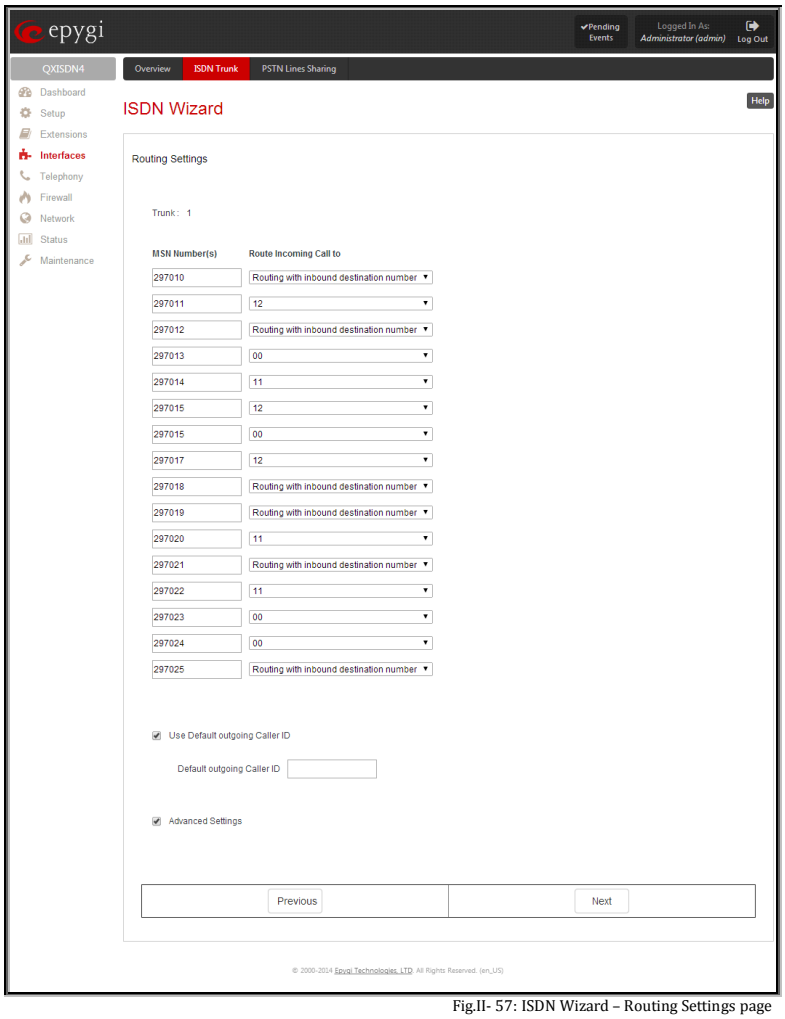


Fig.II- 57: ISDN Wizard – Routing Settings page

Select the **Advanced Settings** checkbox if you wish to adjust trunk's L2 and L3 Settings manually, otherwise leave this checkbox unselected to use the system default values.

The **ISDN Wizard – L2&L3 Settings** is used for advanced configuration only and contains L2&L3 Settings. This page only appears when the **Advanced Settings** checkbox is selected on the previous page of the wizard. This page contains the following components:

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

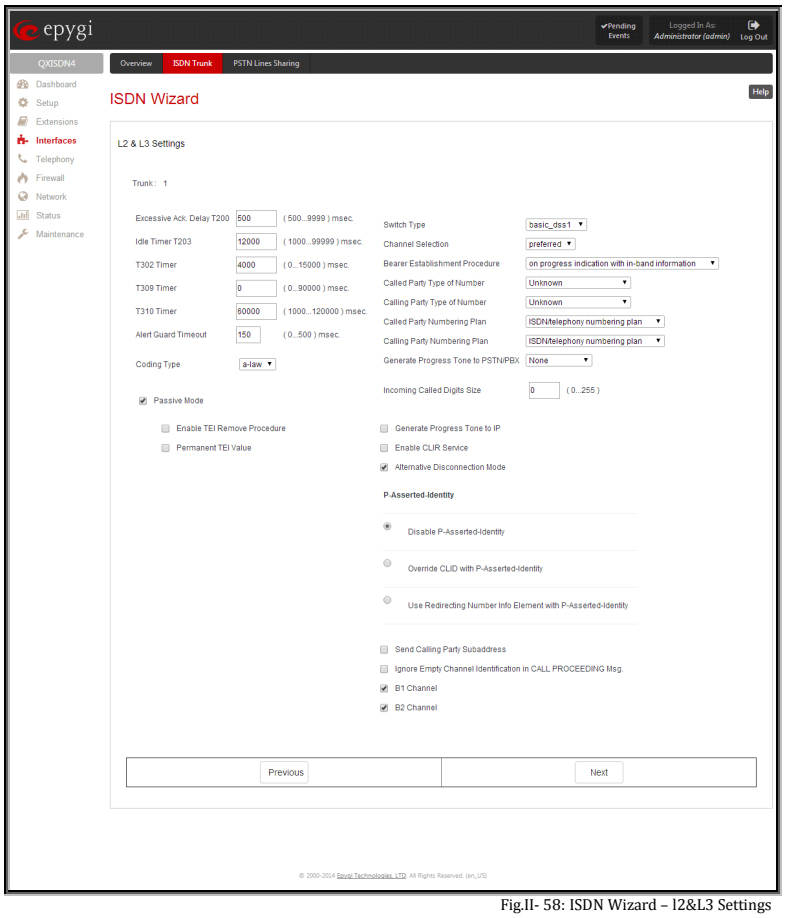


Fig.II- 58: ISDN Wizard – l2&L3 Settings

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

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

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, QX keeps its Layer1 always active. This checkbox enables the **Enable TEI Remove Procedure** and **Permanent TEI Value** checkboxes. With the **Enable TEI Remove Procedure** checkbox is selected, the trunk will lose the assigned TEI when entering into passive mode on the Layer 2. With the **Permanent TEI Value** checkbox is selected, the trunk will keep the assigned TEI when entering into passive mode on the Layer 2 or when QX detected ISDN link DOWN signal from carrier.

These checkboxes are present only for connection types different from **PTP (Point to Point)** selected on the first page of **ISDN Wizard**. In case if **PTP (Point to Point)** connection type is selected on the first page of the ISDN Wizard, these two checkboxes are replaced with a **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.

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 asked in 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 subaddress 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.

When **Generate Progress Tone to PSTN/PBX** checkbox is selected, QX generates ring tones to callers during ISDN call dialing. This feature is mainly applicable to 2-stage dialing mode.

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, QX will disconnect the call as soon as the disconnect message has been received from the peer. When the checkbox is selected, QX's user may hear a busy tone when peer has been disconnected.

P-Asserted-Identity:

The **Disable P-Asserted-Identity** radio button disables the P-Asserted-Identity feature for both incoming and outgoing calls.

The **Override CLID with P-Asserted-Identity** radio button selection enables SIP P-Asserted-Identity support. For the calls from SIP to ISDN if Invite SIP message contains a P-Asserted-Identity, then the CallerID on ISDN is sent with the original Caller ID, which comes from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field.
For the calls from ISDN to SIP with restricted Caller ID, the SIP Invite message contains P-Asserted-Identity field with the value from the Caller ID on ISDN. The SIP From field contains "anonymous".

The **Use Redirecting Number Info Element with P-Asserted-Identity** radio button selection enables full support of the SIP P-Asserted-Identity.
For the calls from SIP to ISDN, if the SIP Invite message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on ISDN contains the number from the user name field and the Redirecting Number IE contains the original number from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field.
For the calls from ISDN to SIP with Caller ID, the SIP Invite message contains P-Asserted-Identity field with the original number value from the Redirecting Number IE on ISDN. The SIP From field contains the value from the user name.

When the **Send Calling Party Subaddress** checkbox is selected, QX will send the extension number as subaddress and the value defined in the **Default outgoing Caller ID** field as caller ID on the outgoing call. When this checkbox is disabled, no subaddress information will be sent and the caller ID will be defined according to the selection of the **Use Default Outgoing Caller ID** checkbox (see above). Caller ID information, along with the Subaddress, can be displayed on the phone display depending on the phone and PBX settings and capabilities.

When the **Ignore Empty Channel Identification in CALL PROCEEDING Msg.** option is selected, QX will ignore the empty ISDN L3 Channel Identification information element in CALL PROCEEDING message and will not response with STATUS message.
When this checkbox is disabled, QX will response with STATUS message on empty Channel Identification information element.

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.

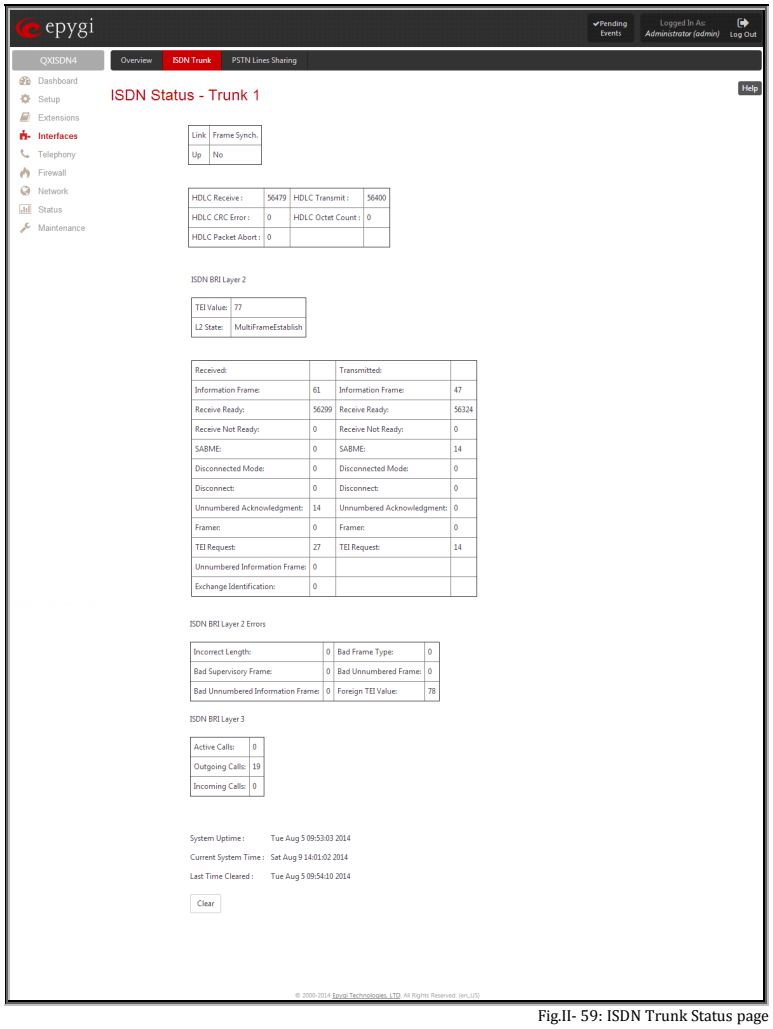


Fig.II- 59: ISDN Trunk Status page

The following **ISDN 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 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

The **PSTN Lines Sharing** page allows QX to use the PSTN lines (FXO lines, E1/T1 and/or ISDN trunks) on other QXs. This provides the option to call not only through local PSTN lines but also through available shared FXO, E1/T1 or ISDN lines in the network of QXs. When the sharing mode is enabled and one QX is configured to use the shared PSTN lines of another QX, the corresponding routing patterns will automatically be created in the Call Routing Tables (see Call Routing Table) on both QXs. This will allow PSTN call routing between the two QXs.

The **Provide PSTN lines for master device** checkbox is used to enable QX to use the shared PSTN lines on a remote device. This selection requires you to configure the Authorization Parameters.

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

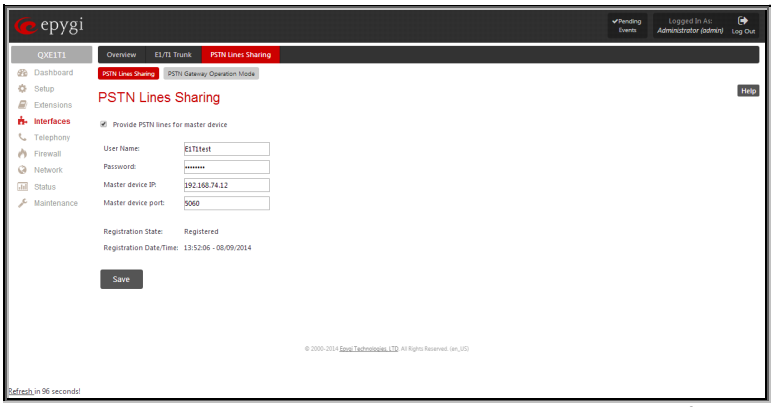


Fig.II- 60: PSTN Lines Sharing page

To use the shared remote PSTN lines on QX IP PBX

1. Enable the **Use PSTN lines of the other device** checkbox from the **Interfaces - PSTN Gateways** page.
2. Press **Save** to apply the selection.
3. Enter the **Authorization Parameters** page.
4. Create an account using a unique **Username** and a **Password**.

PSTN Gateway Operation Mode

This page is used to select the PSTN Gateway operational mode. One of the two modes can be selected:

Slave Mode - is used to adjust settings to share local PSTN lines with other devices.

Master Mode - is used to adjust settings to use PSTN lines of the other PSTN Gateways.

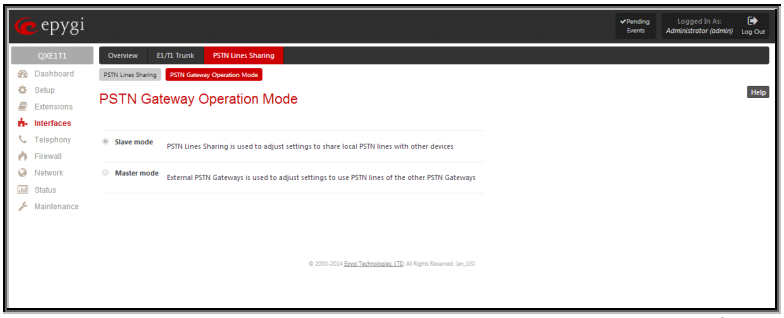


Fig.II- 61: PSTN Gateway Operation Mode page

Telephony Menu

The **Telephony** menu allows you to configure the following settings:

- **VoIP Carrier Wizard**
- **Call Routing Table**
  - Call Routing
  - Local AAA Table
  - Global Speed Dial Directory
  - SIP Tunnel Settings
- **NAT Traversal Settings**
  - General Settings
  - SIP Parameters
  - RTP Parameters
  - STUN Parameters
  - NAT Exclusion
- **RTP Settings**
- **SIP Settings**
  - SIP Aliases
  - TLS Certificates
- **Advanced Settings**
  - RTP Streaming Channels
  - Gain Control
  - RADIUS Client Settings
  - Dial Timeout
  - Call Quality Notification
  - Hold Music Settings

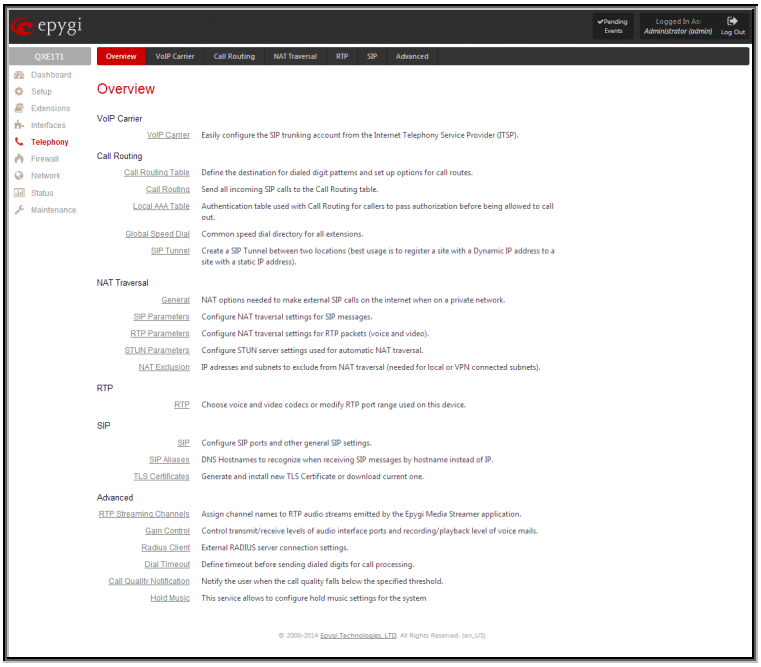


Fig.II- 62: Telephony Menu page

VoIP Carrier Wizard

The **VoIP Carrier Wizard** (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) 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. This entry is available to PBX users only, which means only PBX users can make calls to the corresponding VoIP carrier. Additionally, a virtual extension automatically generated in Extensions Management will be registered on the defined VoIP Carrier's SIP server.

The settings of that extension will be used to make calls from QX'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.

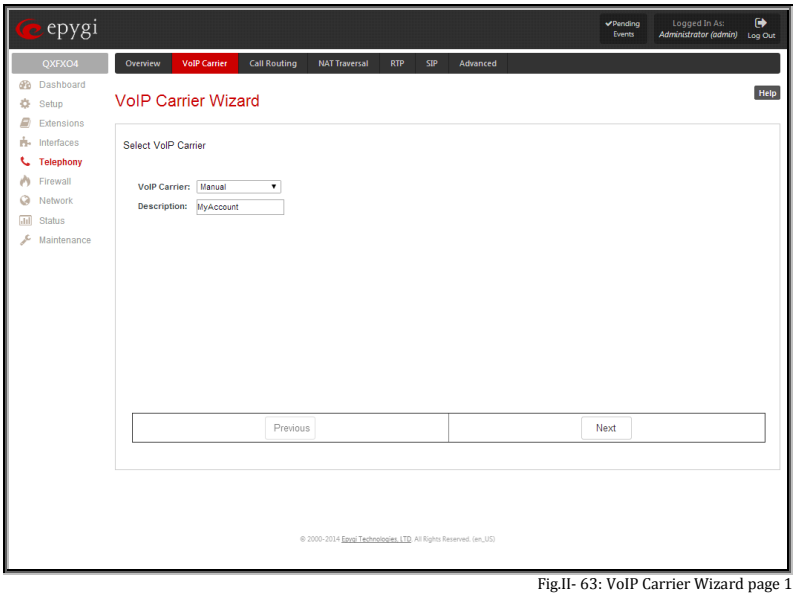


Fig.II- 63: VoIP Carrier Wizard page 1

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.

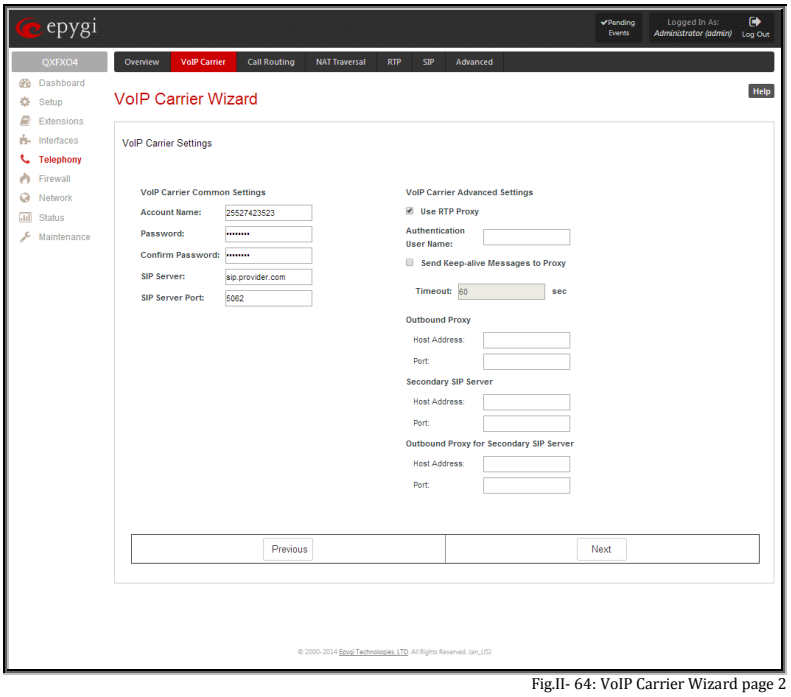


Fig.II- 64: VoIP Carrier Wizard page 2

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 QX. When this checkbox is selected, the RTP streams between external users will be routed through QX. 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 QX to reach the selected SIP servers.

VoIP Carrier Wizard – Page 3 contains the following VoIP Carrier access code selection components:

The **Access code** text field requires a digit combination by dialing which the corresponding VoIP Carrier will be reached. The **Access code** radio buttons allows you to create outbound routing rules.

- **By prefix** text field requires entering the prefix that will be placed in front of the routing pattern instead of the discarded digits. The Prefix field can consist of numeric values only. A corresponding warning appears if any other symbols are inserted.

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

The **Route Incoming Calls to** drop down list allows you to select an extension (or Auto Attendant) on the QX where incoming calls from the configured VoIP Carrier should be routed to. For the selected extension there will be an unconditional forwarding set up which will care for incoming calls forwarding from the VoIP carrier to the corresponding extension.

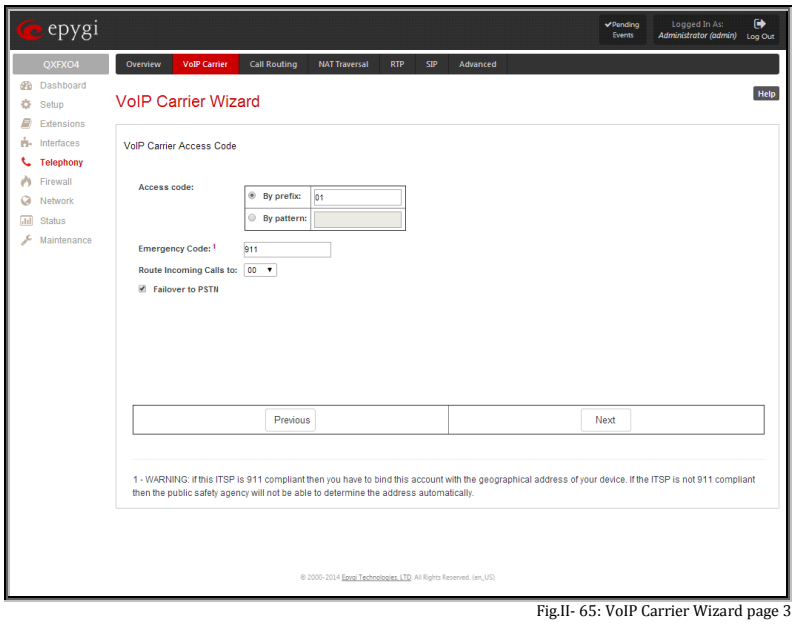


Fig.II- 65: VoIP Carrier Wizard page 3

The **Failover to PSTN** checkbox selection will route the call to the PSTN through the local PSTN 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.

Call Routing Table

The **Call Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and source 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.

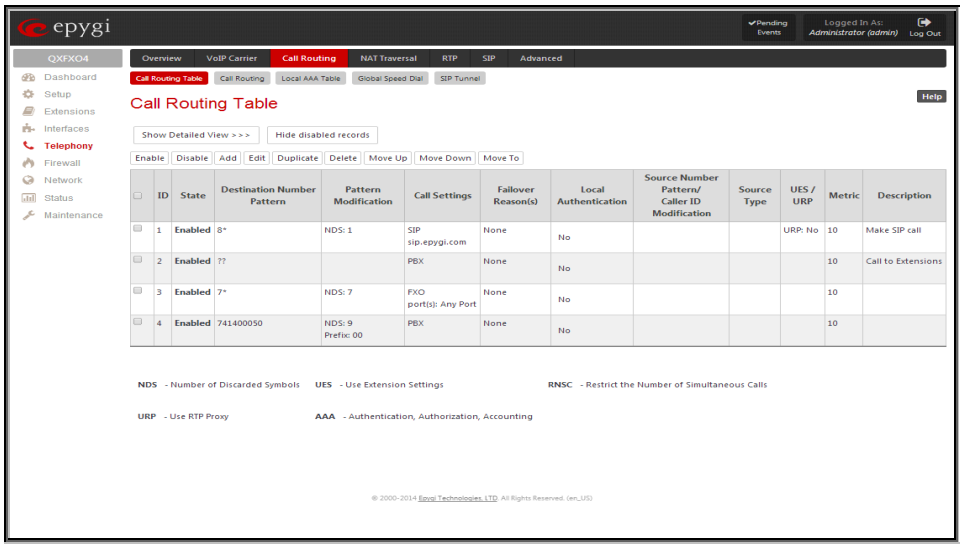


Fig.II- 66: Call Routing Table – brief preview

Defining patterns in the **Call Routing Table** avoids registering QX 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 alternating **Show Detailed View** and **Show Brief View** buttons are used to display entries in the Call Routing table in detailed and brief views correspondingly. The brief view displays the most important settings of the routing rules. The detailed view displays all settings of the routing rules as they are configured in the Call Routing Wizard.

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

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

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

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

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

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

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

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

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

Number of Discarded Symbols 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:

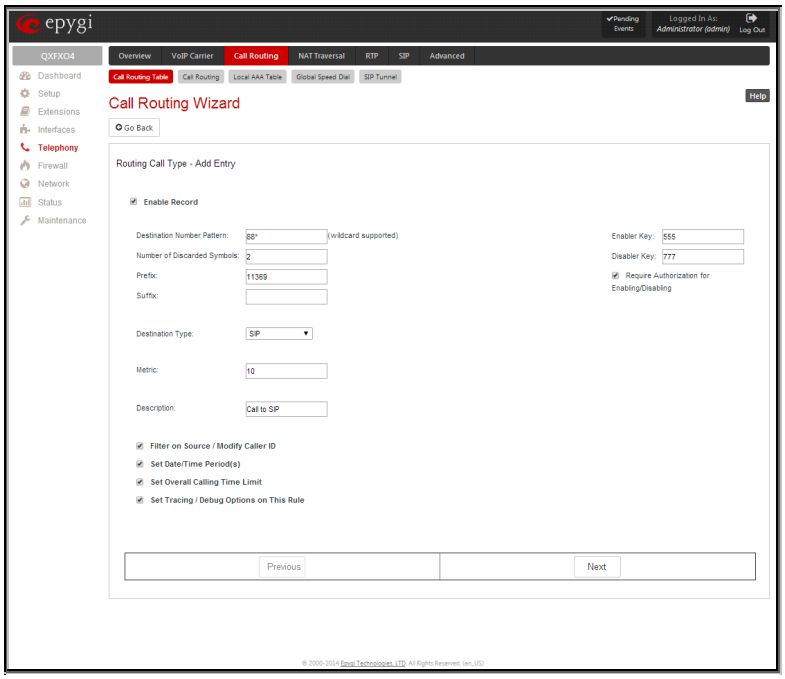


Fig.II- 67: Call Routing Wizard - page 1

- <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.

The syntax aaa,,,bbb in the **Prefix** field allows for two-stage dialing. The aaa and bbb are the numbers to call; bbb can also be a series of digits to inject; a comma indicates a delay of one second. The syntax can be applied to include more call destination numbers separated by time intervals. A two-stage dialing allows successive numbers to be dialed one after another with a delay in-between. For example, 11,,,11018 will call 11, wait until the call is established, wait for three seconds and then dial 11018. The capability of automatically dialing successive numbers allows the caller to bypass the IVR system on the call path and establish a direct call. The two-stage dialing is available for PBX and ISDN destination types.

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.

Destination Type gives you the option to select the destination type. The following destination types are available:

- PBX - local calls to QX gateway extensions
- SIP – calls through a SIP server
- SIP_Tunnel – calls through a SIP tunnels established (see SIP Tunnel Settings)
- IP-PSTN – calls through the IP-PSTN provider to the remote PSTN global telephone network
- FXO – calls to a PSTN global telephone network through FXO lines
- ISDN – calls to the PSTN global telephone network through ISDN trunk
- E1/T1 – calls to the PSTN global telephone network through E1/T1trunk

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 Source / 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, source caller information (**Source Number Pattern**, **Source Type, Source Host**, etc.) will be required later in the **Call Routing Wizard**. This option is enabled by default.

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 - Date/Time Rules - Add Entry** page will be displayed.

The **Set Overall Calling Time Limit** checkbox selection allows a total call duration for all calls to be configured over a specific time frame for each Call Routing entry. Once the total duration has been reached, the entry can be disabled, allowing calls to use the next available route.

If this checkbox is not selected in the **Call Routing Wizard** first page, the overall call duration will be unlimited. When this checkbox is selected, **Call Routing Wizard** - **Routing Overall Call Limitation Settings** page will be displayed.

Please Note: The **Overall Calling Time Limitation** checkbox is not allowed for **PBX** destination types routing rules.
Set Tracing / Debug Options on This Rule checkbox is used to switch events notification on the certain execution results of the corresponding routing rule. When this checkbox is enabled, the **Call Routing Wizard - Tracing/Debug Options** page will be displayed.

Require Authorization for Enabling/Disabling checkbox (not available for QXFXS24 gateway) 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 Call Codes Available in Auto Attendant) or remotely from Auto Attendant. 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 (not available for QXFXS24 gateway) 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 **Destination Type** selected on the previous page.

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

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

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

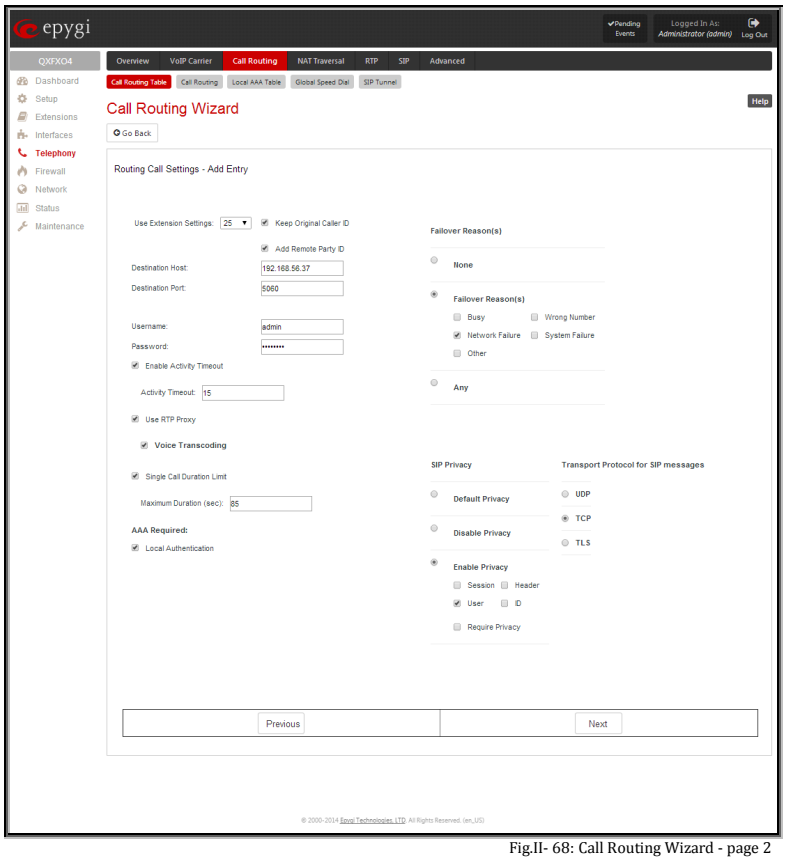


Fig.II- 68: Call Routing Wizard - page 2

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

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

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

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

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

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

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

The **Collect Call** checkbox is available only for **E1/T1** destination type and is used when it is simply preferable for the called phone to pay for the call. This service is applicabe only if the **Collect Call** checkbox is enabled on both calling and called party's IP PBXs.

The **Single Call Duration Limit** checkbox is available for SIP, IP-PSTN and PSTN destination types and is used to limit the duration of the call placed with the selected routing rule. If this checkbox is not selected, the call duration will be unlimited. This checkbox selection enables the **Maximum Duration** text field where the maximum duration of the call (in seconds) should be defined. Once the call duration reaches the value defined here, the call will be disconnected without prior notice.

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 when dialing the current pattern.
- **RADIUS Authentication and Authorization** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, callers will need to pass the authentication through RADIUS server (see above) when dialing the current pattern.

- The **RADIUS Accounting** checkbox is accessible when the RADIUS Client is enabled. With this checkbox selected, no authentication will take place, but CDRs (call detail reports) of the calls made through this routing record will be sent to the RADIUS server. This checkbox selection enables the **Client Code Identification** checkbox. If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.

- The **Client Code Identification** checkbox selection activates the code identification feature: a caller, after dialing the destination phone number, may optionally enter "*" and then an **Identity Code**. An **Identity Code** is an arbitrary digit string entered by the user to identify a specific call or call group. The **Identity Code** is sent with CDR to the RADIUS server and might be used by a billing program for grouping the calls having the same Identity Code.

Attention: It is highly recommended to secure PSTN and IP-PSTN routing rules by selecting **AAA Required** options. Unsecured routing rules may cause unexpected expenses.

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

- **None** - indicates that matching patterns should not be used regardless of the failover reason.

- **Failover Reason(s)** - indicates possible failure reasons. Failure reasons vary depending on the destination type selected on the previous page. If the call cannot be established due to selected Failure Reasons, the call routing table will be parsed for the next matching pattern and, if found, the call will be routed to the specified destination.

  Busy - available for PBX, SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when the dialed destination is busy.

  Wrong Number - available for PBX, SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when the dialed number is wrong.

  Network Failure - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when system overload, network failure or timeout expiration occurred.

  System Failure - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases indicated in **Network Failure** and **Other** fail reasons.

  Cannot Establish Connection – available for FXO, ISDN and E1/T1 destination types and indicates cases when connection cannot be established.

  Other - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when authorization, negotiation, not supported or request rejected or other unknown errors occur.

- **Any** stands for all failure reasons mentioned in the **Failover Reason(s)** group.

Please Note: If an extension does not have a profile specified here or the specified profile name is incorrect, the default Voice Mail Settings of the extension will be used.

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

The **SIP Privacy** manipulation radio buttons group is only available for the **SIP** and **SIP Tunnel** destination types 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, QX 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.

For **E1/T1** destination type, the **Port ID** drop down list contains available E1/T1 trunks. The available Timeslots (TS) should be selected on the next page.

For **FXO** destination types, a group of **Port ID** radio buttons allows you to select whether a specific or any available FXO line will be used to route the call. The **Any@Any** selection indicates that the call will be routed through the first available FXO line. The **Specific Ports** selection is used to select a group of routing settings for shared FXO lines.

Each Shared Gateway Ports radio buttons group is dedicated to one shared FXO device and is used to configure shared FXO lines usage when using the corresponding routing entry. None selection means no shared FXO lines will be used for the call routing of the specific routing rule. Any Port@ipaddress (where ipaddress is the IP address of the FXO gateway that shares its FXO lines) selection means the call will be routed through the first available shared FXO line. FXO@ipaddress port checkboxes are used to select those which shared FXO ports will be used for the corresponding rule routing. In case if multiple shared FXO ports are selected here, the first available port will be used.

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

For **ISDN** destination type, the **Port ID** drop down list contains the following options:

- **Any Port (User)@Any** - any shared ISDN trunks running in User mode.

- **Any Port (Network)@Any** - any shared ISDN trunks running in Network mode.
- **ISDN Trunk@ipaddress** - shared ISDN trunks on the selected gateway (where ipaddress is the IP address of the ISDN gateway that shares its ISDN trunks)
- **Any Port (User)@ipaddress** - any shared ISDN trunks from the selected gateway running in User mode.
- **Any Port (Network)@ipaddress** - any shared ISDN trunks from the selected gateway running in Network mode.

The **Call Routing Wizard** - Page 3 appears if the **Filter on Source / Modify Caller ID** checkbox had been enabled on Page 1 of the **Call Routing Wizard.** It will require information about the source caller.

The **Source Number Pattern** field requires the caller address for which the current route will be applied. The complete list of characters and wildcards is allowed in this text field (see chapter Allowed Characters and Wildcards).

The **Source Type** drop down list gives you the option to select the source type (PBX, SIP, ISDN, FXO, E1/T1, SIP Tunnel, Any) used by the source caller to reach the QX.

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

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

The **Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Source Number 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 Allowed Characters and Wildcards).
The two-stage dialing is available for PBX, ISDN, and E1/T1 destination types.
The **Discard Non-Numeric Symbols** checkbox is used to discard any non-numeric symbols from the **Source Number Pattern**.

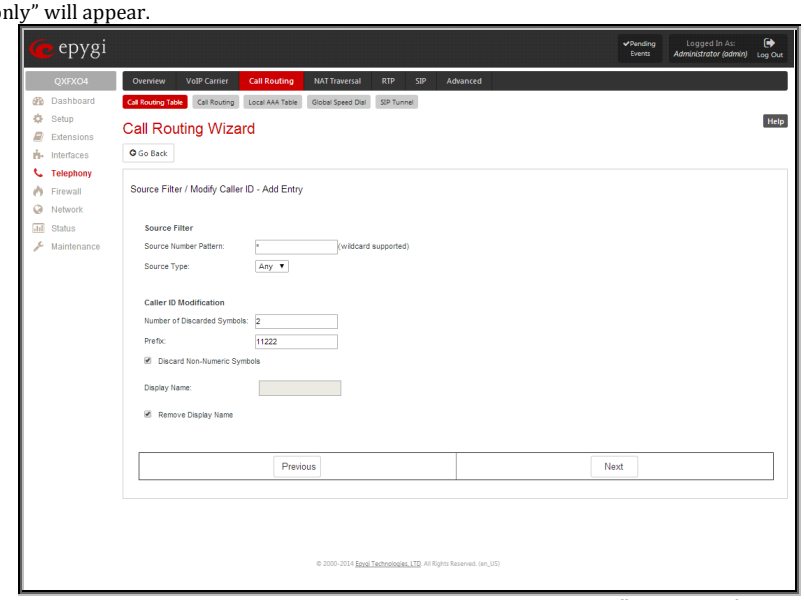


Fig.II- 69: Call Routing Wizard - page 3

The **Display Name** text field allows you to replace an original caller's ID with the custom display name for the corresponding routing rule. This field is optional and when it is left empty, an original caller ID will be displayed on the called destination's phone, otherwise the name inserted here will appear on the phone. This field is not available for PBX-Voicemail destination type routing rules.
The **Remove Display Name** checkbox is used to remove caller IDs from calls made with this routing rule. This checkbox is not available for PBX-Voicemail destination type routing rules.

The **Next** button will open the **Call Routing Wizard** - Page 4 where different information about source caller will be required depending on the selected **Source Type**. For the **SIP** source type, the **Source 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. In case of FXO, ISDN or E1/T1 source types selected, Source Port ID drop down list will require to select the FXO line number, ISDN or E1/T1 Trunk correspondingly, and on the next step, a list of timeslot(s) used to receive calls from the defined caller.
The **Call Routing Wizard – Date/Time Rules - Add Entry** page 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 QX gateway Date and Time Settings.

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

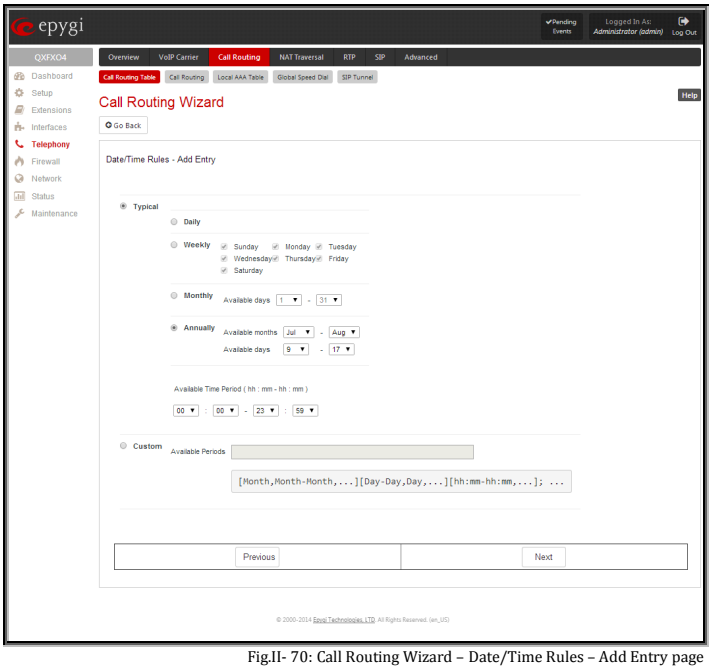


Fig.II- 70: Call Routing Wizard – Date/Time Rules – Add Entry page

The **Call Routing Wizard – Routing Overall Call Limitation Settings - Edit Entry** page appears if the **Set Calling Time Limit** checkbox previously had been enabled on Page 1 and allows to define the available duration of the calls with the selected routing rule as well as to specify the **Expiration/Renewal Date** for the available calls duration.
The **Routing Overall Call Limitation Settings - Edit Entry** page consists of the following components:

- The **Available Calls Duration** text field requires the maximum available duration of the calls (in minutes) placed with the selected routing rule. Once the **Available Calls Duration** reaches the value defined here, the current call will be disconnected without prior notice and no new call will be possible until this field is updated.
- The **Expiration/Renewal Date** settings are used to configure the **Expiration Date** and **Renewal Amount** of the **Available Calls Duration**. **Expiration/Renewal Date** field provides selection between **Periodic** and **Specific Date**.

