Manual II: Administrator's Guide

Edition 2, 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 IP PBX basically.

Manual II: Administrator's Guide

About this Administrator's Guide **8**

QX IP PBX's Graphical Interface **9**

- **Dashboard – Administrator's Main Page** **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 17
- **System Security** **18**
- **Licensed Features** **18**
  - Feature Keys 18
  - Free Trial Activation 19
- **Redundancy** **20**
- **Language Pack** **20**
  - Update Languages for IP Phones 21

Extensions Menu **22**

- **Extensions Management** **23**
  - Add Extension 24
    - User Extension Settings 25
    - Pickup Group Extension Settings 32
    - Call Park Extension Settings 34
    - Paging Group Extension Settings 36
    - ACD Group Extension Settings 37
    - Recording Box Extension Settings 40
    - Recording Box 42
    - Attendant Extension Settings 43
    - Extension Codecs 49
    - Call Park and Directed Call Park Service 51
    - Barge In Service 51
  - Add Multiple Extensions 52
  - User Extension Bulk Import 52
- **Conferences** **53**
  - Conferences Management 54
  - Add Conference 55
  - Email Default Settings 55
- **Upload Universal Extension Recordings** **55**
    - Upload Universal Extension Recordings - Hold music 56
- **Extensions Directory** **56**
- **Receptionist Management** **57**
- **ACD Management** **60**
- **Authorized Phones Database** **64**
    - Call Back Services 65

Interfaces Menu **67**

IP Lines **68**
IP Line Settings 69
Supported SIP Phones 69
Programmable Keys Configuration 70
IP Phone Templates 71
IP Phones Logo 72
FXS Gateways 73
FXS Lines **74**
FXS (On-board) Line Settings 74
Diagnostic Loopback 75
Hot Desking 75
FXO Settings **76**
E1/T1 Trunk Settings **77**
Incoming Interdigit Service 84
ISDN Trunk Settings **85**
External PSTN Gateways **89**
Authorization Parameters 89
Telephony Menu **90**
VoIP Carrier Wizard **91**
Call Routing Table **92**
Call Routing 99
Local AAA Table 100
Global Speed Dial Directory 100
Allowed Characters and Wildcards 101
Best Matching Algorithm 102
Entering SIP Addresses Correctly 105
SIP Tunnel Settings 105
Class of Service 106
Call Recording Settings **107**
NAT Traversal Settings **109**
General Settings 109
SIP Parameters 109
RTP Parameters 109
STUN Parameters 110
NAT Exclusion 110
RTP Settings **111**
SIP Settings **112**
SIP Aliases 113
TLS Certificates 113
Advanced Settings **113**
Voice Mail Common Settings 113
RTP Streaming Channels 114
Gain Control 114
3PCC Settings 115
RADIUS Client Settings 115
Dial Timeout 117
Call Quality Notification 117
Firewall Menu **118**
Firewall **119**
Firewall and NAT 119
Advanced Firewall Settings 119
IDS Log 119
Filtering Rules **120**
View All Filtering Rules 120
Incoming Traffic/Port Forwarding 121
Outgoing Traffic 121
Management Access 121
Call Control Access 121

SIP Access ... 122
Blocked IPs ... 122
Allowed IPs ... 122
Custom Services ... 123
Service Pool Configuration ... 123
IP Groups ... 124
IP Pool Configuration ... 124
SIP IDS Settings ... 126
Network Menu ... 127
IP Routing Configuration ... 128
IP Static Routes ... 128
IP Policy Routes ... 128
PPTP/L2TP Routes ... 129
DHCP Settings ... 129
DHCP Server ... 130
DHCP Advanced Settings ... 131
DHCP Leases ... 131
DHCP Settings for the VLAN Interface ... 132
DNS Settings ... 132
DNS Server Settings ... 132
Dynamic DNS Settings ... 133
PPP/ PPTP Settings ... 134
Advanced PPP Settings ... 134
SNMP Settings ... 135
Global SNMP Settings ... 135
SNMP Trap Settings ... 136
VLAN Configuration ... 136
VPN Configuration ... 137
IPSec Configuration ... 137
PPTP/L2TP Configuration ... 140
Status Menu ... 144
System Status ... 145
General Information ... 145
Network Status ... 145
Lines Status ... 145
Memory Status ... 147
Hardware Status ... 147
SIP Registration Status ... 148
IP Lines Registration Status ... 148
License Status ... 148
Events ... 149
System Events ... 149
Event Settings ... 149
Call History ... 150
Successful, Missed and Unsuccessful Calls ... 150
Call History Settings ... 151
CDR Archive ... 152
Archiving Settings ... 153
RTP Statistics ... 154
FAX Statistics ... 155
Conference History ... 155
Conferences ... 155
Successful Calls and Unsuccessful Outgoing Calls ... 156
CDR Settings ... 156
LAN/WAN ... 157
LAN and WAN Interface Statistics ... 157
Statistics ... 158
Network Transfer ... 158

PSTN Channel Usage ... 159
Maintenance Menu ... 160
Diagnostics ... 161
Security Diagnostics ... 161
Call Capture ... 161
Ping ... 162
Traceroute ... 163
System Logs ... 163
System Logs Settings ... 163
Remote Logs Settings ... 164
Logs Archive ... 164
User Rights Management ... 165
Users ... 165
Roles ... 166
Backup/Restore ... 166
Automatic Backup ... 167
Download Legible Configuration ... 167
Upload Legible Configuration ... 168
Firmware Update ... 168
Upload Firmware ... 169
Get Firmware From Server ... 170
Automatic Firmware Update ... 171
Reboot ... 171
Registration Form ... 172
Appendix: PBX Services for QX IP PBX's Administrator ... 173
Appendix: Conference Services for Moderators and Participants ... 174
Appendix: System Default Values ... 176
Administrator Settings ... 176
Extension Settings ... 182
Appendix: Moderator's Menus ... 184
Conference Moderator's Main Page ... 184
Conference Progress ... 185
Recorded Conferences ... 186
Conference Settings ... 187
General Settings ... 187
Recording Settings ... 188
Customization ... 189
Participants ... 190
New Participants Configuration ... 191
Handset Added Participants Configuration ... 192
Schedule ... 192
Send Notification Mail ... 193
Appendix: Software License Agreement ... 194

Manual III: see Extension User's Guide

Describes detailed the menus available for extension users and includes further all call codes at a glance.

About this Administrator's Guide

The QX IP PBX Manual is divided into three parts:

- Manual-I: Installation Guide gives step-by-step instructions to provision the QX IP PBX and configure the phone extensions with the Epygi SIP Server. After successfully configuring the QX IP PBX, users will be able to make SIP phone calls to remote QX IP PBX devices, make local calls to the PSTN and to access the Internet from devices connected to the LAN.
- Manual-II: Administrator's Guide explains all QX IP PBX management menus available for administrators only. It includes a list of all System Default Values.
- Manual-III: Extension User's Guide explains all QX IP PBX 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 IP PBXs offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular QX IP PBX as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

QX IP PBX's Graphical Interface describes to the QX IP PBX'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 IP PBX management.

Appendix: PBX Services for QX IP PBX's Administrator explains PBX features for administrator accessible from the handset.

Appendix: System Default Values lists all factory defaults.

Appendix: Moderator's Menus explains all menus that can be accessed and configured by conference moderators. (Applicable if the Conference Server and/or the Video Conferencing features are activated on the system.)

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

QX IP PBX's Graphical Interface

Dashboard – Administrator's Main Page

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 below the table.

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

The **Start Recording** button next to each active call (except for calls to Auto Attendant) is used to manually start the recording of the corresponding call. Once the call recording is started, the button changes to **Stop now** used to manually stop the call recording. The call recording can be restarted again if needed.

The following main menus are available on Epygi QX50/QX200/QX2000: **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 or Conference extensions:

- **Your Extension** (see Manual III: Extension User's Guide)
- **Conference**

The **Return** link is used to return to the Epygi QX50/QX200/QX2000 Management page.

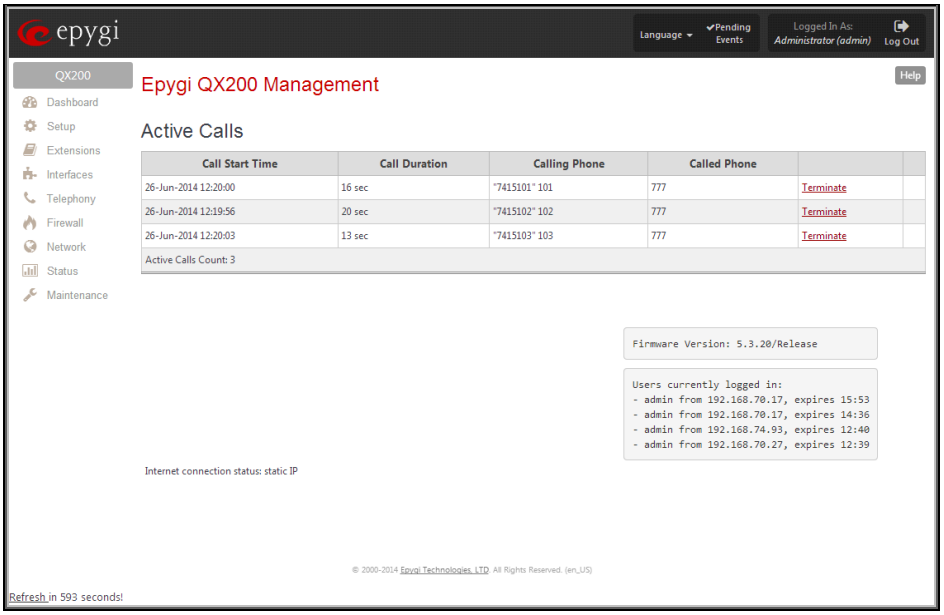


Fig.II- 1: Epygi QX IP PBX Management page

The functional button **Renew Wan IP Address** appears on the administrator's main **QX IP PBX Management** page if the QX IP PBX 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 IP PBX 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 IP PBX 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 IP PBX'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**
  - For **QX50/QX200** - System (LAN)
  - For **QX2000** – System Configuration Wizard
  - For **QX50/QX200** - Internet (WAN)
  - For **QX2000** – Uplink Configuration Wizard
  - Date and Time
  - Email (SMTP)
  - Short Text Messaging (SMS)
- **System Security**
- **Licensed Features**
  - Feature Keys
  - Free Trial Activation
- **Redundancy**
- **Language Pack**

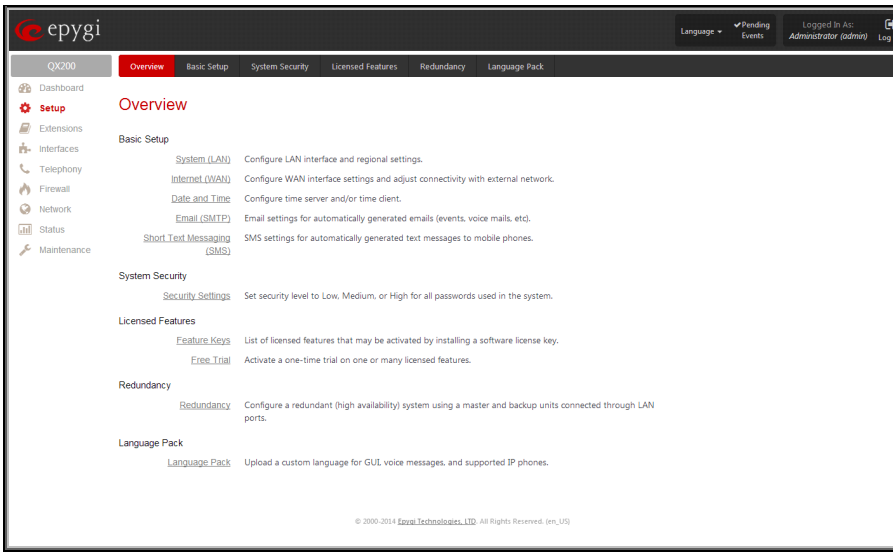


Fig.II- 2: Setup Menu page

Basic Setup

System (LAN) – System Configuration Wizard

The **System Configuration Wizard** allows the administrator to define the QX IP PBX's Local Area Network settings and to specify regional configuration settings to make QX IP PBX operational in its LAN. The **System Configuration Wizard MUST be run upon QX IP PBX'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)
- Emergency Codes and PSTN Access Code Settings (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.

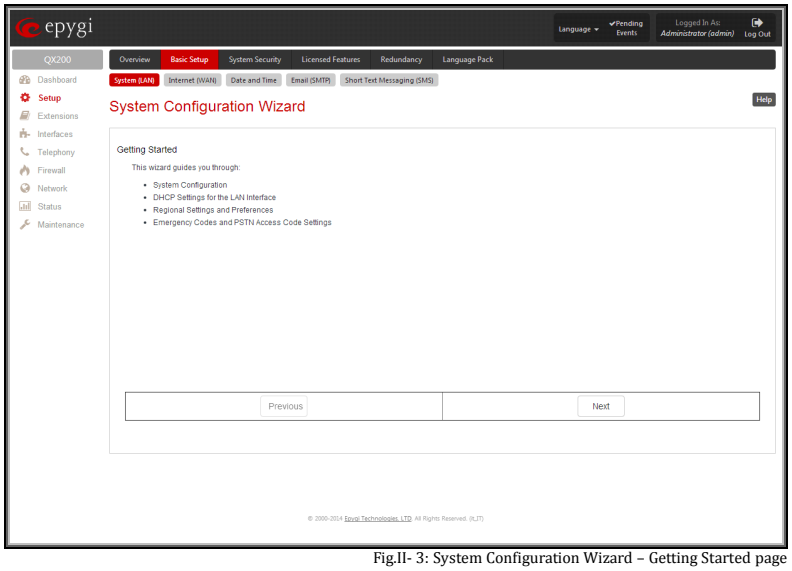


Fig.II- 3: System Configuration Wizard – Getting Started page

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

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

Host Name requires a host name for the QX IP PBX device.

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

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

Subnet Mask requires the QX IP PBX hosts' Subnet Mask.

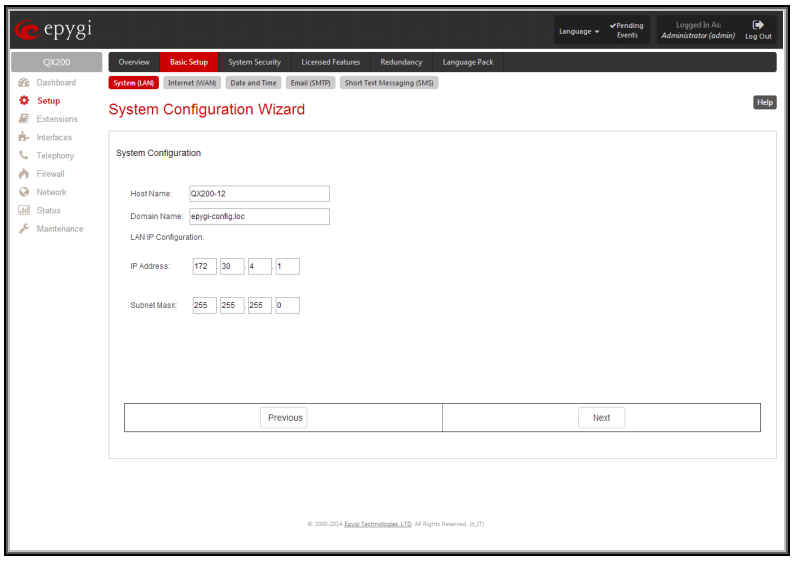


Fig.II- 4: System Configuration Wizard - System Configuration page

The **Regional Settings and Preferences** are used to select settings specific to the location of the QX IP PBX. 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 IP PBX 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.

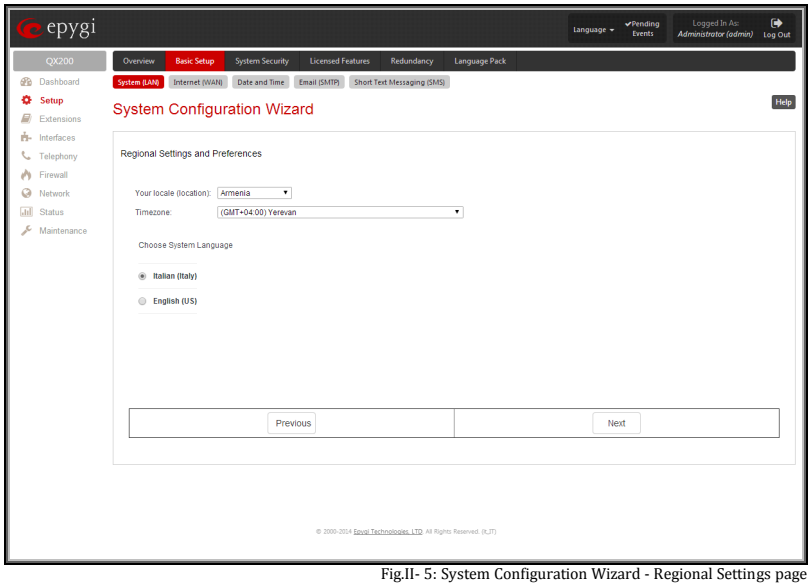


Fig.II- 5: System Configuration Wizard - Regional Settings page

The **Emergency Codes** and **PSTN Access Code Settings** are used to configure the emergency dial plan.

The **Emergency Codes** text field requires the PSTN numbers of the emergency or lifeline services. Multiple emergency codes, separated by commas, can be inserted in this field. For each emergency code, a routing pattern will be generated in the Call Routing Table, which will allow faster and easier calls to emergency destinations.

The **PSTN Access Code** drop down list allows you to select the prefix code for accessing the PSTN line in the routing mode. Dialing the digits inserted in this text field will provide the PSTN dial tone when dialed from the handset.

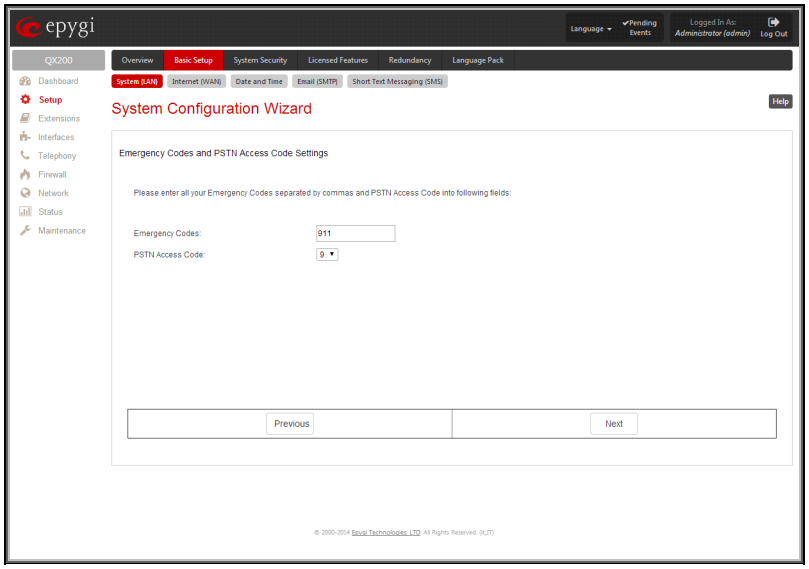


Fig.II- 6: System Configuration Wizard - Emergency Codes and PSTN Access Code Settings page

Internet (WAN) - Internet Configuration Wizard

The **Internet Configuration Wizard** (**Uplink Configuration Wizard** in case of QX2000) allows the administrator to configure the WAN interface settings and to adjust QX IP PBX's connectivity with an external network. The **Internet Configuration Wizard MUST be run for QX IP PBX 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.

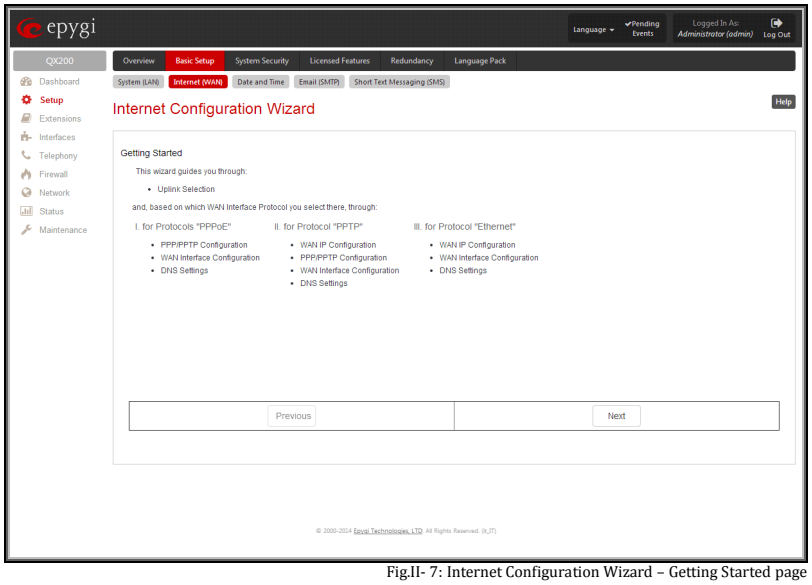


Fig.II- 7: Internet Configuration Wizard – Getting Started page

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

- Uplink configuration (see below)

For Protocols **PPPoE** (available only for QX50/QX200):

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

For Protocols **PPTP** (available only for QX50/QX200):

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

For Protocols **Ethernet**:

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

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

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

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

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

- **PPPoE** (available only for QX50/QX200) - turns on the PPP over an Ethernet connection.
- **PPTP** (available only for QX50/QX200) – turns on the Point to Point Tunneling Protocol (**PPTP**) interface used for the connection between QX IP PBX and ADSL modem. A fixed IP address configuration is needed in this case.
- **Ethernet** - turns on the Ethernet connection

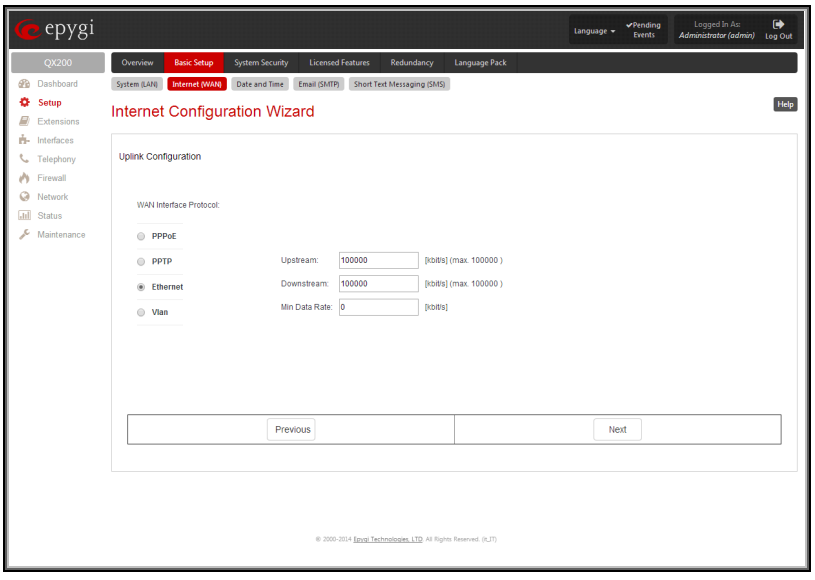


Fig.II- 8: Internet Configuration Wizard - Uplink Configuration page

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

The bandwidth provided by the ISP has to be specified in the text fields **Upstream Speed** and **Downstream Speed**. The default entry in both fields is 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 IP PBX'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 IP PBX WAN interface.

Subnet Mask requires the subnet mask for the QX IP PBX 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.

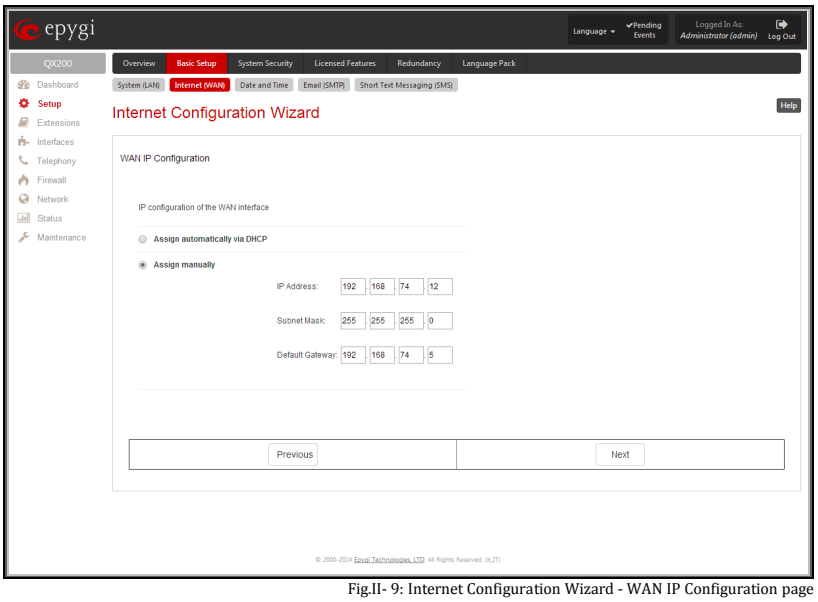


Fig.II- 9: Internet Configuration Wizard - WAN IP Configuration page

The **WAN Interface Configuration** page may be used to modify the MAC address of the QX IP PBX. 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 IP PBX.
- **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.

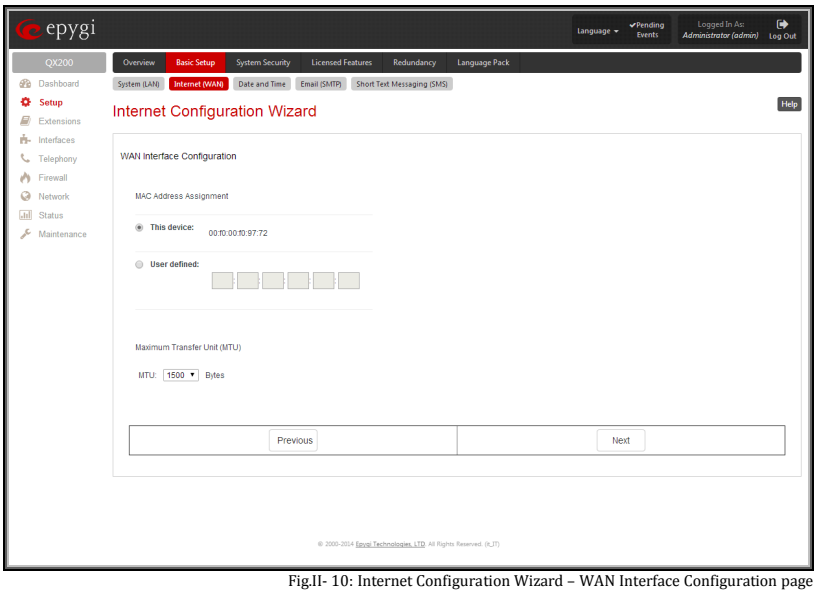


Fig.II- 10: Internet Configuration Wizard – WAN Interface Configuration page

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 IP PBX, thus QX IP PBX becomes the timeserver for its LAN.