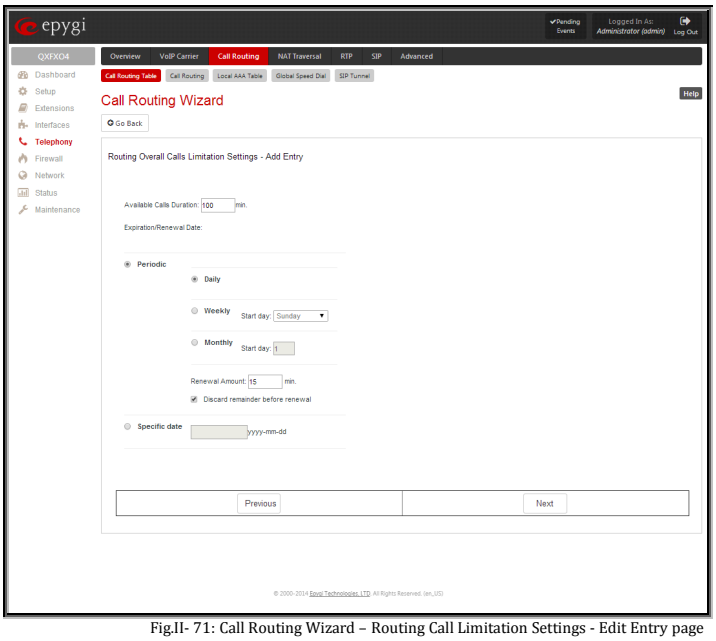


Fig.II- 71: Call Routing Wizard – Routing Call Limitation Settings - Edit Entry page

- The **Periodic** selection is used to define the expiration date of the allocated **Available Calls Duration** for the selected routing rule and has the following options:
  - **Daily**
  - **Weekly**- the preferred week start day should be selected for this option.
  - **Monthly** - the calendar day should be selected for this option.
- The **Renewal Amount** text field requires the renewal amount (in minutes) to be added to the **Available Calls Duration** when the expiration date of the **Available Calls Duration** is reached.
- The **Discard remainder before renewal** option selection allows to discard the remainder of **Available Calls Duration** before renewal and set the **Renewal Amount** as an available calls duration.
- The **Specific Date** selection provides a possibility to manually define the expiration date allocated for the **Available Calls Duration** for the selected routing rule. When the **Specific Date** expires, the selected routing rule becomes unavailable automatically and no new call will be possible until this field is updated.

The **Call Routing Wizard – Tracing/Debug Options** page appears if the **Set Tracing / Debug Options on This Rule** checkbox was previously enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the tracing/debug options.

This page offers result options of the corresponding routing rule execution when the notification event will be printed in the System Events page.

- **In Case of Successful Call** – a notification event is printed when the successful call was established with the routing rule.
- **In Case of Failover** – a notification event is printed when the call ends up on one of the failover reasons selected on the Page 2 of the **Local Call Routing Wizard.**
- **In Case if Call Failed to Establish** – a notification event is printed when the call executed with the routing rule failed.

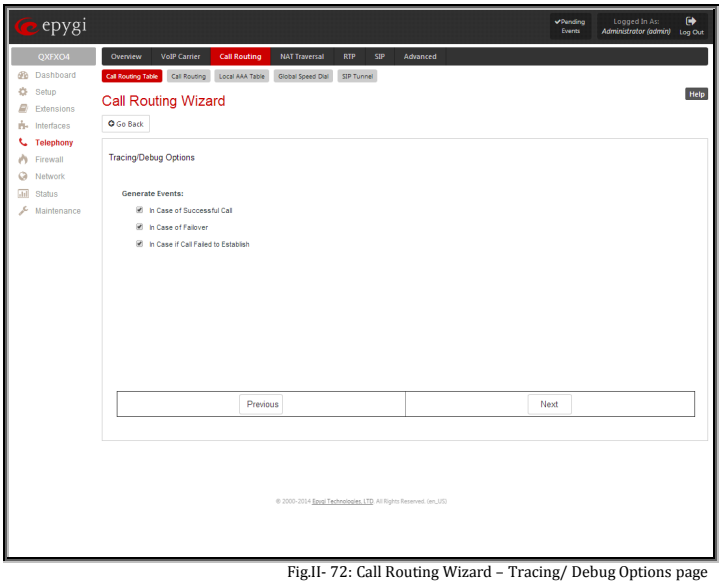


Fig.II- 72: Call Routing Wizard – Tracing/ Debug Options page

Call Routing

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

- When the **Route all incoming SIP calls to Call Routing** checkbox is disabled, for all incoming SIP calls QX will first search the incoming SIP address in the Extensions Management table. If found, the incoming SIP call will ring on the corresponding extension. If not found, QX will look for a matching routing rule in Call Routing Table.
  When the **Route all incoming SIP calls to Call Routing** checkbox is enabled, for all incoming SIP calls QX will directly look for a matching routing rule in Call Routing Table and will ignore the possible matches in the Extensions Management table.

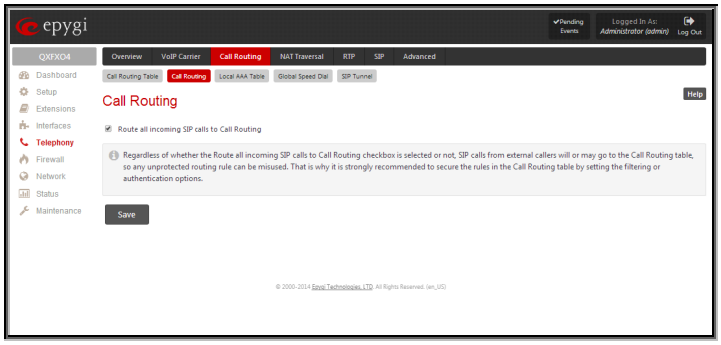


Fig.II- 73: Call Routing page

Attention: Regardless of whether the **Route all incoming SIP calls to Call Routing** checkbox is selected or not, SIP calls from external callers will or may go to the Call Routing table, so any unprotected routing rule can be misused. That is why it is strongly recommended to secure the rules in the Call Routing table by setting the filtering or authentication options.

Local AAA Table

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.

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the type of authorization and the following other parameters:

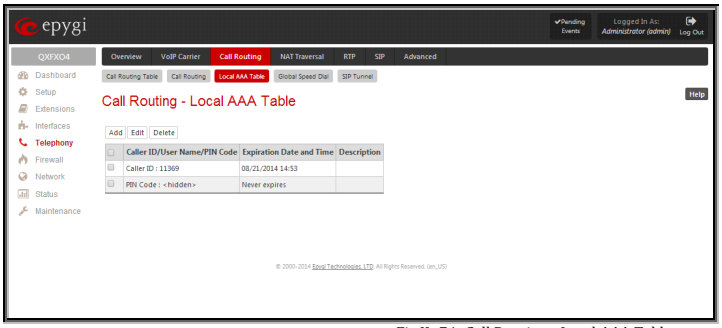


Fig.II- 74: Call Routing - Local AAA Table page

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller's phone number (which is considered to be automatically detected). The **Phone Number/SIP User Name** text field requires the caller's phone number or the SIP username. Only numeric and wildcard characters (see chapter Entering SIP Addresses Correctly) are allowed for this field. '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number. The {11, 15, 23, 38, 45} pattern means that the dialed number may be 11, 15, 23, 38 or 45 to match the pattern.

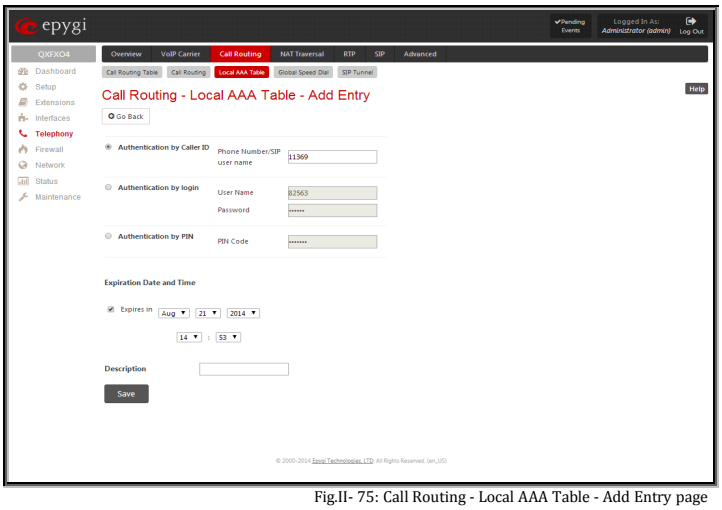


Fig.II- 75: Call Routing - Local AAA Table - Add Entry page

- **Authentication by Login –** this selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication username. Only numeric values are allowed for this field, otherwise the error message "Incorrect Username - digits allowed only" will appear. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the error message "Incorrect Password - digits allowed only" will appear.
- **Authentication by PIN**- this selection is used to set the authentication based on the PIN inserted by the user upon login. Only digit values are allowed for this field, otherwise the appropriate error message will be displayed.

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.

Edit opens the **Edit Entry** page to modify the local AAA entry.

Global Speed Dial Directory

The **Global Speed Dial Directory** page is used to define multiple speed dial rules, write and save them in a file and then upload all of them at once.

To compose the configuration file, any text editor can be used which may produce files compatible to the CSV format: the speed dial code and destination should be separated by commas. There should be a line break after each code defined.

The **View/Download Speed Dial Directory** and **Remove Speed Dial Directory** links appear only if a global speed dial configuration file is uploaded previously.

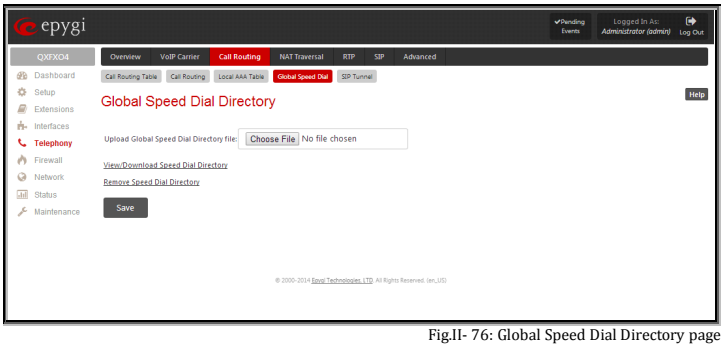


Fig.II- 76: Global Speed Dial Directory page

The **View/Download Speed Dial Directory** link is used to download the configuration file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Speed Dial Directory** link is used to restore the default configuration.

The speed dial configuration file downloaded from the QX is in the CSV format.

To use the global speed dialing rules, user should simply dial the speed dial code assigned to that speed dialing rule. The call will be parsed through the rules of Call Routing Table.

To create a new Call Routing rule

1. Click on the **Call Routing Table** tab on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing Table** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Destination 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 Source / Modify Caller ID** checkbox, if the route functionality should be limited. This is dependent on the source caller information.
9. Enable the **Set Date/Time Period(s)** checkbox if a route should be functional within certain time/date intervals.

10. Enable the **Set Overall Calling Time Limit** checkbox if the overall duration of the calls placed with the selected routing rule should be defined.
11. Enable the **Set Tracing / Debug Options on This Rule** checkbox, if the tracing/debug options should be defined.
12. Press **Next**.
13. Select the user or attendant extension from the **Use Extension Settings** drop down list that the call will be placed on.
14. 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** checkbox if needed.
15. Choose the Authentication and Accounting method from the **AAA Required** drop down list.
16. Choose a **Fail Reason** from the corresponding drop down list.
17. Configure **Transport Protocol for SIP messages** and **SIP Privacy** parameters as needed.
18. Press the **Next** button.
19. If the **Filter on Source / Modify Caller ID** checkbox has been previously enabled and the destination type is different from the FXO, fill in the **Source Number Pattern** into the corresponding text field. Choose the needed value from the **Source Type** drop down list, as well as the **Number of Discarded Symbols** and **Prefix** values.
20. Press the **Next** button.
21. If **IP** has been selected on the previous step in the **Source Type** drop down list, then **Source Host** should be inserted in the current page. If **FXO**, **ISDN** or **E1/T1** has been selected in the **Source Type** drop down list, then the ISDN/E1T1 trunk or the FXO line number should be selected here.
22. 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.
23. If the **Set Overall Calling Time Limit** checkbox has been selected on the first page, pressing **Next** will open the **Routing Overall Calls Limitation Settings** page where the total call duration for all calls can be configured over a specific time frame for each Call Routing Entry.
24. If the **Set Tracing / Debug Options on This Rule** checkbox has been selected on the first page, pressing **Next** will open the **Tracing/ Debug Options** page where the tracing/debug options should be defined.
25. 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** tab 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**, **Username** and **Password** or the **Authentication by PIN** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

Allowed Characters and Wildcards

The following is the set of characters and wildcards allowed in the **Pattern** and **Source Number Pattern** text fields of the Call Routing Wizard:

Characters:

0...9 A...Z

a...z + = $; / ~ _ - . & ( ) ' ! * ? {} , [ ]

Please Note: The symbols * and ? should be prefixed with a slash (\) if they are used as ordinary characters; otherwise the system will interpret them as wildcards.

Please Note: The symbols !, {, }, [,], - and , are used to define a range of characters and cannot be used as ordinary characters.

Wildcards:

* Any number of any characters

? Any single character

{ } A character or a string from the specified set of characters and strings.

The following control symbols are used to specify a set:

- Use a comma (,) to separate the elements of a set.

  Please Note: No spaces are allowed within braces.

  Example:

  The pattern is **9{1,3,11,a}**.

  Numbers matching the pattern are **91, 93 , 911, 9a.**

- Use a minus sign (-) to specify a range of characters. Each successive element of the range is obtained by increasing the previous element (the element code) by one.

  Example:

  The pattern is **2{11-15,a-d}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2145, 2155, 2a5, 2b5, 2c5, 2d5**.

- Use an exclamation point to exclude a character or a string from a set.

  Example:

  The pattern is **2{11-15,a-d,!14,!c}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2155, 2a5, 2b5, 2d5**.

  Please Note: You can use the wildcard ? within the braces, but not *. Thus, **{12-104,15?,36?}** is a valid pattern, whereas **{15*,36*}** is not.

  Please Note: The symbol ! cannot be used to exclude a range of symbols. For example **2{15-60,!23-32}** or **2{15-60,!23-!32}** are not valid patterns. To valid pattern will be to **2{15-22,33-60}**.

[] The same as above with the exception that character ranges can include single-digit/character elements only.

Example:

The pattern is **2[1-5, a-c]5**.

Numbers matching the pattern are **215, 225, 235, 245, 255, 2a5, 2b5, 2c5**.

\ Precedes a control symbol (*, ?, -, ! and ,) to indicate that it is used as an ordinary character, not a wildcard.

Example:

The pattern is **1*[1-3]**

Numbers matching the pattern are: **1*1, 1*2, 1*3**

Please Note: Patterns cannot be prefixed with the * symbol. The system considers the patterns starting with * as feature codes and does not parse them through the Call Routing table.

@ Used to indicate the full SIP address (example: 20233@sip.epygi.com). This pattern is mainly used to call back users registered on the SIP server different from the one where the called party is registered.

Please Note: Patterns containing @ symbol will not be parsed among those that do not have @ symbol in the Call Routing Table. When calling from local extensions (the calling number for local extension is sipnumber@ip_address_of_QX, e.g. 20233@192.168.35.25), only the sipnumber part of the pattern will be parsed among other entries with @ symbol in the Call Routing Table.

Best Matching Algorithm

All calls through and within a QX are made according to call routing patterns that specify a destination based on a dialed number. When a user dials a number to make a call, the QX matches the dialed number against the existing patterns that are specified in the Call Routing table. If the dialed number matches only to a single pattern, this pattern will be used to set up a call. If several patterns have been found to match the number, the QX uses the Best Matching Algorithm to prioritize the matching patterns. Once the patterns are prioritized, the pattern with the highest priority will be used as a preferred route for call setup. The successive patterns will be used only if the destination specified by a higher priority pattern is unreachable.

To prioritize the matching patterns, the following criteria are sequentially applied to matching patterns. The criteria are ordered by their priorities: Each consecutive criterion is calculated only for the patterns that take the same value for the preceding criteria: that is Criterion 3 is calculated only for patterns that take the same value for Criterion 1 and Criterion 2.

Criterion 1	**The presence of asterisks ("*") in a pattern** The patterns without "*" have a higher priority.
Criterion 2	**The total number of matching digits/symbols inside and outside the braces/brackets** The more matching digits a pattern contains, the higher its priority.
Criterion 3	**The number of matching digits/symbols outside the braces/brackets** The more matching digits outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 2.
Criterion 4	**The total number of question marks ('?') inside and outside the braces/brackets** The more question marks a pattern contains, the higher its priority.
Criterion 5	**The number of question marks ("?") outside braces/brackets** The more question marks outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 4.
Criterion 6	**The number of square brackets ("[]")** The more brackets a pattern contains, the higher its priority.
Criterion 7	**The number of braces ("{}")** The more braces a pattern contains, the higher its priority.

Criterion 8	**The number of asterisks ("*")** The fewer asterisks a pattern contains, the higher its priority.
Criterion 9	**The value of the metric** The lower the metric of a pattern is, the higher its priority.
Criterion 10	**The position in the routing table** The higher the position of a pattern in the routing table is, the higher its priority.

Example: The user has dialed 1231 and the following matching patterns have been found.

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

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

Criterion 1

The list split into two subgroups
?2?1
123?
[1-3]???
{100-150, asd, *\?}1
1[1-3]3[0-8]
1231
1
123*
{11-15}3*
[1-3]*
12*31
*2*1
*

Step 2: The two groups of patterns are arranged separately from each other by the total number of matching digits inside and outside the braces/brackets in the descending order (Criterion 2). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 2

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

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

Step 3: The new sub-lists are arranged separately from each other by the number of matching digits outside the braces/brackets (Criterion 3). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 3

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

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

The Best Matching Algorithm will stop after executing step 3 as no new sub-lists are formed. The resultant list of prioritized patterns will be the following:

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

Entering SIP Addresses Correctly

Calls over IP are implemented based on Session Initiating Protocol (SIP) on the QX. 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 the Caller ID Based Services table that are used by **Outgoing Call Blocking** service. To use "*" and "?" alone (as non wildcard characters), use "*" and "\?" correspondingly.

SIP Tunnel Settings

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

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

Optionally, a SIP tunnel can be mutually established on two QXs allowing to route SIP calls back and forth. A QX can be at the same time configured both as a slave and as a master to the same remote device, i.e. the slave QX can act as a master for the master device it is registered on. For example, the QX can act as a slave for the QX -2. In its turn, the QX -2 can act as a slave for the QX -1. With this configuration and the corresponding routing rules added in the Call Routing Table on both devices, the SIP calls will be routed from QX-1 to QX -2 and vice versa.

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

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

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

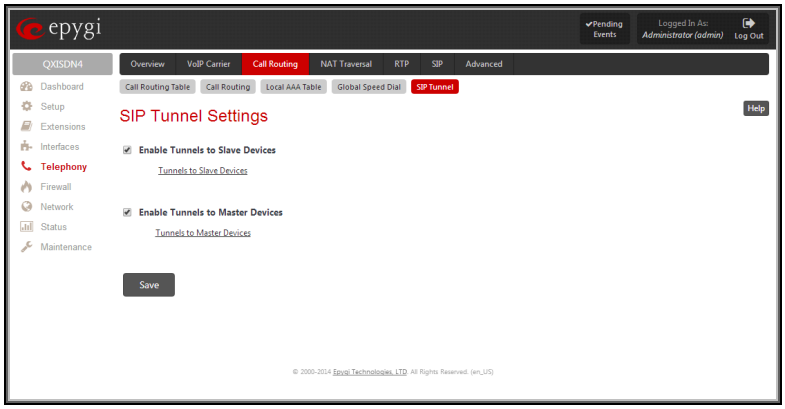


Fig.II- 77: SIP Tunnel Settings page

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

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

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

Fig.II- 78: SIP Tunnel Settings – Tunnels to Slave Devices page

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

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

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

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

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

Fig.II- 79: SIP Tunnel Settings – Tunnels to Slave Devices – Add Entry page

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

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

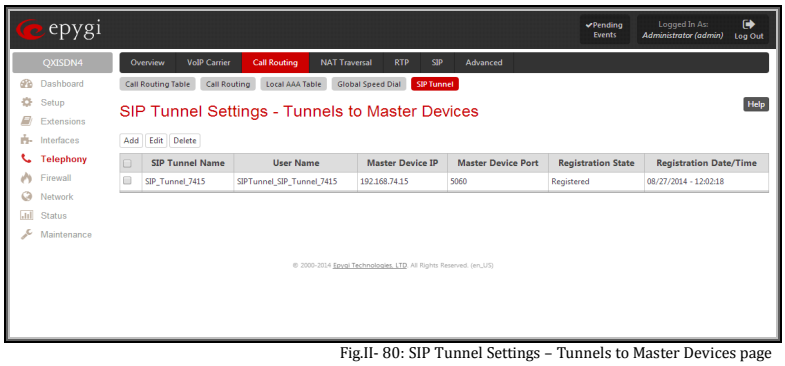


Fig.II- 80: SIP Tunnel Settings – Tunnels to Master Devices page

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

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

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

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

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

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

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

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

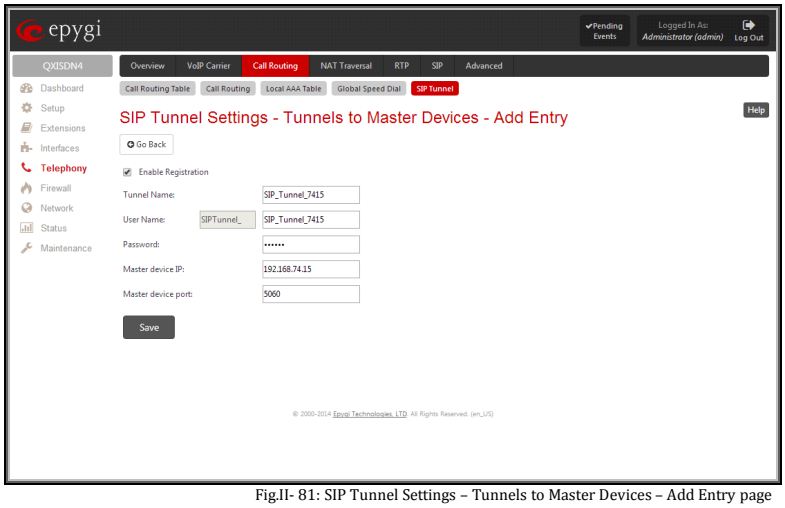


Fig.II- 81: SIP Tunnel Settings – Tunnels to Master Devices – Add Entry page

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

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

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

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

NAT Traversal Settings

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

General Settings

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 QX will be routed through the NAT router).

- **Automatic** – with this selection, system will analyze the QX'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 QX's WAN IP address is outside the specified IP range, no SIP traffic will be routed through NAT router.
- **Force** – with this selection, all the SIP traffic will be routed through the NAT router.
- **Disable** – with this selection, no SIP traffic will be routed through the NAT router.

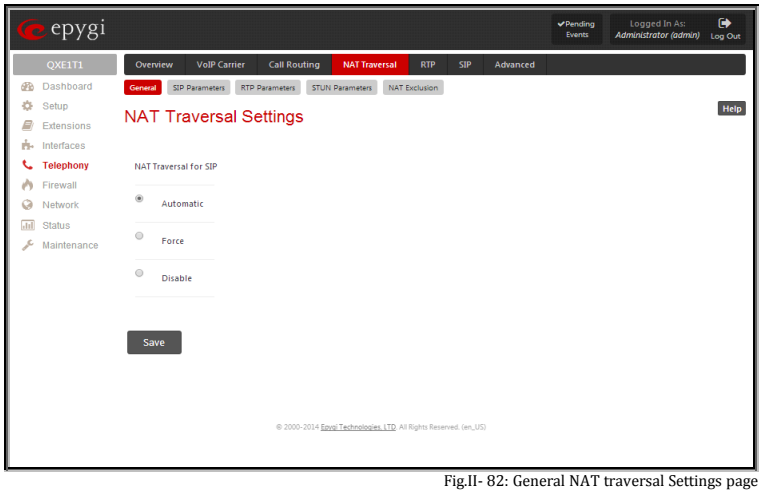


Fig.II- 82: General NAT traversal Settings page

SIP Parameters

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.

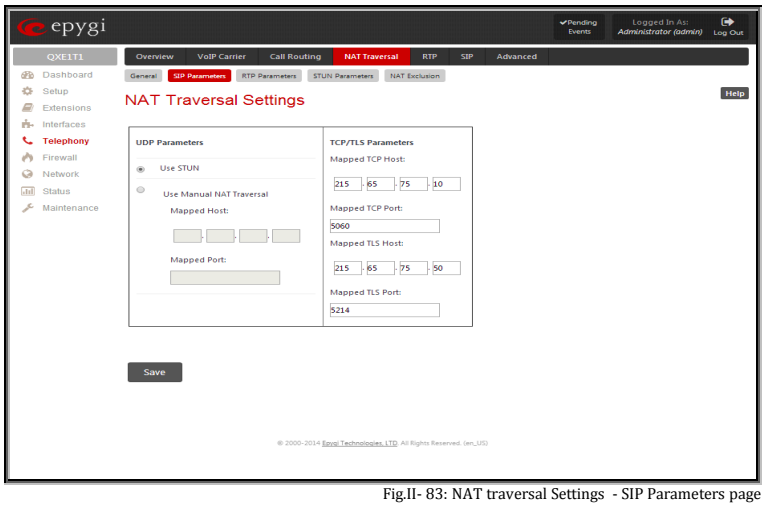


Fig.II- 83: NAT traversal Settings - SIP Parameters page

TCP/TLS Parameters:

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

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

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

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

RTP Parameters

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

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

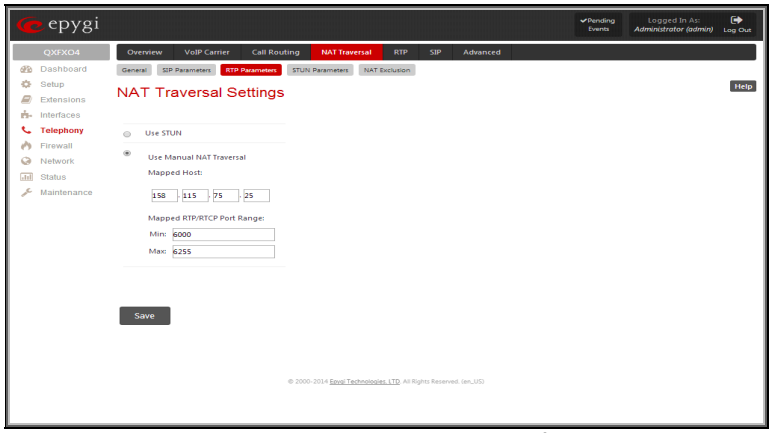


Fig.II- 84: NAT traversal Settings - RTP Parameters page

STUN Parameters

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 QX. 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.

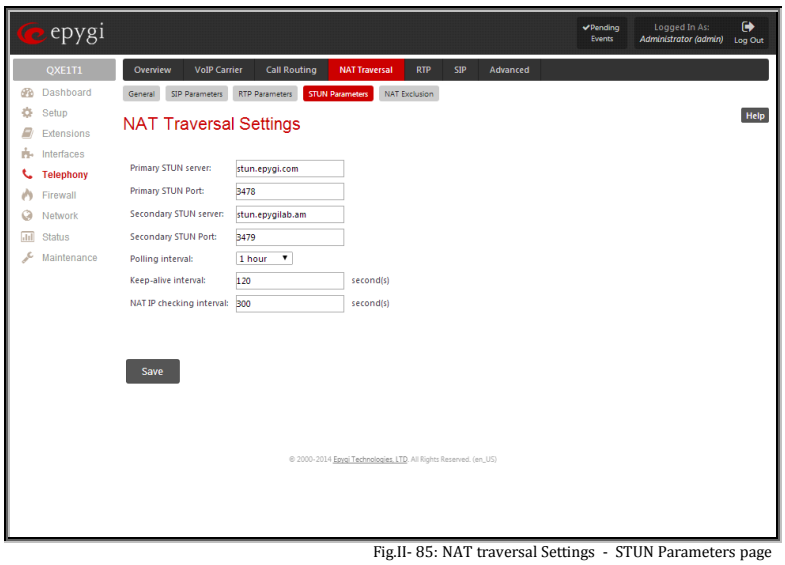


Fig.II- 85: NAT traversal Settings - STUN Parameters page

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 Exclusion

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. For example, if a QX 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.

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

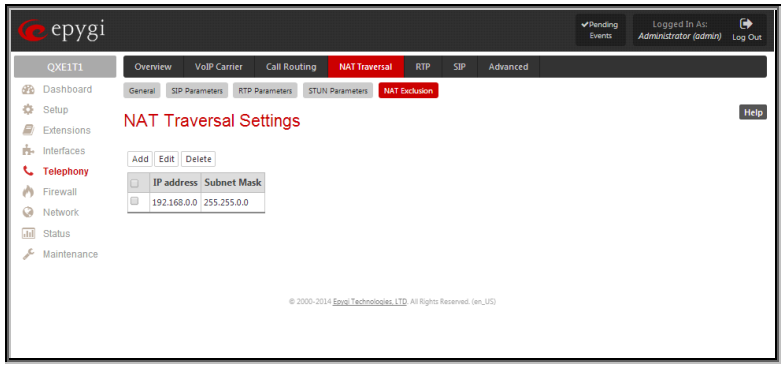


Fig.II- 86: NAT traversal Settings - NAT Exclusion Table page

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

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

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

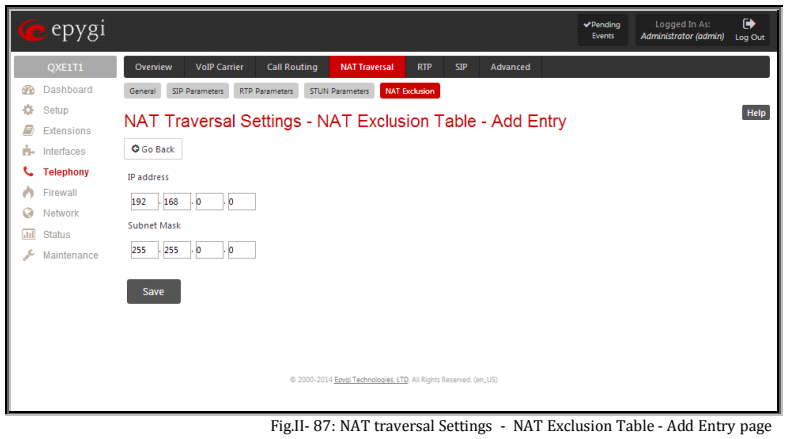


Fig.II- 87: NAT traversal Settings - NAT Exclusion Table - Add Entry page

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**.
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**.

RTP Settings

The **RTP Settings** page allows the administrator to configure the codec's packet size and silence suppression for each voice codec. All parameters listed on this page may be modified and submitted.

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

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

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

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

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

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

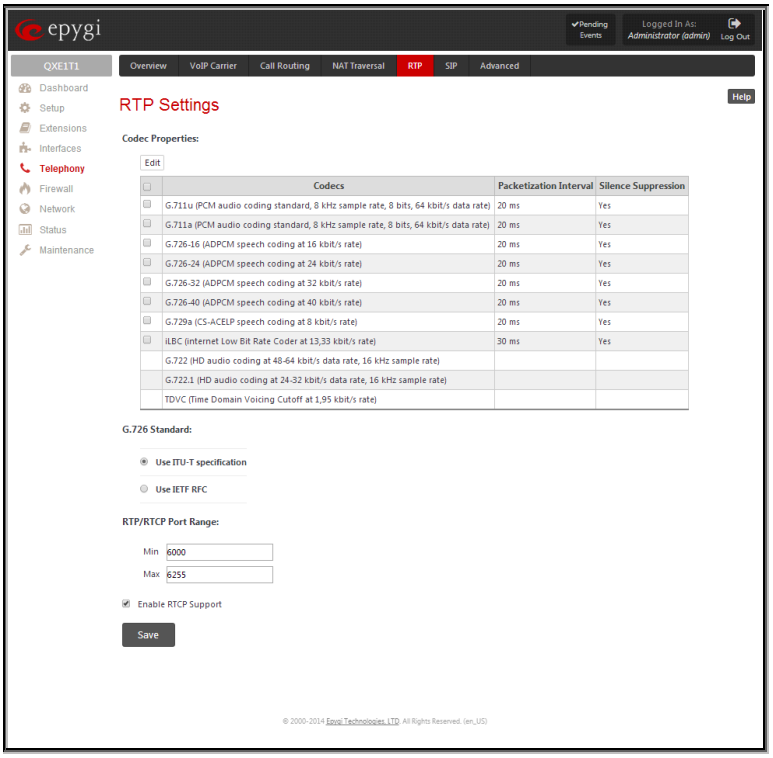


Fig.II- 88: RTP Settings page

RTP/RTCP Port Range:

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

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

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

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

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

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

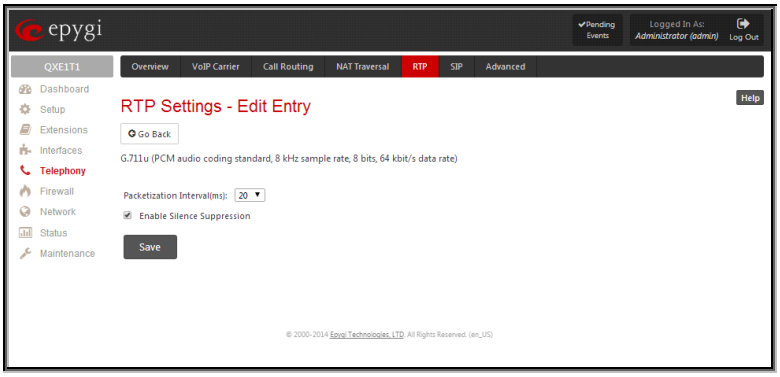


Fig.II- 89: RTP Settings - Edit Entry

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 **Go Back**.

SIP Settings

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

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

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

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

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

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

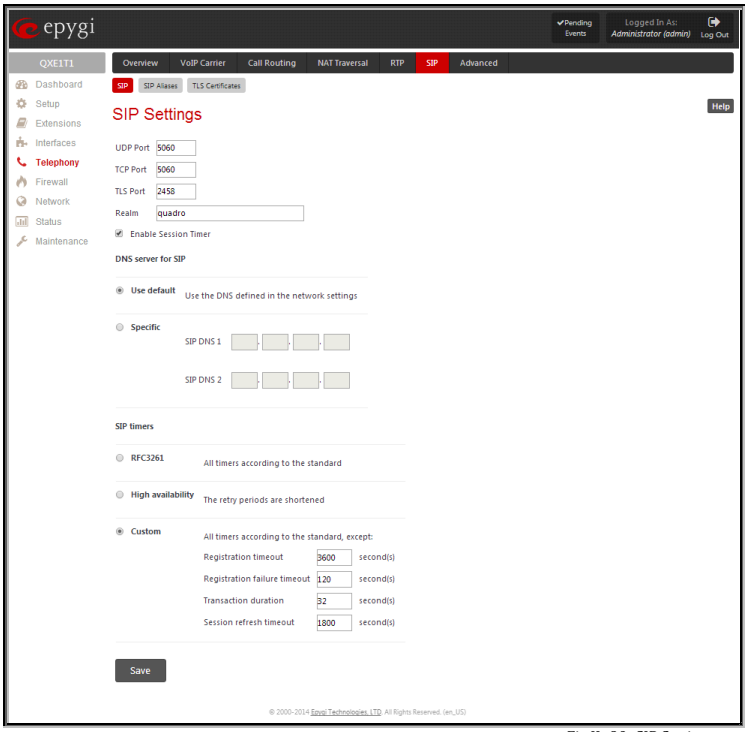


Fig.II- 90: SIP Settings page

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

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

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

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

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

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

SIP Aliases

This page is used to create a list of QX's hostnames register on remote DNS servers. This list will be used to identify SIP packets received from remote servers where QX is registered with different names.

The **Host aliases for SIP page** consists of a table where QX's aliases are listed. Add opens the **Add Entry** page where a new alias name for QX should be defined.

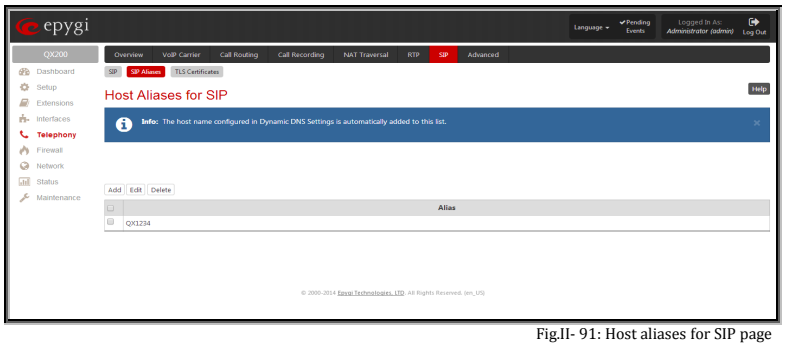


Fig.II- 91: Host aliases for SIP page

TLS Certificates

The **Generate and Install New CA Root Certificate** page is used to define, generate and install a new CA root certificate for SIP TLS traffic. All fields in this page require root certificate specific information.

The **General Certificate and Install** button is used to generate a new CA root certificate based on the defined data and to install it on the QX. QX will get rebooted automatically once the new certificate is installed. You may download the actual copy of the certificate from SIP Settings page.

To ensure a secure TLS connection with the QX's defined CA root certificate, both sides should have the same certificate installed. If the end user is an IP phone, you may activate the TLS certificate update mechanism from it to obtain the latest certificate generated by the QX. If the end user is a server or other device, you may download the certificate from the QX and apply it manually on the remote side.

The **Download Current CA Root Certificate** link is used to download the actual CA root certificate in a .crt format.

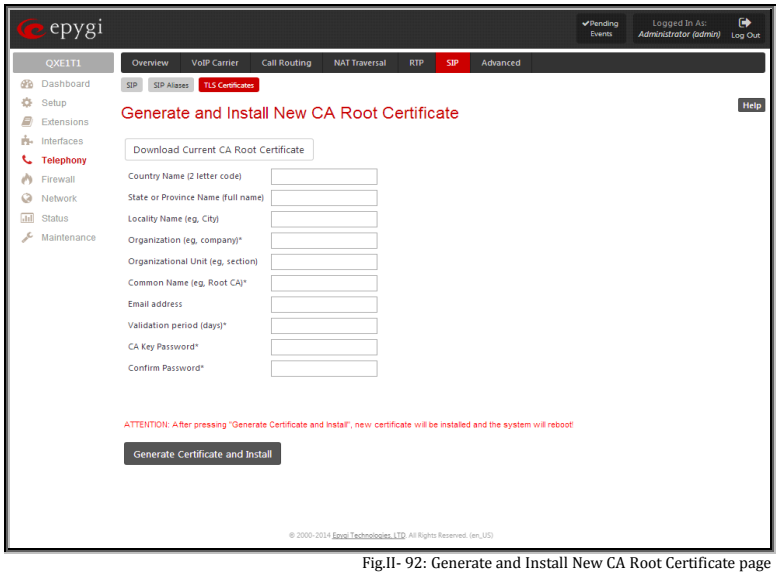


Fig.II- 92: Generate and Install New CA Root Certificate page

Advanced Settings

RTP Streaming Channels

The **RTP Streaming Channels** page (available only for QXFXO4, QXISDN4 and QXE1T1 gateways) is used to configure channels where the broadcast RTP streams are transmitted. These channels may be then configured to be used as hold music (see Hold Music Settings) or any other type of music played to the caller.

The **RTP Streaming Channels** page consists of a table where RTP channels are listed.

Add opens the **Add Entry** page where a new RTP channel can be added.

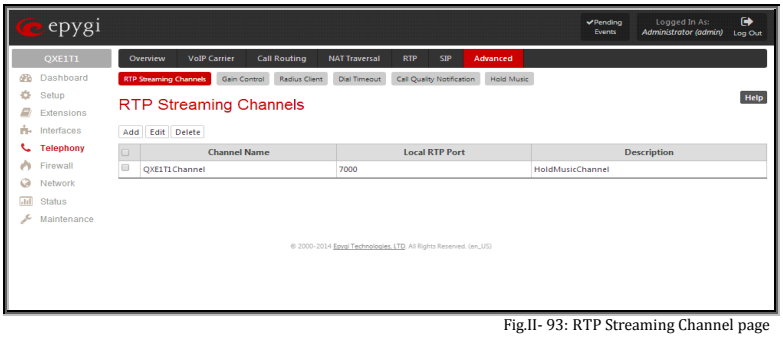


Fig.II- 93: RTP Streaming Channel page

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

The **RTP Channel Name** text field requires the name or the number of the RTP channel.

The **Port Number** text field requires the broadcasting RTP port number.

The **Description** text field requires optional information related to the RTP streaming channel.

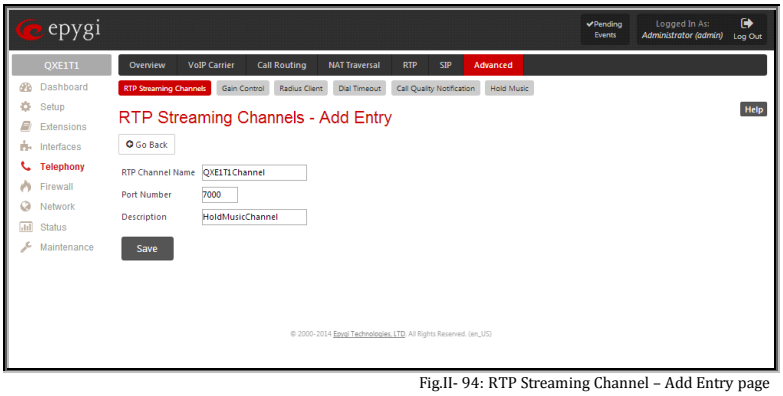


Fig.II- 94: RTP Streaming Channel – Add Entry page

Gain Control

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

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.