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

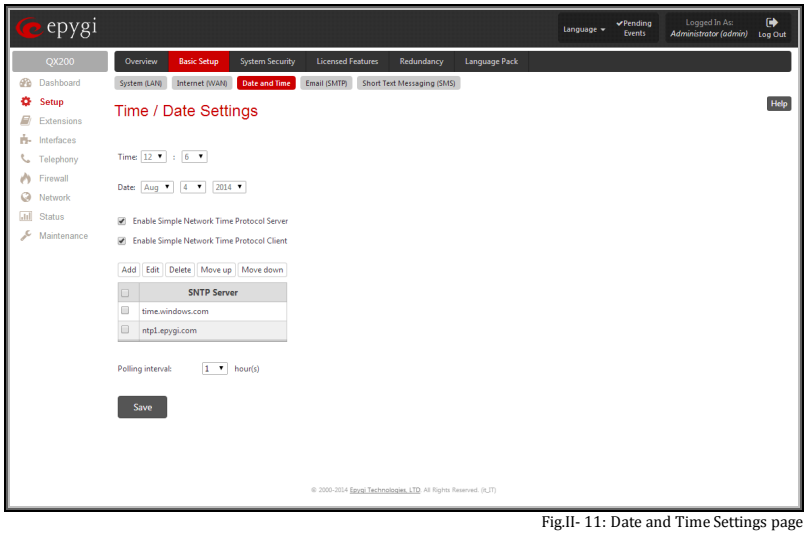


Fig.II- 11: Date and Time Settings page

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 IP PBX's date/time is not being updated automatically).

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

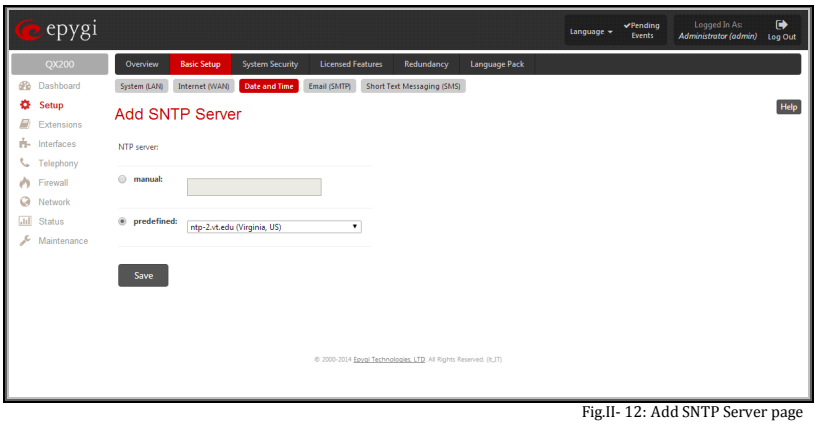


Fig.II- 12: Add SNTP Server page

Attention: Date and Time Settings will be reset if QX IP PBX 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 Events page. System mail must be enabled and the SMTP server needs to be configured for voice message transmission to the extension user's mailing account.

QX IP PBX may automatically generate emails to the administrator:

- If events specified in the Events list occur
- If voice mails are set from the **Voice Mail Settings** (see Manual III: Extension User's Guide) to be sent as e-mail

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 IP PBX 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 IP PBX 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.

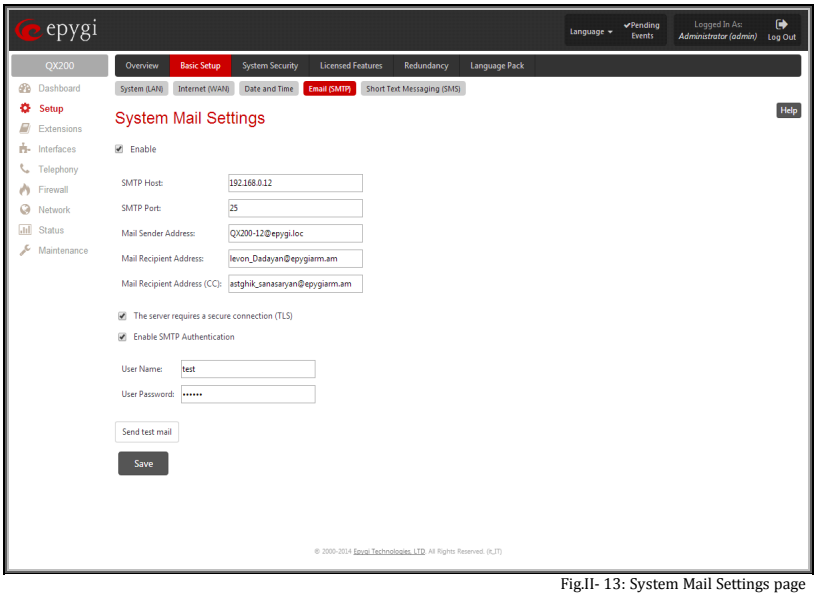


Fig.II- 13: System Mail Settings page

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

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

SMS Sender Address requires the source address for the QX IP PBX 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.

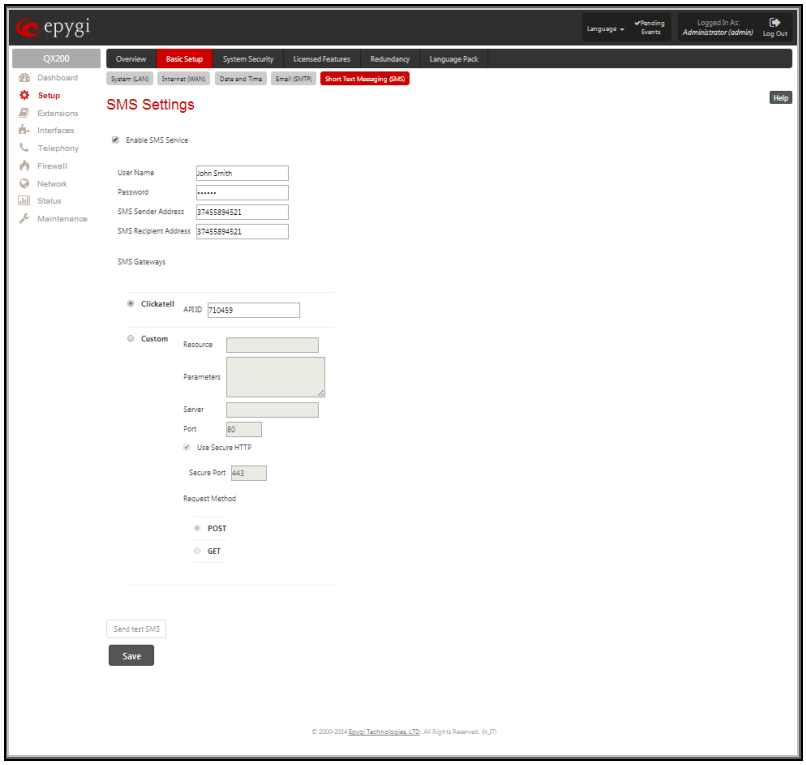


Fig.II- 14: SMS Settings page

- **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 IP PBX (voice mail notification, event notification, etc.)

  Server text field requires the IP address or the host name of the SMS gateway.

  Port text field requires the port number of the SMS gateway.

  Use Secure HTTP checkbox enables access to SMS server via HTTPS. Checkbox selection enables a **Secure Port** text field that requires the port number for HTTPS traffic.

  Request Method manipulation radio buttons allow to select the HTTP request method used by QX IP PBX 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".

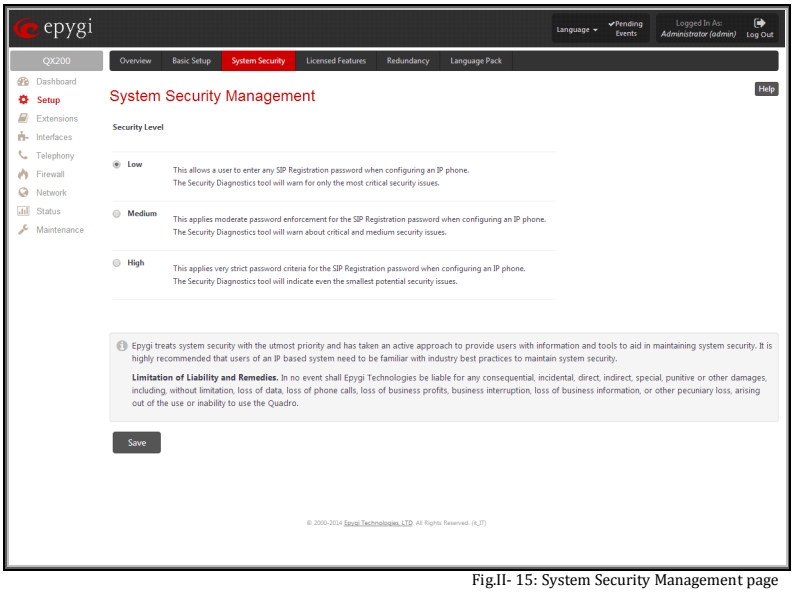


Fig.II- 15: System Security Management page

Licensed Features

Feature Keys

This page lists all features that may be activated by a software key, characterized by a **Feature Description** and provided with its **Status:**

- **No Key Found** - the feature is currently not available.
- **Reboot Needed** - the feature key has been entered and QX IP PBX needs to be rebooted.
- **Activated** - the feature is now available on the QX IP PBX.

Following features may be activated via the software key:

- **Debug** – enables SSH connection towards the QX IP PBX for debugging purposes.
- **3pcc Support** - enables Third Party Call Control feature on the QX IP PBX. The feature allows the call controlling applications running on a user PC to remotely initiate and handle calls on the QX IP PBX and to subscribe for certain event notifications from the QX IP PBX.
- **ACD Support** - enables the ACD Management feature which provides contact center solution for queuing and automatic distribution of the calls between contact center agents.
- **Barge In** – enables the Barge In Service on the QX IP PBX. The feature allows the PBX users to participate to the third party's calls while remaining imperceptible.
- **Redundancy** – activates the Redundancy feature on the QX2000. Redundancy feature is readily available for the QX50/QX200 by default, without a software license key.
- **DCC Pro Support** - allows run with QX IP PBX the Pro-level Desktop Communication Console (the application description can be found at Epygi Technical Support).

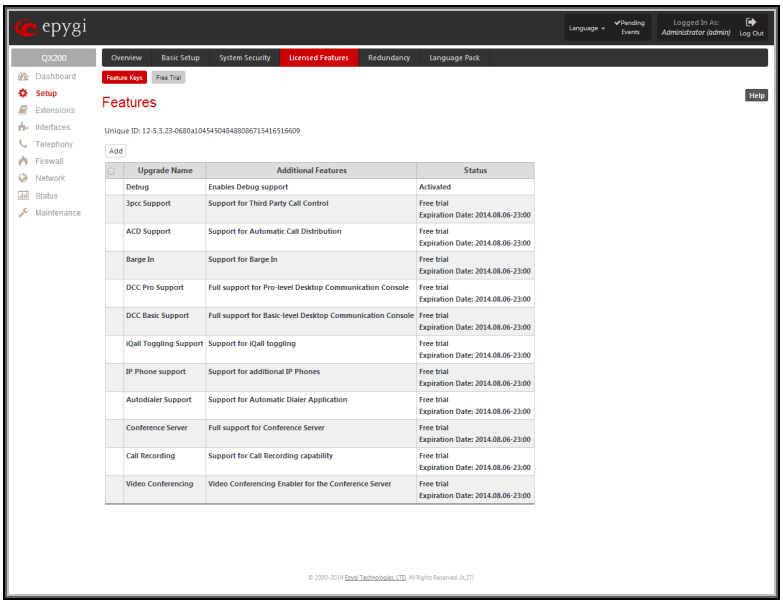


Fig.II- 16: Features page

- **DCC Basic Support** - allows run with QX IP PBX the Basic-level Desktop Communication Console (the application description can be found at Epygi Technical Support).
- **iQall Toggling Support** - this feature enables users to alternate the call from their mobile device iPhone running iQall to their desk phone without the call being dropped.

- **IP Phone Support -** enables additional IP phones support on the Epygi QX50/QX200/QX2000. This feature key allows activating up to 8, 16 or 32 additional IP lines for QX50, up to 8, 16, 32, 64 or 128 additional IP lines for QX200 and up to 8, 16, 32, 64 or 128 additional IP lines for QX2000 which will bring to a maximum 2000 total IP lines for QX2000.
- **Autodialer Support** - allows run with QX IP PBX the Autodialer application (the application description can be found at Epygi Technical Support).
- **Conference Server** - activates the conferencing feature allowing the system to act as a standalone conference server. This allows up to 16 person conference calls for QX50, up to 32 person conference calls for QX200 and up to 288 conference calls for QX2000 to be set up and offers a bundle of helpful features to easily manage the conferences.
- **Call Recording** – activates the **Call Recording** feature which is used to record PBX, SIP or PSTN calls on the QX IP PBX and save the recordings into the local recording box or upload to the remote server.

  Please Note: When using **Call Recording** on the QX50/QX200 it is advisable to use an SD memory card to expand the system memory.
- **Video Conferencing** – activates the Video Conferencing feature on the system. This allows up to 16 person video conference calls on QX200, up to 8 person video conference calls on QX50 and up to 104 video conference calls on QX2000. The other participants of conferences can use only audio connection.

To enter a **Feature Key**, click **Add**. A page with the **Feature Key** text field is opened. Enter the key and press **Save**. The status of the selected feature entry will change to **Reboot needed**. Reboot the QX IP PBX and the feature will receive the status **Activated.**

To receive a **Feature Key**, register the QX IP PBX device and send a corresponding request to Epygi's Technical Support. This request must include the **Unique ID** that is displayed in the **Features** page above the features list.

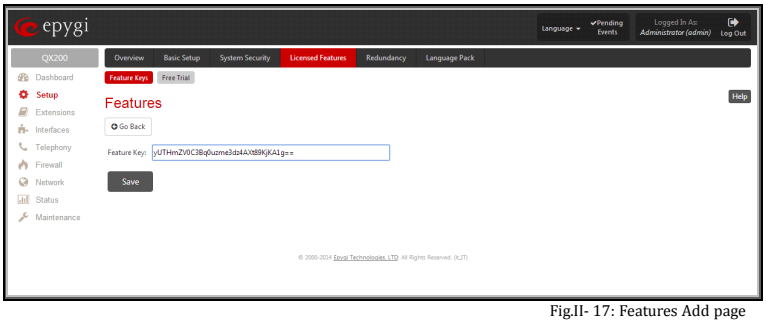


Fig.II- 17: Features Add page

Free Trial Activation

This page allows activating the QX IP PBX optional features for a trial. This page lists all QX IP PBX features that may be activated for a trial, characterized by a **Feature Description** and provided with its **Status**.

Expiration Date/Time used to specify the trial period. Upon expiring the specified period the QX IP PBX will reboot and trial features will disable.

User has to select the appropriate checkboxes under **Activate** column, specify the needed count under **Count Column** and save. The QX IP PBX will reboot and trial features activate. The syntax for values under **Count** is the following:

- **IP Phone support** - the number for additional IP lines.
- **ACD support** - enables the ACD Management feature support on the system.
- **3pcc Support** - enables the 3pcc feature support on the system.
- **Barge In Support** - enables the Barge In feature support on the system.
- **Redundancy** - enables the Redundancy feature support on the QX2000.
- **Call recording** - the number for simultaneous call recordings.
- **DCC Pro Support** - the number for licensed Pro-level DCC extensions.
- **DCC Basic Support** - the number for licensed Basic-level DCC extensions.
- **DCC Basic Support** - the number for licensed Basic-level DCC extensions.
- **iQall Toggling Support** - the number for licensed iQall extensions.
- **Autodialer Support** - the number of maximum simultaneous Auto Dialer calls.
- **Conference Server** - the number for maximum conference calls.
- **Video Conferencing** - the number for maximum video conference calls.

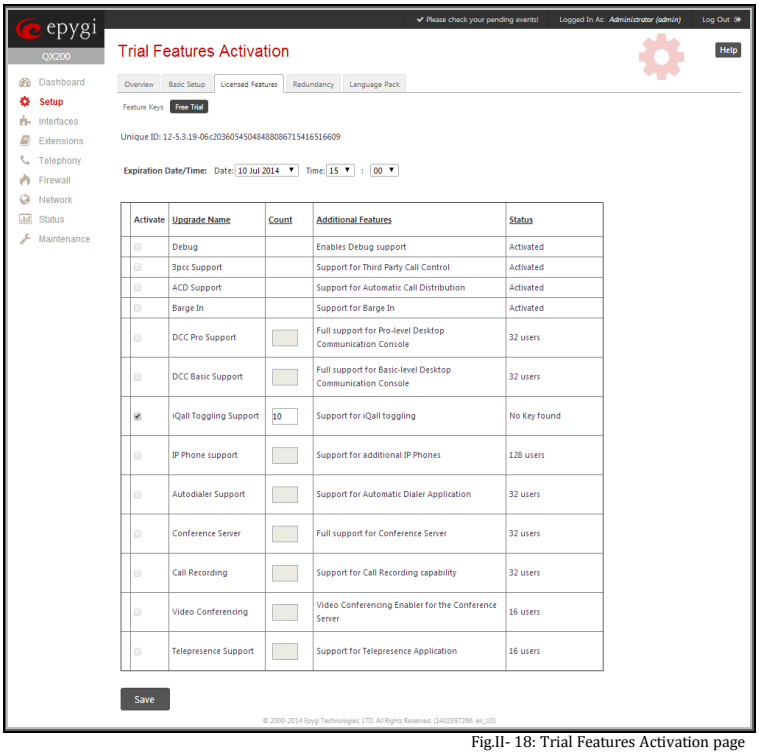


Fig.II- 18: Trial Features Activation page

Redundancy

Redundancy feature is used to increase QX IP PBX device availability using second QX IP PBX as a backup unit. This requires two units running the same firmware version and connected to each other through Ethernet or LAN ports, depending on the device model.

The idea of redundancy is to ensure uninterrupted functionality of the QX IP PBX. The Redundancy Settings should be configured on both QX IP PBXs. One of the QX IP PBXs is configured as a master, the second one as a backup unit.

Please Note: To setup a redundant network, you should first startup the master device with all attached IP phones and other devices, make sure it works normally and then startup the backup device.

If the master device becomes unavailable, which can be caused by power loss, reboot or network malconfiguration, the second QX IP PBX becomes automatically available and starts to run as a master device. Depending on the configuration, the second QX IP PBX can remain master or go to the backup mode once the first device becomes available again.

Attention: During failover procedure all active calls will be disconnected and the system will be out of service during 2-5 minutes (depending on the number of IP phones connected to the system), which is needed for running the applications and rebooting the phones. If there are IP phones in the network that are not auto configured by QX IP PBX (IP phones not supported by Epygi) or IP phones with the changed login name and password, you will need to reboot them manually. After failover the license keys, firmware and language pack are not being transferred from the master to backup QX IP PBX therefore, so make sure both QX IP PBXs are configured identically in the redundant network before enabling redundancy mechanism.

When you login to the device which runs in a backup mode, only **Redundancy Settings** are available. All other GUI configuration settings are non editable and automatically synchronized with the master device's configuration.

To ensure the interaction between the master and slave devices, corresponding configuration should be done in the Redundancy Settings on both devices.

Enable Redundancy checkbox is used to enable the redundancy functionality on the QX IP PBX.

Active Device Mode drop down list is only present on backup device and is used to adjust the behavior of the backup device during unavailability of master device. When **Active** is selected, backup device will become master once the original master device became unavailable. When **Passive** is selected, backup device stops its synchronization with the master device and will not take over the control even when the original master got failed unless **Swap Master Device** button is pressed on the master QX IP PBX. The **Passive** mode is used for firmware update or language pack updates on master device when a reboot is required. After the reboot of master device, the **Active Device Mode** on the backup device should be changed back to **Active** to restore the redundant network functionality.

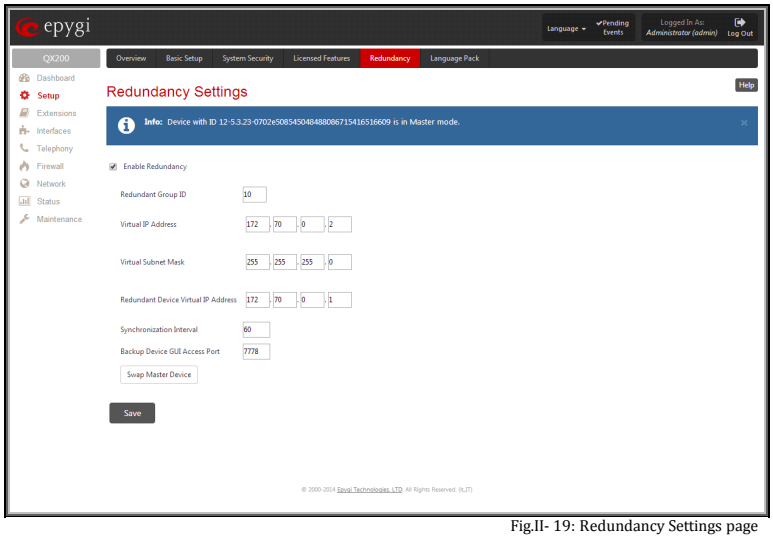


Fig.II- 19: Redundancy Settings page

Redundant Group ID text field unique ID (values 1 and up) identifying master and backup devices. The same value must be set on both QX IP PBXs.

Virtual IP Address text fields require the virtual IP address of the device where the configuration is done. **Virtual Subnet Mask** text fields require the virtual subnet mask of the device where the configuration is done. These two parameters identify an alternate IP network of the LAN interface which stays unchanged when the device switches its mode (from master to backup or vice versa). The configuration and voice data synchronization daemon uses this IP address to communicate with the second QX IP PBX.

Redundant Device Virtual IP Address text fields require an alternate IP address of the LAN interface of the second QX IP PBX.

Synchronization Interval text field requires the period of time (in seconds) between two consecutive configuration and voice data synchronizations from master to backup device.

Backup Device GUI Access Port text field (available only for QX50/QX200) is present on the master device only and requires the port used for accessing the GUI of the backup device through master.

Swap Master Device button is used for manual swapping of functionality of master and backup devices. This action will result in rebooting the current master. After rebooting the current master device will start running in a backup mode. Switching the backup to master starts all applications on QX IP PBX and causes all IP phones to reboot. The swapping takes around 1 minute however another 1-3 minutes are required in order to reboot all the IP phones connected to redundant system. If backup device before swapping was in passive mode then after swapping the master will start running as backup in passive mode, otherwise if it was in active mode then master will start running as backup in active mode.

Download system logs link is only present on backup device and is used to download system 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 IP PBX.

Language Pack

The **Language Pack** page allows you to upload a custom language for GUI and Voice Messages of the QX IP PBX. 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 also change the language of some supported IP phones (Aastra, snom v.6.x, Grandstream GXP2000). After a custom Language Pack is uploaded onto the system, reboot the IP phone to load a matching language onto the phone.

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 IP PBX.

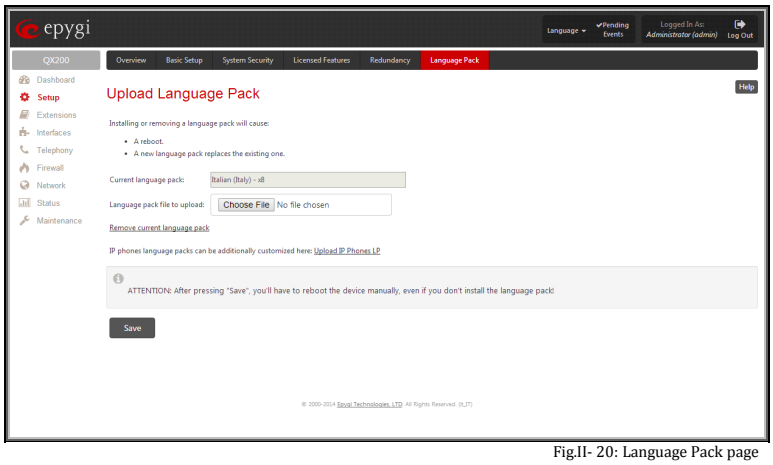


Fig.II- 20: Language Pack page

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.

The **Custom languages for IP phones** link is only seen when a custom language pack is uploaded and is used to move to the Update Languages for IP Phones page where a custom language pack may me uploaded to the IP phone.

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 IP PBX, 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.

Update Languages for IP Phones

The **Update Languages for IP Phones** page is used to upload a custom language pack to the IP phone. This page only contains those IP phones that support custom language pack uploading from the QX IP PBX.

To upload the custom language pack, go to your IP phone related page and **Choose File** the custom language pack file. **Save** the changes to upload the custom language pack to the IP phone.

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

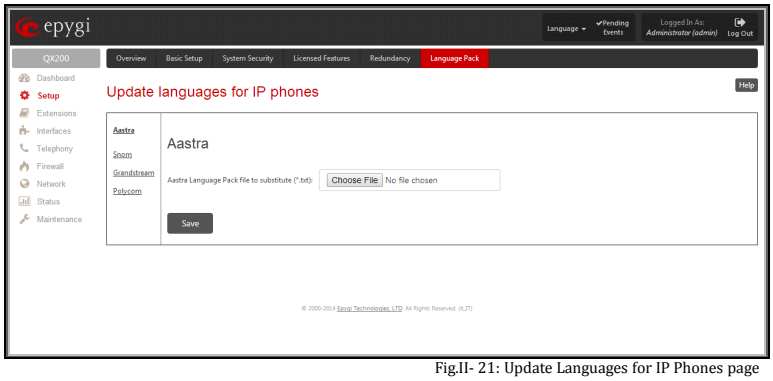


Fig.II- 21: Update Languages for IP Phones page

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, QX IP PBX will upload the selected custom Language Pack to your IP phone. You should then reboot your phone to make the new language pack active.