For **FXS** lines:

Transmit Gain defines the phone speaker volume on the call.

Receive Gain defines the volume of the phone microphone on the call.

For **FXO** lines:

Transmit Gain defines the level of voice transmitted from QX to the FXO network.

Receive Gain defines the volume of voice received by QX from the FXO network.

For **ISDN** trunks:

Transmit Gain defines the level of voice transmitted from QX to the ISDN network.

Receive Gain defines the volume of voice received by QX from the ISDN network.

For **E1/T1** trunks:

Transmit Gain defines the level of voice transmitted from QX to the E1/T1 network.

Receive Gain defines the volume of voice received by QX from the E1/T1 network.

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

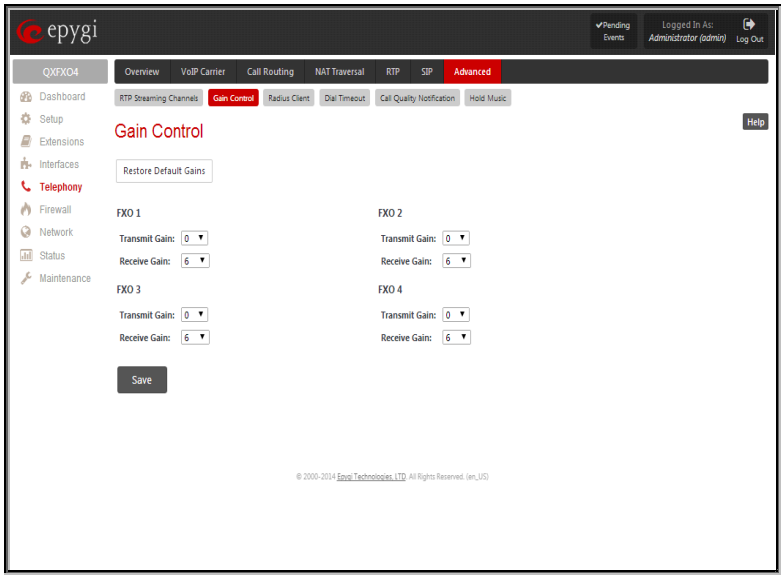


Fig.II- 95: Gain Control page

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 QX to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the QX, 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 QX Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the QX.

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 QX, 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, QX'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 QX.

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 QX is to send the authentication requests.

The **Accounting Port** text field requires the port number on the RADIUS server where QX is to send the accounting messages.

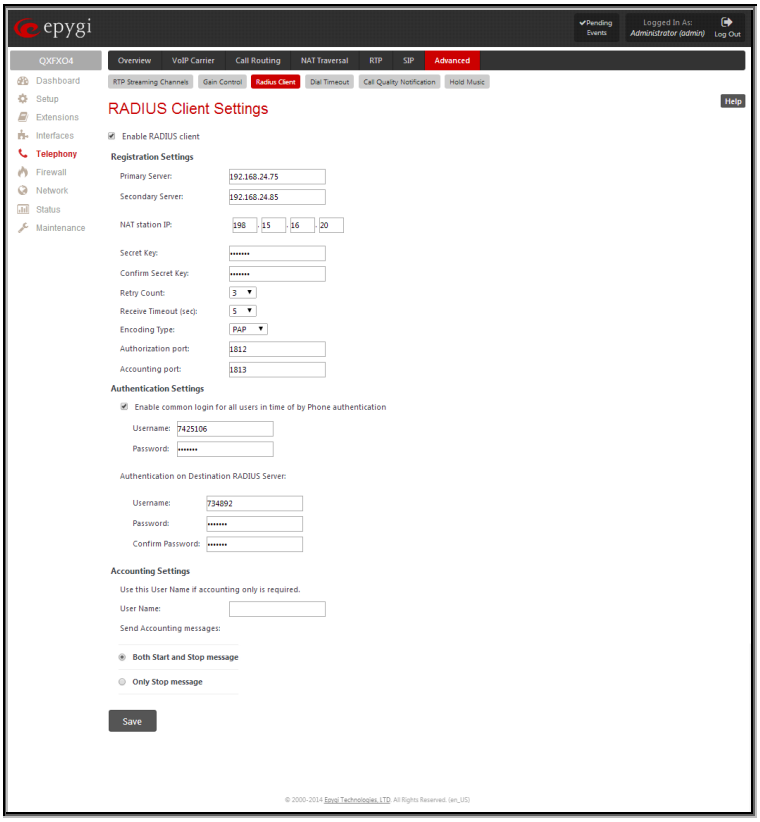


Fig.II- 96: Radius Client Settings page

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 QX. 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 QX. 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.

Dial Timeout

The **Dial Timeout Settings** page is used to adjust the dialing timeout setting.

The **Routing Dial Timeout** setting specifies a period of time after the last dialed digit that the system identifies as a completion of dialing. If the user does not press any key within the specified timeout, the system assumes that the dialing is complete and starts calling the dialed number. Only predefined values included in the drop-down list can be used for this setting.

The **Routing Dial Timeout** setting will also be applied to all the supported IP phones that are auto-configured with the QX and provide the possibility of changing this setting through the auto-configuration file. The modified value of the setting will take effect after rebooting the IP phones.

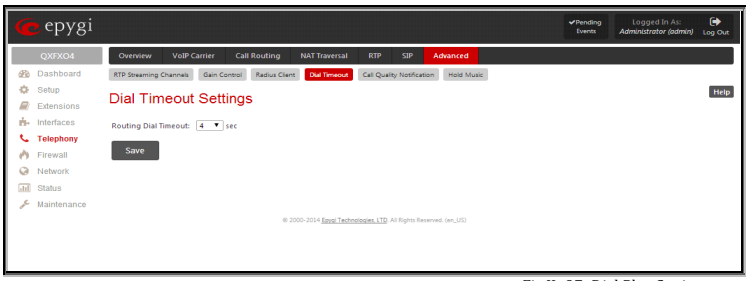


Fig.II- 97: Dial Plan Settings page

Call Quality Notification

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

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

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

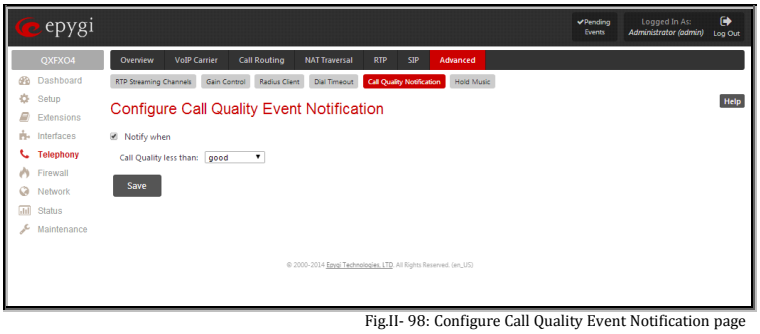


Fig.II- 98: Configure Call Quality Event Notification page

Hold Music Settings

The **System Hold Music Settings** page (not available for QXFXS24 gateways) 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 QX 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.

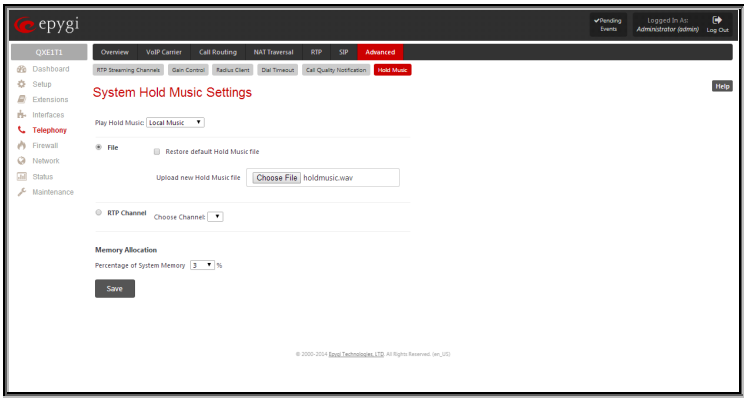


Fig.II- 99: Hold Music Settings page

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 **Choose File** button is used to browse for the hold music file.

The music file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) 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 QX and will then announce "You do not have enough space".

The **Download Hold Music File** link appears only if a file has been uploaded recently. It downloads the audio file to the PC and opens a window where the saving location can be specified.

RTP Channel selection is used to define the channel for the broadcast streaming. The RTP channels are created by the system administrator. Therefore if you are experiencing problems with using the RTP channels as hold music, or no RTP channels are available to select on this page, turn to your system administrator for clarification.

Firewall Menu

The **Firewall** menu allows you to configure the following settings:

- **Firewall**
  - Firewall and NAT
  - Advanced Firewall Settings
  - IDS Log
- **Filtering Rules**
  - View All Filtering Rules
  - Incoming Traffic/Port Forwarding
  - Outgoing Traffic
  - Management Access
  - SIP Access
  - Blocked IPs
  - Allowed IPs
- **Custom Services**
  - Service Pool Configuration
- **IP Groups**
  - IP Pool Configuration
- **SIP IDS Settings**

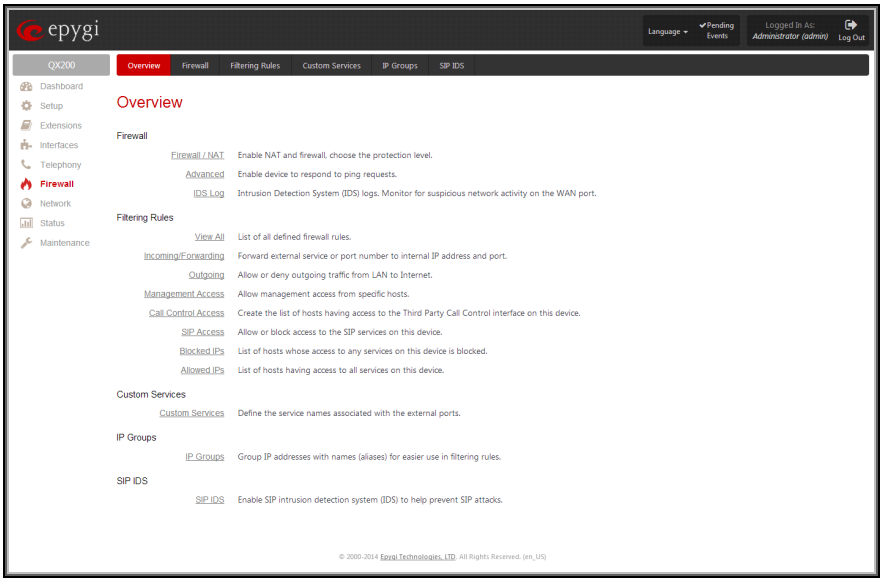


Fig.II- 100: Firewall Menu page

Firewall

The **Firewall Configuration** page allows setting up a firewall, configuring the security level and enabling the NAT and IDS services of QX.

A **Firewall** is a security service configured by the QX 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 QX gateway LAN members to connect to the Internet using QX gateway 's WAN IP address. The QX gateway/NAT also handles forwarding incoming packets from the WAN to the PCs or devices on QX gateway's LAN.

The **IDS** (Intrusion Detection System) is a type of firewall, but together with deleting dangerous packets or packets containing intrusion attacks, IDS generates a log file with information about these dropped packets and the senders responsible for those packets. The log can be viewed on the IDS Log page and notifications about them can be sent to the user in various ways such as e-mail, flashing LED and display notification.

Firewall and NAT

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

The **Enable IDS** checkbox selection enables the Intrusion Detection System. The **Enable NAT** checkbox selection enables Network Address Translation.

The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are the following:

- **Low Security** - Everything that is not explicitly forbidden will be allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

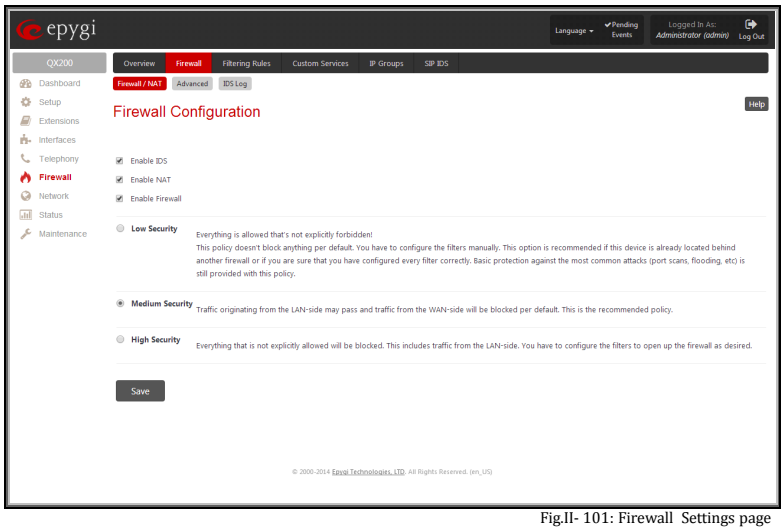


Fig.II- 101: Firewall Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed towards the device. With these features enabled, QX gateway will answer with inscrutable messages to the Ping and Portscanning operations.

Please Note: Operations are available only when the firewall is enabled from the Firewall and NAT page.

This page offers the following components:

The **Ping Stealth** checkbox selection prohibits a Ping operation toward QX gateway from its WAN.

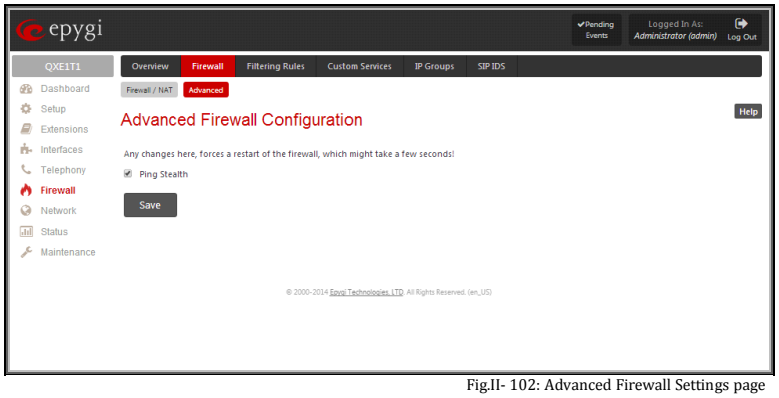


Fig.II- 102: Advanced Firewall Settings page

IDS Log

The **IDS log** page (this page is not available for QXE1T1 gateway) contains information about dropped packets and the senders responsible for those packets. IDS discards dangerous packets or packets including intrusion attacks. It generates a table with the IDS log report. The administrator can be notified about newly logged entries in various ways (mail, display notification, Flashing LED, sms) depending on the settings in the Event Settings page. To make an IDS log reporting table, IDS needs to be enabled on the Firewall and NAT page.

The **IDS Logs** table is a list of new or read IDS entries and descriptions referring to them. The table provides a status row that has the value **New** if the entry is still unread or it is empty if the entry has already been read.

Mark All as Read marks all IDS logged entries as read and removes the **New** status from the **Status** row of the IDS entries table.

Delete Log is used to delete all entries from the IDS table.

A detailed log of the selected entry can be seen by clicking on the **Description** link of the corresponding entry in the **IDS Entries** table.

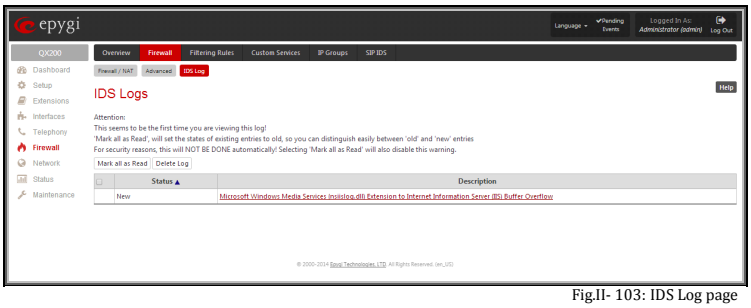


Fig.II- 103: IDS Log page

The IDS Logs detailed page has a following preview:

The **Issue Detailed Log** table is a detailed list of new and read IDS entries. The table contains a **Status** row that has the value **New** if the entry is still unread or that is empty if the entry has already been read.

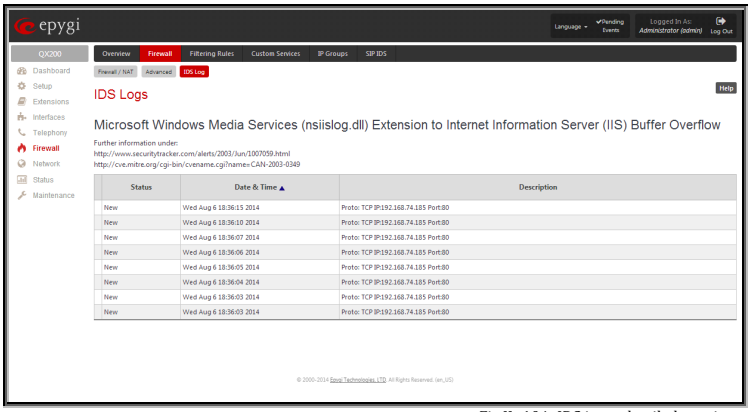


Fig.II- 104: IDS issue detailed preview

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.

Attention: The newly created blocking filtering rules will take effect immediately if there is no any active connection matching to that rule. Otherwise, if there is an active connection matching to the created blocking rule, please restart the QX gateway to make the newly created blocking rule effective immediately. However, if you are unable to restart the QX gateway, you may need to stop an existing active connection to make the newly created blocking rule effective. Please note, that in this case the blocking rule will take effect only in 3 minutes.

View All Filtering Rules

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. Since it is read-only, no modifications are allowed and no functional buttons are available.

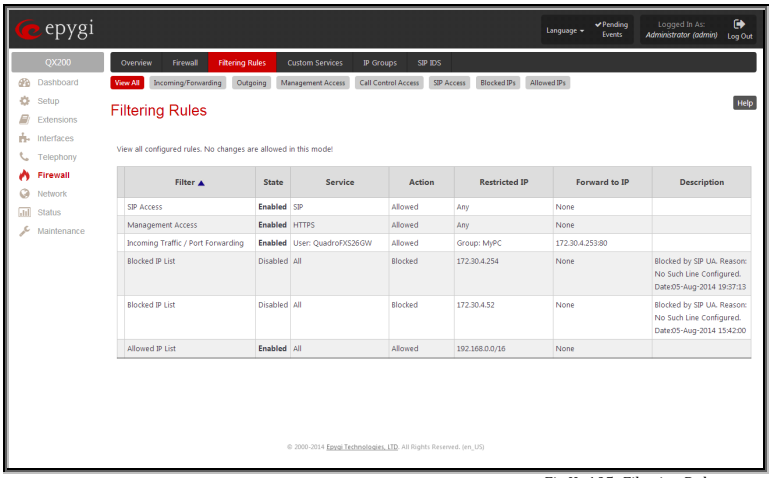


Fig.II- 105: Filtering Rules page

Incoming Traffic/Port Forwarding

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 QX gateway's LAN. The NAT service should be enabled on the QX gateway to provide the possibility of **Port Forwarding** in the **Incoming/ Forwarding** filtering rules. The **Port Forwarding** function will be unavailable if NAT is disabled on the QX IP PBX.

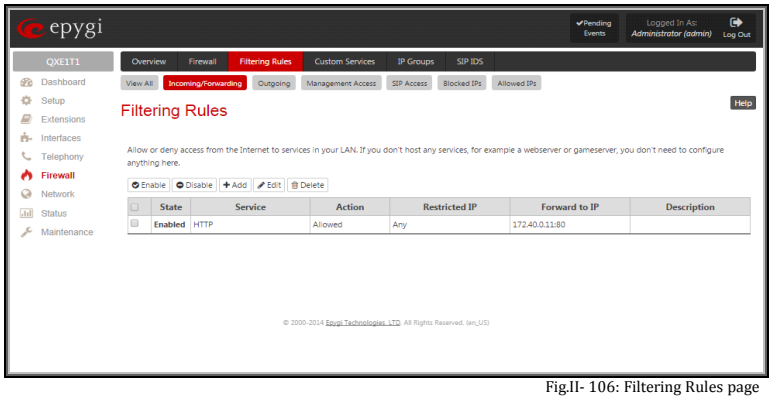


Fig.II- 106: Filtering Rules page

Outgoing Traffic

The **Outgoing Traffic** filter is for outgoing traffic. The rules here allow or deny QX gateway's LAN users to reach external services.

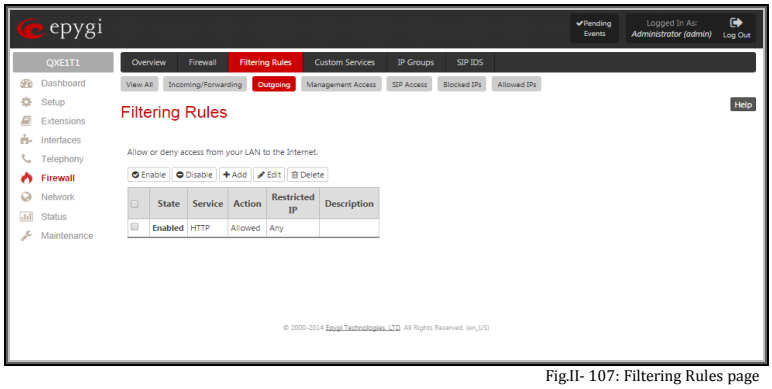


Fig.II- 107: Filtering Rules page

Management Access

Management Access is used to enable management access to the QX gateway from the Internet. A host on the Internet can be allowed to reach the QX gateway.

Fig.II- 108: Filtering Rules page

SIP Access

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).

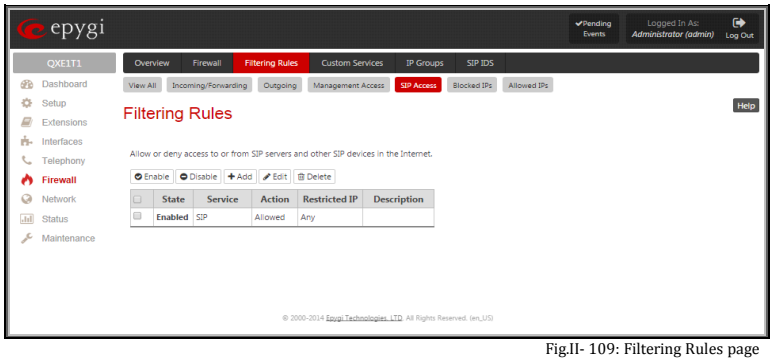


Fig.II- 109: Filtering Rules page

Blocked IPs

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.

Fig.II- 110: Filtering Rules page

Allowed IPs

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.

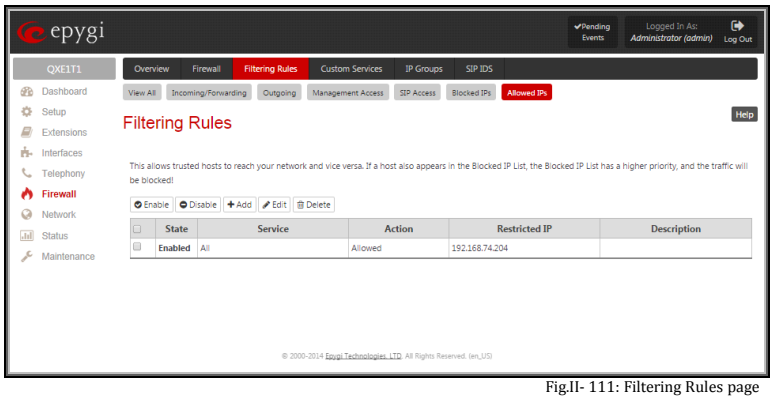


Fig.II- 111: Filtering Rules page

The table displayed on the bottom of this page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Disable** is used to disable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action,** a **Restriction** to certain IP address(es) or IP groups, and if adding a rule for **Incoming Traffic/Port Forwarding**, the destination IP address for **Forwarding**.

The page to add a rule for **Incoming Traffic/Port Forwarding** offers the following input options:

Service includes a list of possible services to be configured. All user-defined services also will be displayed in this list.

Action includes possible actions to setup the rule.

Forward to IP requires the destination IP address where traffic should be transferred to if it comes from the restricted host. The IP address defined in this field will be ignored for blocked action of the **Incoming Traffic/Port Forwarding** rule.

Please Note: It is not allowed to forward incoming packets when the NAT service is disabled on the QX gateway.

Port Translation text field is available for "Allowed" action only and optionally requires the port number that will stand instead of the original port number when incoming packet is being forwarded. If this field is left empty, the original port number will be used when forwarding the packet.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.
- Selecting **Single IP** will require the IP address of the allowed or blocked host.
- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. The following are **Maskbit** examples:
  255.0.0.0= /8,
  255.255.0.0 = /16,
  255.255.255.0 = /24,
  255.255.255.255= /32
- **Single URL** requires the hostname of the allowed or blocked host.
- **Group** indicates the user-defined groups that include IP addresses that should to be allowed or blocked.

The **Description** field is used to insert an optional description of the filtering rule.

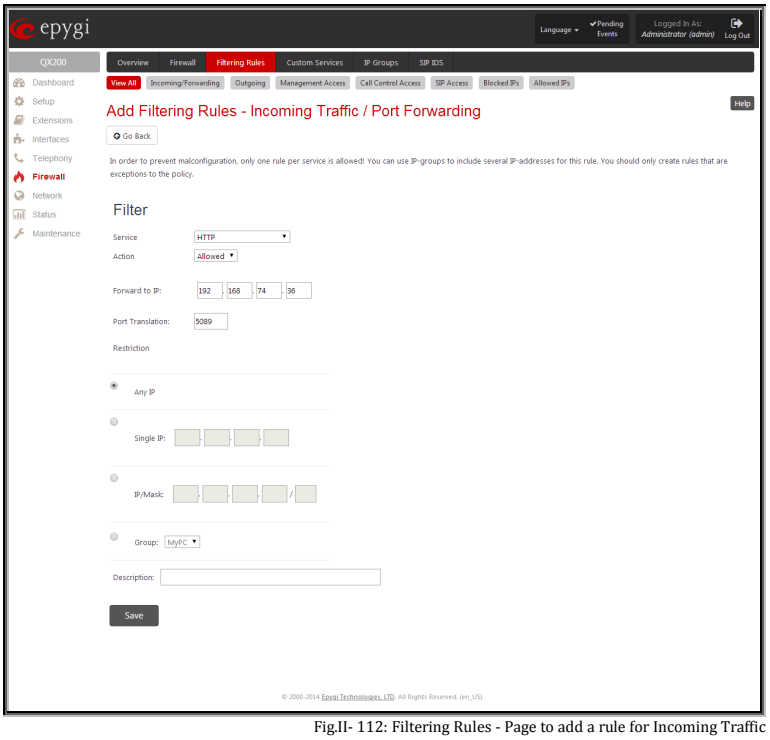


Fig.II- 112: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filtering Rule** (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List or Allowed IP List) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the corresponding filtering rules page.
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 corresponding **Filtering Rule** (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, Blocked IP List or Allowed IP List).
2. Check one or more checkboxes of the corresponding rules that should be deleted from the rules table.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

Custom Services

Service Pool Configuration

The **Service Pool** table is a list of all created services and their parameters. It is used to add new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or permission by defining a new filtering rule with the following:

Add opens the **Add New Service** page where new services may be added.

Edit opens the **Edit Service** page where the service parameters (except for the service name) can be modified. This page includes the same components as the **Add New Service** page. To operate with **Edit** only one record may be selected, otherwise the error message "One row must be selected" will appear.

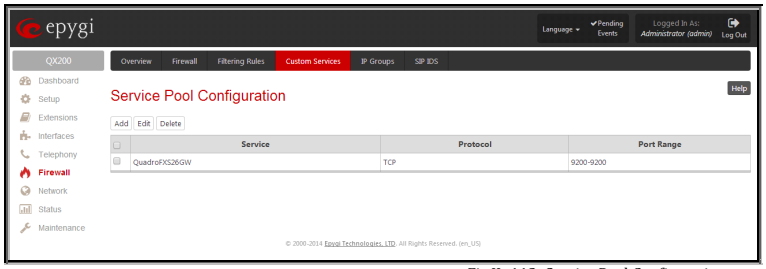


Fig.II- 113: Service Pool Configuration page

The **Add** page is used to add new services and includes the following text fields and buttons:

Service Name requires a name for the service that should be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.

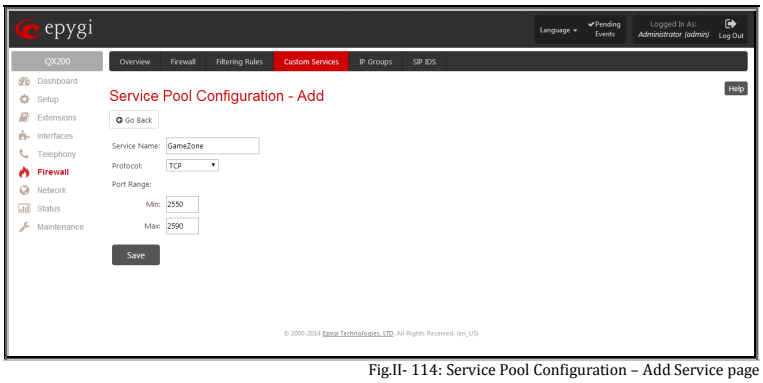


Fig.II- 114: Service Pool Configuration – Add Service page

To Add a new Service

1. 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.
2. Define a service name in the **Service Name** text field.
3. Select the protocol type for the service from the **Protocol** drop down list.
4. Enter the port range in the **Port Range** text fields or leave one of them empty to define a particular port for the service.
5. To add a service with these parameters, click on **Save**.

To Delete a Service

1. Check one or more checkboxes of the corresponding services that should be deleted from the **Service Pool Configuration** table.
2. Click on the **Delete** button on the **Service Pool Configuration** page.
3. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

IP Groups

IP Pool Configuration

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.

Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

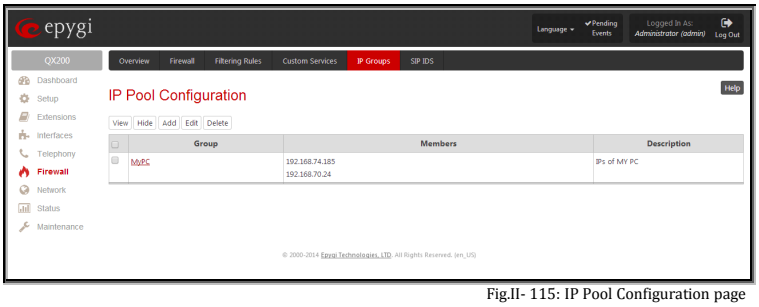


Fig.II- 115: IP Pool Configuration page

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Go Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains). Deleting a group will also delete any reference to the corresponding group, including filter-rules and member relations to the other groups.

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

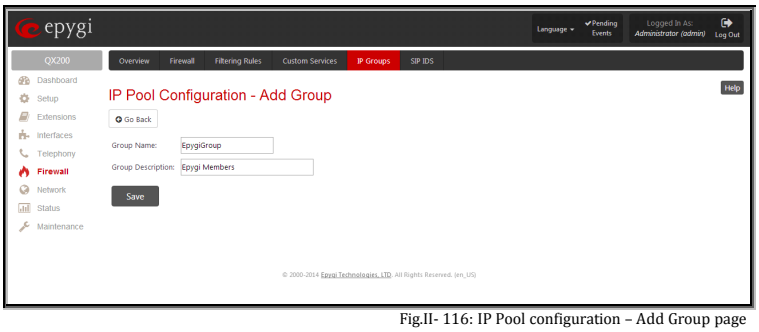


Fig.II- 116: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

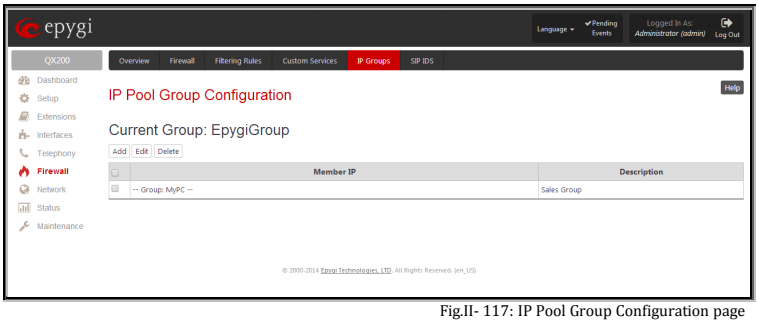


Fig.II- 117: IP Pool Group Configuration page

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

IPaddress requires the member IP address that is to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

URL Address requires the member hostname to be added to the group.

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

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

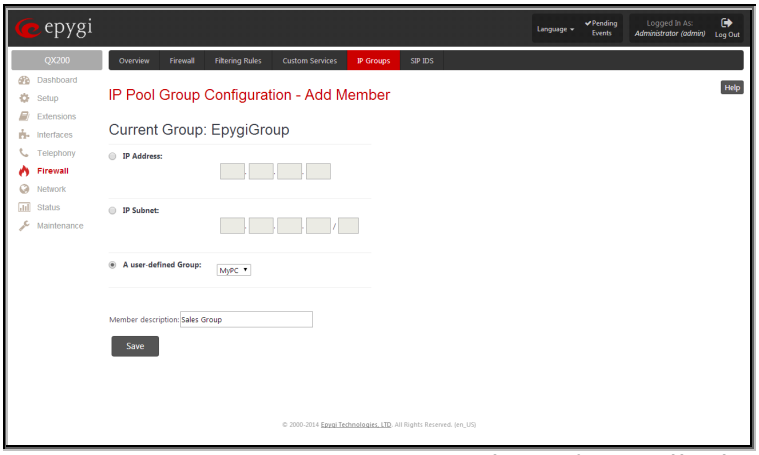


Fig.II- 118: IP Pool Group Configuration – Add Member

To Add a new Group with Members

1. 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.
2. Define a group name in the **Group Name** text field and fill in the **Group Description**, if needed.
3. To add a group with the given parameters, press **Save**.
4. Open the **IP Pool Group Configuration** page by clicking on the group name.
5. Select the **Add** button on the **IP Pool Group Configuration** page. A page opens where new members may be added to the group.
6. Enter an IP address for the member in the **IP Address** text fields, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
7. Enter a **Member Description** in the corresponding text field, if needed.
8. To add a member with these parameters to the selected group press **Save**.

To Delete a Member

1. Check one or more checkboxes of the corresponding members that should be deleted from the **Members** table.
2. Press the **Delete** button on the **IP Pool Group Configuration - Members** page.
3. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

To Delete a Group

1. Check one or more checkboxes of the corresponding groups that should be deleted from the **IP Pool Configuration** table.
2. Press the **Delete** button on the **IP Pool Configuration** page.
3. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

SIP IDS Settings

The **SIP IDS Settings** page includes the following components:

Enable SIP IDS checkbox selection allows to prevent the SIP attacks.

The **Add the IP address into the Blocked IP list in Firewall** checkbox allows to block SIP attacker's IP address. SIP attacker's IP address will be blocked by QX gateway Firewall and will be added on the Firewall **Blocked IP List** table.

The **Discard SIP messages from IP address for** checkbox allows to discard the accumulated SIP messages from the QX gateway SIP cash after defined timeout (default timeout value of "Discard SIP messages from IP address for" service is 32 seconds).

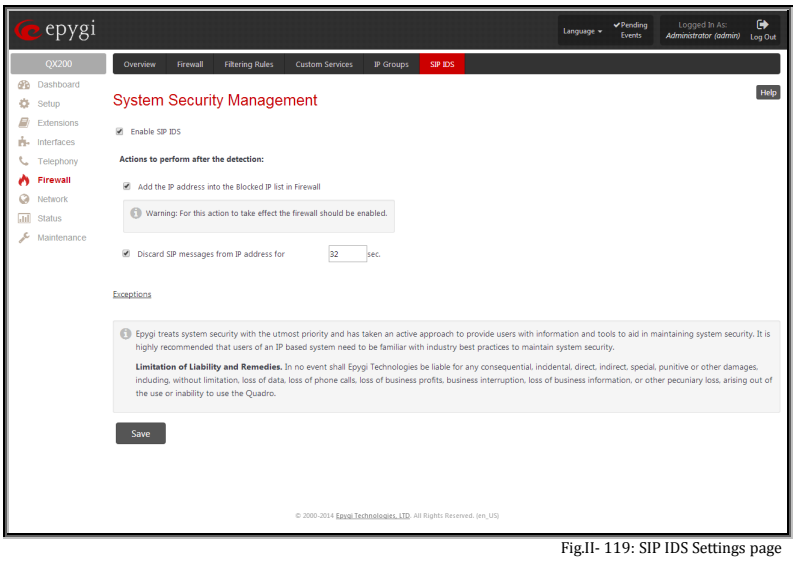


Fig.II- 119: SIP IDS Settings page

The **Exceptions** link leads to the **Exceptions for SIP IDS** page where user can require the trusted IP address(es) that can't be blocked.
Add opens the page **Exception IP- Add Entry**, where a trusted IP address can be established.

Fig.II- 120: Exceptions for SIP IDS Table

Network Menu

The **Network** menu allows you to configure the following settings:

- **IP Routing Configuration**
  - IP Static Routes
  - IP Policy Routes
  - PPTP/L2TP Routes
- **DHCP Settings**
  - DHCP Server
  - DHCP Leases
  - DHCP Settings for the VLAN Interface
- **DNS Settings**
  - DNS Server Settings
  - Dynamic DNS Settings
- **PPP/ PPTP Settings**
  - Advanced PPP Settings
- **SNMP Settings**
  - Global SNMP Settings
  - SNMP Trap Settings
- **VLAN**
- **VPN Configuration**
  - IPSec Configuration
  - PPTP/L2TP Configuration

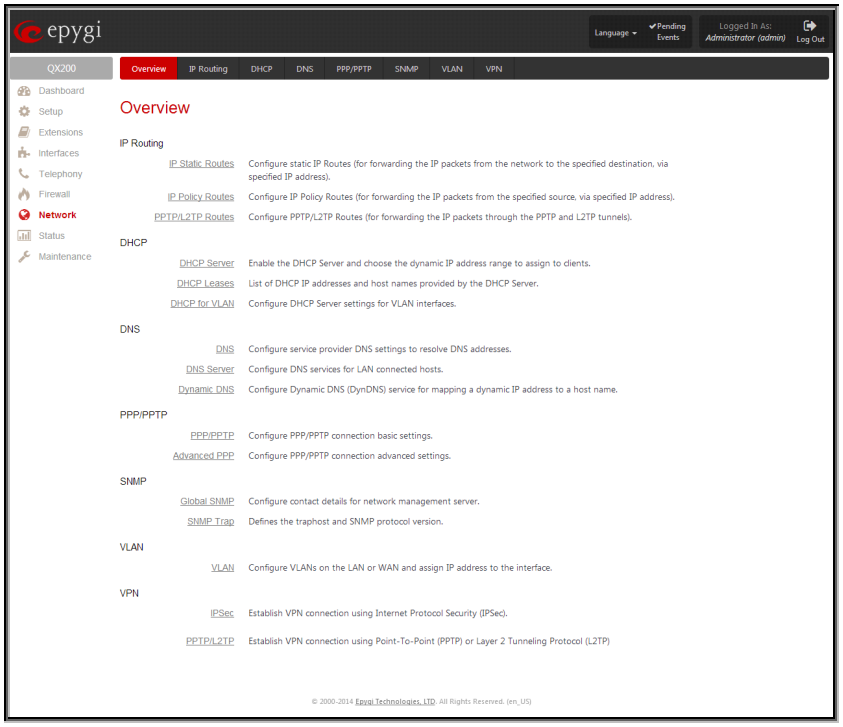


Fig.II- 121: Network Menu page

IP Routing Configuration

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

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

The **IP Routing** page is used to make IP Static, IP Policy and PPTP/L2TP 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

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

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

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

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

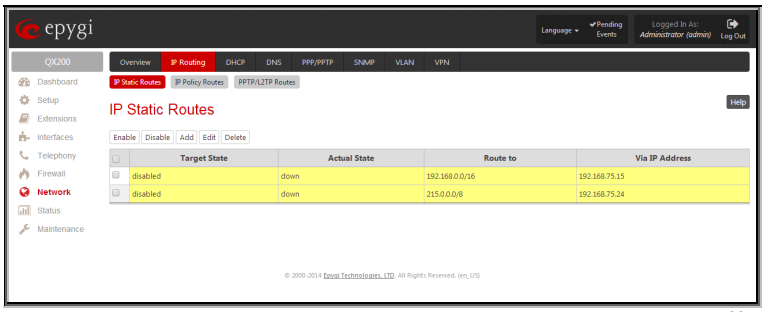


Fig.II- 122: IP Static Routes table

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

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

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

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

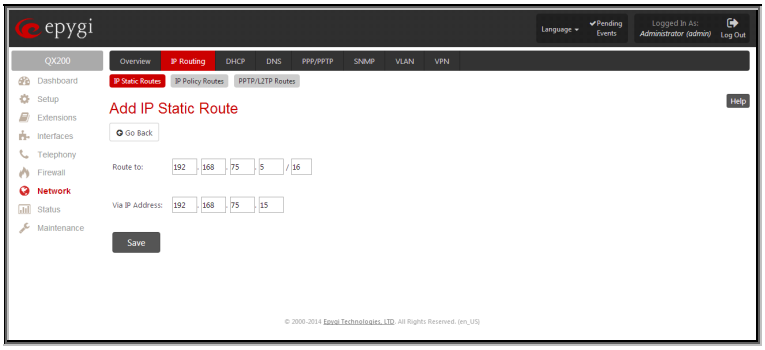


Fig.II- 123: Add IP Static Route page

IP Policy Routes

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).