Extensions Menu

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

- **Extensions**
  - Add Extension
  - Add Multiple Extensions
  - Bulk Import
- **Conferences**
  - Add Conference
  - Email Defaults
- **Recordings**
- **Directory**
- **Receptionist**
- **ACD**
- **Authorized Phones**

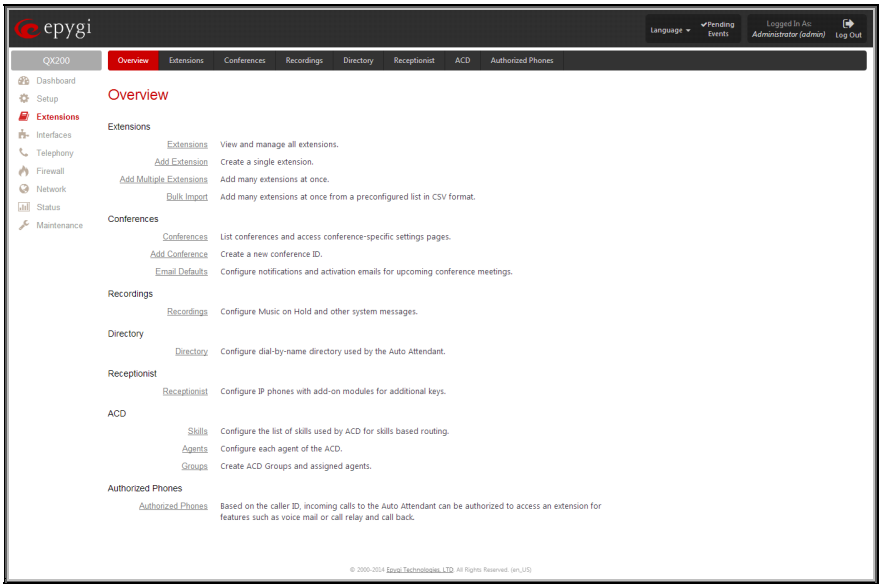


Fig.II- 22: Extensions Menu page

Extensions Management

The **Extensions Management** page is used to create a variety of extensions and auto attendants on the QX IP PBX. 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 IP PBX'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 IP PBX. This page disappears once being saved.

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

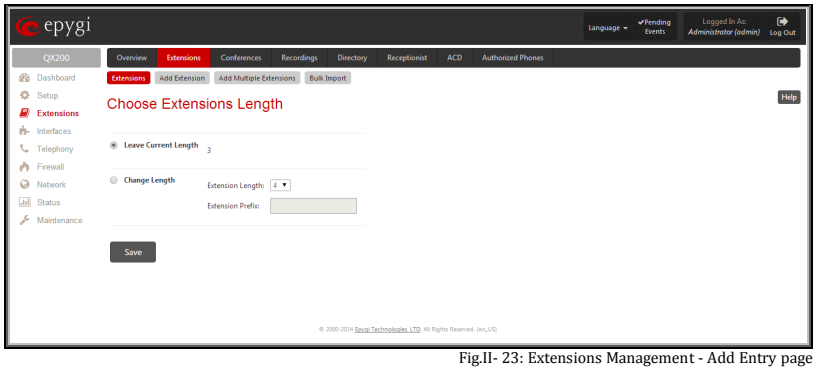


Fig.II- 23: Extensions Management - Add Entry page

- **Leave Current Length** radio-button selection is used to leave the current length of extensions on the QX IP PBX. Per default the extensions length on the QX50/QX200 is 3 and on the QX2000 is 4. 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 IP PBX. 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 IP PBX. This number will apply to all existing extensions on the QX IP PBX as well as to any newly created extensions. The length of the extension can be 3, 4 or 5.

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

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

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

QX50/QX200 has two available FXS lines.

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

Attention: QX50 is limited to 200 extensions, QX200 is limited to 400 extensions and QX2000 is limited to 2400 extensions.

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

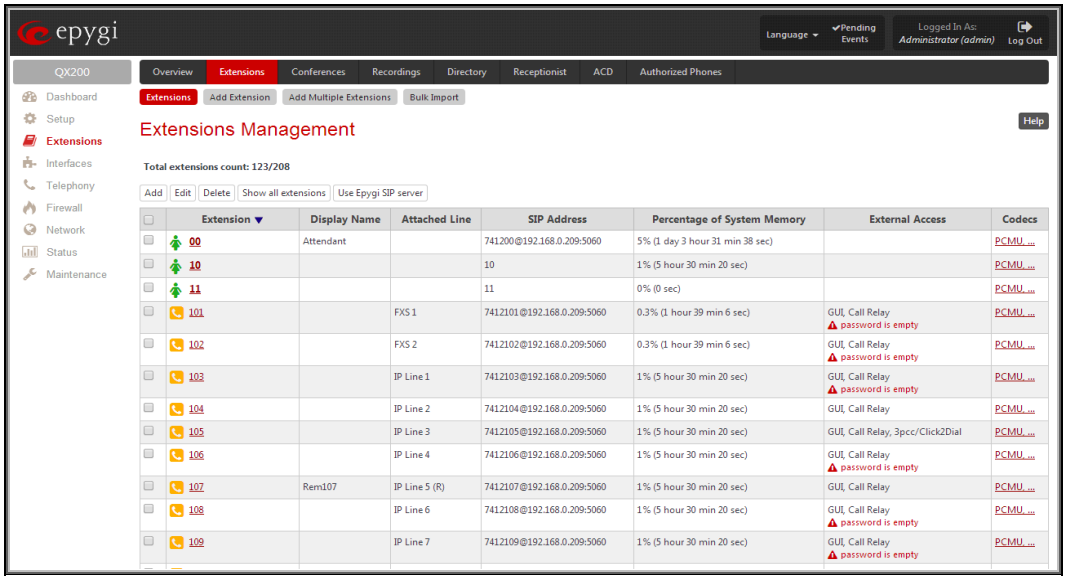


Fig.II- 24: Extensions Management page

The following columns are present in the table:

- **Extension** - lists user or attendant extensions on the QX IP PBX. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **Attached Line** - indicates the FXS or IP line corresponding extension it is attached to. "R" is displayed in this column when **SIP Remote Extension** (see below) functionality is enabled on the extension.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **Percentage of System Memory** - indicates the user space (in percentages) configured for each extension. The actual available duration (in minutes) for the extension voice mails, uploaded/recorded greetings and blocking messages is also displayed here. The available minutes corresponding to the selected user space are dependent on the Voice Recording codec selected from the Voice Mail Common Settings page. For example, for the same amount of marked out user space, selection of the G726 voice recording codec will provide more space for voice mails and user defined voice greetings than the G711 codec selection.
- **External Access** - indicates whether the GUI Login, 3pcc/Click2Dial 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 (see Manual III: Extension User's Guide). The Pickup Group, Call Park and Paging Group extensions are displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible for this type of extensions. Clicking on the Recording Box extension will move to the corresponding extension's Recording Box where the recorded calls can be managed.

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.

Hide extensions attached to disabled IP lines functional button is used to hide extensions which are attached to the disabled IP lines. When this functional button is pressed, it transforms to **Show all extensions** functional button, which is used to show all hidden extensions. To enable the lines, install a feature key from the Feature Keys page.

Add Extension

Add Extension tab 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- 25: 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
- Pickup Group
- Call Park
- Paging Group
- ACD Group (if the ACD feature is previously activated from Feature Keys page)
- Recording Box (if the Call Recording feature is previously activated from Feature Keys page)

User Extension Settings

1. General Settings

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

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

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

Attached Line lists all free lines an extension may be attached.

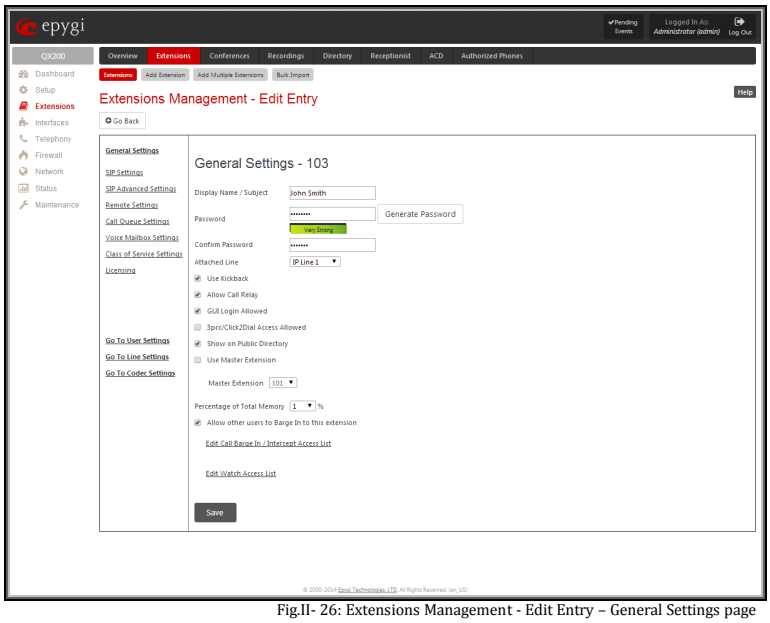


Fig.II- 26: Extensions Management - Edit Entry – General Settings page

Please Note: Extensions cannot be detached from the line if the **SIP Remote Extension** service is enabled on it. To detach the extension from the line, disable the SIP Remote Extension service on the extension first.

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

Allow Call Relay enables the current extension to be used to access the Call Relay service in the QX IP PBX'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 checkbox enables the current extension to be used to access the QX IP PBX via WEB interface by extension name and password.

3pcc/Click2Dial Access Allowed checkbox enables the current extension to be used with applications based on QX IP PBX 3PCC interface and QX IP PBX Click to Dial application.

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

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

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

The **Edit Call Intercept Access List** link leads you to the page where the extensions that are allowed to intercept calls should be defined.

The **Allow other users to Barge In to this extension** checkbox and the **Edit Call Barge In / Intercept Access List** link appears only if a **Barge In** feature is activated from the Feature Keys page.

- The **Allow other users to Barge In to this extension** checkbox is used to enable the Barge In Service on the extension.
- The **Edit Call Barge In / Intercept Access List** link leads you to the **Call Barge In / Intercept Access List** page where the extensions that are allowed to barge in to the current extension or intercept calls should be defined.

Please Note: After activating Barge In feature, the extensions that are previously configured to intercept calls from the **Call Intercept Access List** page, will be automatically redirected to the **Call Barge In / Intercept Access List** page along with the Barge In options.

The **Edit Watch Access List** link leads you to the page where the extensions that are allowed to watch calls should be defined.

Call Intercept Access List

The **Call Intercept Access List** page is used to define a list of extensions that are capable to intercept the current extension calls and to define the appropriate permissions.

The **Call Intercept** service allows you to intercept the calls assigned to an individual extension. The extensions that are allowed to intercept calls are defined in the **Call Intercept Access List**. With the special feature codes (for details, see Feature Codes in the Manual III – Extension User's Guide), you may pick up a ringing call of the extension.

This page contains the following functional buttons:

Add functional button opens an **Add Entry** page where extensions may be added to the **Call Intercept Access List**.
This page requires the extension number in the **Address** text field that will be allowed to intercept calls. The wildcard is supported in the **Address** field to add a group of extensions with one entry.

The **Allow Intercept** checkbox on this page allows to select the Intercept option for the added extension:

Attention: Intercepted calls are not displayed in **Active Calls** table on the Administrator's Main Page , nor are registered in the Call History.

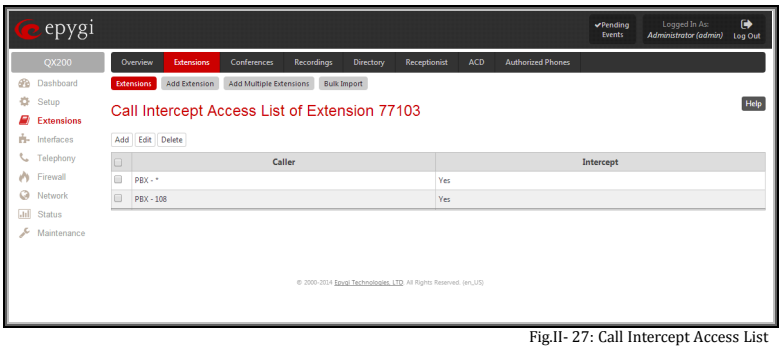


Fig.II- 27: Call Intercept Access List

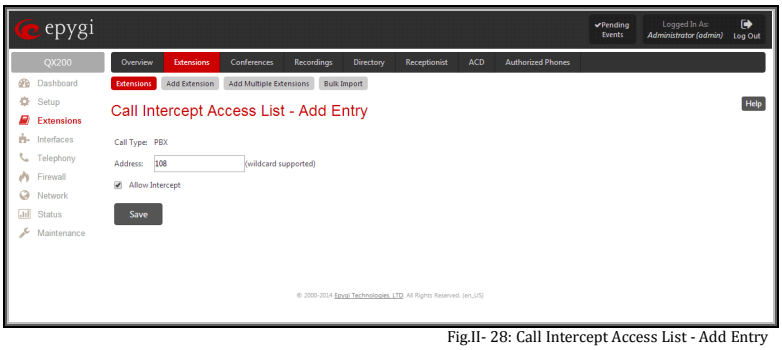


Fig.II- 28: Call Intercept Access List - Add Entry

Call Barge In/Intercept Access List

The **Call Barge In / Intercept Access List** page is used to define a list of extensions that are capable to Barge In/Intercept the current extension calls and to define the appropriate permissions. This page is only available when the Barge In Service is enabled from the Feature Keys page.

This page contains the following functional buttons:

Add functional button opens an **Add Entry** page where extensions may be added to the **Call Barge In / Intercept Access List**. This page requires the extension number in the **Address** text field that will be allowed to intercept calls. The wildcard is supported in the **Address** field to add a group of extensions with one entry.

The checkboxes on this page allow to select one or more options of the Barge In Service and **Call Intercept** for the extension:

- **Allow Listen In**
- **Allow Whisper**
- **Allow Barge In**
- **Allow Intercept**

Attention: **Barge In/Call Intercept** calls are not displayed in **Active Calls** table on the Administrator's Main Page, nor are registered in the Call History.

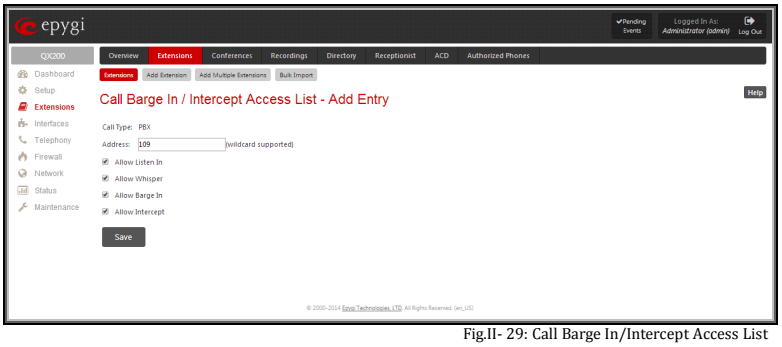


Fig.II- 29: Call Barge In/Intercept Access List

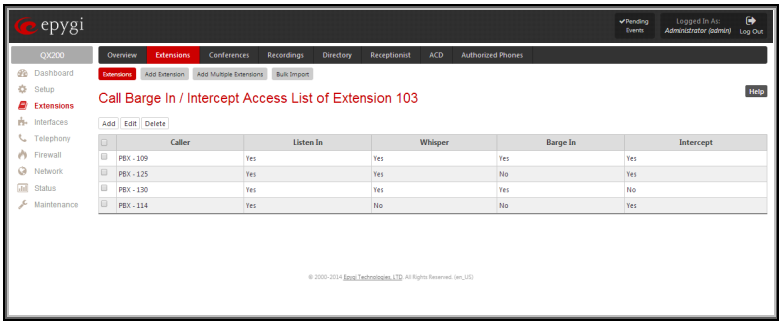


Fig.II- 30: Call Barge In/Intercept Access List - Add Entry

Watch Access List

The **Watch Access List** page is used to define a list of extensions that are capable to watch the current extension calls and to define the appropriate permissions.

This page contains the following functional buttons:

Add functional button opens the **Watch Access List - Add Entry** page where extensions may be added to the Watch Access List.
The **Watch Access List - Add Entry** page consists of the following components:

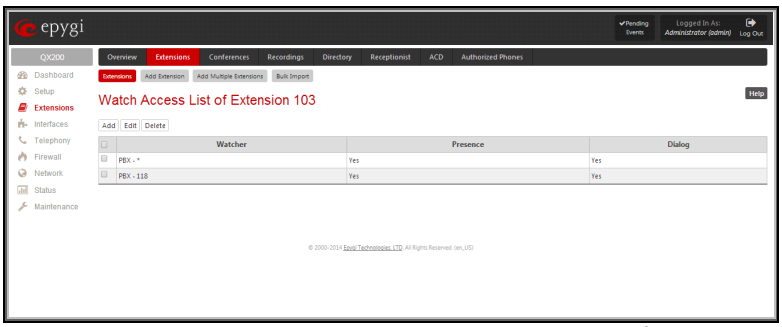


Fig.II- 31: Watch Access List page

- **Call Type** lists the available call types:
  PBX - local calls to QX IP PBX's extensions.
  SIP - calls through a SIP server.
  Auto - used for undefined call types. The destination (independent on whether it is a PBX number or a SIP address) will be reached through the Call Routing Table.

- The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined. For the **Auto** call type, a routing pattern needs to be defined. wildcard is allowed in this field.

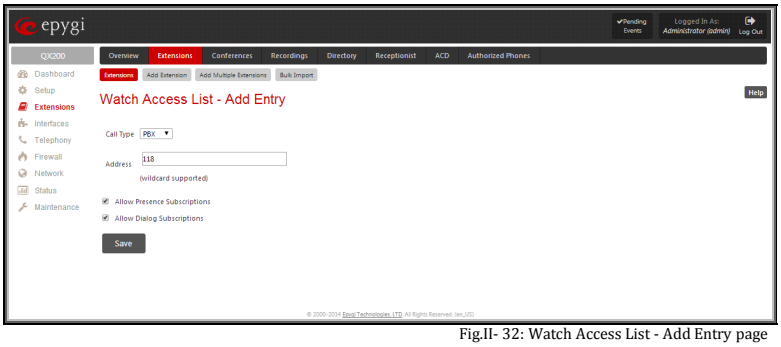


Fig.II- 32: Watch Access List - Add Entry page

The checkboxes on this page allow to select one or more options of the Watch Access List for the extension:

- **Allow Presence Subscriptions**
- **Allow Dialog Subscriptions**

Edit opens a page **Watch Access List-Edit Entry** where the permissions of the added extensions may be modified.

2. SIP Settings

This page provides two functions. It allows an extension on the QX IP PBX 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 IP PBX 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.

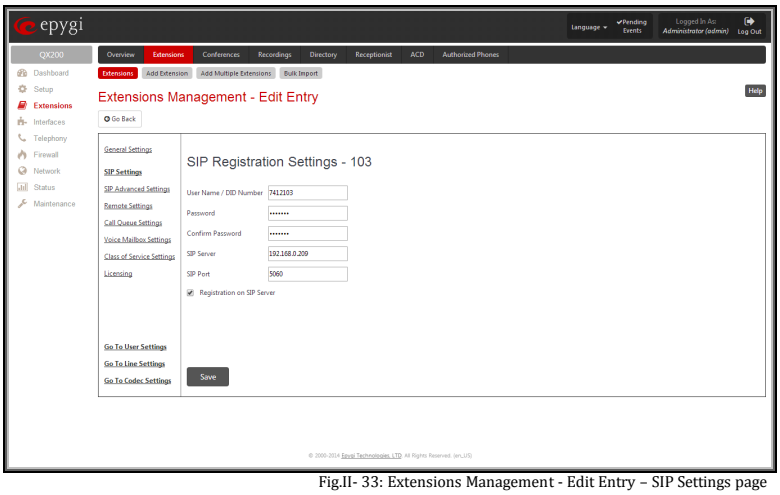


Fig.II- 33: Extensions Management - Edit Entry – SIP Settings page

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 IP PBX 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 IP PBX 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 IP PBX.

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 IP PBX to reach the selected SIP servers.

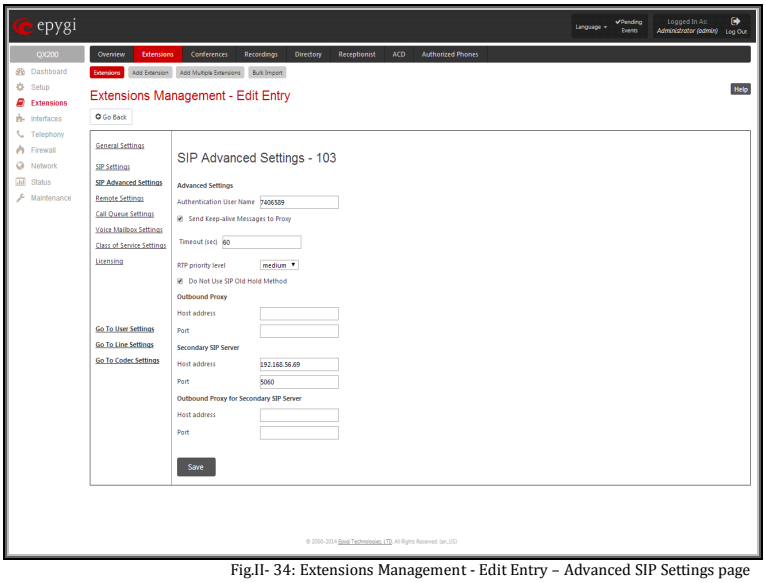


Fig.II- 34: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Remote Settings

This group is used to configure **SIP Remote Extension** functionality. This is an advanced telephony feature that allows QX IP PBX users to remotely operate QX IP PBX. Users need to register a hardware or software SIP phone on the QX IP PBX by defining the QX IP PBX's global IP address and an appropriate Username/Password. A registered SIP Remote phone can act fully as a phone connected locally to QX IP PBX, i.e. it can use QX IP PBX's PBX features, place and receive calls, access voice mails, etc.

The **Enable** checkbox activates the SIP Remote Extension's functionality.

Please Note: **SIP Remote Extension** functionality may be enabled only for active (attached to an onboard FXS or IP line) extensions.

Identification parameters used by the remote SIP device for registration on the QX IP PBX should be defined in the **Username** and **Password** text fields. They should match on both QX IP PBX and SIP phone for a successful connection. The **Password** field is checked against its strength and you may see how strong is your inserted password right below that field. To achieve the well protected strong password minimum 8 characters of letters in upper and lower case, symbols and numbers should be used. If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

Line Appearance text field requires a number of simultaneous calls supported by the SIP phone.

When the **Enable RTP Proxy** checkbox is selected, incoming and outgoing RTP streams to and from the remote SIP phone will be routed through QX IP PBX. When the checkbox is not selected, RTP packets will be moving directly between peers.

When the **Fallback To Local Extension When Not Registered** checkbox is selected, incoming calls towards the corresponding extension on the QX IP PBX will be forwarded to the remote SIP phone only if it is registered. Otherwise, when the remote SIP phone is unregistered, incoming calls will be routed to the line extension it is attached to. When this checkbox is not selected, all incoming calls will be routed to the remote SIP phone only if it is registered. Otherwise, if the remote SIP phone is unregistered, calls will be forwarded to the extension's voice mailbox.

The **Symmetric RTP** checkbox should be selected when the remote extension is located behind the symmetrical NAT.

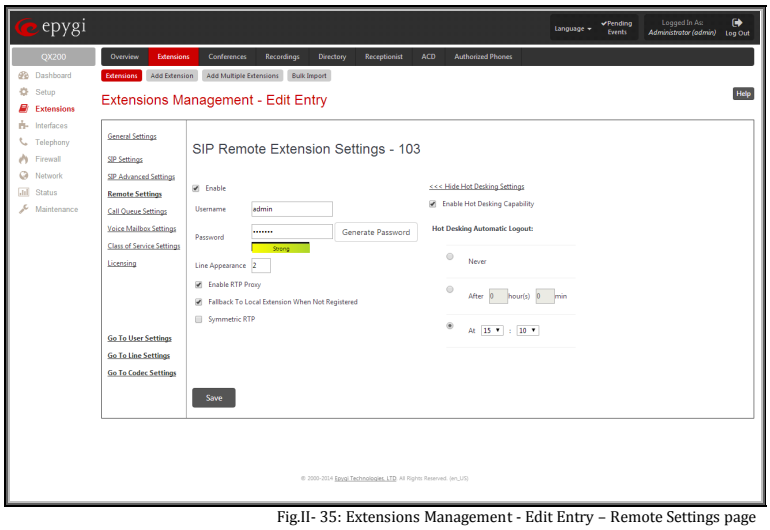


Fig.II- 35: Extensions Management - Edit Entry – Remote Settings page

The **Show Hot Desking Settings** and **Hide Hot Desking Settings** links are correspondingly used to show or hide the Hot Desking settings on this page.

The **Enable Hot Desking Capability** checkbox is used to enable the Hot Desking feature on the corresponding remote extension.

The **Hot Desking Automatic Logout** section is used to configure Hot Desking functionality expiration on the corresponding extension. This may be useful when someone who logged in to the public phone with this extension forgot to log out after using it. With this option enabled, once the expiration time arrives, the extension will automatically log out from the public phone.

The following options are available:

- **Never** – the extension will never expire and will remain logged in to the public phone.
- **After the defined period of time** – requires the period after which the extension will automatically log out from the public phone.
- **At the certain moment** – requires the moment (hour and minute) when the extension will automatically log out from the public phone.

5. Call Queue Settings

This group is used to configure the **Call Queue** service that allows multiple incoming calls to be kept in the queue when being on the line and enables the calls to be answered in the order they have been received. This feature can be also used within Receptionist Management (see below for more details).

The **Enable** checkbox activates the Call Queue functionality on the extension.

The **Call Queue Size** text field requires the length of the call queue. This is the maximum number of calls that will be accepted into the queue and kept on hold while the extension user is on a call. If a maximum number of calls are already held in the call queue, the next incoming call will be routed to the extension's Voice Mail, if enabled, or will be disconnected.

Please Note: By configuring Call Queue size, Call Forwarding if Busy and Voice Mail telephony services will not take effect on the corresponding extension until the call queue is not filled. These telephony services will affect only the calls out of the call queue.