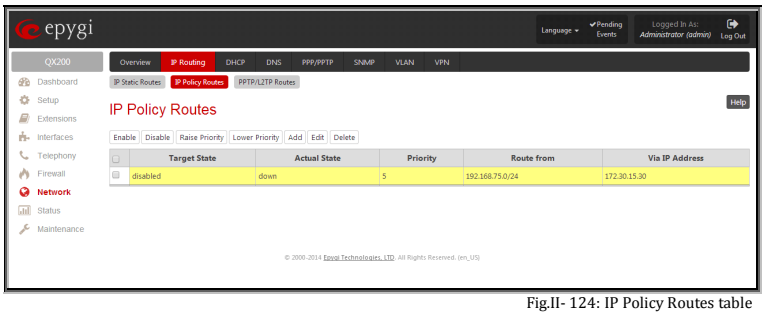


Fig.II- 124: IP Policy Routes table

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.

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

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

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

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

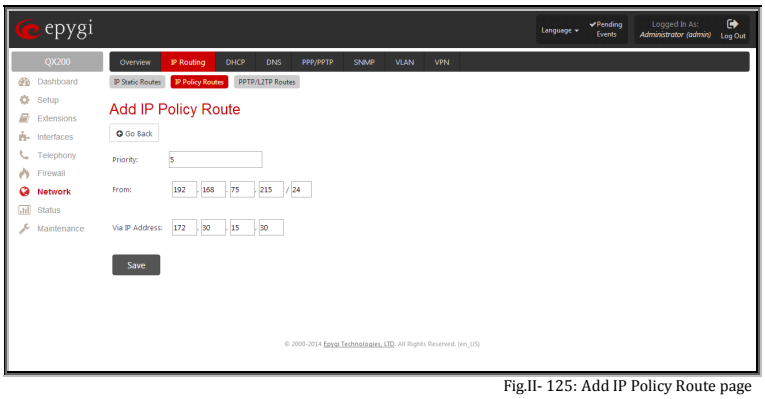


Fig.II- 125: Add IP Policy Route page

PPTP/L2TP Routes

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

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

The **Add** button opens the **Add PPTP/L2TP Route** page where a new VPN route can be generated.

Fig.II- 126: PPTP/L2TP Routes table

The **Add PPTP/L2TP Route** page offers the following components:

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

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

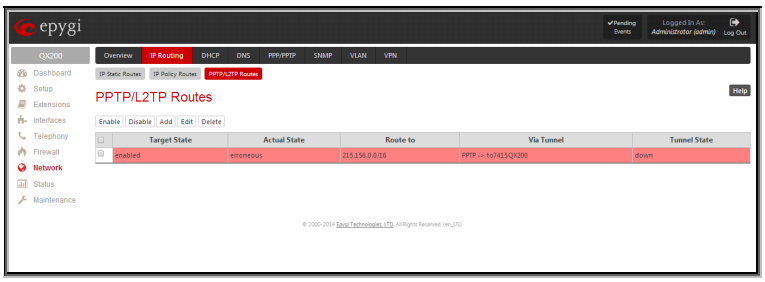


Fig.II- 127: Add PPTP/L2TP Route page

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.

DHCP Settings

The **DHCP Settings** page provides the option of enabling a DHCP server and controlling the QX gateway user's LAN settings. Therefore, QX gateway LAN users will automatically be provided with the following settings using the configured parameters:

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

DHCP Server

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

Enable DHCP Server checkbox activates the DHCP server on QX gateway . With this checkbox enabled, QX gateway 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 **Special Devices** table. With this checkbox selected, no DHCP services will be provided to the other devices.

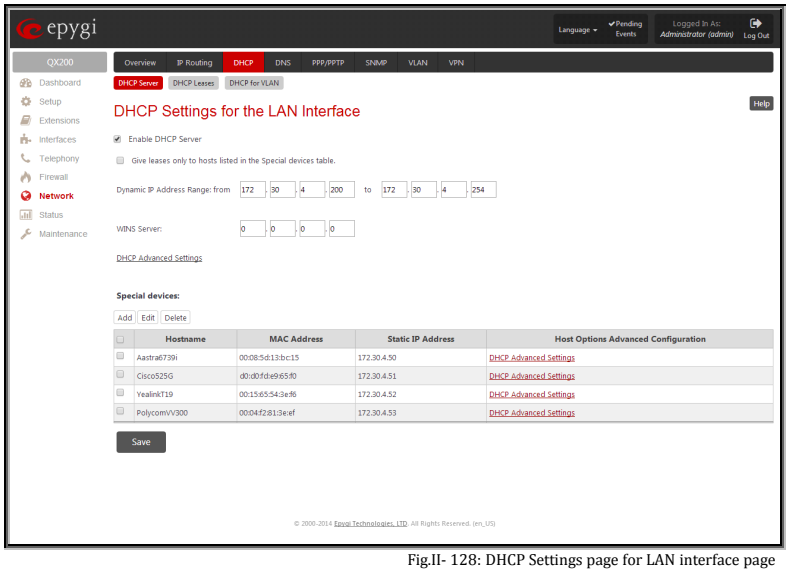


Fig.II- 128: DHCP Settings page for LAN interface page

IP Address Range defines a range of IP addresses that will be assigned to the QX gateway 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 exceeds the allowed IP address range defined by subnet mask (it could be up to 508).

WINS Server defines a WINS server IP address for the QX gateway LAN users.

DHCP Advanced Settings link leads to the page where the advanced options of the QX gateway's DHCP server can be configured.

The **Special Devices** table on this page allows you to set a static IP address binding on the MAC address of the device in the QX gateway's LAN. When this table is configured, the devices with defined hostnames and MAC addresses will always get the same LAN IP address from the DHCP server. Otherwise, devices not listed in this table will get dynamic LAN IP addresses. This table is also displayed in the System Configuration Wizard.

Add functional button opens an **Add Host** page where a new static MAC address binding can be defined. The page consists of the following components:

Hostname text field requires the hostname of the device in the QX gateway's LAN.

MAC Address text fields require the MAC address of the device in the QX IP PBX's LAN.

Static IP Address text fields require a fixed IP address of the device in the QX gateway's LAN.

Please Note: If you leave this field empty, the device in the QX gateway's LAN will get the first available IP address from range defined in the **DHCP Settings** page (see above).

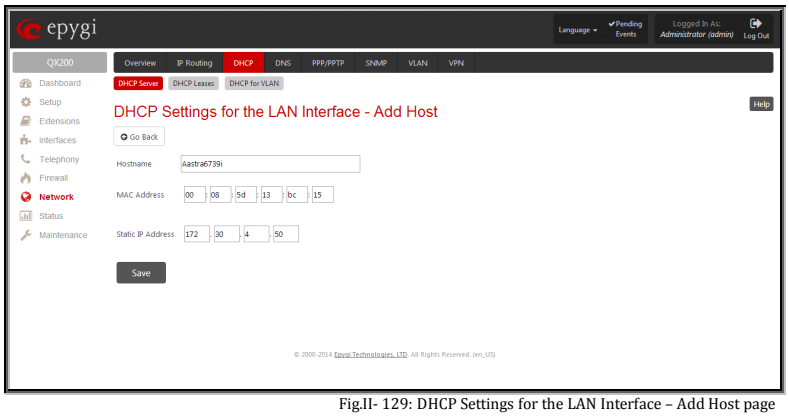


Fig.II- 129: DHCP Settings for the LAN Interface – Add Host page

DHCP Advanced Settings

The **DHCP Advanced Settings** page is used to modify the advanced options of the DHCP server on the QX gateway. This page contains a table where a list of default DHCP server options is already defined. More options can be added from this page, as well as settings of the existing options can be modified. All options in the table on this page are then sent to the DHCP clients.

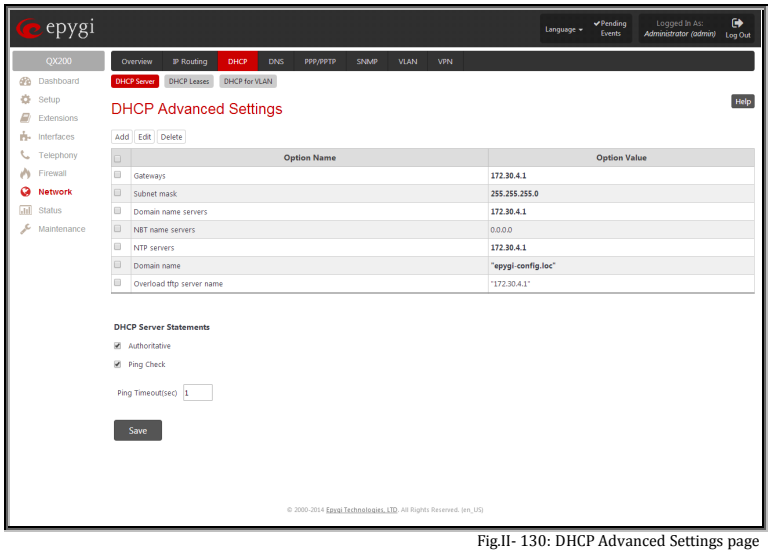


Fig.II- 130: DHCP Advanced Settings page

- The **Authoritative** checkbox is used to enable/disable authoritative mode on the QX gateway DHCP server. Disabling the checkbox is recommended if several DHCP servers are used on the network and the QX gateway should provide network parameters to IP phones only.
- The **Ping Check** checkbox enables checking the availability of an IP address on the network before providing it to a client. If this checkbox is selected, the QX gateway will first ping an IP address retrieved from the IP pool and wait for a reply. If no a reply is received within a timeout specified in the **Ping timeout** text field (by default 1 sec), the retrieved IP address will be provided to the client. If otherwise, a new IP address will be retrieved from the IP pool and the procedure will be repeated. If this checkbox is not selected, the QX IP PBX will provide an IP address immediately when requested.

The following functional buttons are available for managing DHCP options:

Add opens a page **Add Entry** page where a new DHCP server option can be defined. The Add Entry page contains a group of manipulation radio buttons to select between the predefined DHCP server options or to define your own DHCP server option:

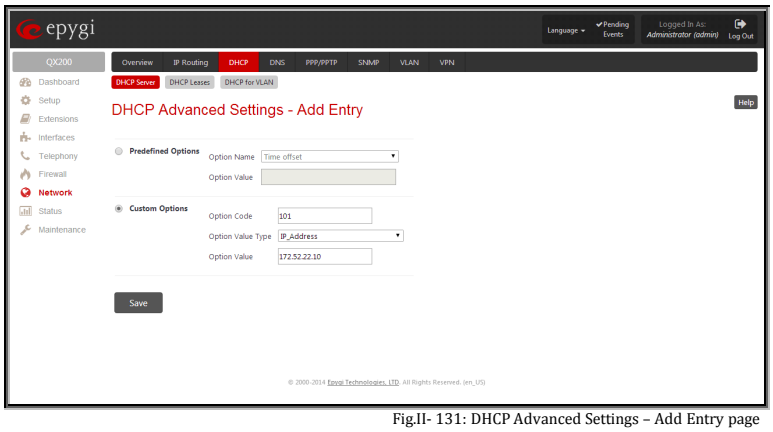


Fig.II- 131: DHCP Advanced Settings – Add Entry page

- **Predefined** - this selection allows you to select from the predefined DHCP server options.

  The **Option Name** drop down list contains the most common DHCP server options.

  The **Option Value** text field requires the value for the selected option. The type and format of the value inserted in this field is dependent on the option selected from the Option Name drop down list.

- **Custom** - this selection allows you to define a new DHCP server options. The following parameters are required to be inserted for a new option:

  The **Option Code** text field is used to insert a code of the option. It may have values in a range from 0 to 255.

  The **Option Value Type** drop down list is used to select the type of the option value. It may be an IP address, a boolean or integer value, etc.

  The **Option Value** text field is used to insert the value of an option. Depending on the selected Option Value Type, this field should have the corresponding value. Warning messages will prevent saving if the value inserted in this field does not correspond to the requirements of the Option Value Type. If an array should be inserted here, the values should be separated with a comma.

DHCP Leases

The **DHCP Leases** page includes a list of the leased host addresses that are part of the QX gateway's LAN. For these hosts, QX gateway 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:

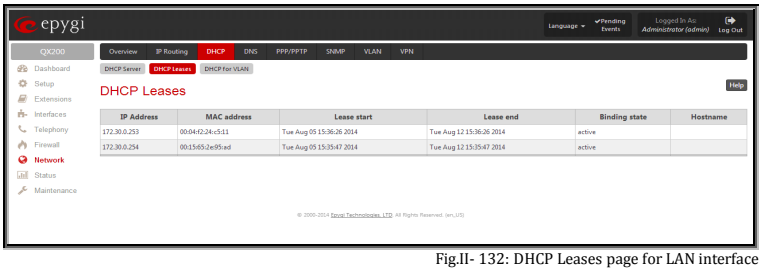


Fig.II- 132: DHCP Leases page for LAN interface

IP address - host IP address, assigned by QX gateway.

MAC address - host MAC address, provided by the host itself.

Lease Start - date and time when the leased IP address has been activated.

Lease End - date and time when the leased IP address has been or will be deactivated.

Binding State – indicates the state of the DHCP lease.

Hostname - hostname, provided by the host itself.

DHCP Settings for the VLAN Interface

DHCP Settings for the VLAN Interface is used to establish virtual networks in the QX gateway's LAN or to integrate the QX gateway into the corporate network's virtual LAN/WAN. DHCP service can be activated both on LAN or WAN interfaces. VLAN is useful in corporate companies to divide large networks into groups and to have devices like QX gateways and IP phones in each network separated (for example, to separate networks for data and voice transmission). Priorities may be assigned to the interfaces for packets prioritization.

With VLAN configuration, each virtual network will be characterized with a VLAN ID (tag). Packets addressed to that network will be checked towards the ID and if the ID number defined in the incoming packets matched the corresponding network's ID, the packets will be accepted. Otherwise, if the ID does not match, the packets will be dropped. In the same way, if the QX IP PBX is integrated into the network that uses VLAN technology, outgoing packets should have the ID number of the corresponding virtual network, for the remote party to accept the packets from the QX gateway.

The **DHCP Settings for the VLAN Interface** page contains a table with all enabled VLAN interfaces created in VLAN Settings page (see below) and the corresponding parameters (VLAN ID, IP Address Range and WINS Server). This page contains the following components:

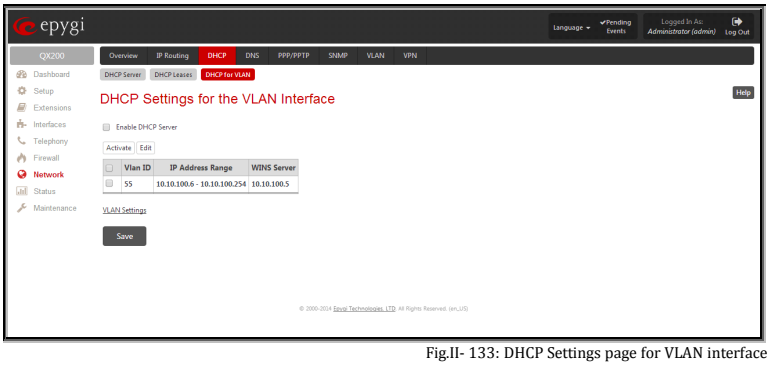


Fig.II- 133: DHCP Settings page for VLAN interface

Enable DHCP Server checkbox activates the DHCP server on QX IP PBX for VLAN. With this checkbox enabled, QX gateway will be able to assign dynamic IP addresses to the devices in its VLAN.

Activate functional button is used to activate DHCP service on one of the VLAN interfaces in the list. Only one VLAN interface can have DHCP service activated.

Edit functional button opens a page where the corresponding VLAN interface can be configured and controlled. This page contains all the same components as the DHCP Server page does.

VLAN Settings link moves to the VLAN Configuration page where virtual LAN/WAN interfaces may be created.

DNS Settings

The **DNS Settings** page provides the option of setting up a name server for the QX gateway. It offers the following components:

The **Nameserver Assignment** radio buttons are as follows:

- The **Dynamically by provider** selection automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** is a manually selected name server. The **Nameserver** text field requires the IP address of an external name server. The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.

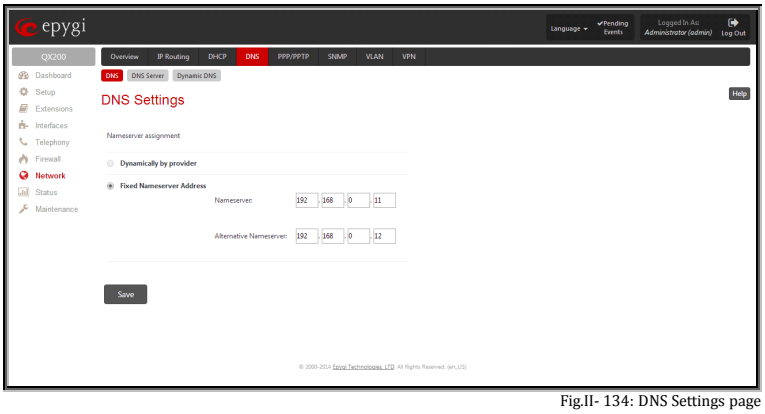


Fig.II- 134: DNS Settings page

DNS Server Settings

The **DNS Server** on the QX gateway provides the services to the hosts in the QX gateway's LAN. With this service, QX gateway 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 QX gateway and to define a list of aliases for the devices in the QX gateway's LAN. This page contains the following components:

Zone field displays the QX IP PBX's host domain name as it is configured in the System Configuartion 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 QX gateway.

The table on this page lists aliases for each of the device in the QX gateway's LAN to be resolves through the DNS server.

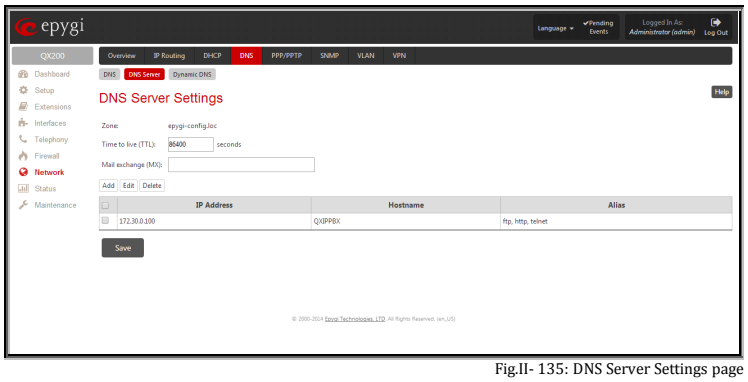


Fig.II- 135: DNS Server Settings page

Add functional link opens the page **Add Host** where a list of aliased can be defined for the certain device in the QX gateway's LAN. The page contains the following components:

IP Address text fields require the IP address of the device in the QX gateway's LAN.

Hostname text field requires the hostname of the device in the QX gateway's LAN.

Alias text fields are used to enter up to 5 alias names by which the device in the QX gateway's LAN will be resolved.

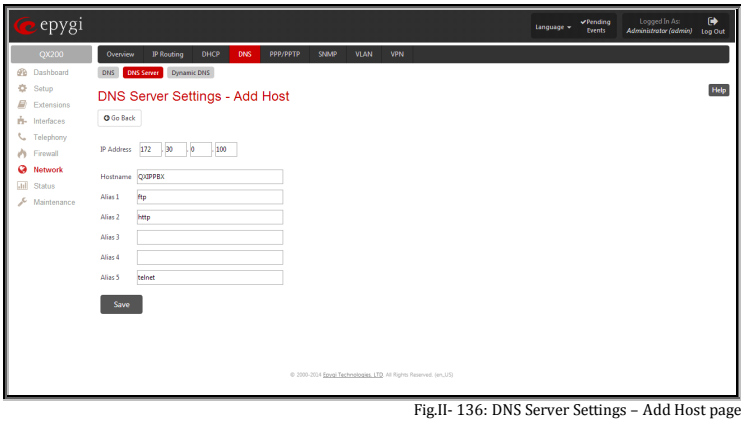


Fig.II- 136: DNS Server Settings – Add Host page

Dynamic DNS Settings

The **Dynamic DNS** (DynDNS) is a service that is used to map a dynamic IP address to a host name. This service is used if you are connected to the Internet with a dynamic IP address (and PPP, DHCP client) and want to allow access from the Internet to a device behind the firewall. For example, if you want to run your own WEB server.

To enable the DynDNS service on QX gateway, you first have to choose a DynDNS provider and register at their website.

The **Dynamic DNS Settings** page provides the following components:

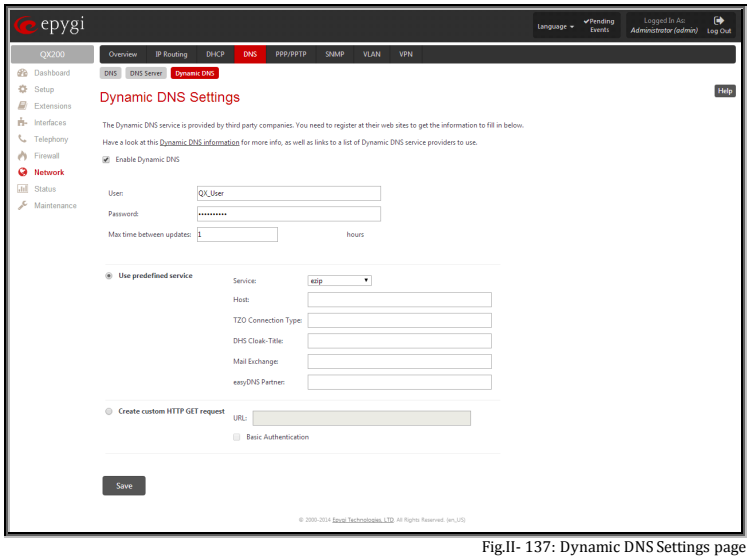


Fig.II- 137: Dynamic DNS Settings page

The **Enable Dynamic DNS** checkbox selection enables the dynamic DNS service.

The **User** text field requires the username specified during the registration at the DynDNS provider.

The **Password** text field requires the password specified during the registration at the DynDNS provider.

The **Max time between updates** text field requires entering the period between two updates (in hours). The values entered in these fields should be greater than 24, otherwise the error message "Update interval times smaller than 24 hours are too small" will appear. Normally, whenever you set up a connection to the Internet, the DynDNS is updated at least once in the period indicated in this field.

The **Use predefined service** radio button leads to the manual configuration of the DynDNS service. The selection enables the following optional settings:

The **Service** drop down list contains the provider list where the administrator needs to select the one that it has been subscribed to.

The **Host** text field requires the name of the host on the Internet.

The **TZO Connection Type** text field is used for a special parameter required by the DynDNS provider TZO.

The **DHS Cloak-Title** text field is used for a special parameter required by the DynDNS provider DHS.

The **Mail Exchange** text field requires the address of the e-mail server where the DynDNS service provider will relay your e-mails.

Attention: If this service is used, ensure that there is port forwarding configured for SMTP (port 25) to the internal e-mail server.

The **easyDNS Partner** text field is used for a special parameter required by the DynDNS provider easyDNS.

Selecting the **Create Custom HTTP GET Request** radio button will switch to the custom settings of the DynDNS service. Normally, the DynDNS provider uses HTTP get requests to map dynamic IP addresses to host names. If the HTTP receive request is known to you, choose the **Create Custom HTTP GET Request** radio button and enter the appropriate value into the **URL** text field.

The selection enables the following optional settings:

The **URL** text field requires the complete request to be sent to the DynDNS server. Normally it has the following format:

http://www.server.domain:port/scriptpath/scriptname?param1=value1&param2=value2

The request modifies the nameserver database so that the hostname will be resolved to the new IP address.

The **Basic Authentication** checkbox enables the encoding of the username and password entered in the text fields above, and then uses the **Basic Authentication** method to notify the provider about the user authentication settings.

Most of the DynDNS providers require an authentication for security. Authentication parameters can be provided in the **URL** text field to be used for the HTTP get request. The **Basic Authentication** checkbox can be selected if no authentication parameters to be provided.

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 QX gateway and the provider, QX gateway users will be able to make and receive calls at any time.

The **PPP/PPTP Settings** page offers the following components:

The **PPTP Server** text fields are only enabled when QX gateway is running with the PPTP interface and require the IP address of the PPTP server.

The **Encryption** drop down list is only enabled when QX gateway 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 QX gateway first.
- **Always connected** - QX gateway stays in the always connected mode. This will allow always being online in the network.

IP Address Assignment radio buttons are used to define the IP address assignment for the PPP interface with the following options:

- **Dynamic IP Address** – the IP address to the PPP interface will be assigned dynamically by the DHCP server.
- **Fixed IP Address** – the fixed user defined IP address will be assigned to the PPP interface.

The **Keep Connection alive** checkbox enables keeping the connection alive by sending control packets dedicated for the link state verification.

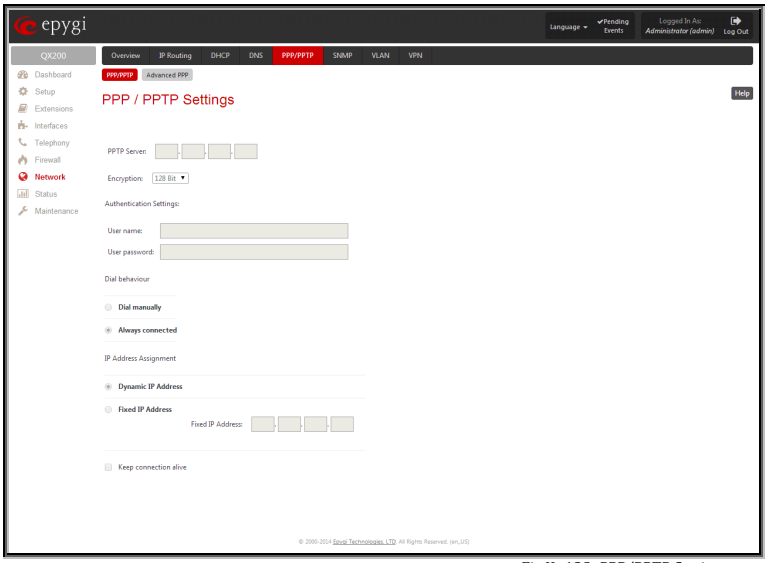


Fig.II- 138: PPP/PPTP Settings page

Advanced PPP Settings

The **Advanced PPP Settings** page is used to enable/disable certain parts of the negotiation process during connection establishment. These settings are available only if QX IP PBX 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.

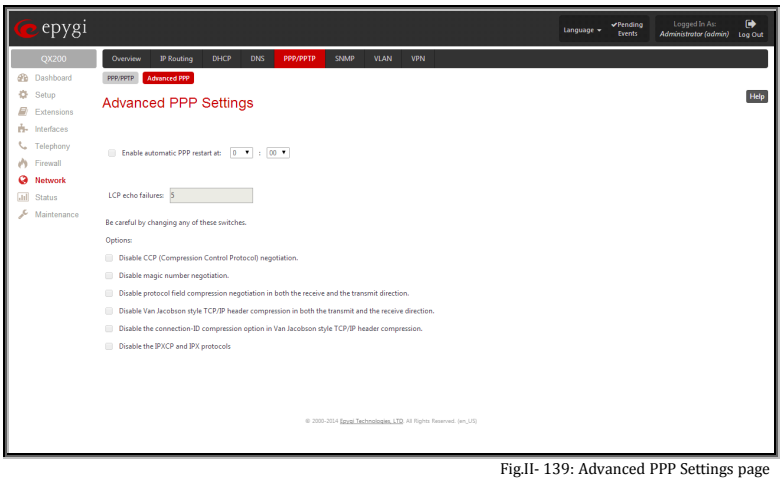


Fig.II- 139: Advanced PPP Settings page

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.

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 QX gateway, SNMP agent is running to allow administrators to remotely manage QX gateway'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 QX gateway or remotely modify QX gateway'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 QX IP PBX, to select the SNMP protocol version for communication with the administrating application and to define the community for administrating application to connect the QX gateway.

Global SNMP Settings

Enable SNMP checkbox is used to enable SNMP agent on the QX gateway.

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 QX gateways SNMP agent and the administrating application. If this checkbox is not selected, **SNMP v1** will be implied.

SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about QX gateway's). Field may contain some kind of password which should be matching both on QX gateway 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 QX gateway for the SNMP monitoring application. With this checkbox enabled, administrator will be able to remotely configure the QX gateway via SNMP administrating program.

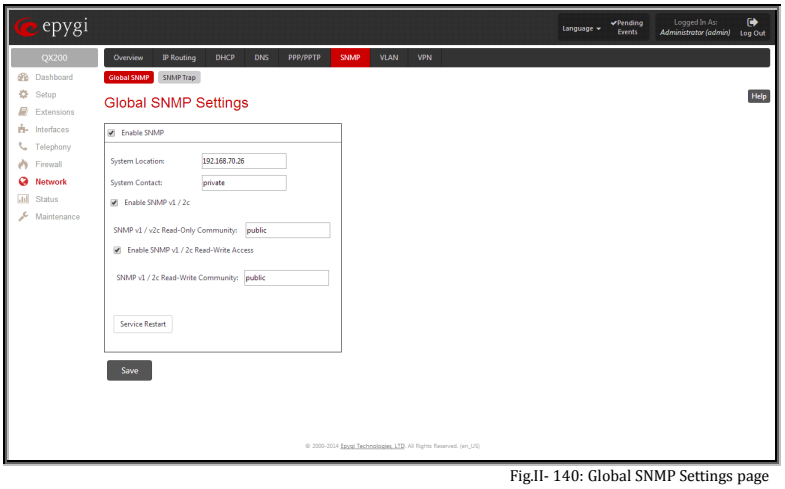


Fig.II- 140: Global SNMP Settings page

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 QX gateway's and remotely changing QX gateway's configuration). Field may contain some kind of password which should be matching both on QX gateway and on the administrating application for successful SNMP management.
The **Service Restart** button restarts the SNMP sub-system on the QX gateway. Restarting the SNMP sub-system is recommended if it does not respond to a SNMP manager's requests.

SNMP Trap Settings

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

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

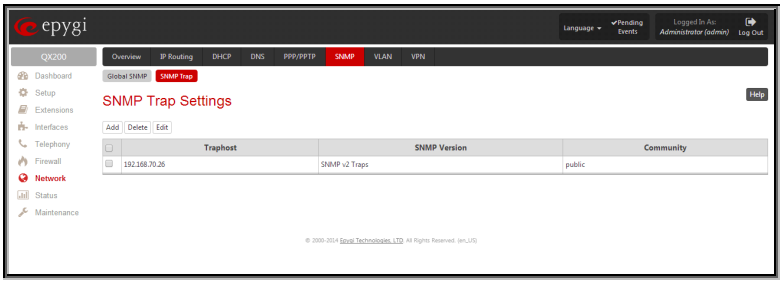


Fig.II- 141: SNMP Trap Settings page

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 QX gateway. Field may contain some kind of password which should be the same both on QX gateway 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 QX gateway to the administrating application.

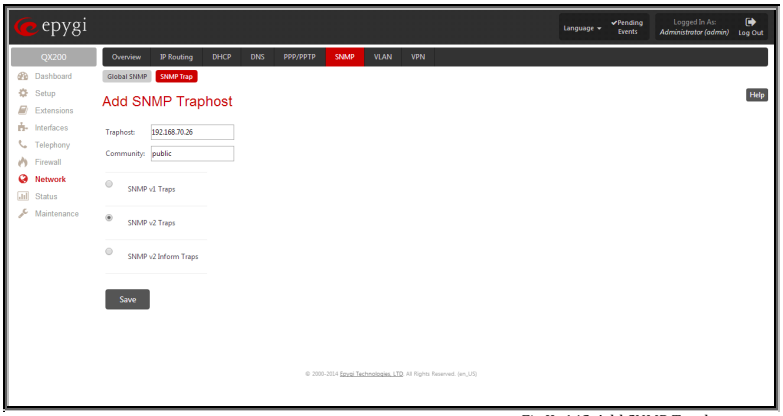


Fig.II- 142:Add SNMP Traphost page

VLAN Configuration

VLAN Settings page lists all existing virtual interfaces created on the QX gateway and allows you to create new interfaces.
Enable and **Disable** functional buttons are used to correspondingly enable and disable the selected virtual interface(s).

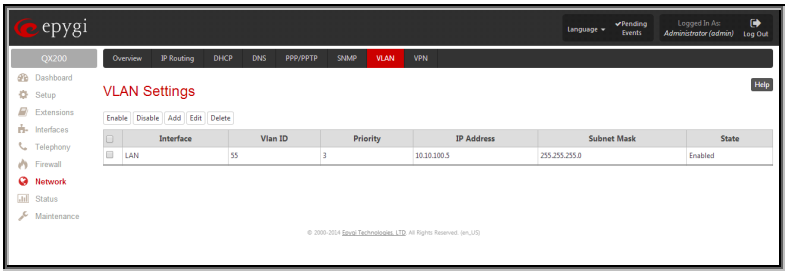


Fig.II- 143: VLAN Settings page

Add functional button opens an **Add Entry** page where a new virtual network can be defined. The page consists of the following components:

Enable checkbox is used to select whether the corresponding virtual interface will be enabled or disabled after it is created.

Interface Type manipulation radio buttons selection allows to choose whether the virtual interface will be LAN or WAN.

VLAN ID text field requires the virtual network ID. Numeric value in a range from 0 to 4094 is allowed in this field.

Priority drop down list is used to select the priority of packets in the corresponding interface. Packets with the lower priority (0) will be delivered first.

IP Address text field requires the IP address of the virtual interface.
Subnet Mask text field requires the subnet of the virtual interface.

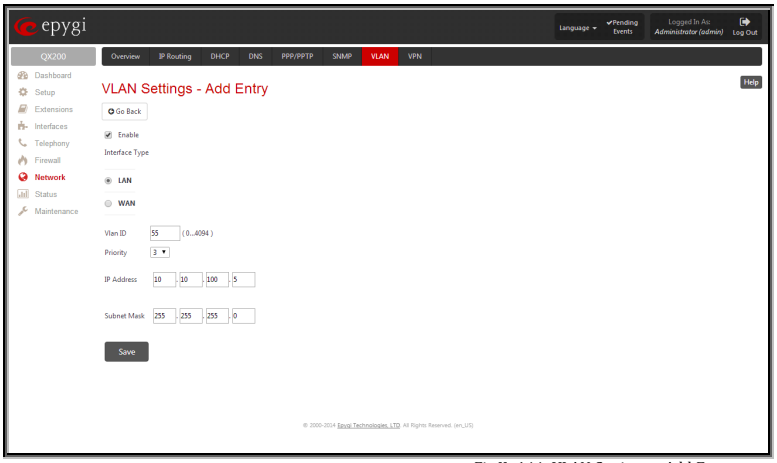


Fig.II- 144: VLAN Settings – Add Entry page

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 QX gateway 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.

QX gateway supports several kinds of VPN connections such as **IPSec** and **PPTP/L2TP**.

Attention: It is strongly recommended not to run different types of VPN tunnels between the same endpoints simultaneously.

IPSec Configuration

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 QX gateway 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 QX gateway, 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 QX gateway is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. QX gateway 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.

QX gateway can also be set up to act as a Road Warrior. If a home office is connected to the Internet via QX gateway with PPPoE (Point-to-Point Protocol) and dynamic IP addressing, setting up QX gateway 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 QX gateway 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 QX gateway's public key can be decrypted with QX gateway'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. QX IP PBX generates such a pair of keys automatically when it is set up. The user cannot see the private key, but must know the public key because their IPSec connection partner will need it.

Please Note: A pair of keys will always be generated, a public one and a private one. The previously generated pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

The **IPSec Configuration** link refers to the page where IPSec connections can be created and managed.

The **IPSec Configuration** page consists of two sub-pages: **Connection** and **RSA Key Management**.

Connection

The Connection sub-page provides an overview of all existing IPSec connections characterized by their **Connection Name**, the **Remote Gateway** (the IP address or the hostname of the IPSec connection partner), the **State** of the IPSec connection (Stopped, Connecting, Activated, Waiting or Connected) and the dedicated **Keying Type** (the encryption type). The content of the table can be sorted in ascending or descending order by clicking on the header of the respective column. There is a checkbox for every IPSec connection to select it for further editing.

Start activates the connection establishment of the selected IPSec connection. The **State** of the IPSec connection will change into "Connected" or "Activated" depending on the IPSec connection type. If no record is selected, the error message "One Record should be selected" appears.

Attention: It is not recommended to simultaneously start a static and a dynamic connection configured to use the same secret key. A dynamic connection may capture the static connection peer and vice versa, depending on which connection established first.

Stop disconnects the selected IPSec connection. The state of the IPSec connection will change into "Stopped". If no record is selected, the error message "One Record should be selected" will appear. More than one record may be selected at a time to be

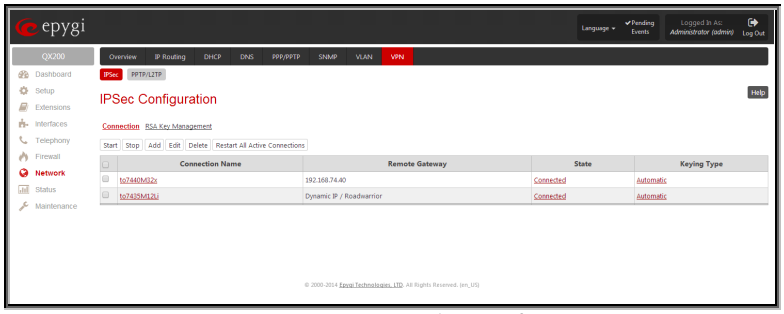


Fig.II- 145: IPSec Configuration - Connection Settings page

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 Active Connections restarts all active IPSec connections. The **State** of these IPSec connections will turn into **Connected** or **Activated** if the restart procedure has been successfully completed.

The first IPSec Connection Wizard page **Add IPSec Connection** has the **Connection Name** text field that requires a new mandatory IPSec connection name. If the text field is not filled in, the error message otherwise an error will occur "Error: Incorrect connection name" will appear.

Please Note: The input in the **Connection Name** field should only be in Latin characters, otherwise an error occurs and IPSec connection cannot be created.

The **Peer type** drop down list is used to choose the remote machine type for the IPSec Connection to be established. If the list does not include the required type of machine, choose **Other**.

The **VPN Network Topology** drop down list allows you to select the location of the peers participating to the VPN connection. The following options are present in the list:

- This device<>Peer – direct connection between QX gateway and a peer.
- This device <>[Internet]<>Peer – connection between QX gateway and peer over Internet.
- This device <>NAT<>[Internet]<>Peer – connection between QX gateway and peer over Internet through QX gateway provider's NAT.
- This device <>[Internet]<>NAT<>Peer – connection between QX gateway and peer over Internet through peer provider's NAT.

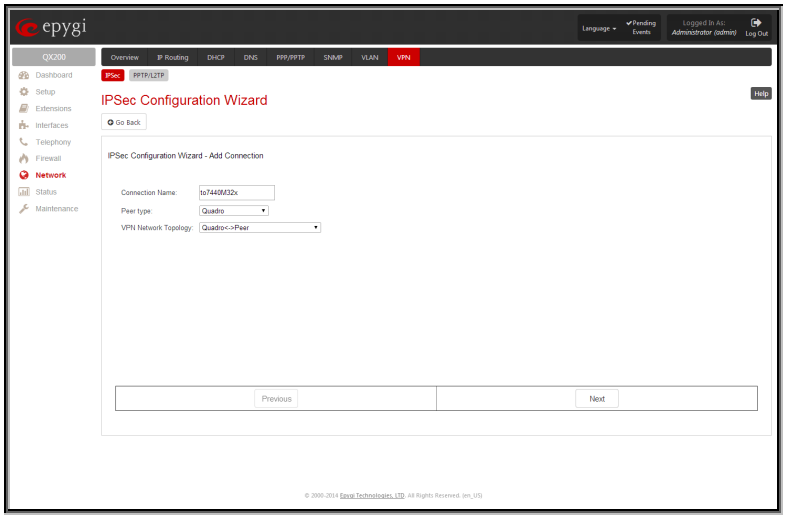


Fig.II- 146: IPSec Connection Wizard - Add IPSec Connection page

The next page of the wizard is **IPSec Keying Properties** which is used to select IPSec connection's security encryption settings.

Auto Keying requires the **IKE** (Internet Key Exchange) and **ESP** (Encapsulated Security payload) settings defined. **Encryption** and **Authentication** parameters should be defined.

The **Encryption** drop down list offers the following standards for selection:

- **Triple DES** uses three DES encryptions on a single data block with three different keys to achieve a higher security than is available from a single DES pass (block cipher algorithm with 64-bit blocks and a 56-bit key).
- **AES 128** bit cryptography scheme is a symmetric block cipher, which encrypts and decrypts 128-bit blocks of data.
- **AES 192** bit cryptography scheme is a symmetric block cipher, which encrypts and decrypts 192-bit blocks of data.
- **AES 256** bit cryptography scheme is a symmetric block cipher, which encrypts and decrypts 256-bit blocks of data.

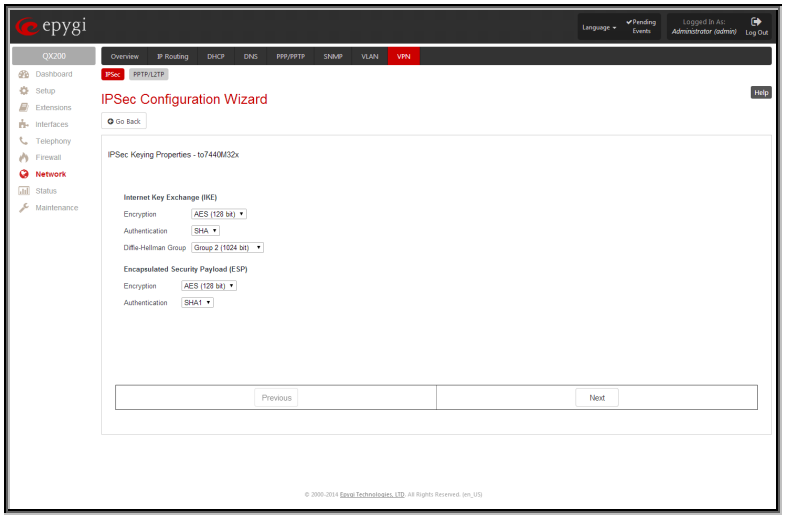


Fig.II- 147: IPSec Connection Wizard -IPSec Keying Properties page

The area Authentication offers the following parameters to be selected:

- **SHA/SHA1** (Secure Hash Algorithm) is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPSEC.
- **MD5** (Message Digest) is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.

The **Diffie-Hellman** parameter is used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group, which is based upon the prime numbers. The higher is the group bit rate, the better is encryption. If mismatched groups are specified on each peer, negotiation fails.

The third page of the IPSec Connection wizard, **Automatic Keying**, is used to setup a type of password (**Shared Secret**) or the **RSA** public key to secure your IPSec Connection. The functionality of **Perfect Forward Secrecy** (PFS) can be added to both. Following ways of automatic keying are available.

- **Shared Secret** is a type of password consisting of any characters that both of the IPSec Connection partners must know. The authentication will be done with this shared secret. All encryption functions below will remain concealed.

  Please Note: It is also not recommended to start multiple road warrior connections with the **Shared Secret** automatic keying selected. For multiple road warriors to be started at the same time, it is recommended to use RSA keying with **Local ID** and **Remote ID** fields configured.

- **RSA** requires the public RSA key of your IPSec Connection partner.

Please Note: System prevents to start a connection with **Shared Secret** automatic keying selected if there is already a connection with RSA automatic keying started, and vice versa.

The **Local ID** requires an IP address, QX gateway 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: qx@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: The **Local ID** and **Remote ID** values are mandatory for **RSA** selection and are optional for **Shared Secret** selection. However, it is recommended to define the **Local ID** and **Remote ID** values for multiple road-warrior connections.

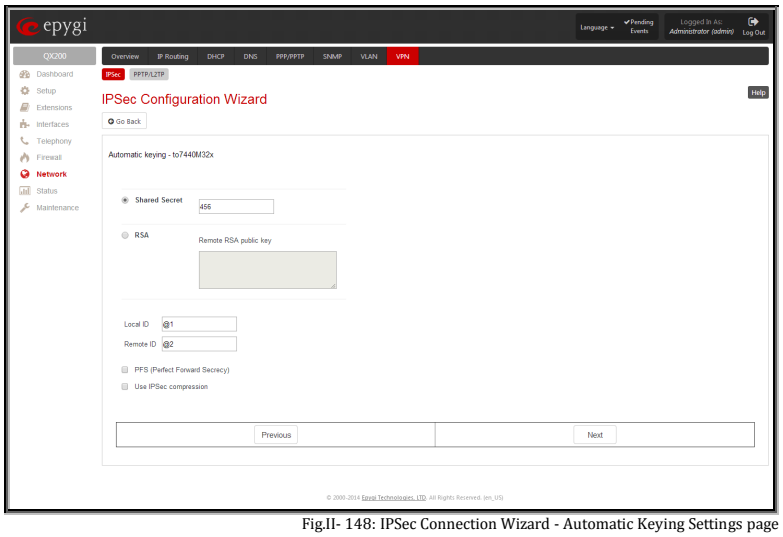


Fig.II- 148: IPSec Connection Wizard - Automatic Keying Settings page

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 forth page of the **IPSec Connection Wizard** contains **IPSec Connection Properties** which serve 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 QX IP PBX (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 QX gateway (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.

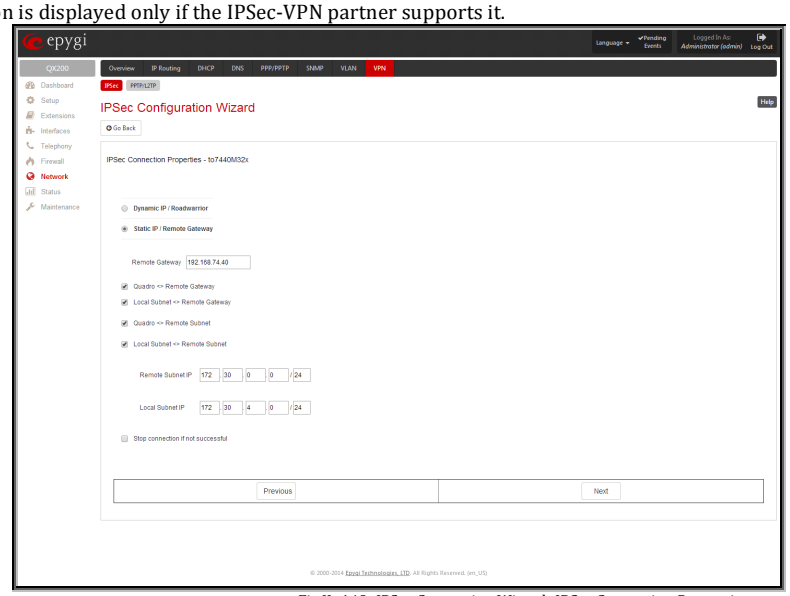


Fig.II- 149: IPSec Connection Wizard -IPSec Connection Properties page

This device <> Remote Gateway allows access from the local QX IP PBX to the remote VPN gateway (local subnet and remote subnet are not included). This includes management access. The checkbox is disabled when "This device<>NAT<>[Internet]<>Peer" or "This device<>[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 QX gateway and remote subnet are not included). The checkbox is disabled when "This device<>[Internet]<>NAT<>Peer" is selected from the **VPN Network Topology** drop down list on the first page of the **IPSec Connection Wizard**.

This device <> Remote Subnet allows access from the local QX gateway to all stations of the remote LAN (local subnet and remote VPN gateway devices are not included). The checkbox is disabled when "This device<>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.

To Delete/Stop/Start an IPSec Connection

1. Select one or more checkboxes of the corresponding connections that should to be deleted/stopped/started from the **Connections** tables.
2. Click on the **Delete/Stop/Start** button from the table's menu to perform the corresponding operation for the selected IPSec connection(s).
3. If deleting, confirm it with pressing on **Yes**. The IPSec connection will be deleted. To abort the deletion and keep the IPSec connection in the list, click **No**.

RSA Key Management

The **RSA Key Management** sub-page is used to see the current RSA key and to generate a new one. This page contains the following components:

The public key is displayed in the **RSA Public Key** text field so that the user may inform their IPSec connection partner about it, for example, via fax.

The user has the option of generating a new pair of keys by specifying the key length with the corresponding radio buttons **Generate a new 1024bit RSA Key** and **Generate a new 2048bit RSA Key** and then clicking the **Generate** Button.

A valid RSA key should fit to following requirements:

- RSA key doesn't start with "0s"
- RSA key doesn't end with "=="
- RSA key contains symbols other than Alphanum, +, /, =

The **Email this to the peer** text field requires the mailing address of the IPSec connection partner. The **Send** button will insert QX gateway's public RSA key into an e-mail and send it to the IPSec connection partner.

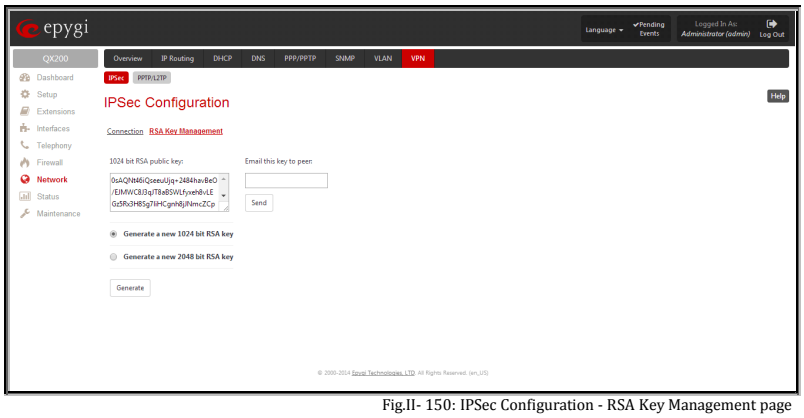


Fig.II- 150: IPSec Configuration - RSA Key Management page

PPTP/L2TP Configuration

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) is used to establish a virtual private network (VPN) over the Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers. PPTP encapsulates any type of network protocol (IP, IPX, etc.) and transports it over IP. Therefore, if IP is the original protocol, IP packets ride as encrypted messages inside PPTP packets running over IP. PPTP is based on point-to-point protocol (PPP) and the Generic Routing Encapsulation (GRE) protocol. Encryption is performed by Microsoft's Point-to-Point Encryption (MPPE), which is based on RC4.

L2TP (Layer **2 T**unneling **P**rotocol) is a protocol from the IETF, which allows a PPP session to run over the Internet, an ATM, or frame relay network. L2TP does not include encryption (as does PPTP), but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP network server (LNS) at the corporate side. Large carriers also may use L2TP to offer remote POPs to smaller ISPs. Users at the remote locations dial into the modem pool of an L2TP access concentrator, which forwards the L2TP traffic over the Internet or private network to the L2TP servers at the ISP side, which then sends them on to the Internet.

For **PPTP** and **L2TP Connections**, two parties are required: a **Client** and a **Server**. The client is responsible for establishing the connection. The server is waiting for clients, it is not able to initiate the connection itself.

Attention: L2TP tunnels have no data encryption mechanism.

The **Host Name** and a **Password** specify each side. The client should know the server's name and password (QX server has no password) and the server should set the client's host name and a password. The client and server settings have to match on both sides for successful connection establishment.

Clients and Servers are identified by their hostnames, which means that only one client can be connected to the server in the same network. Servers also define the range of IP addresses that are assigned to the Server and Client hosts participating in a connection.

The **PPTP/L2TP Configuration** link displays a page where a new PPTP and L2TP connection can be configured, as well as PPTP and L2TP server settings can be adjusted. The page consists of 3 sub-pages.

Connections

The **Connections** page lists all existing connections are listed, characterized by their **Connection Name**, **Type** of the connection (PPTP or L2TP), the **Client/Server** mode, the **State** of the connection and the **Remote Hostname IP** (the IP address or the hostname of the connection peer). The state of the PPTP and L2TP Connections, except for the "Stopped" state, is established as a link that refers to the page where logout information about the connection status is displayed. Logs can be useful to determine problems on PPTP or L2TP connections failure.

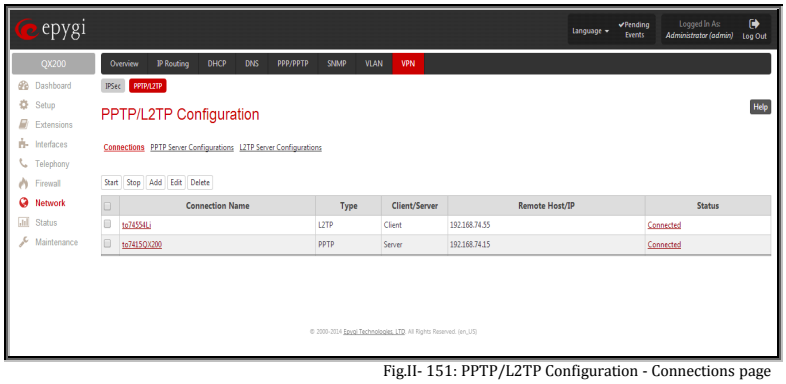


Fig.II- 151: PPTP/L2TP Configuration - Connections page

Add functional button leads to the **PPTP/L2TP Connection Wizard** page, where a new connection can be established.

Please Note: After creating a PPTP server connection, PPTP connections between devices placed on the QX gateway LAN and external devices will no longer be possible. The PPTP pass-through service for incoming and outgoing traffic will be automatically disallowed once a PPTP server connection is created.

The **PPTP/L2TP Connection Wizard** consists of several pages and allows you to create a new PPTP or L2TP connection.

The **PPTP/L2TP Connection Wizard – Page 1** consists of the following components:

Connection Name text field requires a connection identification name. The name of the connection cannot start with a digit symbol, however it can contain digits further in the name.

Connection Type drop down list allows to select the type of the connection (PPTP or L2TP).

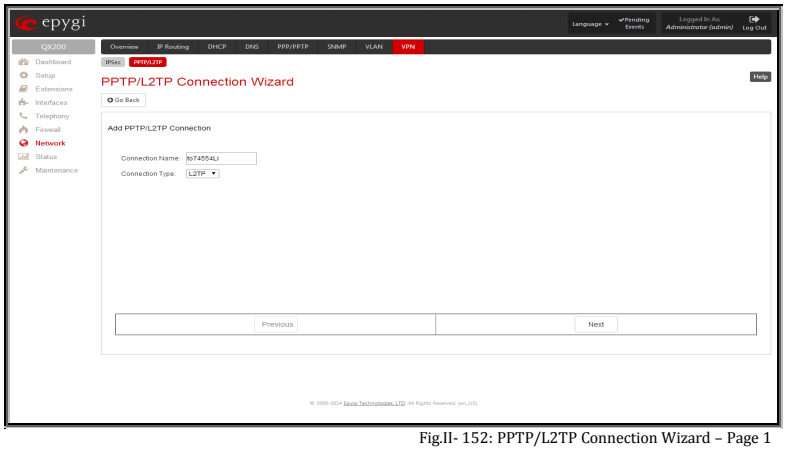


Fig.II- 152: PPTP/L2TP Connection Wizard – Page 1

The **PPTP/L2TP Connection Wizard – Page 2** consists of the following components:

The **Peer Name** text field requires the connection peer name. If you are about to create a client connection, then the server's name should be defined here. If you are creating a server connection, then the client's name should be defined here.

Please Note: When creating a connection with a Windows Server, ensure that a user with the QX gateway's host name and Dial-in access exists on the server. When creating a connection with a Windows Client, ensure that the Peer name specified on this page matches the Dial-in connection's username.

Please Note: The input in the **Peer Name** field should only be in Latin characters, otherwise an error occurs and no connection can be created.

The **Password** text field requires the password for the connection establishment.

Please Note: These authentication settings should be identically configured on both peers for the successful connection establishment.

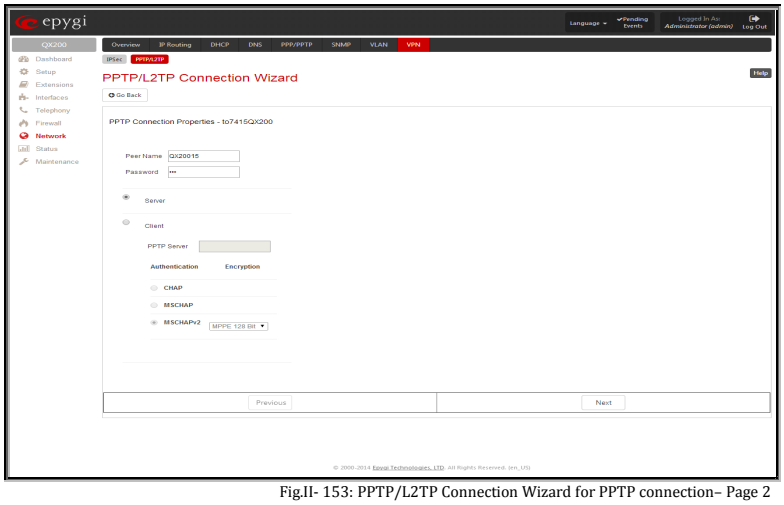


Fig.II- 153: PPTP/L2TP Connection Wizard for PPTP connection– Page 2

The manipulation radio buttons selection on this page allows you to choose whether the new connection will be a client or a server. For the **Client** radio button selection, no further details need to be provided. For the **Server** radio button selection, the following information needs to be provided:

For PPTP connection, the **PPTP Server** text field requires an IP address or a host name of the PPTP server. For L2TP connection, the **L2TP Server** text fields require an IP address of the L2TP server.

The **Authentication** manipulation radio buttons are only present if the **Connection Type** selected on the previous page is PPTP. They are used to select the corresponding authentication protocol by which the client communicates with the server. The **MSCHAPv2** selection enables the **Encryption** drop down list where the encryption method can be selected.

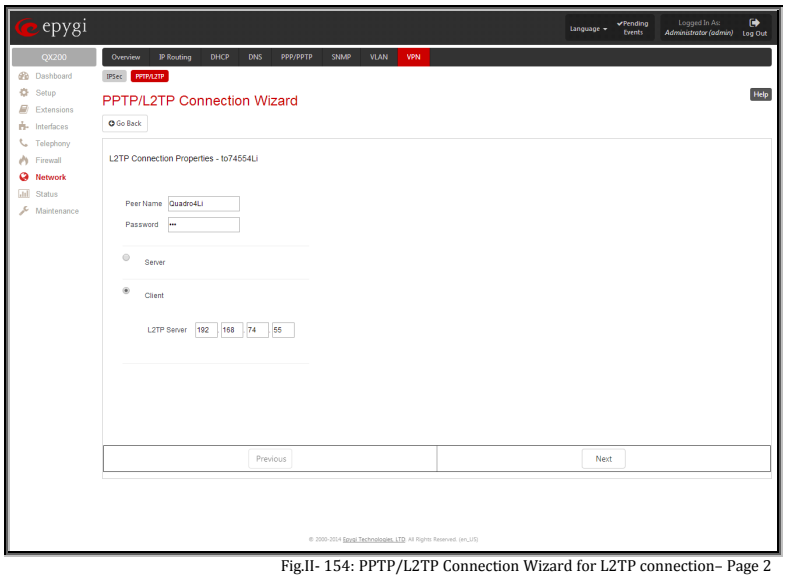


Fig.II- 154: PPTP/L2TP Connection Wizard for L2TP connection– Page 2

The **Start** functional button initiates the selected connection(s). If it is a client connection, then this button initiates a client activity of reaching the server. The **Start** option is applicable for multiple connections selected at the same time.

The **Stop** functional button is used to stop the selected connection(s). Stopping the server connection will disconnect all connected clients and close the PPTP/L2TP tunnel. The **Stop** option is applicable for multiple connections selected at the same time.

PPTP Server Configurations

The **PPTP Server Configuration** page is used to configure the PPTP server settings and offers the following components:

The **PPTP Subnet** text fields are used to enter the IP address range for the PPTP server and clients within the PPTP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the PPTP connection.

Please Note: The first address specified in the PPTP Subnet will be assigned to the PPTP server; others will be assigned to the clients. The PPTP server subnet should be different from the L2TP server subnet, otherwise a corresponding error message will appear.

The **Authentication** manipulation radio buttons are used to select the corresponding authentication protocol by which the client communicates with the server. The **MSCHAPv2** selection enables **Encryption** drop down list where the encryption method can be selected.

Fig.II- 155: PPTP Server Configuration page

L2TP Server Configuration

The **L2TP Server Configuration** page is used to configure the L2TP server settings and provides the following input options:

The **L2TP Subnet** text fields are used to enter the IP address range for the L2TP server and clients within the L2TP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the L2TP connection.

Please Note: The first address specified in the L2TP Subnet will be assigned to the L2TP server; others will be assigned to the clients. The L2TP server subnet should be different from the PPTP server subnet, otherwise a corresponding error message will appear.

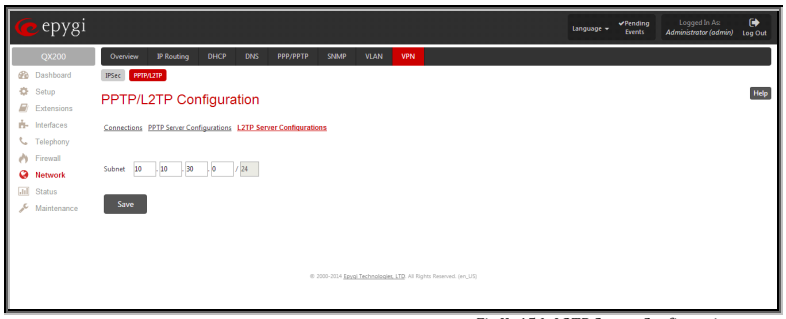


Fig.II- 156: L2TP Server Configuration page

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**.

To Manage an RSA key for the IPSec Connection

1. Press the **RSA Key Management** button on the **IPSec Connection Settings** page. The **IPSec Connection RSA Key** will appear in the browser window.
2. Select the RSA key length and press **Generate** to generate a new RSA public key. This may take several seconds.
3. Enter a destination e-mail address in the **Email this key to peer** text field, then press **Send** to send the new RSA public key.

To Delete/Stop/Start a PPTP/L2TP Connection

1. Select one or more checkboxes of the corresponding connections that should to be deleted/stopped/started from the **Connections** tables.
2. Click on the **Delete/Stop/Start** button from the table's menu to perform the corresponding operation for the selected PPTP/L2TP connection(s).
3. If deleting, confirm it with pressing on **Yes**. The PPTP/L2TP connection will be deleted. To abort the deletion and keep the PPTP/L2TP connection in the list, click **No**.

Status Menu

The **System Status** menu consists of the following sections:

- **System Status**
  - General Information
  - Network Status
  - Lines Status
  - Memory Status
  - Hardware Status
  - SIP Registration Status
- **Events**
  - System Events
  - Event Settings
- **Call History**
  - Successful, Missed and Unsuccessful Calls
  - CDR Settings
  - Automatic Backup
- **LAN/WAN**
  - LAN and WAN Interface Statistics
- **Statistics**
  - Network Transfer
  - PSTN Channel Usage

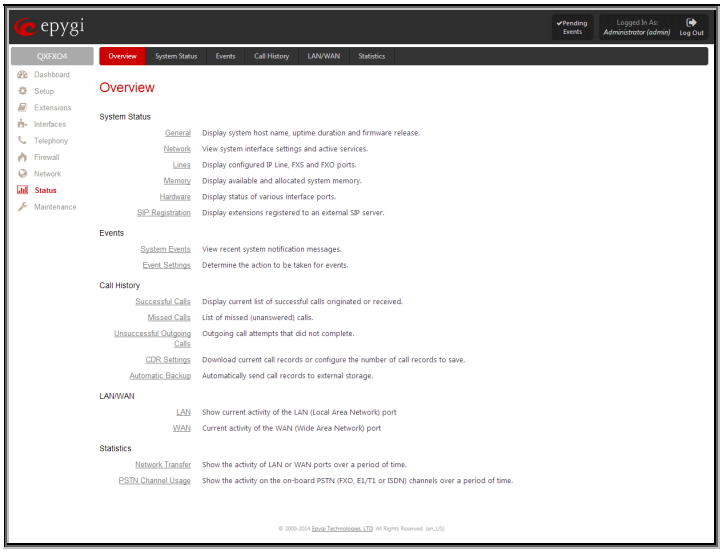


Fig.II- 157: System Status Menu page

System Status

General Information

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

- **Uptime duration -** Period QX is running since last reboot.
- **Device hostname -** QX device host name.
- **Application Software -** Software and file system versions of the QX.
- **Language Pack** – this field is present only when the custom language pack is uploaded and it indicates the version.

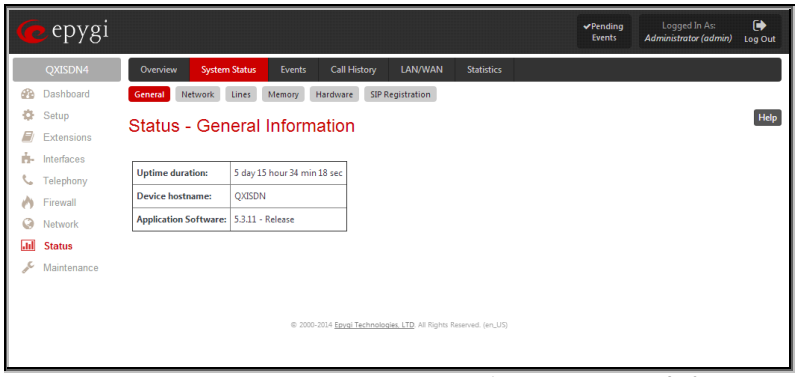


Fig.II- 158: System Status - General Information page

Network Status

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

Interface Name lists the Network interfaces available on the QX (LAN, WAN and a number of PPPs, depending on the number of active PPP connections).

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

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

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

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

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

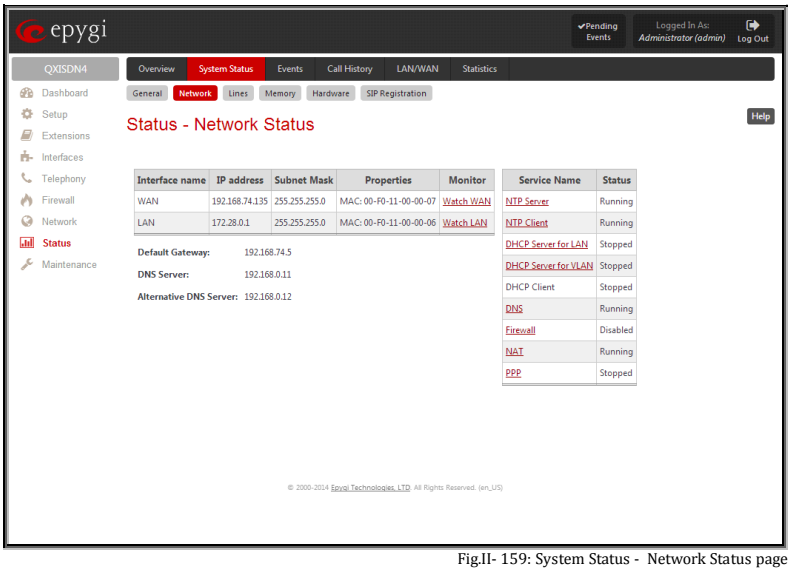


Fig.II- 159: System Status - Network Status page

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 QX 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**.

Lines Status

The table **Status - Lines Status** shows the current status of each FXS, FXO line, ISDN or E1T1 trunk (depending on QX gateway model) with all details of active call. Since only one line information is displayed at a time, the FXS, FXO line, ISDN or E1T1 trunk functional buttons are used to navigate through the other lines'/trunks' information. It shows only the information for one of the line/trunk at a time. To navigate through the other lines'/trunks' information select the link with the appropriate line number on the top of the page.

The **FXO Channel Usage Statistics** link (available for QXFXO4 gateways only) is only present for local FXO lines (this option is not available for shared FXO lines) and leads to the Statistics - PSTN Channel Usage page where diagram chart of FXO lines usage can be viewed.

The **ISDN Channel Usage Statistics** link (available for QXISDN4 gateways only) is only present for local ISDN lines (this option is not available for shared ISDN trunks) and leads to the Statistics - PSTN Channel Usage page where diagram chart of ISDN trunks usage can be viewed.

The **E1/T1 Channel Usage Statistics** link (available for QXE1T1 gateways only) is only present for local E1/T1 lines (this option is not available for shared E1/T1 trunks) and leads to the Statistics - PSTN Channel Usage page where diagram chart of E1/T1 trunks usage can be viewed.

Memory Status

The **Memory Status** page includes tables with the available **User Space** information for each extension. These tables display the space used by the 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 QX 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 History shows the current number of calls with recorded statistic entries.

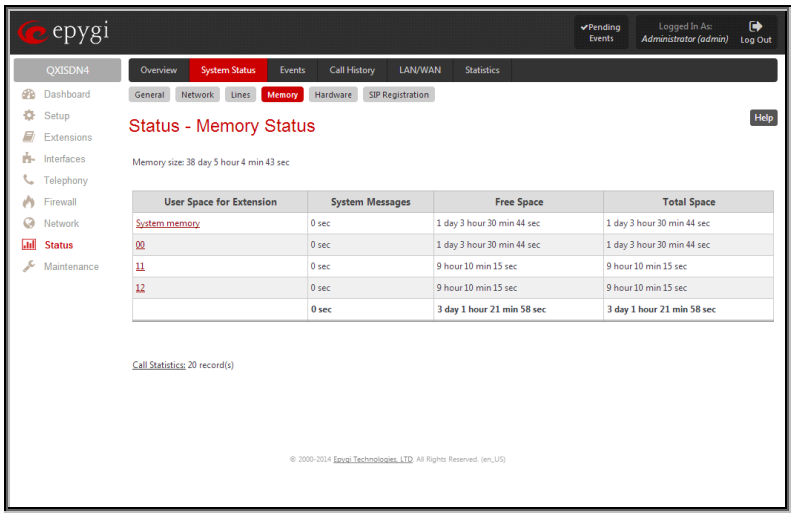


Fig.II- 160: System Status - Memory Status page

Hardware Status

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

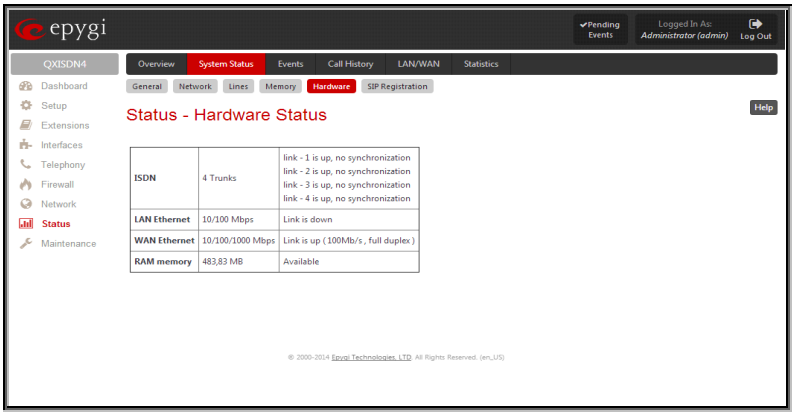


Fig.II- 161: System Status - Hardware Status page

SIP Registration Status

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

The table contains a list of all the registered extensions of the QX, 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 page where the SIP registration settings may be altered.

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

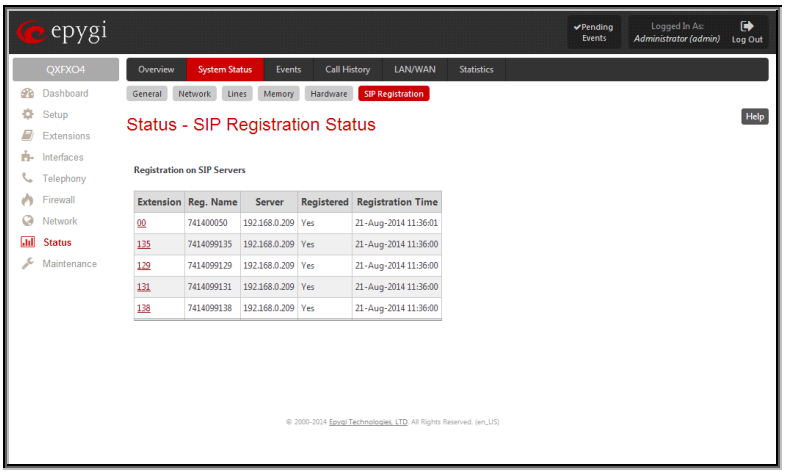


Fig.II- 162: System Status - SIP Registration Status page

Events

System Events

The **System Events** page lists information about system events that have occurred on QX gateway. 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 upper-right corner 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".

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 by the IDS service, the **Check IDS** link appears in the reference row that will lead to the IDS Log page, or if the event has occurred due to incorrect mail sending or SIP registration, the corresponding links will be seen in the **Reference** column of the table. The administrator can view the detailed log for each event that has occurred.

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

Current System Time displays the local date and time on QX gateway.

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

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

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

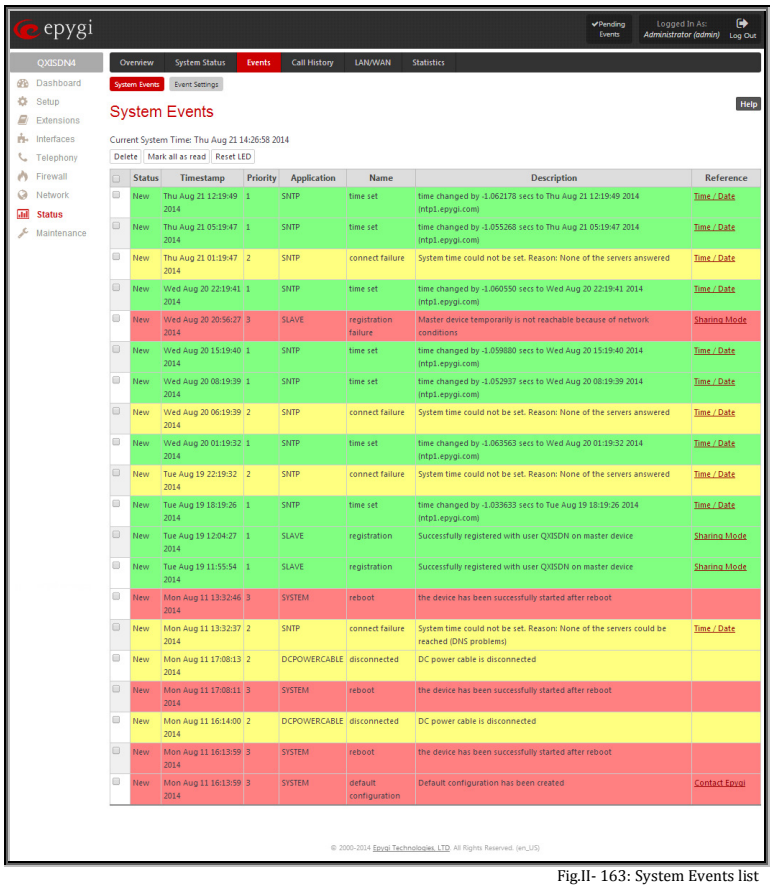


Fig.II- 163: System Events list

Event Settings

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

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

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

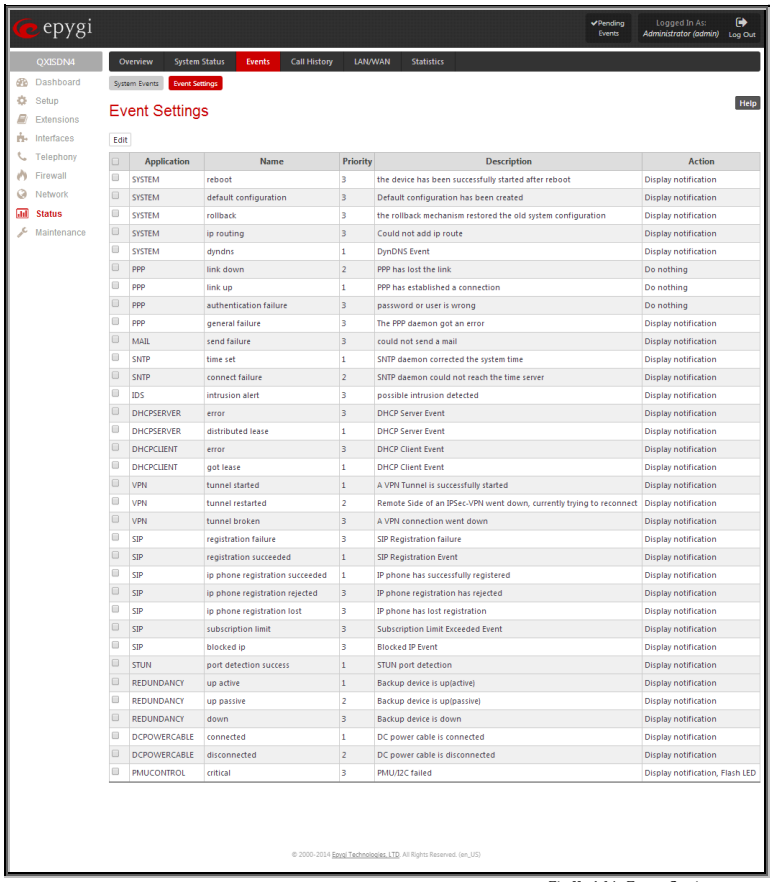


Fig.II- 164: Event Settings page

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 QX gateway administrator when an event(s) takes place. The following actions can be available:

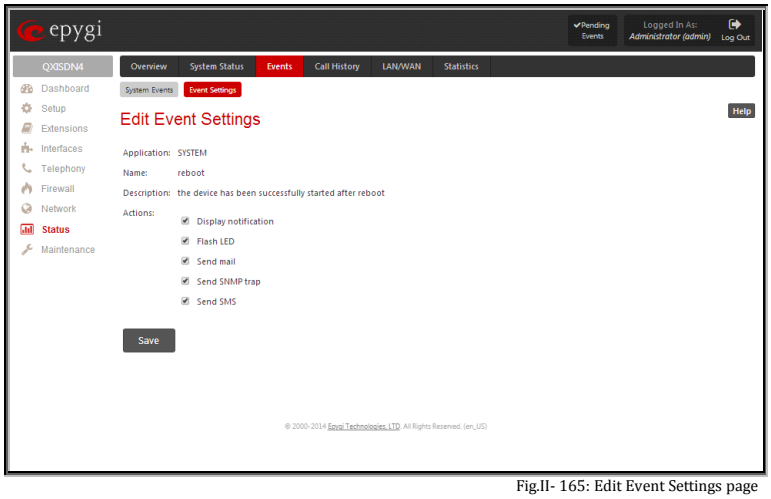


Fig.II- 165: Edit Event Settings page

- **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 your 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 flash LED (ORANGE) will blink every second and a notification will be displayed on the bottom of all pages. For some events the LED will start flashing after a delay.
- **Send Mail** – an email notification about the new event on the QX gateway will be sent to the e-mail address specified in the Mail Settings page.
- **Send SNMP Trap** – SNMP notification will be sent to the traphost(s) listed in the SNMP Trap Settings table (see SNMP Trap Settings).
- **Send SMS** – SMS notification (not available for QXFXS24 gateway) about the new event on the QX gateway will be sent to the mobile phone specified in the SMS Settings page.

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

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

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

To Assign an Action to the Event

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

Call History

The **Call History** page provides information on Successful, Missed, Unsuccessful Outgoing Calls, Call History Settings, CDR Settings and Automatic Backup. Call History allows the collecting of call events on the QX gateway with their parameters and to search them by various criteria. The selected number of statistics entries will be displayed in the Call History tables.

The Call History page reports successful, non-successful and missed incoming/ outgoing calls and shows the Call History settings. Only administrator is allowed to enable or disable the call statistic services.

Successful, Missed and Unsuccessful Calls

The **Successful Calls**, **Missed Calls** and **Unsuccessful Outgoing Calls** pages lists successful, missed and unsuccessful incoming and outgoing calls and their parameters (Call Start Time, Call Duration, Calling Phone and Called Phone). Each column heading in the tables is 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 close to the column heading.

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 History: 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 Filter button performs searching within the statistics tables. The search may be done with several criteria at the same time.

The following search criteria are available:

- The text fields **From** and **To** are used for the search by **Call Start Time**. The data must be entered in the format dd-mm-yyyy hh:mm:ss. The time criteria are optional, if it is not needed, leave the text fields empty. The **From** field must indicate an earlier date and time from that which is indicated in the **To** field. Otherwise the error message "Minimal date should be less than maximal date" prevents filtering and searching.
- The **From** and **To** drop down lists offer a search by the **Call Duration**, specified by the list of values. The field **From** must indicate a shorter duration than the field **To**. Otherwise the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.

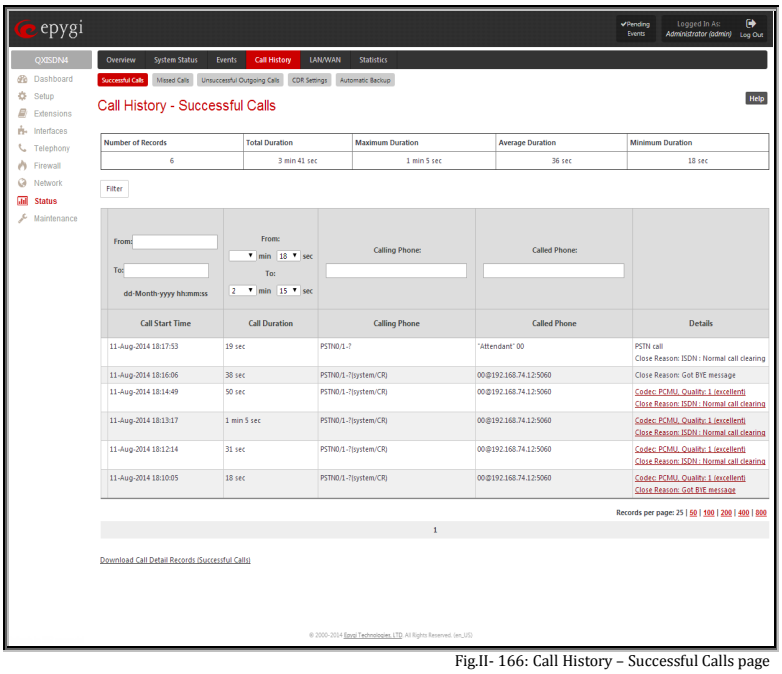


Fig.II- 166: Call History – Successful Calls page

- The text fields **Calling Phone** and **Called Phone** require the calling and called party's SIP address, extension number or PSTN number as search criterion. Wildcard symbols are allowed here.

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

The **Details** column (available for the administrator) is only present in **Successful Calls** table and provides the following information:

- Brief information about the call quality, voice codec used to receive and transmit packets and the close call reason. The close call reason appears to provide more information about the call termination reason which can be a network problem, termination by one of the call parties, voice

mail service activation, etc. Clicking on the details information will open the RTP Statistics page where all RTP parameters of established call are provided.

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

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

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

The **Records per page** are used to select the number of displayed statistic records per page. The **Previous** and **Next** can be utilized to switch between these pages.