The **Max Calls Presented to Extension** text field requires the maximum number of active calls on the line. For example, if 1 is configured in this field and the extension is in use, the next incoming call will go to the call queue. If 2 is configured in this field and extension is in use, the next incoming call alert will be heard in the background (if Call Waiting service is enabled on the corresponding extension) and the extension will hold the first call to answer the second one or they can be joined for a call conference. However, the next incoming call will again go to the call queue.

Enable Redirection Timeout checkbox is used to enable the call redirection to the other destination after some time spent in the queue. This will avoid the caller to wait in the queue for too long. This checkbox selection enables the following components:

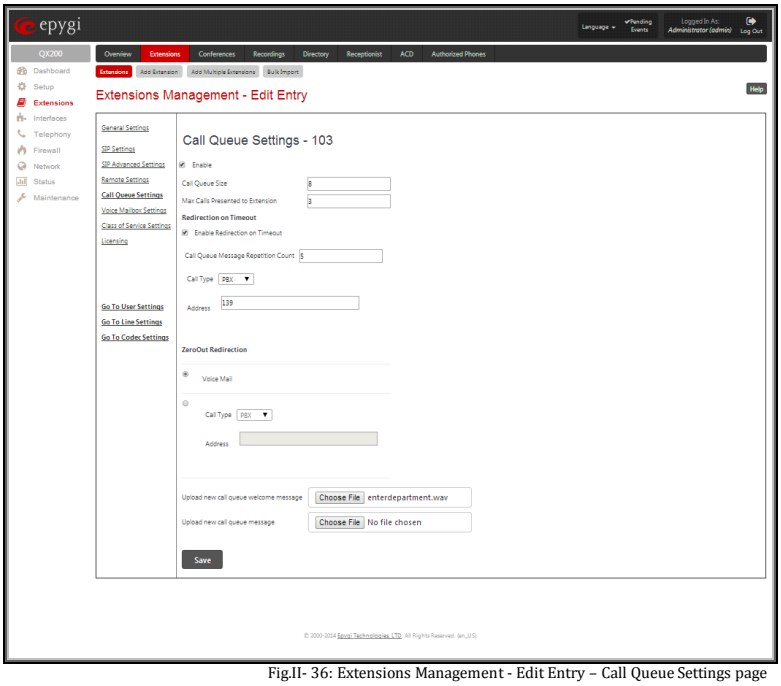


Fig.II- 36: Extensions Management - Edit Entry – Call Queue Settings page

Call Queue Message Repetition Count text field requires the number of call queue messages (played during the caller is in the queue) after which the call in the queue will be automatically redirected to the destination defined below.

Call Type lists the available call types:

- **PBX** - local calls to QX IP PBX's extensions
- **SIP** – calls through a SIP server
- **PSTN** – calls to a global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here. For the **Auto** call type, a routing pattern needs to be defined.

The **ZeroOut Redirection** radio buttons are used to enable the call redirection to the extension voice mailbox or other destination after some time spent in the queue. This will avoid the caller to wait in the queue for too long.

- The **Voice Mail** radio button selection allows the user to redirect the call to the extensions voicemail.
- The second radio button selection allows the callers to redirect the call to the specified destination instead of holding in the extension's queue.The caller will then be automatically transferred to the destination specified in this page. This selection activates the following fields to be inserted:

Call Type lists the available call types:

  - **PBX** - local calls to QX IP PBX's extensions.
  - **SIP** - calls through a SIP server.
  - **PSTN** - calls to a global telephone network.
  - **Auto** - used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here. For the **Auto** call type, a routing pattern needs to be defined. wildcard is allowed in this field.

Please Note: To activate the **ZeroOut Redirection** feature, the caller should dial **0** digit.

Upload new call queue welcome message allows updating the active Call Queue welcome message (played when a caller joins the extension's call queue), downloading it to the PC, or restoring the default one.

The **Remove call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Upload new call queue message allows updating the active call queue message (played when a caller is being held in the queue), downloading it to the PC, or restoring the default one.

The **Remove call queue message** functional link appears only when the custom call queue message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue message** functional link appears only when the custom call queue message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Choose File button opens the file chooser window to browse for a new Call Queue welcome message file. The uploaded files should to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading if there is not enough memory available for the corresponding extension, which will cause the "You do not have enough space" warning message.

6. Voice Mailbox Settings

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

- **Disable Voice Mail** – disables the Voice Mail service for the corresponding extension. With this selection, the extension user will be unable to reach their Voice Mail Settings, but will be able to access their Voice Mailbox and manage the existing voice mails.

- **Use Internal Voice Mail** – enables the Voice Mail service for the corresponding extension and defines the QX IP PBX's internal storage as a location for the Voice Mails.

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

changed to **Passed** and a **Reactivate** button appears. Using **Reactivate** button you might re-enable the **Voice Mail Configuration Wizard** so the user will be again prompted about his/her personal settings next time entering his/her Voice Mailbox.

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

The **Shared Mailbox** section is used to setup a mailbox sharing. The **Edit Voice Mailbox Access List** link goes to the page where a list of PBX extensions can be defined for which the mailbox of the current extension will be shared and accessible without password authentication. For more details on how to access Shared Mailboxes, see **Feature Codes**.

- **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 IP PBX 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.

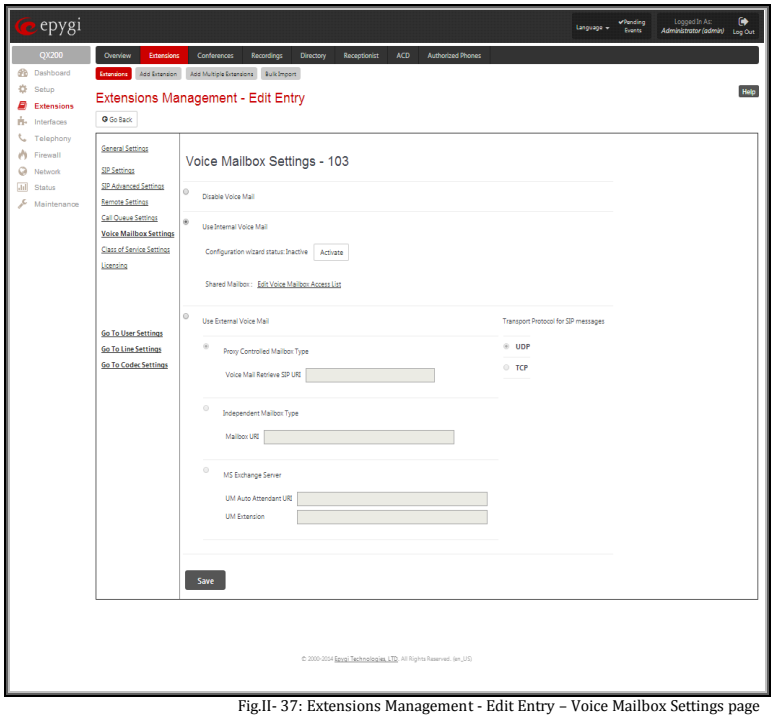


Fig.II- 37: Extensions Management - Edit Entry – Voice Mailbox Settings page

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.

- 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.

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

7. Class of Service Settings

The **Class of Service Settings** page is used to assign the defined classes to a PBX extensions.

To use **Class of Service** feature it should be enabled from the Class of Service page.
Class of Service feature allows to specify which PBX/Conference extensions can use which routing rules to make a call. For example, if an extension is not assigned to a certain class of service and an attempt is made to place a call from that extension using routing rule with the **Class of Service** feature enabled, then "Number dialed does not exist" message will be played to the caller.

The **Go to Class of service** link leads to the Class of Service page where the class of services can be configured.

The **Go to Call Routing Table** link leads to the Call Routing Table page where the call routing rules can be assigned to a certain class of service(s). The classes defined in the **Class of Services** page will appear on this page to assign the PBX extensions to a certain class of service(s).

PBX/Conference extensions can be attached to a several class of services at the same time.

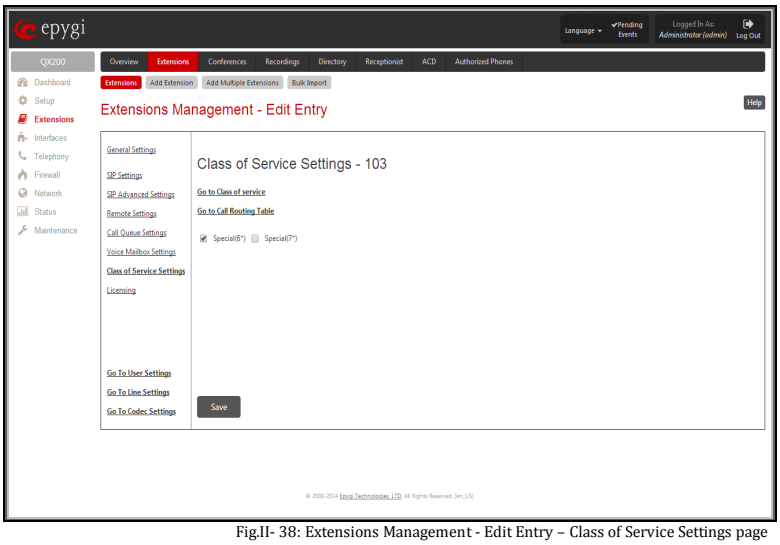


Fig.II- 38: Extensions Management - Edit Entry – Class of Service Settings page

8. Licensing

This page is only available if the corresponding licensing is enabled from the Feature Keys page.

This group allows you to configure the extension to be used by the iQall application and the Pro/Basic level Desktop Communication Console (DCC).

The page contains the following components:

Enable DCC Pro license checkbox which allows you to set the corresponding extension to be used by the DCC Pro level application. When the checkbox is not selected on this page, the DCC will be functional with the extension only during trial period.

Enable DCC Basic license checkbox which allows you to set the corresponding extension to be used by the DCC Basic level application. When the checkbox is not selected on this page, the DCC will be functional with the extension only during trial period.

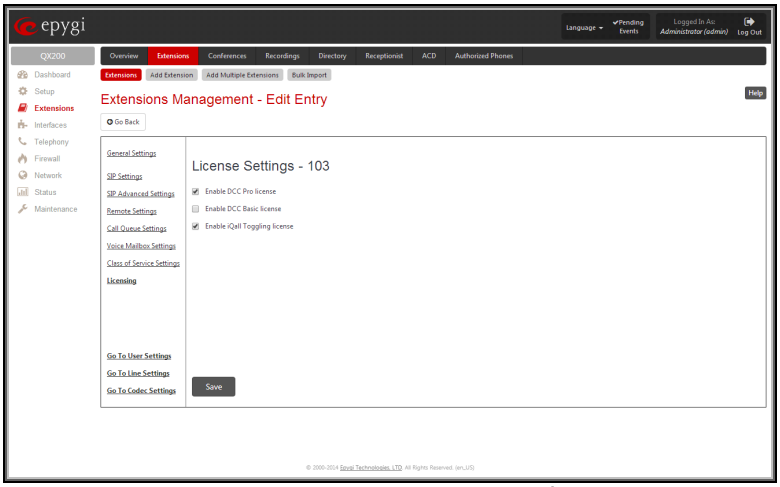


Fig.II- 39: Extensions Management - Edit Entry – License Settings page

Please Note: These checkboxes can be simultaneously selected on as many extensions as iQall and/or DCC Pro/Basic Level licenses are available on the QX IP PBX.

Enable iQall Toggling license checkbox allows you to allocate the iQall Toggling licenses to the corresponding extensions.

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

The **Go to Line Settings** link is used to make a quick jump to the IP Lines page of the corresponding extension.

The **Go to Codec Settings** link is used to make a quick jump to the Codec Settings page of the corresponding extension.

Pickup Group Extension Settings

Pickup Group & Access List

The **Pickup Group** service is used to monitor calls addressed to a certain list of extensions and to pick up calls ringing on the listed extensions. This service may be used when a group of extensions are located in the same area so the persons nearby can hear the ringing on one of the extensions. This feature allows you to pick up the call ringing on a certain extension by dialing the number of the pickup extension.

The **Pickup Group** list is used to define the extensions that can be monitored by calling a certain pickup extension.

The **Access List** is used to define PBX, SIP or PSTN users that are allowed or forbidden to intercept calls ringing on extensions in the Pickup Group.

If a user dials the pickup extension when several extensions of the pickup group are ringing, the first (oldest in time) call will be picked up. When the user dials the pickup extension and no extensions of the pickup group are ringing, the "No call is available to pickup" message will be played to the user. When

the user that is not listed in the **Access List** dials the pickup extension, password authorization (of the pickup extension) will be required to answer the call. When a denied user dials the pickup extension, the "Party does not accept your call" message will be played to the user.