The **Download Call Detail Records** links are available below for all Call History tables (for administrator's access only) and allows you to download the displayed Call History in a text file.

CDR Settings

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

The **Enable Call Reporting** checkbox enables Call History reporting. The selected number of statistics entries will be displayed in the Call History 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 History** tables. If the record numbers exceed the numbers specified in these drop down lists, the oldest record will be removed.

The **Download All Call Detail Records** link is used to download the entire displayed statistics in a file that can be viewed with a simple text editor. This type of Call History file is easy-to-read and can be displayed in a spreadsheet.

The **Download All Call Detail Records (CSV format)** link is used to download the entire displayed statistics in CSV (Comma-Separated Values) formatted file.

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

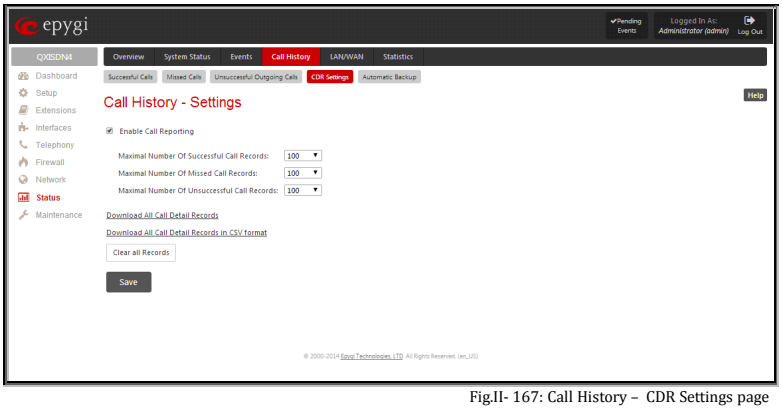


Fig.II- 167: Call History – CDR Settings page

When the number of Call History entries exceeds the numbers specified in the **CDR Settings** page, the oldest entries are being automatically deleted. In order to keep the Call History entries safe, QX IP PBX allows you to configure the Automatic Backup service of the Call History.

Automatic Backup

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

The **Enable Automatic Downloading of Call Detail Records** checkbox enables automatic downloading mechanism of the call statistics.

Please Note: This service only refers to the statistics collected from the moment of enabling this service and forward; any previously generated statistics will not be downloaded.

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

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

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

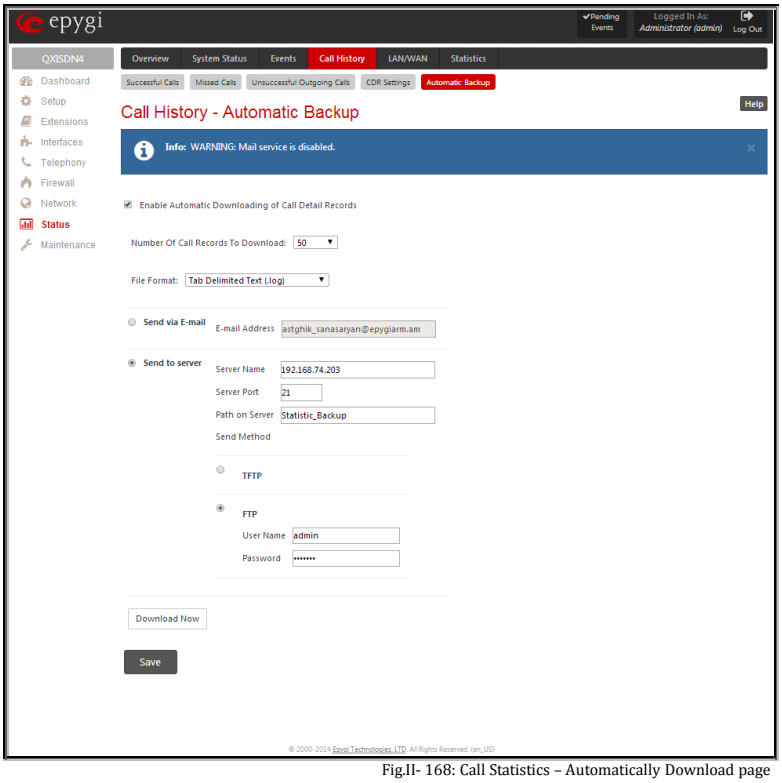


Fig.II- 168: Call Statistics – Automatically Download page

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

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

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

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

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

To Enable/Disable the Call History

1. Enter the **CDR 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 Call History

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

Please Note: To return to the complete **Call History** table, clear all search criteria and press **Filter**.

To Reset the Call History

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

RTP Statistics

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

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

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

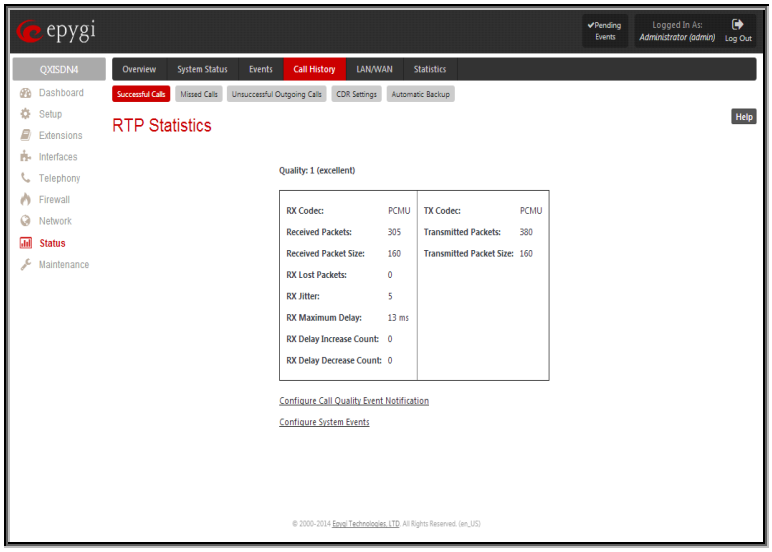


Fig.II- 169: RTP Statistics page

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

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

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

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

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

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

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

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

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

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

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

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

Rx Maximum Delay = max V(i) / 8

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

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

Please Note: RTP Statistics is logged only when at least one of the call endpoints is located on the QX. 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 QX gateway's routing rules.

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

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

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

FAX Statistics

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

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

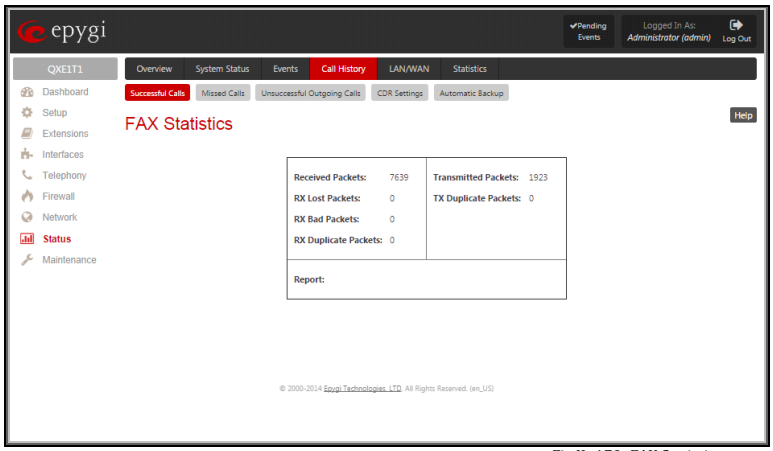


Fig.II- 170: FAX Statistics page

LAN/WAN

LAN and WAN Interface Statistics

The **LAN** and **WAN Interface Statistics** pages display the LAN and WAN statistics. The table displayed here shows the number of receive and transmit events that occurred since the last resetting of the counters by pressing the **Clear** button.

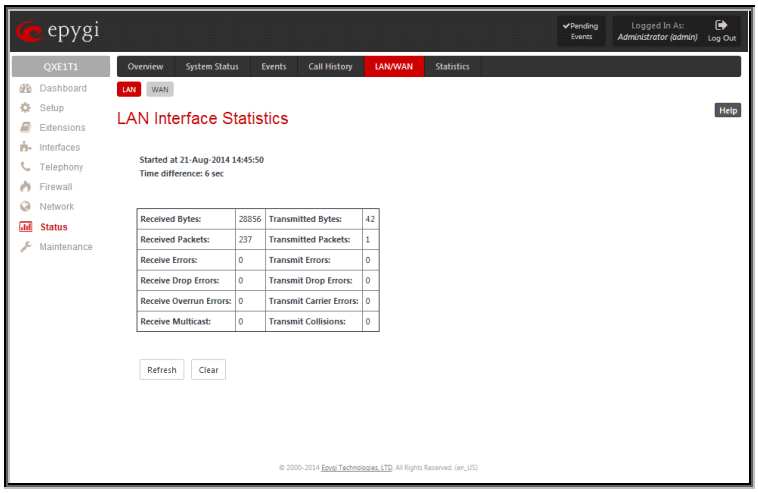


Fig.II- 171: lAN Interface Statistics page

Depending on the **Watch LAN** or **Watch WAN Monitor** link selected on the Network Status page, the **LAN Interface Statistics** or **WAN Interface Statistics** page will be diaplayed.

The page is automatically refreshed every minute. Additionally the **Refresh** button allows to initiate refreshing directly.

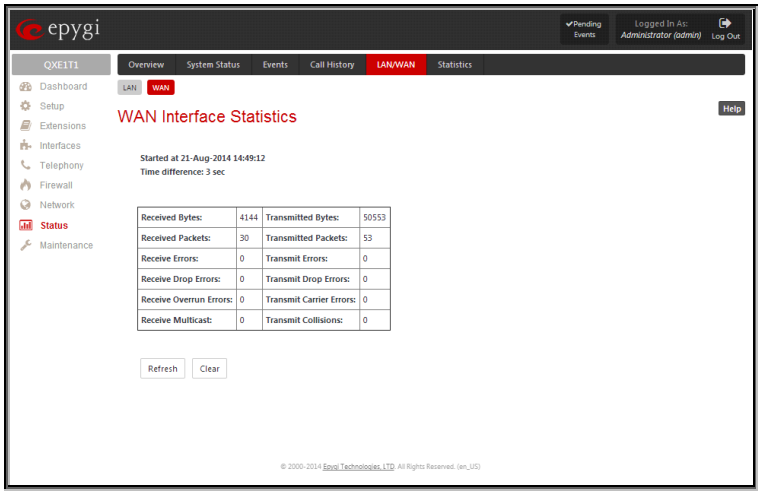


Fig.II- 172: WAN Interface Statistics page

Statistics

Network Transfer

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

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

Interface - the drop-down list offer the values:

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

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

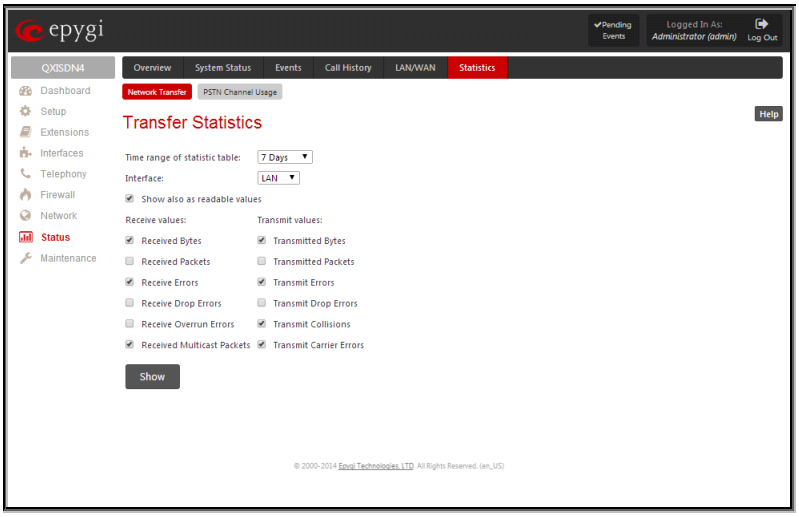


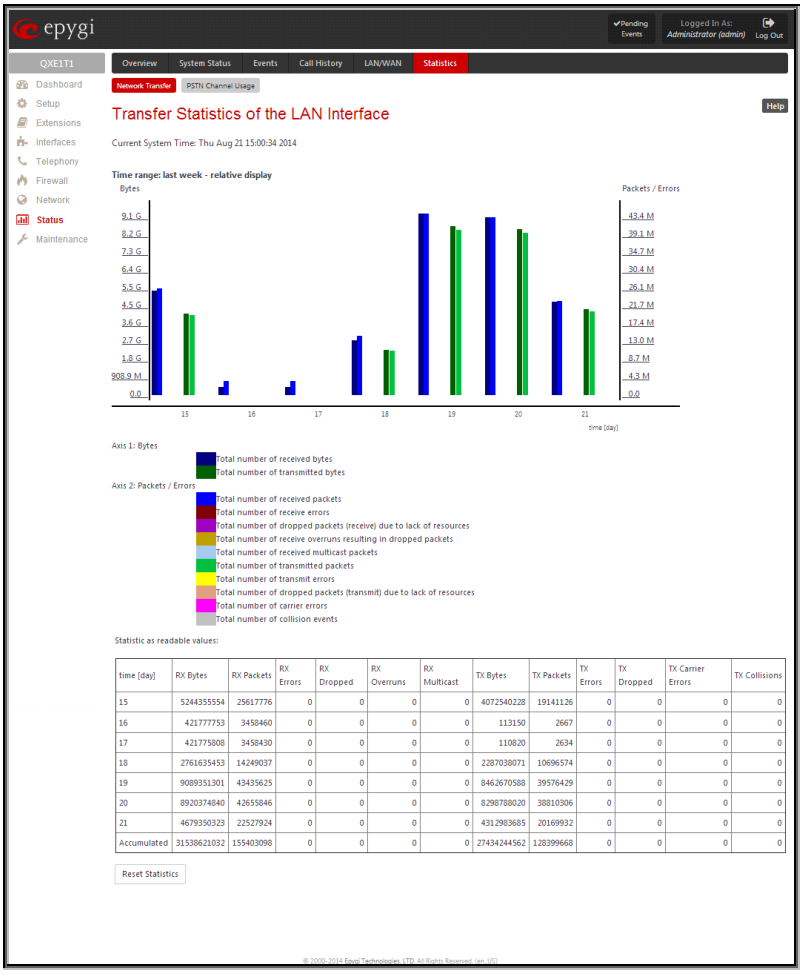
Fig.II- 173: Transfer Statistics page

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.



time [day]	RX Bytes	RX Packets	RX Errors	RX Dropped	RX Overruns	RX Multicast	TX Bytes	TX Packets	TX Errors	TX Dropped	TX Carrier Errors	TX Collisions
15	5244355554	25617776	0	0	0	0	4072540228	19141126	0	0	0	0
16	421777753	3458460	0	0	0	0	113150	2667	0	0	0	0
17	421775808	3458430	0	0	0	0	110820	2634	0	0	0	0
18	2761635453	14249037	0	0	0	0	2287038071	10696574	0	0	0	0
19	9089351301	43435625	0	0	0	0	8462670588	39576429	0	0	0	0
20	8920374840	42655846	0	0	0	0	8298788020	38810306	0	0	0	0
21	4679350323	22527924	0	0	0	0	4312983685	20169932	0	0	0	0
Accumulated	31538621032	155403098	0	0	0	0	27434244562	128399668	0	0	0	0

Fig.II- 174: 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).

PSTN Channel Usage

The trunk checkboxes are used to select the port number(s) over which the FXO, ISDN or E1/T1 (depending on QX gateway model) traffic chart will be built. At least one **Trunk** checkbox should be selected, otherwise error message appears.

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

Incoming Calls and **Outgoing Calls** checkboxes are used to select whether the FXO, ISDN or E1/T1 (depending on QX gateway model) traffic statistics for only incoming or outgoing or for both type of calls should be displayed in the diagram chart.

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

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

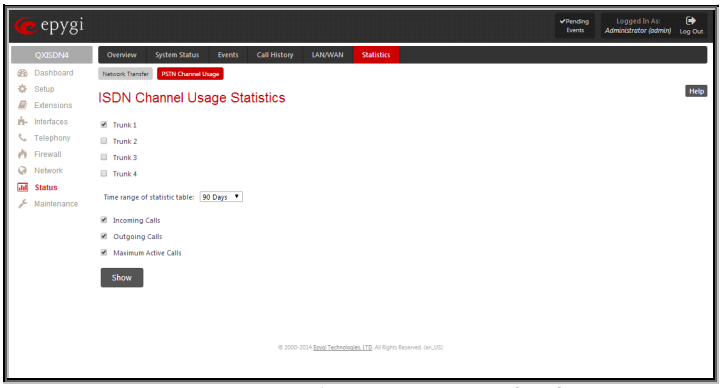


Fig.II- 175: QXISDN4 gateway - ISDN Channel Usage Statistics page

Show button is used to generate an FXO, ISDN or E1/T1 (depending on QX gateway model) channels usage diagram chart over the parameters selected above.

When this button is pressed, **FXO, ISDN** or **E1/T1** (depending on QX gateway model) **Channel Usage Statistics** chart appears. It represents dependency between the time frame and the number of calls performed during that period. Additionally it may display the maximum number of calls performed in the selected time frame.

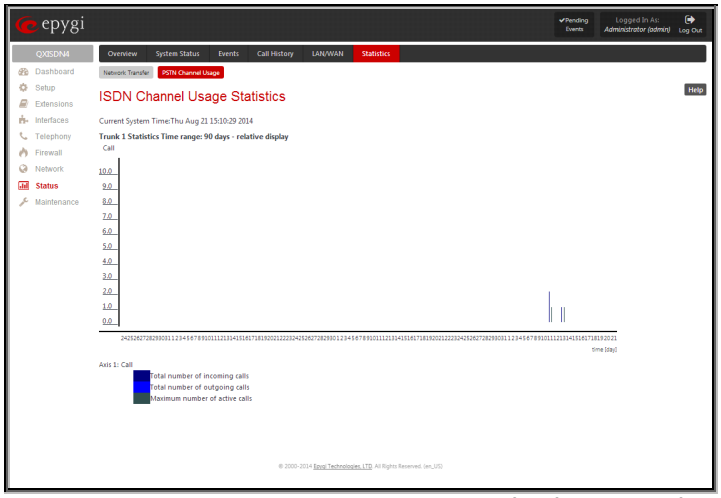


Fig.II- 176: QXISDN4 gateway - ISDN Channel Usage Statistics chart

Maintenance Menu

The **Maintenance** menu allows you to configure the following settings:

- **Diagnostics**
  - Security Diagnostics
  - Call Capture
  - Ping
  - Traceroute
- **System Logs**
  - System Logs Settings
  - Remote Logs Settings
- **User Rights Management**
  - Users
  - Roles
- **Backup/Restore**
  - Automatic Backup
  - Download Legible Configuration
  - Upload Legible Configuration
- **Firmware Update**
  - Upload Firmware
  - Get Firmware From Server
  - Automatic Firmware Update
- **Reboot**

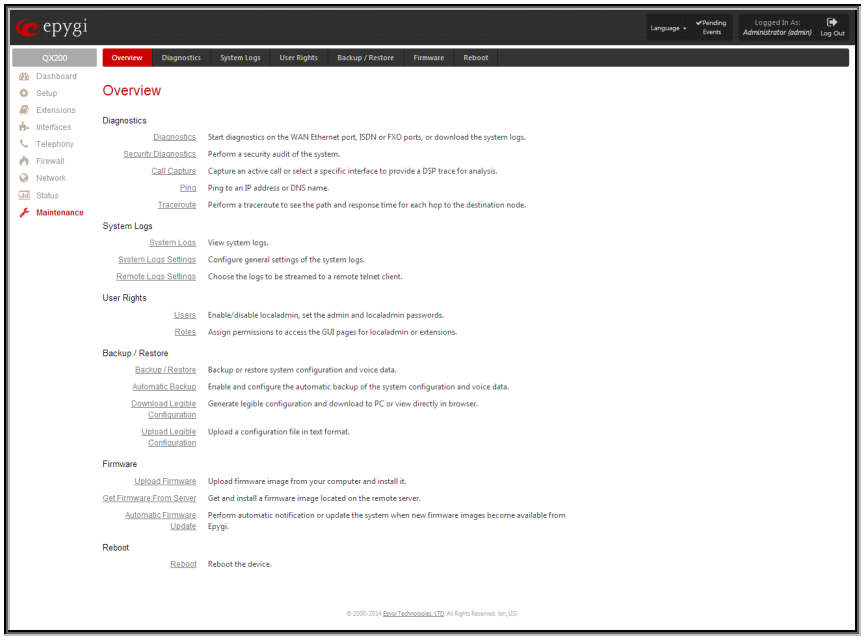


Fig.II- 177: Maintenance Menu page

Diagnostics

The **Diagnostics** page gives a possibility of running Network protocol diagnostics to verify QX gateway's connectivity and to download all system logs for possible problems recovery.

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 FXO Diagnostics** button (available only for QXFXO4 gateway) runs FXO diagnostic tests to determine the optimal value for the FXO country specific regional setting (CSRS) appropriate to your PSTN provider. Once the FXO diagnostic is complete, the recommended value should be set manually on the fxocfg hidden page. Setting this value may resolve echo or poor audio quality issues on FXO lines.

The **Start ISDN Diagnostics** (available only for QXISDN4 gateway) 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.

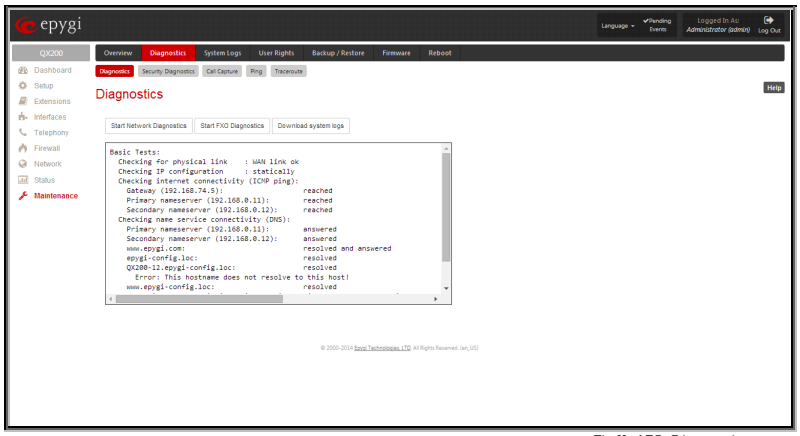


Fig.II- 178: Diagnostics page

The **Start E1/T1 Diagnostics** (available only for QXE1T1 gateway) button is used to initiate E1/T1 **Link Diagnostic** and **Diagnostic Loopback**. With these tests E1/T1 physical link is checked, Frame Synchronization and Red Alarm states are verified. For successful **Link Diagnostic**, remote side should have Line_loopback or Payload_loopback settings configured or a loopback terminator should be plugged to the QX gateway's E1/T1 port. **Diagnostic Loopback** will be initiated if **Link Diagnostic** is failed or E1/T1 link is down.

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 QX gateway.

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

Security Diagnostics

The **Security Diagnostics** page allows running the security audit and getting the security reports. The **Start Security Audit** functional button is used for running the security audit. The QX Security Audit is a security reporting system, which generates the warnings regarding the QX gateway's weaknesses relative to the selected **Security Level**. The warnings may vary depending on the selected global Security Level. The Security Audit will detect the security related configuration issues in Firewall, IDS, Call Routing and extension settings.

The output of Security Audit may look as follows:

Start security audit ...

Checking ...
Firewall ... done
Call Routing ... done
Extensions ... done
Users ... done

Settings do not correspond to selected security level.
You can view the complete report by clicking the 'Show the latest security report' link below.

done.

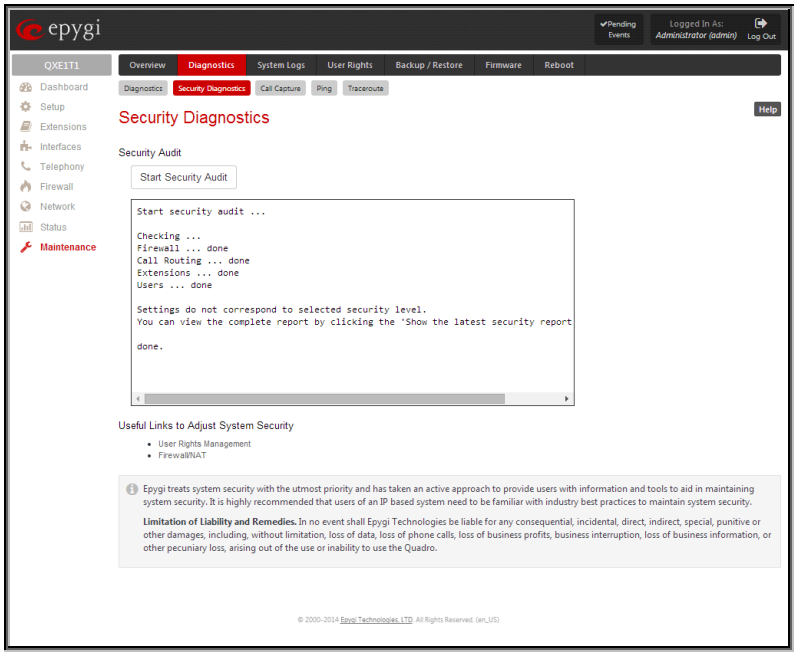


Fig.II- 179: Security Diagnostics page

The **Show Security Report** link allows to display the last security audit report.

This page also contains the following useful links to adjust the system security:

- User Rights Management
- Firewall/NAT

Call Capture

The **Call Capture** page is used to capture the voice streams on the active calls and the available interfaces on the QX gateway (FXS, FXO, E1/T1 or ISDN – depending on QX gateway model). This page consists of two sub-pages:

The **Active Calls** sub-page lists all FXO, FXS, ISDN or E1/T1 (depending on QX gateway model) active calls on the QX gateway for the certain moment.

- **Capture Timeout** text field requires the time period (in seconds) during which the call will be captured.
- **Start** button is used to start the active call capture. To do that a checkbox beside an active call in the table should be selected and **Start** button should be pressed. Note, that only one call can be captured at the same time. The **Stop** button appears when the call capture procedure is in progress and is used to stop the capture procedure.
- **Download Capture** and **Remove Capture** links appear on the page once the call is already captured. The **Download Capture** link is used to download the captured call as an archived *.tar file which contains two streams (receive and transmit) of the corresponding call. The files can be then played with an audio application. The **Remove Capture** link is used to remove the captured audio stream.

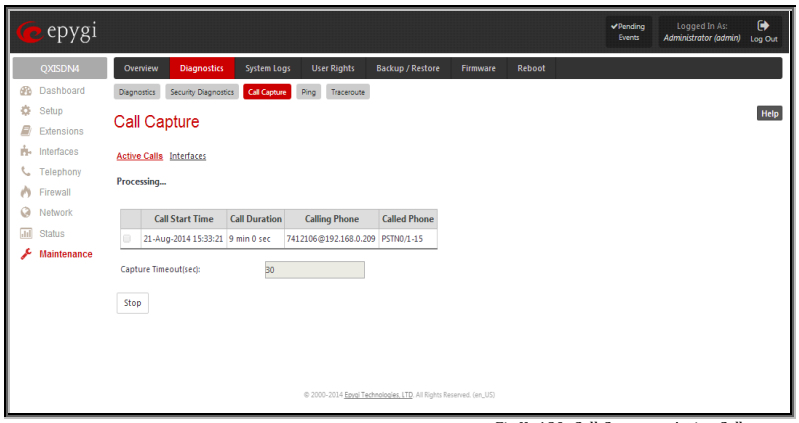


Fig.II- 180: Call Capture – Active Calls page

The **Interfaces** sub-page lists all available interfaces on the QX gateway. Manipulation radio-buttons allow you to select the needed line or trunk to be captured.

- **Capture Timeout** text field requires the time period (in seconds) during which the selected interface will be captured.
- **Start** button is used to start the capture of the selected interface. The **Stop** button appears when the interface capture procedure is in progress and is used to stop the capture procedure.
- **Download Capture** and **Remove Capture** links appear on the page once the selected interface is already captured. The **Download Capture** link is used to download the captured stream as an archived *.tar file which contains two streams (receive and transmit) of the corresponding stream. The files can be then played with an audio application. The **Remove Capture** link is used to remove the captured audio stream.

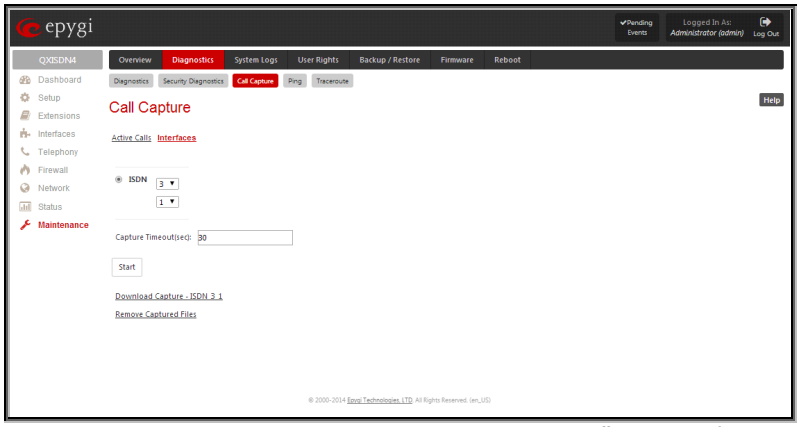


Fig.II- 181: Call Capture - Interfaces page

Ping

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.

Ping Target requires the destination (IP address or host name) for the ping request. If **Use ICMP** checkbox is selected, an ICMP request will be send to the ping destination (MS Windows standard). Otherwise, if checkbox is not selected, a UDP request will be send (Linux standard).

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

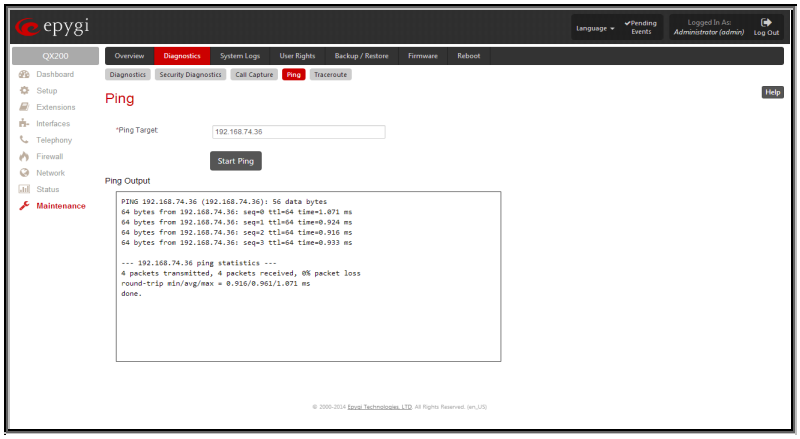


Fig.II- 182: System Diagnostic - Ping page

Traceroute

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

The **Start 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.

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.

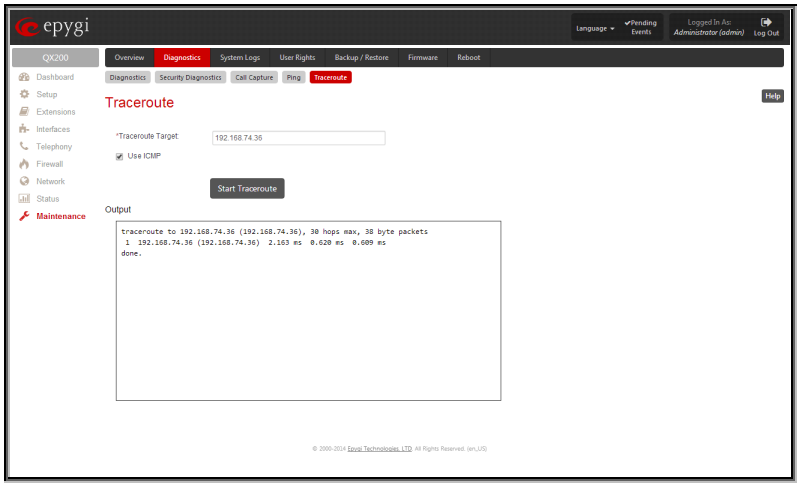


Fig.II- 183: Diagnostics – Traceroute page

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.

To Check the Internet connection

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

System Logs

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

On the left side of the page, a list of main logs is displayed. Clicking on the needed link will display the most recent log lines. The number of log lines displayed on this page is set on the System Logs Settings page.

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

If the user has used **Logs Collection** (*82) feature code after or during (from another phone connected to the same QX gateway) the call, a special log file will be generated containing the details of that call and few last calls done in the system. This log file will be internally kept in the system until the next time someone used the **Logs Collection** feature code again. The collected logs will be a part of the **System Logs** when user downloads them next time, so it can be reviewed by appropriate support staff. This could be used to collect the logs at the exact moment when a problem has happened.

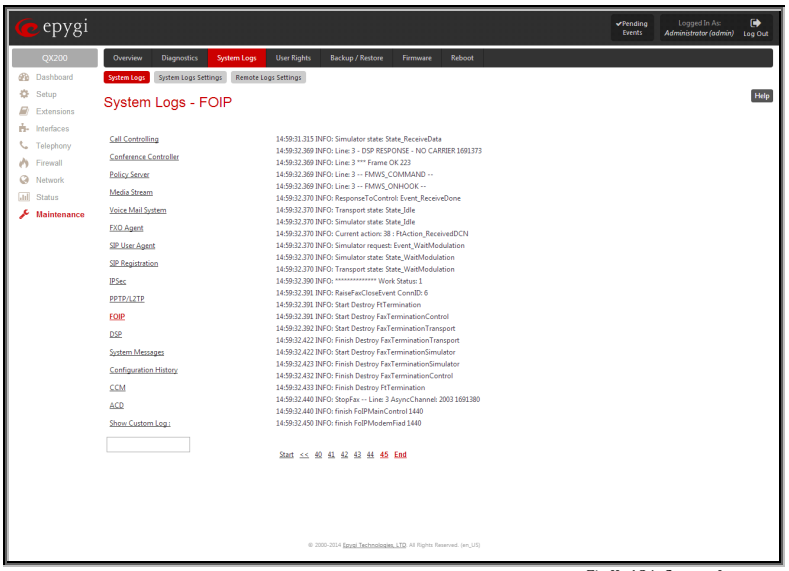


Fig.II- 184: System Logs page

System Logs Settings

This page is used to adjust system logging settings, view system logs directly in your browser or download them locally to your PC.

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

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

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

The **Log Lines to Show** drop down list is used to choose the maximum number of log lines to display on the System Logs page.

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

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

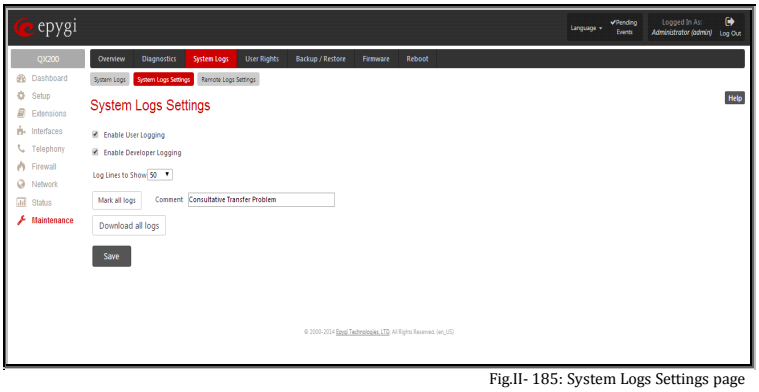


Fig.II- 185: System Logs Settings page

Remote Logs Settings

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

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

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

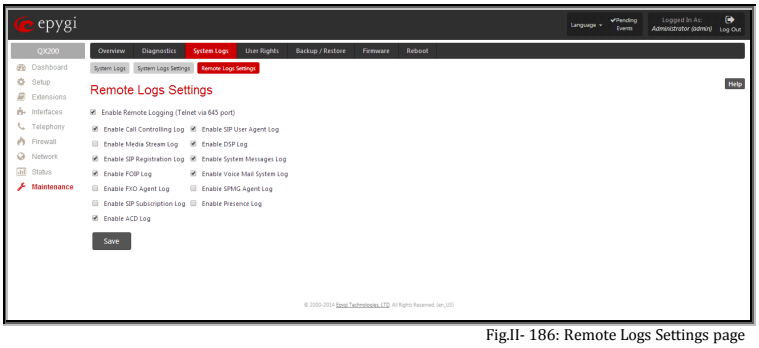


Fig.II- 186: Remote Logs Settings page

User Rights Management

The **User Rights** 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 QX gateway. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the QX gateway's configuration. The **User Rights Management** page consists of two pages. The Users page is used to manage the available users on the QX gateway. The Roles page is used to assign the corresponding permissions to the users.

Users

The **Users** page contains a table where the Administrator and Local Administrator users are listed. This page allows them to modify the passwords of available users in the table and to manage the Local Administrator's account.

Two levels of QX gateway 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 QX gateway. 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 following functional buttons are available on this page:

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

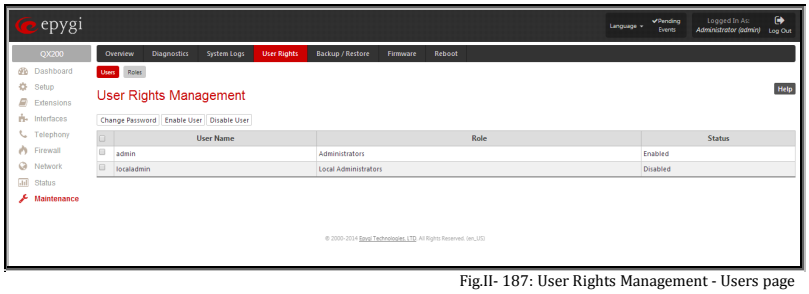


Fig.II- 187: User Rights Management - Users page

For **Administrator** or **Local Administrator** account the **Change Password** page contains two parts - one for **GUI Access Password**, the other one for **Phone Access Password**.

The **GUI Access Password** 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 **New Password** field is checked against its strength and you may see how strong is your inserted password right below that field.

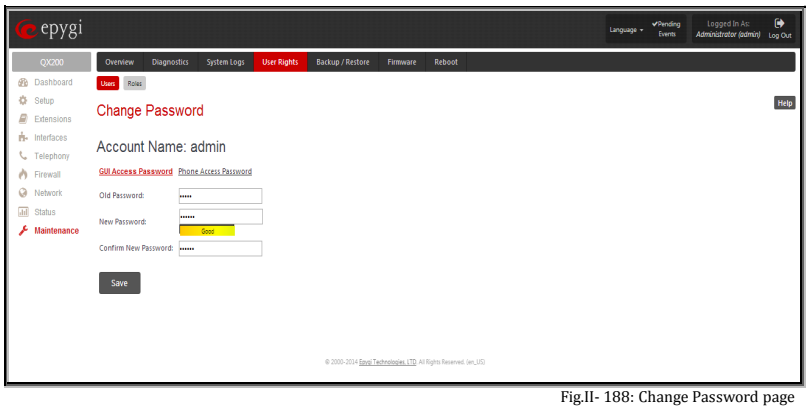


Fig.II- 188: Change Password page

Please Note: The password can consist of numeric values and symbols. Up to twenty (0-20) digits and symbols are allowed.

The **Phone Access Password** offers the following components:

- The **Old Password** text field is 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 **New Password** field is checked against its strength and you may see how strong is your inserted password right below that field.

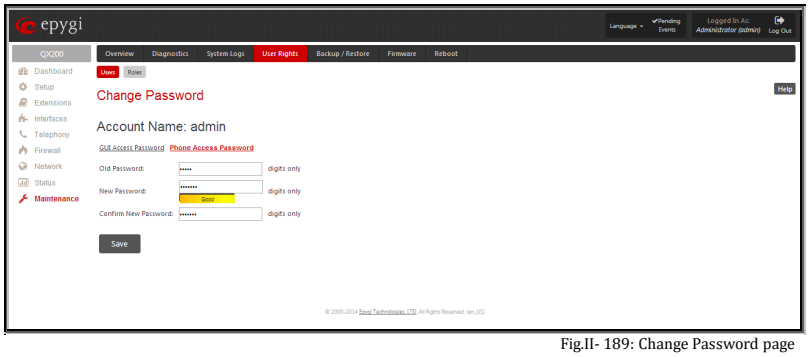


Fig.II- 189: Change Password page

Please Note: The password can consist of numeric values only. Up to twenty (0-20) digits are allowed. A corresponding warning appears if any other symbols are inserted.

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

Attention: 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 QX's Auto Attendant.

Roles

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

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

Fig.II- 190: User Rights Management – Roles page

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

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

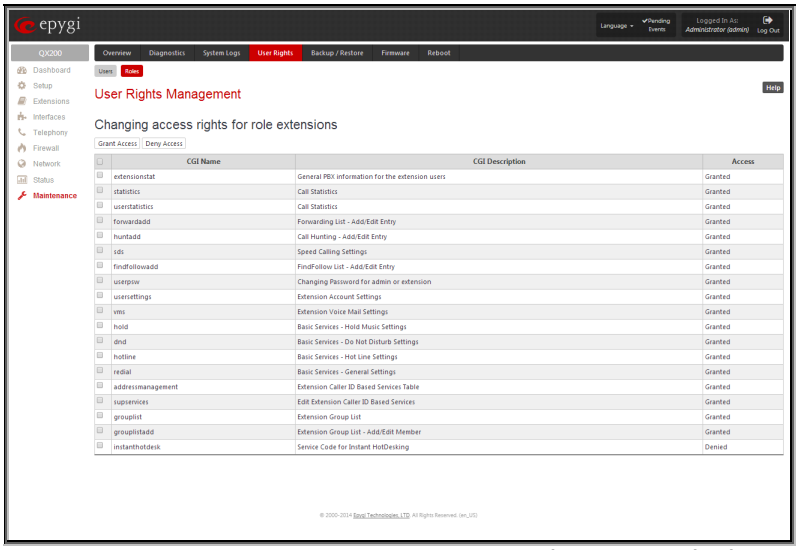


Fig.II- 191: User Rights Management – Edit Roles page

Backup/Restore

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

The **Backup and download current Configuration**- **Download** button generates a backup file with all configuration settings and user uploaded greeting messages. It opens a file chooser window for immediate download to the users PC.

The **Restore previously backed up Configuration - Upload** button opens a page that has a **Choose File** 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 to Factory Default settings** 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 QX gateway's configuration. A warning message will ask you to confirm your selection before restoring the default configuration.

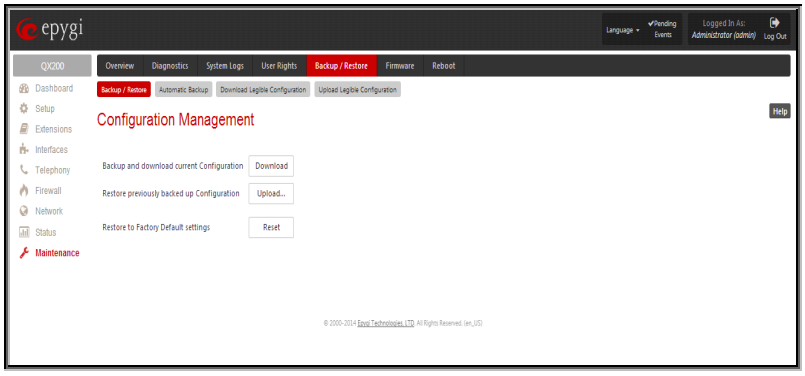


Fig.II- 192: Configuration Management page

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

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

Automatic Backup

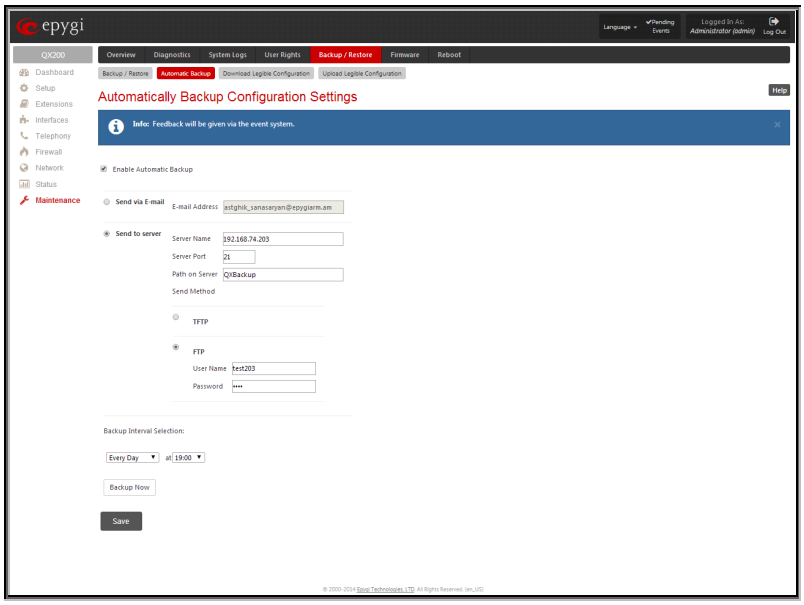


Fig.II- 193: Automatic Backup page

The **Automatic Backup** page allows you to enable the automatic backup of the system configuration and the voice data on the QX gateway. With this service, QX gateway 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 Automatic Backup** checkbox enables automatic backup mechanism on the QX gateway.

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

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

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

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

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

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

The **Backup Interval Selection** drop down lists is used to select the frequency and the time when the automatic backup of the QX gateway's system configuration and the voice data will take place.

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

Download Legible Configuration

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

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

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

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

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

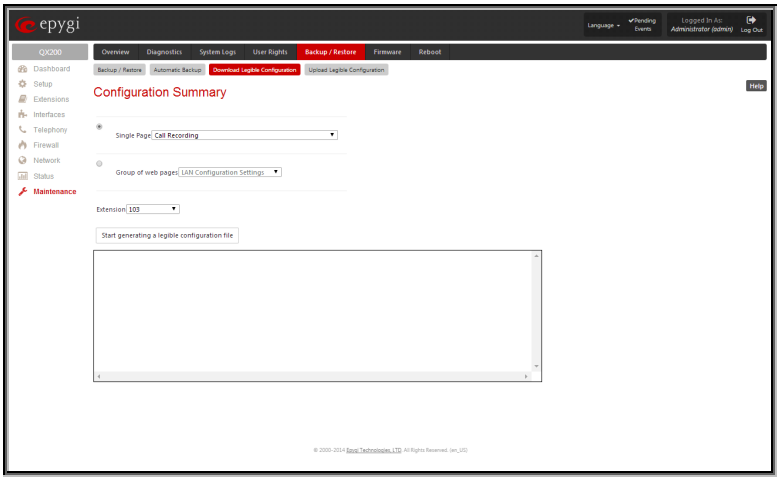


Fig.II- 194: Download Legible Configuration page

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

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

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

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

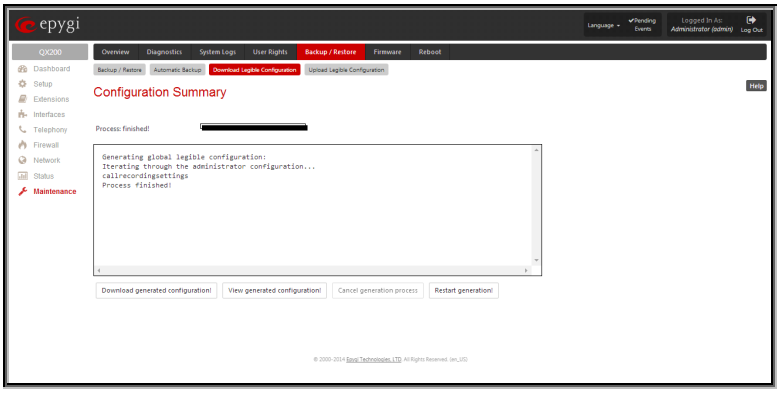


Fig.II- 195: Download Legible Configuration - Configuration Summary Preview page

Upload Legible Configuration

The **Upload Legible Configuration** page is used to upload a configuration file in a text format. The **Choose File** button in the opened page is used to browse certain legible configuration file to be uploaded and updated into the system. The configuration files to be uploaded should be in the *.txt format, otherwise a system error occurs. Configuration file upload progress will be displayed in the area below. During legible configuration file upload, QX gateway's functionality failures may occur.

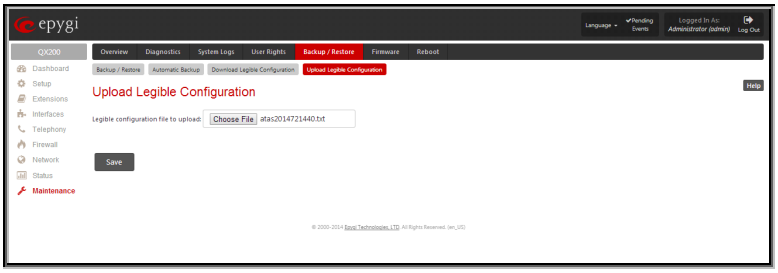


Fig.II- 196: Upload Legible Configuration page

Firmware Update

This window allows updating the software of QX gateway 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. QX gateway 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, QX gateway, telephony and Internet access will be disabled.

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

Please Note: It is recommended to backup the configuration prior to upgrading the firmware. You can do that by clicking the **Download Configuration** link, which 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.

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

- All pending events

- User specific GUI states

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

To update firmware manually select one of the following pages: Upload Firmware or Get Firmware From Server. For automatic firmware update select the Automatic Firmware Update tab.

Upload Firmware

The **Upload Firmware** procedure is created in 3 pages. In the first page of **Upload Firmware** the image file should be selected.

Specify Image text field displays the selected image filename.

Choose File button used to browse the image file.

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.

The **Cancel Uploading** button appears when the update procedure starts and it is used to stop it.

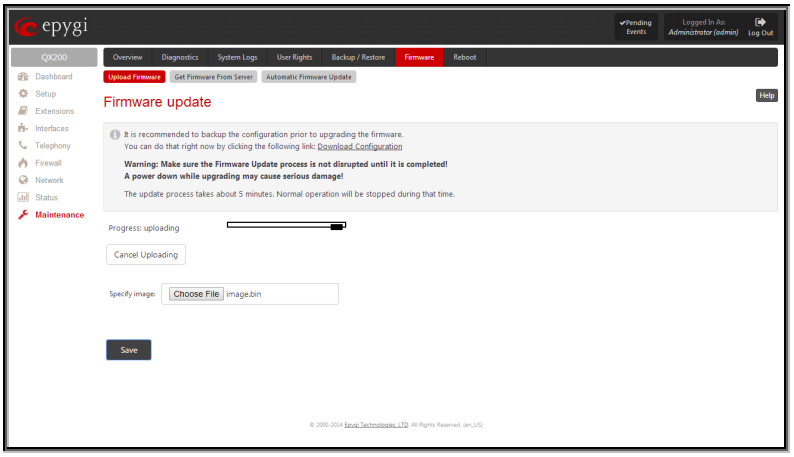


Fig.II- 197: Firmware Update page

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 **Yes,** otherwise press **No**.

After pressing **No**, press **Discard this image** button to start upload a new image.

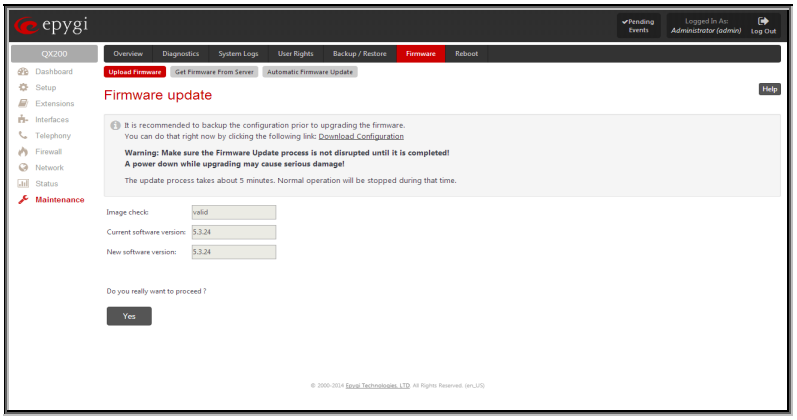


Fig.II- 198: Firmware Check page

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 QX gateway.

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

Attention: After the firmware update, all IP phones attached to the QX gateway should be restarted.

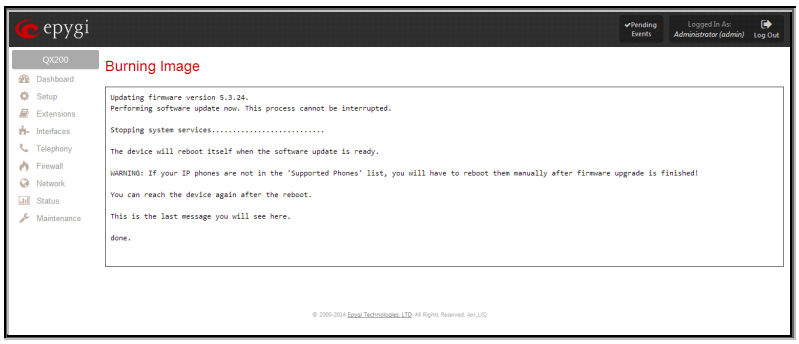


Fig.II- 199: Firmware Update – Burning Image page

Get Firmware From Server

The **Get Firmware From Server** page allows you to get a new Firmware (image) from the FTP server.

Firmware URL text field requires the path of new firmware image which located on the FTP server.

Username and **Password** text fields require the FTP server authentication parameters.

You should save changes before **Download** or **Download and Update**.

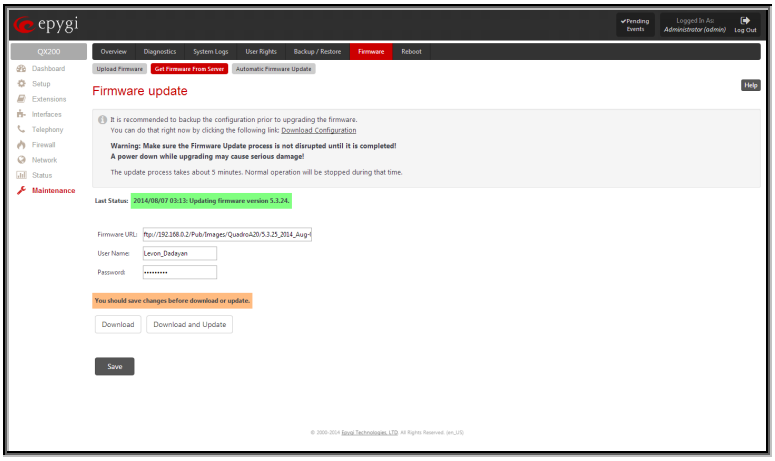


Fig.II- 200: Firmware Update page

Pressing the **Download** functional button a new page with firmware download process will be displayed.

This page displays non-editable information about the image validity. **Last Status** shows that firmware download process is running and whether the new firmware version is downloaded or not.

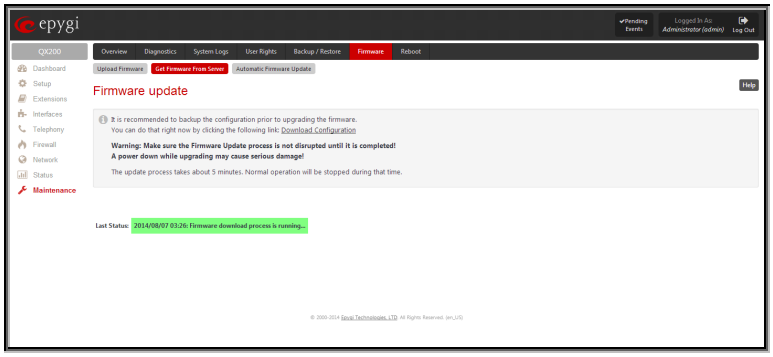


Fig.II- 201: Firmware Update page

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 **Update**, otherwise press **Discard**.

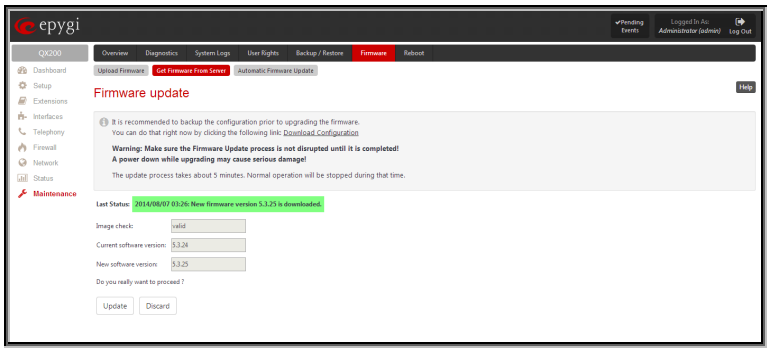


Fig.II- 202: Firmware Update page

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 last status 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 QX gateway.

The **Download and Update** functional button will automatically download and update the firmware version from the FTP server.

Pressing the **Download and Update** functional button a new page with firmware download process will be displayed.

This page displays non-editable information about the image validity. **Last Status** shows that firmware download and updating process is running.

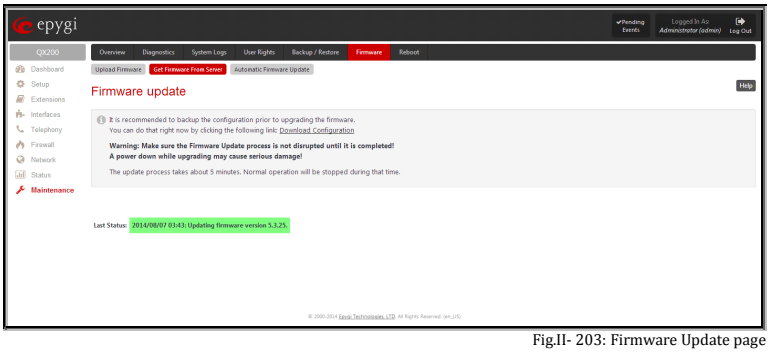


Fig.II- 203: Firmware Update page

Automatic Firmware Update

The **Automatic Firmware Update** page allows you to configure an automatic update of the QX gateway's firmware (software image) as it becomes available on the server. When this service is enabled, on the configured day and time QX gateway 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.

Please Note: Independent on the selected server type, there should be an "**auto-update**" folder in the root directory of the server. QX gateway 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 QX.

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 FTP, HTTP or HTTPS methods. For some of these selections, authentication **Username** and **Password** can be entered.

Please Note: In order to use Epygi's public ftp server leave the **Server Name**, **Server Port**, **Update Method, User Name** and **Password** text fields to their default values (*ftp.epygi.com*, *21*, *ftp* and *anonymous* respectively, use blank for password).

Check for updates options allow 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 QX will check for a new firmware available on the server. The way of notification is configured from the Event Settings page.
- **Check and update** – choose this selection to check and automatically install the new firmware on the QX as it becomes available on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the QX will check for a new firmware available on the server, will automatically download and install it on the QX.

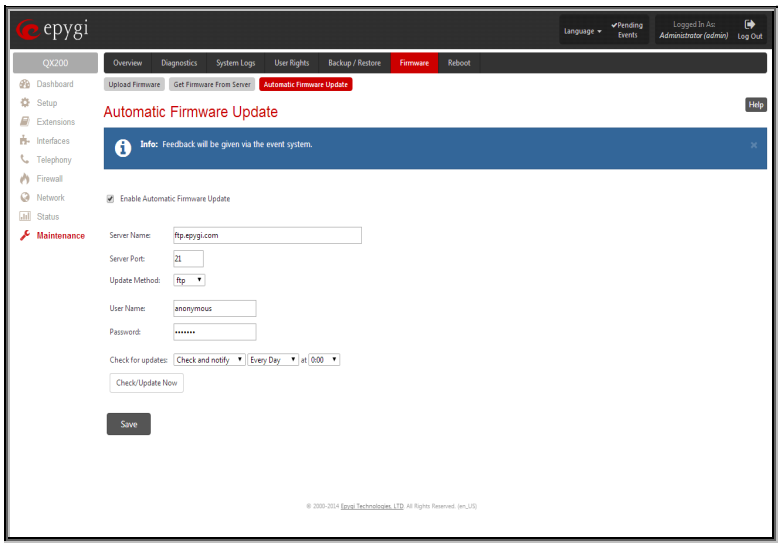


Fig.II- 204: Automatic Firmware Update page

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

Reboot

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

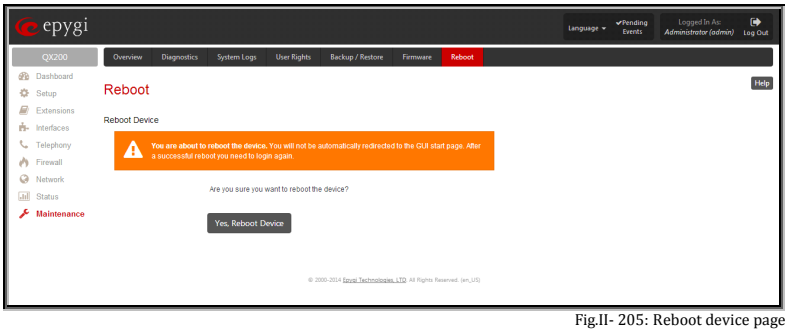


Fig.II- 205: Reboot device page

Registration Form

The **Register Your Device in Technical Support Center** page appears when administrating an unregistered QX gateway, 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 QX gateway registration form.

Remind me later hides the registration notification in the QX gateway through System Configuration Wizard or Internet Configuration Wizard until the next administrating activities.

Don't remind me again hides the registration notification forever.

Fig.II- 206: Device Registration page

Extension User's Menus

QX gateway **Your Extension** management may be accessed on two different levels: for users (extensions) and administrators. If you are an extension user, log in with the extension number and the password (if any) you received from your system administrator.

If you are an admin, additionally the **Return** link will appear to go back to the QX gateway Management page.

Log Out is used to close the session between the user PC and QX and to leave the QX gateway **Your Extension** Management.

Your Extension menus allows you to access the following settings to operate and perform actions that are private for each user:

- **Call History**
- **PBX Information**
- **Account Settings**
- **Basic Services**
- **Caller ID Based Services**
  - Incoming Call Blocking
  - Outgoing Call Blocking
  - Unconditional Call Forwarding

Call History

The **Call History** page allow collecting the call events and their parameters over the QX, i.e. incoming and outgoing calls reporting. It contains three tables and provides reports on successful, not successful and missed incoming and outgoing calls for the current extension only. The page also gives a possibility to filter the collected **Call History** based on various criteria. The search components are as follows.

- The **From** and **To** text fields are used to search by date and time. The data must be inserted in the following format: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The **From** field has to indicate an earlier date and time than the **To** field. If the entered data does not correspond with this condition, the "Minimal date should be less than maximal date" error message prevents statistics filtering.
- The **From** and **To** drop down lists are used to search by duration. The duration needs to be specified from the listed values. The **From** field has to indicate a shorter duration than the **To** field. If the entered data does not correspond with this condition, the "Minimal duration should be less than maximal duration" error message prevents statistics filtering.
- **Called Phone** requires the called party's SIP address, extension or PSTN number as a search criteria.
- **Calling Phone** requires the caller party's SIP address, extension or PSTN number as a search criteria. For **Called** and **Calling Phone** wildcards are available (see chapter Entering SIP Addresses Correctly). If the defined caller or called addresses are inserted incorrectly the "Calling (Called) address is incorrect" error will prevent filtering.

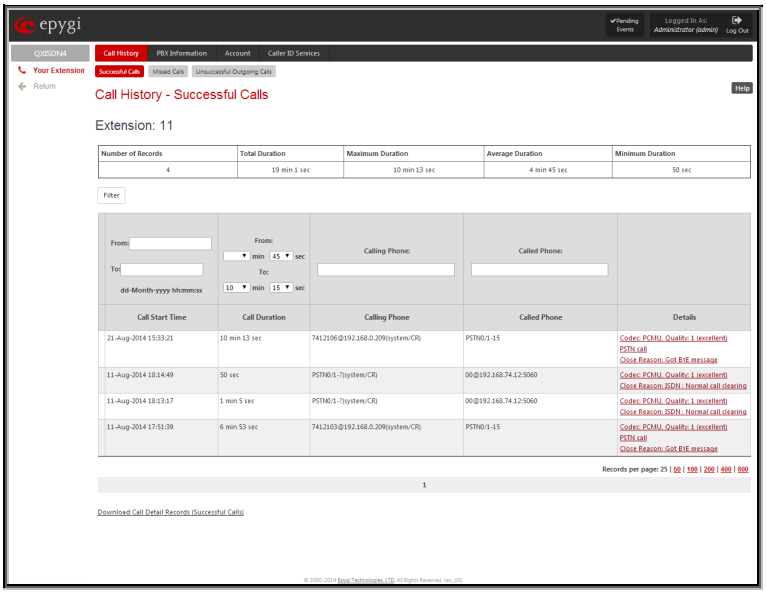


Fig.II- 207: Extension's Call History page

The **Call History- Successful Calls, Missed Calls and NonSuccessful Calls** tables list the successful, missed and not successful incoming and outgoing calls and their parameters (Call Start Time, Call durations, Calling and Called phones) for the current extension. Each column heading in the tables are created as links. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

Number or records displays the current number of statistics entries in the table. For Successful calls **Total Duration, Maximum Duration, Average Duration** and **Minimum Duration** are displayed at the top of the table.

Call Detail column is present in the **Non Successful Calls** table only and indicates the reason of the call being unsuccessful.

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

The **Records per page** are used to select the number of displayed statistic records per page. The **Previous** and **Next** can be utilized to switch between these pages.

To Filter the Call History

1. Enter the desired search criteria.
2. Click on the **Filter** button to search call reports within the **Call History** table.

Please Note: To return to the complete statistics table clear all search criteria and press **Filter**.

PBX Information

The **PBX Information** page provides read only information about the extension codecs, other existing extensions and available PSTN lines on the QX.

The **PBX Information** displays a list of available codecs for the corresponding extension, the list of other extensions on the QX, their Display names and the SIP registration username It also displays the destination to route incoming calls and the allowed call types for PSTN lines.

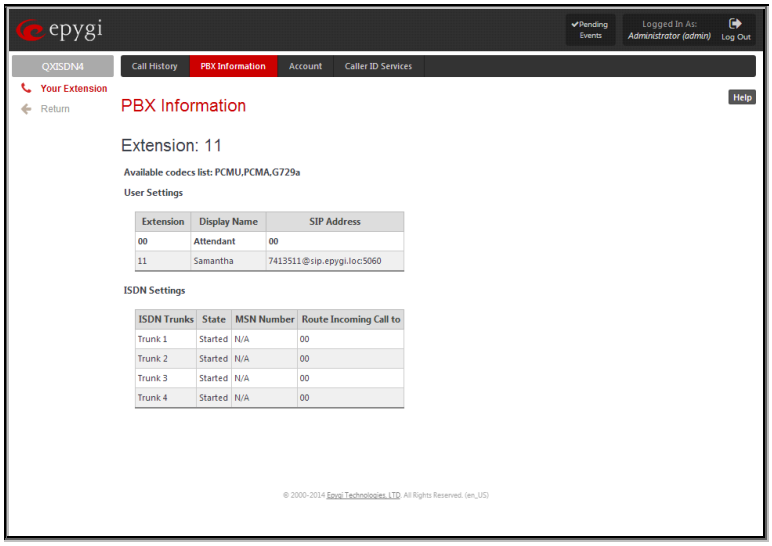


Fig.II- 208: PBX Information page

Account Settings

The **Account Settings** page provides information on the extension display name, allows changing the user password, enabling user password protection for incoming/outgoing calls and downloading/uploading of a file with the user-defined voice greetings. All parameters listed on this page may be modified and submitted. The page consists of the following components:

Extension shows a non-editable parameter providing information about the current user extension number.
Display Name defines an optional parameter used to identify the calling party. Usually the display name appears on the phone display if a call is placed or a voice mail is sent. The field is not limited regarding symbol usage but its length is limited to 20 characters.
User Permissions selection indicates password protection for:

- **Incoming Calls** enables password protection for incoming calls. If the service is enabled a user password is required to be able to accept the incoming calls.
- **Outgoing Calls** enables password protection for outgoing calls. If the service is enabled a user password is required to be able to make calls.

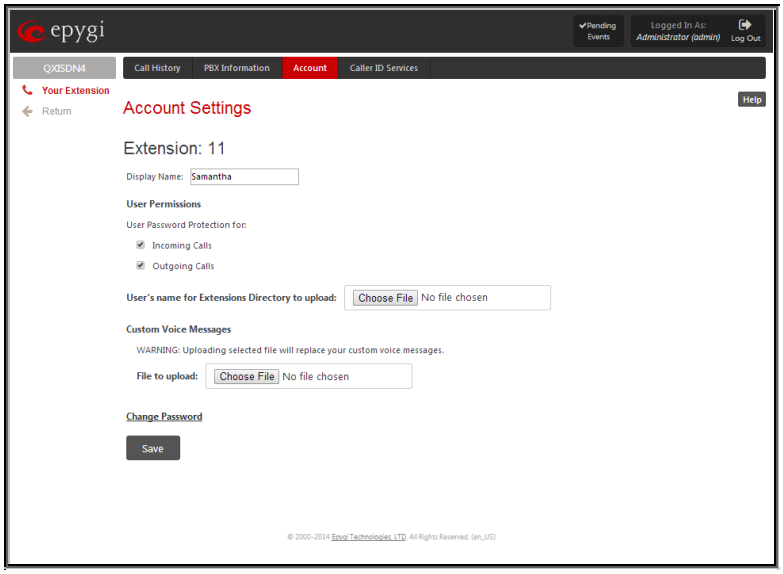


Fig.II- 209: Account Settings page

The **File to upload** text field can be used to type in the path where backed up file with voice messages is located. If voice greetings are browsed with the help of a file-chooser, this field displays the path of the browsed file. The **Choose File** 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 QX 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 QX, they may be completely different on the other one upon the uploading of the voice data.

The link **Download custom voice messages** appears only when there are some user-defined custom greetings recorded and is used to download a compressed file with all user specified voice messages. The link opens the file-chooser window to specify the saving location.

The link **Change Password** refers to the page where the user password can be changed.

The **Change Password** page is used to change the user's password.

- The **New Password** field requires a new password for the Extension. The Password field is checked against its strength and you may see how strong is your inserted password right below that field.
- Reentering the new password in the **Confirm New Password** field will confirm the new password. The password can consist of numeric values only.

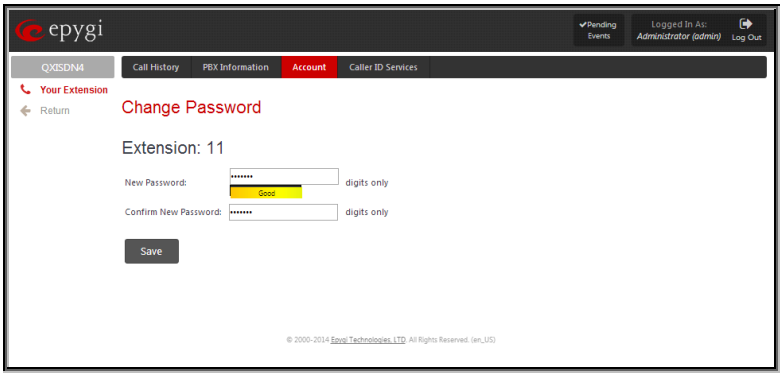


Fig.II- 210: Change Password page for extension access

Please Note: Up to twenty (0-20) digits are allowed. A corresponding warning appears if any other symbols are inserted. 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 QX's Auto Attendant.

Basic Services

The **Basic Services** page (available only for QXFXS24 gateway) allows you to configure the basic telephony features of QXFXS24 gateway, such as Call Waiting service.

The **Basic Services** page consists of two frames. The left frame lists all services. When you click on a service, its corresponding settings will be displayed in the right frame.

Please Note: Remember to save changes before moving between the service configuration pages.

General Settings

The **General Settings** page consists of the following component:

Call Waiting

Call Waiting is used to receive an incoming call when you are currently on a call. The caller will hear a ringing tone and the QX gateway user will hear a special beeping on the telephone when the call arrives. For analog phones, to switch between the current call and the new incoming call, use the appropriate calling code. For IP phones to switch between the current call and the new incoming call, use the corresponding **Hold** or **Line** softkey/button (for more details refer to the "**Epygi IP PBX Features on Epygi Supported IP phones**" document on the Epygi's Web portal).
Enable Call Waiting Service activates this service and makes it available for the phone handset.

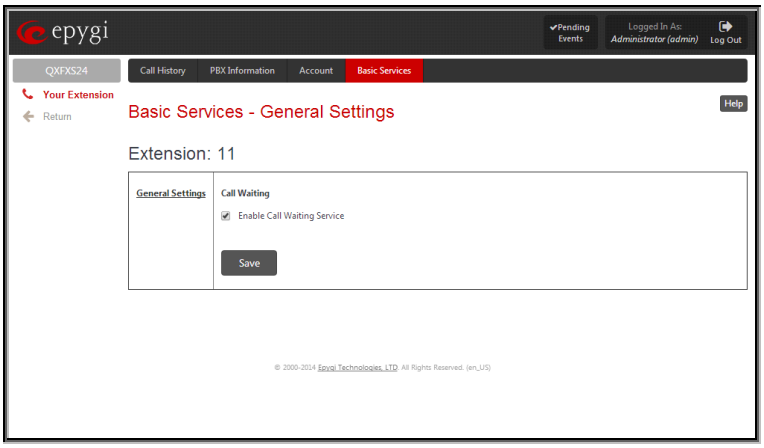


Fig.II- 211: Basic Services – General Settings page

Caller ID Based Services

The **Caller ID Based Services** page provides a possibility to configure a set of telephony settings from the same page. Incoming and Outgoing Call Blocking Settings and Unconditional Call Forwarding services are configurable from this page.

The **Caller ID Based Services** page contains a table where all caller or called destinations and the states (ON or OFF) of caller ID based services for each of them are listed. Caller or called destinations are used to configure caller ID based services based on them. The column headings of the table are designed as links. By clicking on the column heading the table will be sorted by the selected column. Upon sorting (ascending or descending) arrows will be displayed close to the column heading.

The table also has **Any Address** entry that is undeletable. It is used to configure caller ID based services for all addressed. When adding a new caller address **Any Address** is changed to **Other Addresses**. Now there could be different configurations for the specified addresses and for all others.

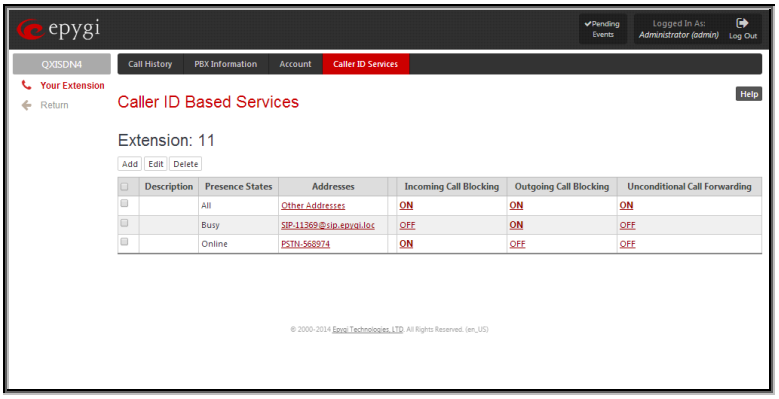


Fig.II- 212: Caller ID Based Services page

Add opens the **Caller ID Based Services - Add Entry** page where a new address and presence states can be defined Page consists of the following components:

The **Description** text field requires optional information about the address owner.

Call Type lists the available call types:

- PBX - local QX extensions and Auto Attendant
- SIP – caller or called destinations reached through a SIP server
- PSTN – caller or called destination dialed from or to PSTN
- Auto – used for undefined call types. In this case, for incoming calls from specific address, configuration of caller ID based services will apply either to PBX, SIP or PSTN callers. For outgoing calls, the called destination will be reached through Routing.

Addresses text field requires a SIP address (see chapter Entering SIP Addresses Correctly), an extension or a PSTN number, for whom supplementary services should be applied. If the address already exists in the table, selecting **Save** will give the error "Caller address already exists". Wildcard is allowed in this field (see chapter Entering SIP Addresses Correctly). Entering "*" as PBX or PSTN addresses will apply configuration of supplementary services to all extensions or PSTN users.

The extension number should be inserted in the **Addresses** text field for the PBX call type. The PSTN number length depends on the area code and phone number.

The **Presence State** radio buttons allows to set the Presence State of an extension.

- **All States** selection is used to select all states for an extension.
- **Specific States** selection contains a group of radio buttons that are used to select the state of the corresponding extension:
  - Online
  - Offline
  - Busy
  - Away
  - DND
  - Meeting
  - Vacation
  - Lunch

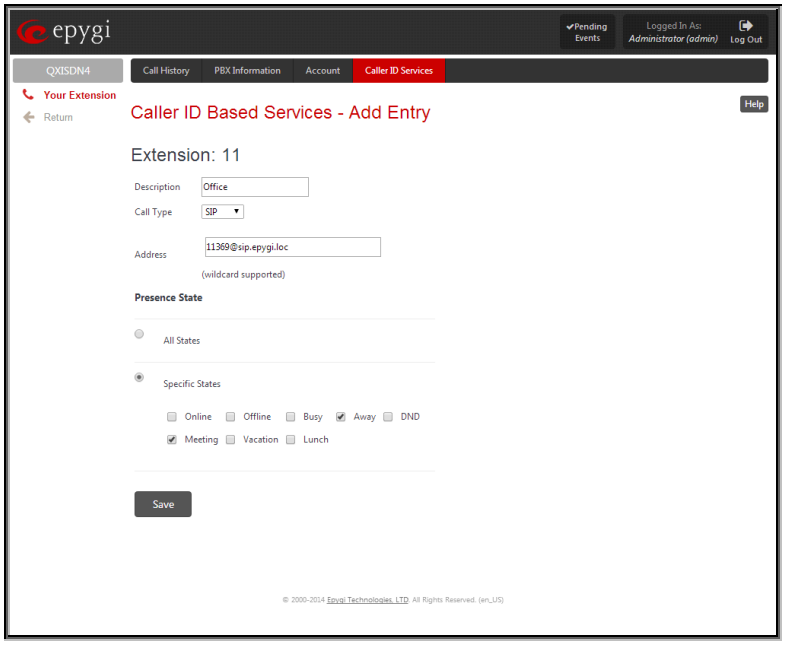


Fig.II- 213: Caller ID Based Services – Add Entry page

When clicking on the **Address** in the **Caller ID Based Services** table, the caller ID based services configuration pages for the corresponding extension will be displayed.

The **Caller ID Based Services for Address** page consists of two frames. In the left frame all caller ID based services are listed. Clicking on the corresponding caller ID based service, its settings will be displayed in the right frame.

Please Note: Pay attention to save changes before moving among caller ID based services configuration pages.

Below is the guidance on configuration of each caller ID based service available to the user.

To Configure Caller ID Based Services

1. Press the **Add** button on the **Caller ID Based Services** page. The **Caller ID Based Services - Add Entry** page, where new 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. Select the **Presence State** of an extension.
6. To add an address to the **Caller ID Based Services** table, click **Save**.
7. Click on the newly created **Address** in the **Caller ID Based Services** table to open the **Caller ID Based Services for Address** page.
8. 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. Change the **Presence State** of the extension, if needed.
5. **Save** changes.
6. 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.
7. 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 QX gateway extension. This page provides the necessary settings for incoming call blocking. It indicates if the service is enabled for the particular caller and whether or not the custom message will be used to inform the caller about the call being blocked. If the service for the particular caller has been enabled by the administrator and has been stated as protected, it cannot be disabled by the user.

Please Note: Since the administrator can protect the service from being disabled by you, contact the administrator if callers complain that they cannot reach you.

The **Enable Service** checkbox selection blocks all calls to the current extension from corresponding **Address** listed in Caller ID Based Services table Incoming Call Blocking service is configured for.

The **Send Message to Caller Party** checkbox is available when the service is enabled and initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without notification.

The **Restore Default Blocking Message File** restores the default incoming call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Message File** requires the name of the desired voice message file. The file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) 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.

Choose File is used to browse custom voice message used for incoming call blocking.

The **Download Voice Message File** link only appears if a file has been previously uploaded. The link is used to download the audio file to the PC and opens a window where the saving location can be specified.

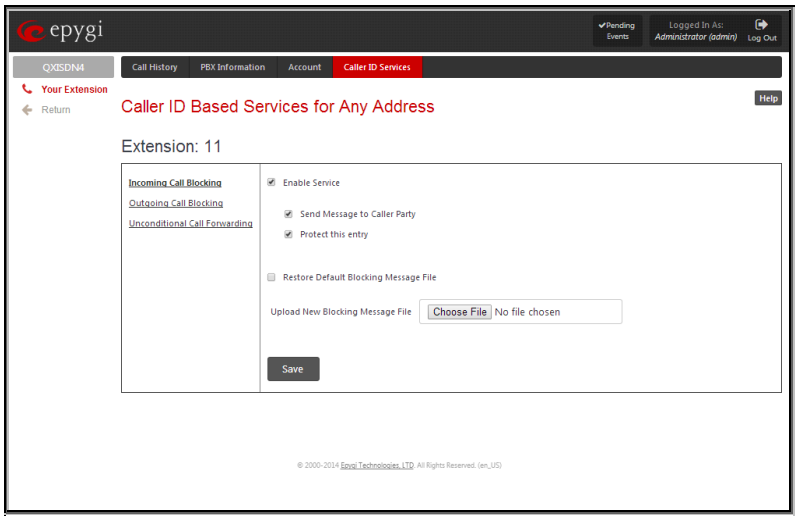


Fig.II- 214: Incoming Call Blocking page

Outgoing Call Blocking

Outgoing Call Blocking allows blocking unwanted outgoing calls for a QX gateway extension towards the destination **Address** service is configured for. This page provides the necessary settings for the outgoing call blocking service. It indicates whether service is enabled for the particular caller and whether or not a custom message will be used to inform caller about the call being blocked. If the service for particular caller has been enabled by administrator and has been stated as protected, it cannot be disabled by the user.

Please Note: Since the administrator can protect the service from being disabled by you, contact the administrator if you have problems establishing certain calls.

The **Enable Service** checkbox selection blocks all calls to the corresponding **Address** listed in Caller ID Based Services table from current extension.

The **Send Message to Caller Party** checkbox is available when service is enabled and it initiates a message to inform the caller that their line has been blocked. Otherwise, the calling party will be disconnected without a warning.

The **Restore Default Blocking Message File** restores the default outgoing call blocking message if another user-defined file has been previously selected. When the checkbox is selected, the file upload possibility will be disabled.

The **Upload New Blocking Message File** requires the name of the desired voice message file. The file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) 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.

Choose File is used to browse custom voice message used for outgoing call blocking.

The **Download Custom Blocking Message File** link appears only if a file has been previously uploaded. This link is used to download the audio file to the PC and opens a window where the saving location can be specified.

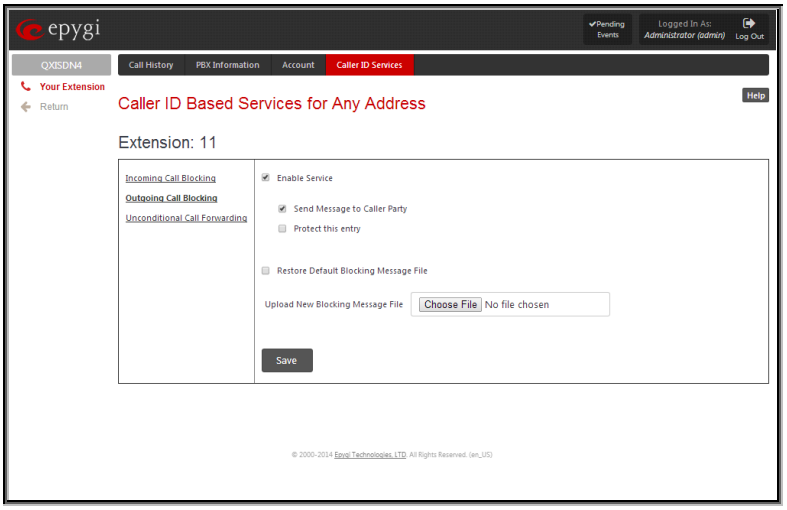


Fig.II- 215: Outgoing Call Blocking page

Unconditional Call Forwarding

Unconditional Call Forwarding is a service of QX that allows the automatic unconditional transfer of incoming calls to varying other destinations.

The following rules are applicable to all call forwarding types:

- PSTN destinations (with **PSTN** or **Auto** call type) have priority in **Forward to** list. If there are different destinations in the **Forward to** list, the call will be forwarded to PSTN destination (in the same time any available SIP or PBX destinations will receive a short ring). If the PSTN

destination was not successful, the next PSTN destination will be dialed, otherwise if there are no more PSTN destinations in the table, the call will be forwarded to any available SIP and PBX destinations simultaneously.

- If there are multiple entries with any combination of PBX or SIP call types, then all destinations will ring simultaneously and the call will be established with the destination that will pick up the call the first.

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.

The **State** column indicates whether the corresponding forwarding destination is **Enabled** or **Disabled**.

The **Forward to** column indicates the forwarding destination.

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 QX 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 Call Routing Table.

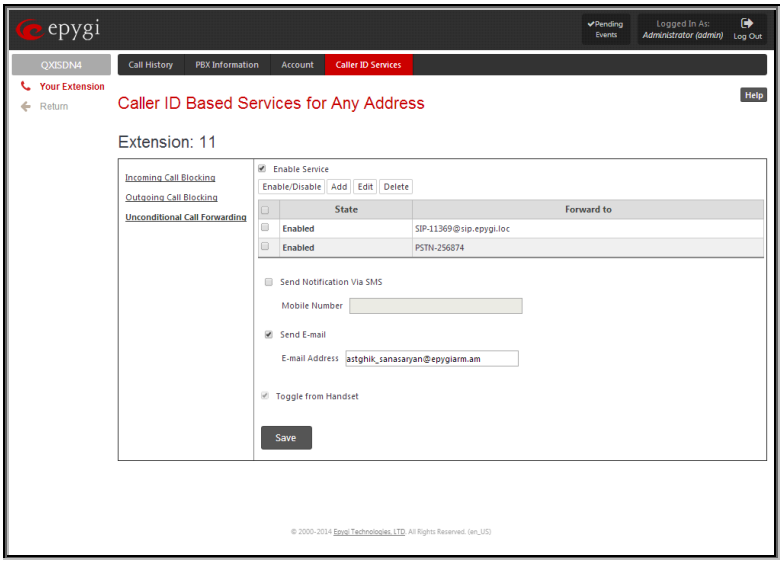


Fig.II- 216: Unconditional Call Forwarding page

The **Forward To** text field requires the SIP address (see chapter Entering SIP Addresses Correctly), a PBX extension or a PSTN number, where an incoming call from a certain caller should be unconditionally forwarded. If the address already exists in the table, selecting **Save** will display the error "Caller address already exists". A wildcard is allowed in this field (see chapter Entering SIP Addresses Correctly). Entering "*" as PBX or PSTN addresses will apply the configuration of Caller ID Based services to all extensions or PSTN users.

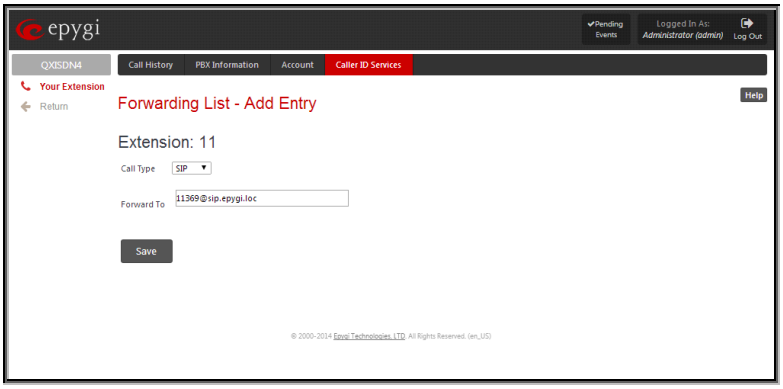


Fig.II- 217: Call Forwarding – Add Entry page

The extension number should be inserted in the **Forward To** text field for the PBX call type. The PSTN number length depends on the area code and phone number.

Send Notification Via SMS checkbox enables SMS notifications sending to the user's mobile phone when unconditional call forwarding on the corresponding extension from the certain caller takes place. This checkbox selection enables the **Mobile Number** text field where the user's mobile phone number should be defined. If you feel this service is not working, contact your system administrator to configure the SMS Settings.

Send E-mail checkbox enables email notifications sending to the user's mailbox when unconditional call forwarding on the corresponding extension from the certain caller takes place. This checkbox selection enables the **E-mail Address** text field where the user's email address should be defined. If you feel this service is not working, contact your system administrator to configure the Mail Settings.

When saving the unconditional call forwarding configuration, a message will notify the user that Many Extension Ringing and Call Hunting services have been disabled.

Log Out

This option is used to close the session between the user PC and QX and to leave the QX gateway Your Extension Web Management or enter into the management with another login.

QX's Auto Attendant Services

QX's Auto Attendant is addressed to provide remote access to the QX voice connectivity services. Specifically it supports remote connection to QX extensions, their mailboxes and making pass-through calls to other destinations. Remote access to the QX auto attendant is possible through IP and PSTN calls.

QX'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 QX's PSTN number) if the calls addressed to the QX's PSTN number are routed to the Auto Attendant.

Attention: If the Auto Attendant authentication attempts have been failed for the five times, QX'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 QX device without restrictions: All QX extensions may call each other dialing the extension number. And all external callers (using PSTN or IP calling) can reach every QX extension dialing QX'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 QX Auto Attendant is registered at Epygi's SIP server by default, it may be used as a kind of private switching center, if the Auto Attendant is routed to the particular telephone line (FXO, ISDN or E1/T1) as a "default user". Then it allows e.g. establishing cost-saving long-distance calls: Via PSTN to the QX Auto Attendant (e.g. USA headquarters), via IP to the remote QX Auto Attendant (e.g. Office Asia) and via PSTN to the desired destination (see call codes below).

Access to **Call Relay** needs authorization.

Remote Configuration Menu

This menu allows extension owners to remotely enable/disable the Unconditional Call Forwarding Service for **Any Address** or **Other Addresses** entries of the Caller ID Based Services table on the corresponding extension, as well as to change the certain forwarding number in the Unconditional Call Forwarding table. The menu requires extension authorization.

Call Back

With the QX's Call Back service callers can save the call charge when calling to/through the QX to the third party SIP or PSTN destinations. The QX allows you to configure a list of trusted callers that are allowed to make free of charge calls. Two types of Call Back configurations are available on the QX: **Pre-configured Call Back** and **Remote Call Back Configuration**.

Pre-configured Call Back

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

To use Pre-configured Call Back, the caller registered in the Authorized Phones Database should simply call to the QX's Auto Attendant through SIP or PSTN, let the call to ring twice and then hang up. Call Back will be instantly activated, and QX will call back to the defined Call Back destination. By answering the incoming call caller will be connected to the Auto Attendant menu.

Remote Call Back Configuration

The **Remote Call Back Configuration** service is used by authorized callers to configure or reconfigure existing call back configuration on the QX. Remote Call Back Configuration is divided into two modes accessible from the QX's Auto Attendant:

- 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 the Call Back settings for the trusted user.

Permanent Call Back

Permanent Call Back service allows callers registered in the Authorized Phones Database to create a new trusted caller with Call Back enabled. They can also modify the Call Back destination of existing callers in the Authorized Phones Database. By calling QX's Auto Attendant and entering the Auto Attendant menu, the caller can use the * 6 code to create a new trusted caller as well as to modify the Call Back destination for the already registered callers in the Authorized Phones Database.

By entering Permanent Call Back reconfiguration menu, system asks caller to login by dialing the number and an appropriate password for the QX's extension that is used as login extension in the Call Back settings. After passing the login, callers should follow the voice instructions for configuring a new entry or reconfiguring existing entries in Authorized Phones Database.

When system accepts the inserted settings, the corresponding entry will be logged to the Authorized Phones Database. The caller will then be disconnected from the QX's Auto Attendant and the defined Call Back destination will receive a call from the QX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX's Auto Attendant.

Please Note: The detected caller number must correspond to the one applied by the caller. In case of PSTN call back at least one PSTN line must be available on the QX. There must be network connectivity and the destination must be reachable.

Non-Permanent Call Back

Non-Permanent Call Back configuration service allows trusted caller to organize one-time Call Back to the defined destination. In this situation, no entry will be logged to the Authorized Phones Database. By calling QX's Auto Attendant and entering the Auto Attendant menu, the caller can use *5 menu to modify the Call Back destination for already registered callers in the Authorized Phones Database.

The system will ask to login by dialing the number and an appropriate password for the QX's extension that is used as login extension in the Call Back settings. After login, caller should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database. The caller will then be disconnected from the QX's Auto Attendant and the defined Call Back destination will receive a call from the QX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX's Auto Attendant.

Please Note: For both Permanent Call Back and Non-Permanent Call Back, the detected caller number must correspond to the one configured for trusted caller. In case of PSTN call back at least one PSTN line must be available on the QX. There must be network connectivity and the destination must be reachable.

Call Routing Management Menu

This menu (not available for QXFXS24 gateway) 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 *77 at the Auto Attendant welcome message, will ask for an enabler/disabler key used to enable or disable the routing rule(s) correspondingly. Since multiple routing rules may have the same enabler/disabler key combinations (the same key may be used as enabler for one routing rule, and as disabler for another one), dialing the certain key will affect all pre-configured routing rules.

If the routing record has an authorization enabled on the enabler/disabler key, administrator's password will be required to be inserted after the key. Once the administrator's password is dialed, system plays a confirmation about the accepted configuration and the state of the certain routing rule(s) is getting modified.

If administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.

Call Codes Available in Auto Attendant

For external calls addressed to the Auto Attendant or incoming calls from mainline routed to the Auto Attendant or local by dialing the 2-digit attendant extension, following key combinations are available to access and manipulate within Auto Attendant services:

Please Note: The following key combinations are not available for QXFXS24 gateway.

Incoming call to Auto Attendant Services or dial locally	Keys
Extensions Menu - establishing a connection to an extension on the called QX	- (already in)
Call Relay Menu - mainly for external calls (IP/FXO or IP/ISDN), local calls are allowed, too. Service allows you to avoid hanging up and redo the entire dialing, if QX 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 QX Auto Attendant (calling from one Auto Attendant to another)	
Remote Configuration Menu – allows remote enabling/disabling of Unconditional Call Forwarding service for **Any Address** or **Other Addresses** entries in the Caller ID Based Services table on the extension and to modify the certain forwarding destination.	* 4
Non-Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to change the callback destination for a one-time callback. After the caller hangs up, QX 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
Administrator Login Allows to modify Auto Attendant greeting and menu messages, as well as to manage universal extension messages.	* 7 5
Call Routing Management Menu – allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain routing rules by dialing key combinations pre-configured on each routing entry.	* 7 7
Quits the Auto Attendant and starts a dial tone.	Flash 4

Remote Configuration Menu

* 4 **Remote Configuration Menu** (when this menu is accessed, the Unconditional Call Forwarding service is already getting toggled)	
1 Toggle (enable or disable) the Unconditional Forwarding service again	2 Change the Forwarding Number
	Dial a new **Forwarding Number** and press #
	Confirm the new Forwarding Number with # or press * to dial a new Forwarding Number.

Please Note: Using the **Change the Forwarding Number** option will change the first entry in the **Unconditional Call Forwarding** table with **Auto** call type to the inserted **Forwarding Number**. Any other entries with **Auto** call type, as well as with other call types will not be modified.

Call Codes available for QXFXS24 Gateway

The table below presents the feature codes for PBX services accessible at the dial tone.

PBX Services accessible during the call	Keys for FXS lines
Call Hold (used both for call waiting and for switching from one line to another)	**Flash 0**
Call Blind Transfer and **Call Transfer with Consultation**	**Flash**
Call Conference	**Flash 3**
To terminate the call	**Flash 4**

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name – admin Password – 19
QX Host Name for QXE1T1 gateway	e1t1gw
QX Host Name for QXFXO4 gateway	fxogw
QX Host Name for QXISDN4 gateway	isdngw
QX Host Name for QXFXS24 gateway	fxsgw
QX Domain Name	epygi – config.loc
LAN IP Address	172.28.0.1 Subnet Mask – 255.255.0.0
DHCP Server	Enabled
Regional Settings and Preferences	Locale – US TimeZone – Central Time (US&Canada)
WAN Interface Protocol	Ethernet
WAN Interface Bandwidth	Upstream – 100000 Downstream – 100000 Min Data Rate – 0
WAN IP Configuration	Assign automatically via DHCP
MAC Address	Assigned by device MTU – 1500 Bytes
DNS Server	Dynamically by provider
Date/Time Settings	Simple Network Time Protocol Server and Client – enabled SNTP Server – ntp1.epygi.com Polling interval – 6
Email Settings	System Mail Settings – disabled SSL – disabled Enable SMTP Authentication-disabled User Name – empty User Password – empty
System Security	Security Level - Medium
Language Pack	Default – English Current Language Pack – none
Extensions Management	Extension Length – 2 extension 00 appear for QXFXO4, QXISDN4 and QXE1T1 gateways extensions 11-34 appear for QXFXS24 gateway
Extension Settings – General (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Display name – none Password – empty Call Relay – disabled GUI Login Allowed – disabled Show on Public Directory – disabled Enable Ringing Simulation – disabled
Extension Settings – General (for QXFXS24 gateway)	Display name – none Password – empty 11 - 34 extensions attached to the FXS lines 1-24
Extension Settings – SIP (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Registration User Name/DID Number – same as extension number Registration password – empty SIP server – empty SIP Server port – 5060

Parameter	System Default Value
	SIP Server Registration – disabled
Extension Settings – SIP Advanced	Authentication User Name – undefined Send Keep-alive Messages to Proxy – disabled RTP Priority Level – medium Do Not use SIP Old Hold Method - disabled Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined
Extension Settings – Voice Mailbox (for QXFXS24 gateways)	External Voice Mail for all extensions
Extension Settings – Codecs	Codecs - G711u (preferred), G711a, G729a, G726/32, G726/16, G726/24, G726/40, iLBC– enabled, H.263,H.263+ and H.264 – disabled 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 SRTP Policy – Make unsecure calls, accept anything
Attendant 00 Settings – General (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Display name – empty Enable FAX forwarding – disabled Show on Public Directory – enabled
Attendant 00 Settings – Attendant Scenario (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Scenario – default Send AA digits to Routing Table – disabled Redirection on Timeout – disabled ZeroOut – disabled Welcome Message – enabled Ringing Announcement – disabled Welcome Message, Recurring Attendant Prompt and Attendant Ringing Announcement – default
Attendant 00 Settings – SIP (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Registration User Name/DID Number – empty Registration password - empty SIP server - empty SIP Server port – 5060 SIP Server Registration – disabled
Attendant 00 Settings – SIP Advanced (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Same as for extensions
Attendant 00 Settings – Codecs (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, iLBC – enabled, H.263, H263+ and H.264 – disabled 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 SRTP Policy – Make unsecure calls, accept anything
Universal Extension Recordings	Default, Percentage of System Memory – 1%
Authorized Phones	No entries
General Operation Mode (for QXFXS24 gateways)	Stand-alone mode
FXS (On-board) settings	24 FXS Lines exists on QXFXS24 Onboard Lines Configuration: CallerID – Standard 2 FSK for all lines Ringer type: Type A for all lines Busy Tone and Power Disconnect indications: disabled for all lines

Parameter	System Default Value
	Off-hook caller ID – disabled for all lines Hot Desking Capability – disabled for all lines
FXO Settings (for QXFXO4 gateways)	4 FXO lines exists on QXFXO4 All lines enabled, incoming and outgoing calls allowed and routed to 00 Attendant on all lines
E1/T1 Settings (for QXE1T1 gateways)	Trunk 1 exists on QXE1T1 Trunk mode - E1 Interface Type – User Signaling – CCS Line Code – HDB3 Frame Mode – NO_CRC Line Build Out – 120-ohm Coding - a-law LoopBack Mode - No_loopback Clock Mode – Slave TEI mode – non automat, TEI address -0 SAPI Value – undefined Alternative Disconnect Mode – enabled Excessive Ack. Delay T200 – 4000 Idle Timer T203 – 12000 T302 timer – 4000 T309 timer – 0 T309 timer – 60000 D Channel Timeslot for Transmit/Receive – 16 B channels - 1-31 timeslots are enabled Echo Cancellation - enabled for all B channels Channels Selection – preferred Channels Selection Ordering – ascending Bearer Establishment Procedure – on progress indication with in-band information, Called Party Type of Number and Calling Party Type of Number – Unknown, Called Party Numbering Plan and Calling Party Numbering Plan – ISDN/telephony numbering plan Route Incoming Call to – 00 Switch Type - primary_dss1 Generate Progress Tone to PSTN/PBX – None Incoming Called Digits Size – 1 Generate Progress Tone to IP – disabled Send ALERT Message on Call Routing – disabled Enable CLIR Service – disabled Enable Connect Acknowledge Option – enabled Override CLID with P-Asserted-Identity –disabled
ISDN Settings (for QXISDN4 gateways)	ISDN Trunks – 4 trunks exists on QXISDN4. Settings for all available Trunks: State – started Interface Type – User Connection Type - PTMP(Point To Multi Point) Service Type – No MSN Route Incoming Call to - 00 Use Default outgoing Caller ID – enabled Default outgoing Caller ID – undefined Advanced Settings – disabled
PSTN Lines Sharing (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Provide PSTN lines for master device – disabled
PSTN Gateway Operation Mode (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Slave mode
VoIP Carrier (for QXFXO4, QXISDN4 and QXE1T1 gateways)	VoIP Carrier – Manual Description – undefined
Call Routing Table	2 entries defined for a call - calls to extensions and calls to SIP
Call Routing	Route all incoming SIP calls to Call Routing – disabled
Local AAA Table	Local AAA Table – Authentication by Caller ID – enabled
Global Speed Dial Directory	Undefined
SIP Tunnel Settings	Enable Tunnels to Slave Devices – disabled

Parameter	System Default Value
	Tunnels to Slave Devices – no entries Enable Tunnels to Master Devices – disabled Tunnels to Master Devices – no entries
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
RTP Settings	Properties for all Codecs Packetization – 20ms Silence Suppression – yes iLBC properties: Packetization –30ms Silence Suppression – yes G.726 Standard - ITU-T specification RTP/RTCP port range - 6000-6255 RTCP Support - disabled
SIP Settings	UDP and TCP Port – 5060 TLS Port – empty Realm – epygi Session Timer – disabled DNS Server for SIP – default SIP timers – RFC 3261
SIP Aliases	Host Aliases for SIP – undefined
RTP Streaming Channels (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Undefined
Gain Control Settings	For **QXFXS24** FXS lines: Transmit Gain: - 6 Receive Gain: 0 For **QXFXO4** FXO lines: Transmit Gain: 0 Receive Gain: 0 For **QXE1T1** E1/T1 trunk: Transmit Gain: 0 Receive Gain: 0 For **QXISDN4** ISDN trunks: Transmit Gain: 0 Receive Gain: 0
RADIUS Client Settings	RADIUS client – disabled
Dial Timeout	4 seconds
Call Quality Notification	Disabled
Hold Music (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Play Hold Music – Local Music Percentage of system memory – 1%
Firewall	Enable NAT – enabled Enable Firewall - disabled Enable IDS - disabled Ping Stealth – enabled Fool Portscanner (for QXFXS24 gateways only) – disabled
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all) SIP Access (Allowed for all) No user defined services and IP pool groups
SIP IDS Settings	Enable SIP IDS – enabled

Parameter	System Default Value
	Add the IP address into the Blocked IP list in Firewall – enabled Discard SIP messages from IP address – enabled
IP Routing Configuration	No Routes
DHCP Advanced Settings	DHCP Options Gateways – 172.28.0.1 Subnet mask – 255.255.0.0 Domain name servers – 172.28.0.1 NBT name servers – 0.0.0.0 NTP servers – 172.28.0.1 Domain name – epygi-config.loc Overload tftp server name – 172.28.01 DHCP Server Statements: Authoritative – enabled Ping Check – enabled Ping timeout – 1 sec
DNS Server Settings	Time to live (TTL) – 86400 seconds, Mail Exchange (MX) – undefined, No aliases defined.
Dynamic DNS	Disabled
SNMP Settings	SNMP – disabled
VLAN Settings	Undefined
IPSec, PPTP and L2TP	No connections. RSA Key Management - 1024 bit key defined PPTP Server Configuration Subnet – 172.31.1.0/24 Authentication - MSCHAPv2, MPEE 128 bit L2TP Server Configuration Subnet – 172.31.2.0/24
Event Settings	"Display notification" for all events except Login and Firmware Update events. Those events have a "Do nothing" action assigned.
Call History – CDR Settings	Enable Call Reporting– enabled, 100 entries for all type of calls
Call History – Automatic Backup	Enable Automatic Downloading of Call Detail Records – disabled Number of Call Records To Download – 50 File Format –Tab Delimited Text (.log)
Statistics – Network Transfer	Time range of statistic table - Intraday Interface - LAN Show also as readable values - disabled
Statistics – PSTN Channel Usage (for QXFXO4, QXISDN4 and QXE1T1 gateways)	Time range of statistic table - Intraday Incoming Calls, Outgoing Calls and Maximum Active Calls - disabled
System Logs Settings	Enable User Logging – enabled Enable Developer Logging – enabled Log Lines to Show – 50 Comment – undefined
Remote Logs Settings	Disabled
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Extension (all accessible pages for extension), Local Administrators (all accessible pages for localadmin). GUI Access Password-Old Password (empty), New Password (empty), Confirm New Password(empty). Phone Access Password- Old Password (empty), New Password (empty), Confirm New Password(empty).
Automatic Backup	Disabled
Automatic Firmware Update	Disabled

Extension Settings

Parameter	System Default Value
Account Settings	Display Name – undefined

Parameter	System Default Value
	User Password Protection – disabled both for incoming and outgoing calls User's Name for Extensions Directory – default Custom Voice Messages – default
Basic Services – General (for QXFXS24 gateways only)	Enable Call Waiting Service – enabled
Caller ID Services (for QXFXO4, QXISDN4 and QXE1T1 gateways)	No entries in the table. For Any Callers – all services are disabled Call Blocking message files – default

Appendix: Glossary

A

Asymmetric Digital Subscriber Line (ADSL) - is a method for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. An ADSL circuit must be configured to connect two specific locations, similar to a leased line. A commonly discussed configuration of ADSL would allow a subscriber to receive data (download) at speeds of up to 1.544 Megabits per second, and to send (upload) data at speeds of 128 kilobits per second. Thus the 'Asymmetric' part of the acronym. Another commonly discussed configuration would be symmetrical: 384 kilobits per second in both directions. In theory ADSL allows download speeds of up to 9 megabits per second and upload speeds of up to 640 kilobits per second. ADSL is often discussed as an alternative to ISDN, allowing higher speeds in cases where the connection is always to the same place.

Asynchronous Transfer Mode (ATM) - a 53-byte cell-switching technology well suited for carrying voice, data, and video traffic on the same infrastructure. It is inherently scalable in throughput and was designed to provide Quality of Service (QoS).

Auto Attendant (AA) - a feature providing remote access to QX voice connectivity services. Specifically, it supports remote connection to QX extensions, to their mailboxes and for making calls to other destinations. Remote access to QX AA is possible through IP and PSTN calls.

Auto Redial - a service that allows automatically recalling the destination that was busy.

C

Call - establishment of (or attempt to establish) a voice or data connection between two endpoints, or between two points that provide a partial link (e.g., a trunk) between two endpoints.

Call Blocking - a QX service that allows blocking unwanted incoming or outgoing calls over QX.

Call Forwarding - a QX service that allows transferring a call to another destination in case the QX user is busy, not answering or unconditional.

Call Hold - a QX service that allows holding the call in order to make another one, or to answer the second incoming call. The first call partner will listen to music while being on hold.

Call Waiting - a QX service that allows receiving a second call while being busy with the first one. The waiting party will hear a beeping during the conversation.

Caller ID - caller information is displayed on the called party's phone.

Central Office (CO) - a local switching system that connects lines to lines and lines to trunks. Sometimes used to refer to the building in which a switching system is located and the associated equipment. It is also the physical point where calls enter the long distance network.

CODEC - COmpression/DECompression that transforms analog voice into a digital bit stream and vice-versa. It is now an overall term for the technology used in digital audio and video.

D

D-channel - In ISDN, the 16-kb/s segment of a 144-kb/s, full-duplex subscriber service channel that is subdivided into 2B+D channels, i.e., into two 64-kb/s clear channels and one 16-kb/s channel for the ISDN basic rate. **Note 1**: The D channel is usually used for out-of-band signaling. The two 64-kb/s clear channels are used for subscriber voice and data services. **Note 2**: The D-channel specifications are addressed in the CCITT Recommendation for the Integrated Services Digital Network (ISDN). **Note 3**: The D-channel may be 64 kb/s for the primary rate ISDN service.

Data Encryption Standard (DES) - a block cipher algorithm for encrypting (coding) data so it is nearly impossible for anyone without the decryption key to get the data back in unscrambled form. The DES standard enciphers and deciphers data using a 64-bit key.

Daylight saving time (**DST)** - a convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

Dial peer - an addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

Dial plan - a description of the dialing arrangements for customer use on a network.

Digital Signal Processor (DSP) - A specialized microprocessor that performs calculations on digitized signals that were originally analog, and then forwards the results. The big advantage of DSPs lies in their programmability. DSPs can be used to compress voice signals to as little as 4,800 bps. DSPs are an integral part of all voice processing systems and fax machines.

Digital Subscriber Line (DSL) - public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Since most DSL technologies do not use the entire bandwidth of the twisted pair, there remains room for a voice channel.

Distinctive Ringing - QX service that allows a specific ringing pattern assignment for particular callers over QX.

Domain - a place on the Internet you can visit with your browser, i.e., a www site. It also might be a single computer or computers masqueraded as a single computer. On the Internet, the domain is the address that gets you there.

Domain name - in a network using the TCP/IP, the full domain name consists of a sequence of names (labels) separated by periods (dots), for example, qx.epygi.com.

Domain Name System (DNS) - a system used on the Internet for translating names of network nodes into their addresses.

Downstream - in communications, there are two circuits. One coming toward you and the other going away from you. Downstream is another term for the transmission coming toward you.

Dual-Tone Multifrequency (DTMF) - a method of signaling consisting of a push-button or touch tone dial that sends out a sound consisting of two discrete tones that are picked up and interpreted by telephone switches (either PBXs or central offices).

Dynamic Host Configuration Protocol (DHCP) - a network standard regulating the IP address and other information assigned to the clients by the server.

Dynamic Host Control Protocol (DHCP) - a protocol that is used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention.

E

E1 - wide area network digital transmission scheme. E1 is the European equivalent of a T1 line. The E1's higher clock rate (2.048 MHz) allows for 32 separate 64Kbps channels, which include one channel for framing and one channel for D-channel information.

Ethernet - a localarea network used for connecting computers, printers, workstations, terminals, servers, etc., within the same building or campus. Ethernet operates over twisted pair and/or over coaxial cable at speed up to 10Mbps.

Ethernet Controller - the unit that connects a device to the Ethernet cable.

Ethernet Switch - the device that connects local area networks.

Extensions - users over QX.

External User - users connecting QX by IP or PSTN calls.

F

Firewall - a combination of hardware and software that limits the exposure of a computer or group of computers to an attack from outside. A firewall is a system or combination of systems that enforce a boundary between two or more networks. One purpose of an Internet firewall is to provide a single point of entry where a defense can be implemented, allowing access to the Internet resources from within the organization, and providing controlled access from the internet to hosts inside the organization's internal networks.

Firmware - is computer or OS required software that resides on ROM

Foreign Exchange (FX) - a Central Office trunk that has access to a distant Central Office. A dial tone is returned from that distant Central Office and a location can be reached in the area of the foreign Central Office by dialing a local number.

Foreign Exchange Office (FXO) - a service that can be ordered from the telephone company that provides local telephone service from a central office that is outside (foreign to) the subscriber's exchange area. To generate a call from the computer telephony system to the POTS set, you will need a FXS connection configured. See also FXS.

Foreign Exchange Station (FXS) - Interface that connects directly to a standard telephone, fax machine, or similar device over a standard RJ-11 modular telephone cable, and supplies ringing voltage, dial tone, and similar signals to it. see FXO

Framing - A procedure for controlling errors. Consists of inserting bits so the receiver can identify the time slots allocated to each subchannel

G

Gatekeeper - is the central control entity that performs management functions in a Voice and Fax over IP network and for multimedia applications such as video conferencing. Gatekeepers provide intelligence for the network, including address resolution, authorization, and authentication services, the logging of call detail records, and communications with network management systems. Gatekeepers also monitor the network for engineering purposes as well as real-time network management and load balancing, controlling bandwidth, and providing interfaces to existing legacy systems.

Gateway - an entrance into and out from a communications network. Technically, a gateway is an electronic repeater that intercepts and steers electrical signals from one network to another.

Greeting - voice messages that are played to the QX users or users calling to the QX activating specific services.

H

Hold Music - music played to the party that is on hold.

Host - an intelligent device attached to the network; can be also a mainframe computer.

Host Name - the name given to a mainframe computer or device.

Hunt Grouping - the QX service that allows configuring several users over QX to ring in series when a specific call arrives.

Hypertext Transfer Protocol (HTTP) - the protocol used by Web browsers and Web servers to transfer files, such as text and graphics files.

I

Integrated Services Digital Network (ISDN) - is a system of digital phone connections which allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. There are two basic types of ISDN service: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI is a basic service is intended to meet the needs of most individual users. PRI is intended for users with greater capacity requirements

Internet Control Message Protocol (ICMP) - a network-layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

Internet Protocol (IP) - a unique, 32-bit number for a specific TCP/IP host on the Internet, normally printed in decimal form (for example, 128.122.40.227). Part of the TCP/IP family of protocols, it describes the software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages.

Internet Service Provider (ISP) - a vendor who provides direct access to the Internet or a company that provides Internet access to other companies and individuals.

Intrusion Detection System (IDS) - is a firewall, but together with deleting the dangerous packets or packets including intrusion attacks, IDS also keeps information about dropped packets and the senders responsible for them.

IP address - also known as the Internet Address, is a unique 32-bit identifier for a specific TCP/IP host computer on a network. IP addresses are in dotted decimal form, such as 192.168.10.26, with each of the four address fields assigned as many as 255 values.

IP address Mask - A range of IP addresses defined so that only machines with IP addresses within the range are allowed access to an internet service. To mask a portion of the IP address, replace it with the asterisk wild card character (*). For example, 192.44.*.* represents every computer on the internet with an IP address beginning with 192.44

IP Gatekeeper - defines the policies that govern a multimedia system such as dialing plans, user privileges, bandwidth consumption, and others. The gatekeeper also provides the means to extract information from such a system for various purposes, e.g., billing information, users that are logged in, etc. The gatekeeper is also a focal point for the introduction of supplementary services.

IP Gateway - most commonly, a network device that converts voice and fax calls, in real time, between the public switched telephone network (PSTN) and an IP network. The main IP gateway functions include voice, fax, compression/decompression, packetization, call routing, and control signaling. Additional features may include interfaces to external controllers, such as gatekeepers or soft-switches, billing systems, and network management systems.

IP PBX - an enterprise-based IP data network device that switches VoIP telephone traffic.

IP Telephony - a technology that allows voice phone calls to be made over the Internet or other packet networks using a PC via gateways and standard telephones.

IPSec - is used to provide security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

J

Jitter Buffer - the buffer that collects incoming packets to place them in the right order. If the network has a high delay variation, increasing the Jitter Buffer can improve the audio quality, but this also increases the delay.

L

LED - Light-Emitting Diode, A semiconductor device that emits visible light when conducting current. Has replaced incandescent lamps as indicators in most electronic equipment.

Lifeline POTS - a voice telephone line that works even if electricity is cut off at the customer premises, since the line is powered from emergency backup at the central office. Multiple lifeline POTS lines can be delivered on one copper pair with the use of a digital line powered pair gain system. A basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

Local Area Network (LAN) - a short distance data communications network (typically within a building or campus) used to link computers and peripheral devices under some form of standard control.

Login -the procedure of identifying a user with a username and a password to enter into the protected field.

M

Many Extensions Ringing - a QX service that allows configuring several users over QX to ring simultaneously when a specific call arrives.

Media Access Control (MAC) Address - the address for a device as it is identified at the Media Access Control layer in the network architecture.

Media Access Control (MAC) Layer - is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

Media Gateway - a generic class of products grouped under the Media Gateway Control Protocol (MGCP). A major function of the media gateway is simple IP/TDM conversion under the control of a softswitch.

N

Name server - a directory service that provides a mapping between a resource's global name and its physical location in the network.

Network Address Translation (NAT) - is used to allow LAN devices that do not have their own static IP addresses to connect to the Internet sharing an IP address. NAT will assume control of assigning their IP address. Furthermore, the NAT takes care that packets will reach the LAN PC that originated the traffic. This mechanism is absolutely transparent for the users (or the PCs in the LAN).

Network Time Protocol (NTP) - a protocol that is used for time counting in the Internet, based on the atomic clocks with the precision in milliseconds. This is the recommended protocol for synchronizing the time of hosts in the network.

P

Packetization Interval - the time interval between two RTP packets of the same stream. If the interval is increased, the overhead is decreased but the voice quality might deteriorate. If the interval is decreased, the network load is increased and the delay is reduced.

Password - a secret alphanumeric string used to identify and to allow the user to have access to a system.

PCM - a form of modulation in which the information signals are sampled at regular intervals and a series of pulses in coded form are transmitted representing the amplitude of the information signal at that time.

Point-to-Point Protocol (PPP) - allows a computer to connect to the Internet with a standard dial-up telephone line and a high-speed modem and to enjoy most of the benefits of the direct connection.

Point-to-Point Tunneling Protocol (PPTP) - enables virtual private networking - enabling secure remote access to corporate networks over the Internet.

POTS (Plain Old Telephone Service) - is the standard telephone service that most homes use. It is also referred to as the PSTN, or the Public Switched Telephone Network

Private Branch Exchange (PBX) - a telephone switch owned privately, usually by a large company. If it owns a PBX, a company does not need to lease a telephone line for each telephone set at a site.

Proxy server - an intermediate device that receives SIP requests from a client and then initiates requests on the client's behalf.

Public Switched Telephone Network (PSTN) - refers to the local telephone company.

R

Real-Time Transport Protocol (RTP) - the Internet-standard protocol for the transport of real-time data, including audio and video, allows applications to synchronize audio and video information. RTP connections are established between servers across the Internet after voice has been converted to IP format. RTP is used in virtually all Voice-over-IP architectures, for videoconferencing, media-on-demand, and other applications.

Real-Time Transport Control Protocol (RTCP**)** - is the control protocol that works in conjunction with RTP. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants. Feedback of information to the application can be used to control performance and for diagnostic purposes.

Registration - procedure of user subscribing to a server. Usually some personal parameters such as username, password, etc., are required upon registration.

Remote Testing - remote connection from the Epygi Support office to the customer's QX for testing and/or for troubleshooting.

Router - A device that determines the next network point to which a data packet should be forwarded enroute toward its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet

RSA - is an asymmetric key system. It must be available on both sides of the VPN and generates on each side a different pair of keys, a private and a public key.

S

Security Parameter Index (SPI) - is an index to keep VPN tunnels distinct. A security association is defined by destination, protocol and SPI. Without the SPI, connections to the same gateway using the same protocol would not be distinguishable.

Session Initiation Protocol (SIP) - is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. SIP is increasingly used for Internet telephony signaling, in gateways, PC phones, softswitches, and softphones, but it is not limited to Internet telephony, and can be used to initiate and manage any type of session, including video, interactive games, and text chat.

Signaling - a process of sending a transmission signal over a physical medium for communication.

Silence Suppression - a method that allows disabling RTP packet transmission when there is no voice activity. This feature helps to avoid extra traffic when the RTP stream doesn't contains voice data.

Simple Network Management Protocol (SNTP) - the Internet standard protocol developed to manage nodes on an IP network.

SIP address - unique address of the users registered on the SIP server. The address can be used to connect the user. The full SIP address has the following format: "display name" <username@ipaddress:port>.

SIP server - this server is used for registering users. It gives a possibility to make IP connections between users registered on the same SIP server.

Software - PC programs.

Software PBX - a telephone system that converges voice and data on an industry-standard computing platform and uses computer telephony components that conform to industry standards. Since they conform to industry standards, software PBXs are interoperable with third-party systems and CT components. Conformance also allows software PBXs to run third-party enhanced applications such as desktop call control, graphical voice mail, automatic call distribution (ACD), IP gateways, follow-me call forwarding, unified messaging, and CRM integration.

Speed Calling - a service that allows making a personal address book for every QX user. A simple digit combination can be assigned to any destination phone number.

T

Transfer - a service giving a possibility to readdress incoming calls. Call Transfer can be conditional (with consultation) and unconditional (without consultation).

Transmission Control Protocol (TCP) - a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Transmission Control Protocol/Internet Protocol (TCP/IP) - is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

Trunk: - is a communications channel between two points, typically referring to large-bandwidth telephone channels between switching centers that handle many simultaneous voice and data signals.

Trunk Level 1 (T1) - a high-speed (1.544Mb/s) digital telephone line with the equivalent of 24 individual 64Kb/s channels that are joined via time division multiplexing. A T1 line can be used to transmit voice or data, and many are used to provide connections to the Internet. T1 is the North American equivalent of an E1 line.

U

UDP - a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagram without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.

Universal Serial Bus (USB) - is an interface with a protocol that is designed to handle a broad range of devices - telephones, modems, printers, etc.

Upstream- in communications, there are two circuits - one coming toward you and the other going away from you. Upstream is another term for the name of the channel going away from you.

URL - an identifier used to locate content that is transported via the HTTP protocol.

Username - identification name of the user. Usually used for registration and login.

V

VCI - parameter used to configure ATM settings and is usually given by the Internet provider.

Virtual Private Network (VPN) - connects two local networks (intranets) over the insecure Internet securely. VPN routers manage authentication between servers and clients and handle data encryption for the connection. Only authorized users can access the network and the data exchange cannot be intercepted. A VPN 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 VPN 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.

Voice mail - a brief message that external users can leave for the QX users in the event that nobody answers the call.

Voice Mail System (VMS) - a feature providing the possibility of leaving brief voice messages at the unavailable or busy QX extension's mailbox.

Voice mailbox -is the mailbox where voice mails are collected.

Voice message - help messages that are played to the user giving a hint on how to manipulate the menus within QX using the phone handset.

Voice Over Internet Protocol (VOIP) - technology used to transmit voice conversations over a data network using the Internet Protocol. This provides ability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality.

VPI - parameter used to configure ATM settings usually given by the Internet provider.

W

Wide Area Network (WAN) - a communications network used to connect computers and other devices across a large area.

Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD.
Software License Agreement

THIS IS A CONTRACT.
CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE HARDWARE OR SOFTWARE.

1. **License.** Epygi Technologies, LTD. (the "Licensor"), hereby grants to you a non-exclusive right to use the Quadro or QX Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may use the Licensed Materials only in connection with your operation of your Quadro or QX. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.

2. **Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or the transfer of the Licensed Materials is subject to the terms of this Agreement.

3. **Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.

4. **No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language under penalty of law.

5. **Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro or QX product. If you sell your license rights in the Licensed Materials, you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

6. **Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.

7. **Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

   EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES AND ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

8. **LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OF OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.

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

9. **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

10. **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227-19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.

11. **Entire Agreement.** It is understood that this Agreement, along with the Quadro or QX installation and administration manuals, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.

12. **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.

13. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.

14. **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.

    If you have any questions about this Agreement, please write to Epygi at 1400 Preston Road, Suite 300, Plano, Texas 75093 or call Epygi at (972) 692-1166.

15. **Free Software.**Certain software utilized in the Epygi products is free software in its original form or in its modified form. Both types of free software are available to you free of charge for redistribution or modification under certain conditions. Permission is granted to copy, distribute and or/modify any free software you wish to download, whether in its original or modified forms, under the GNU General Public License or Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation. **BECAUSE THE FREE SOFTWARE IS LICENSED FREE OF CHARGE, THERE IS ABSOLUTELY NO WARRANTY**. Please make sure you download the GNU license from www.gnu.org . For a list of free software go to http://www.epygi.com/about/free-software-list .