For **Pickup Group** extensions, the **Extensions Management - Edit Entry** page consists of **General Settings, SIP Settings** and **Advanced SIP Settings** pages. The **SIP Settings** and **Advanced SIP Settings** pages are the same as for regular extensions (see User Extension Settings) described above. The **General Settings** page has a different content as follows:

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

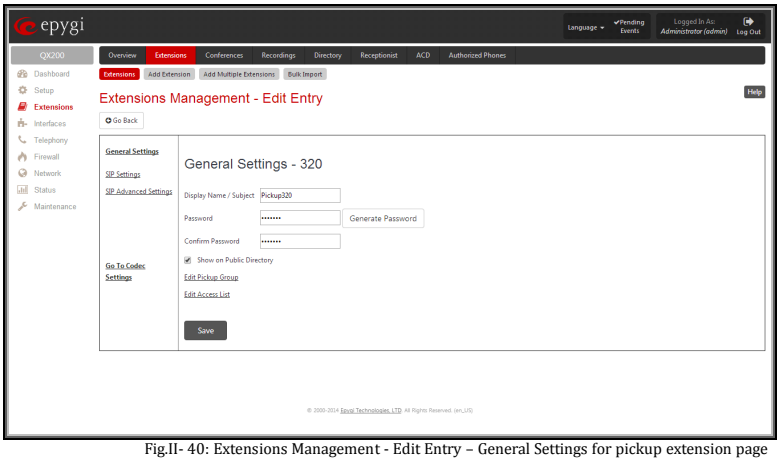


Fig.II- 40: Extensions Management - Edit Entry – General Settings for pickup extension page

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

Password requires a password for the new extension.

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

The **Edit Pickup Group** link leads to the page where a list of monitored extensions can be defined.

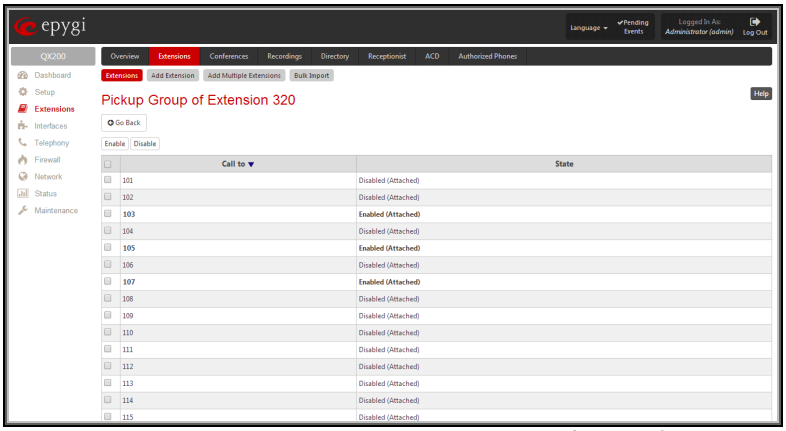


Fig.II- 41: Pickup Group of Extension page

The **Pickup Group of Extension** page lists all available regular and virtual extensions on the QX IP PBX and allows you to manage the Pickup Group.

The **Enable** functional button is used to include the selected extension(s) to the Pickup Group of the corresponding pickup extension. The extensions in the Pickup Group can be monitored by the pickup extension. The calls addressed to the extensions in the Pickup Group can be answered by the pickup extension.

The **Disable** functional button is used to exclude the selected extension(s) from the Pickup Group of the corresponding pickup extension.

The **Edit Access List** link leads to the page where permissions for the users to use the pickup service can be defined.

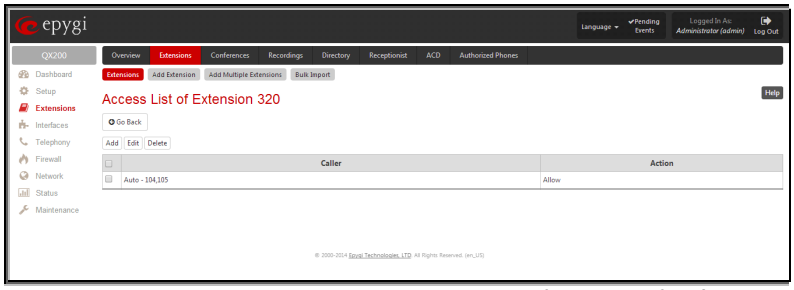


Fig.II- 42: Access List of Extension page for Pickup Group

The **Access List of Extension** page lists all users (or a group of users if a wildcard is used) and the appropriate permissions to pickup the calls ringing on the extensions from the Pickup Group.

The **Add** functional button opens an **Add Entry** page where a new user with corresponding permissions might be created. This page consists of the following components:

Call Type lists the available call types:

- **PBX** - local calls from QX IP PBX's extensions
- **SIP** – calls through a SIP server
- **PSTN** – calls from global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through the Call Routing Table.

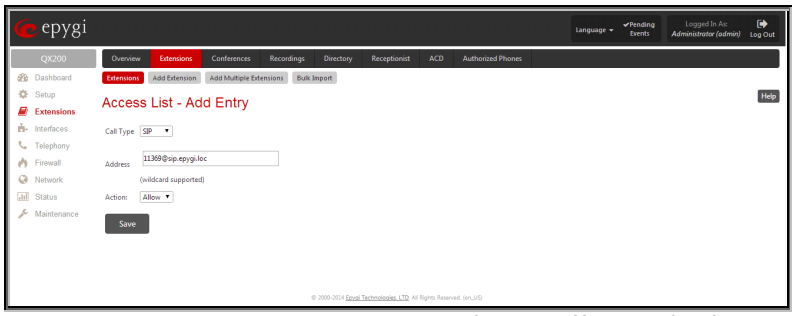


Fig.II- 43: Access List of Extension –Add Entry page for Pickup group

The **Address** text field is used to define the address to be included in the Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here.

The **Action** drop down list is used to select the defined user's permissions (allow or deny) to use the pickup service for the extensions included in the Pickup Group.

Call Park Extension Settings

For **Call Park** extensions, the **Extensions Management - Edit Entry** page consists of **General Settings, SIP Settings**, **Advanced SIP Settings, Park Access List** and **Retrieve Access List** pages. The **SIP Settings** and **Advanced SIP Settings** pages are the same as for the regular extensions (see User Extension Settings).

1. General Settings (for call park extension)
This group requires personal extension 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 whenever a call is performed or a voice mail is sent.

Password requires a password for the new extension.

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

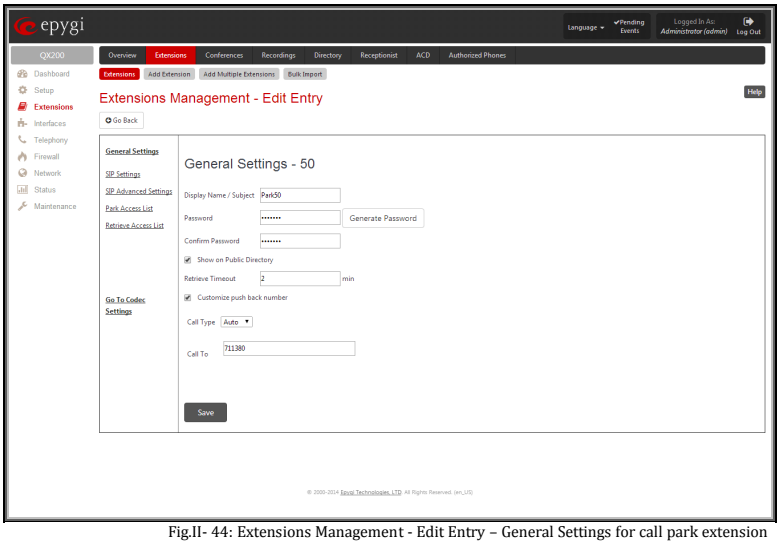


Fig.II- 44: Extensions Management - Edit Entry – General Settings for call park extension

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

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

Retrieve Timeout text field requires a timeout (in minutes) during which the parked call will stay active, i.e. the parked user will remain on-hold.

- If the **Customize push back number** checkbox is not enabled and the call park retrieve timeout expires, the hold music stops playing to the parked user and a new call is being placed towards the extension initiating the call park. If the extension initiating the call park does not answer the call, the caller which has been recently parked will reach the extension's Voice Mailbox, if enabled, otherwise will be disconnected.
- If the **Customize push back number** checkbox is enabled and the call park retrieve timeout expires, the hold music stops playing to the parked user and a new call is being placed towards the push back number configured in the **Customize push back number** field. If the push back number configured in the **Customize push back number** field does not answer the call, the caller which has been recently parked will reach the extension's Voice Mailbox, if enabled, otherwise will be disconnected.

The **Customize push back number** field consists of the following components:

Call Type drop down list includes possible incoming call types (PBX, PSTN, SIP or Auto).

- **PBX** selection means that the call will be push back to the local extension.
- **SIP** selection means that the call will be push back to the SIP destination correspondingly.
- **PSTN** selection means that the call will be push back 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 push back number dialed in the format depending on the selected **Call Type**. The Wildcard is supported in this field.

2. Park Access List

This page is used to define a list of extensions that are allowed to park the call to the corresponding call park extension. Wildcard is supported in the **Address** field to add a group of extensions with one entry.

If the extension is not in the Park Access List for the corresponding call park extension, it will not be able to park a call to this call park extension.

By default, this table contains a "*" entry which allows any PBX users to park the call to this extension.

Attention: If you modify the Park Access List by adding new extensions, do not forget to remove the default "*" entry from the list for the new configuration to take effect.

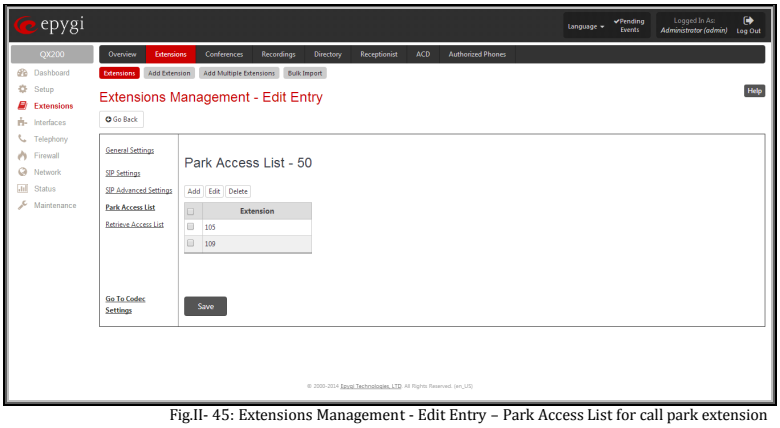


Fig.II- 45: Extensions Management - Edit Entry – Park Access List for call park extension

3. Retrieve Access List

This page is used to define a list of callers that are allowed to retrieve a call parked to the corresponding call park extension.

If the caller is not in the Retrieve Access List for the corresponding call park extension, it will not be able to pickup a call parked to this call park extension.

By default, this table contains an "Auto-*" entry which allows any caller to pickup the call parked to this extension.

Attention: If you modify the Retrieve Access List by adding new callers, do not forget to remove the default "Auto-*" entry from the list for the new configuration to take effect.

The **Add** functional button opens an **Add Entry** page where a new caller can be added to the list. This page consists of the following components:

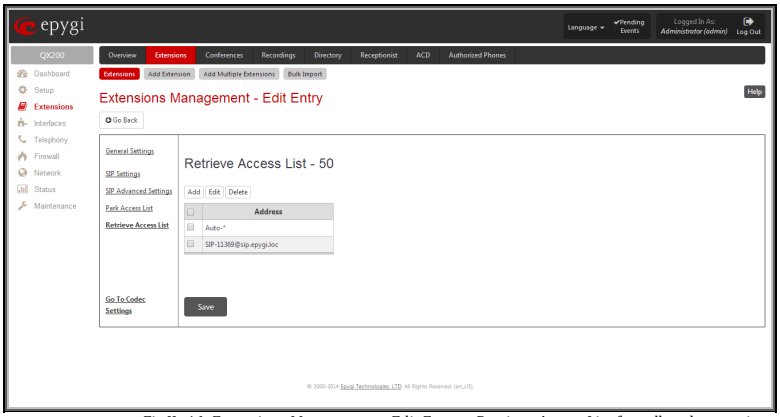


Fig.II- 46: Extensions Management - Edit Entry – Retrieve Access List for call park extension

Call Type lists the available call types:

- **PBX** - local calls from QX IP PBX's extensions
- **SIP** – calls through a SIP server
- **PSTN** – calls from global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be passed through Call Routing Table.

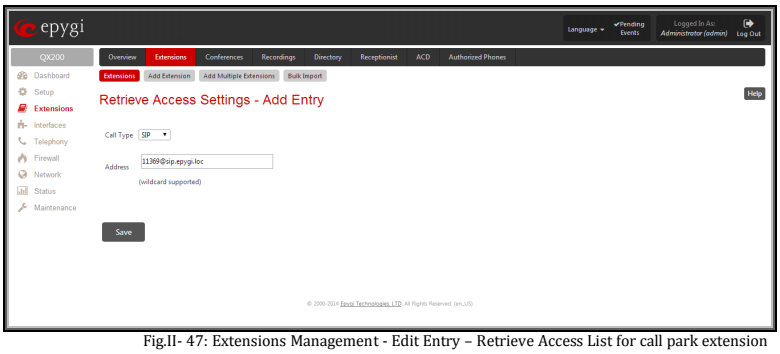


Fig.II- 47: Extensions Management - Edit Entry – Retrieve Access List for call park extension

The **Address** text field is used to define the address to be included in the Retrieve Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here. The wildcard is supported in this field. Wildcard is available for this field.

Paging Group Extension Settings

Paging Group & Access List

The **Paging Group** service is used to page a group of extensions by forcing extensions to go off-hook and opening one-way communication. The service is particularly used for announcements addressed to a group of extensions. Service allows to page multiple extensions by dialing the **Paging Group** extension.

Please Note: The **Paging Group** service requires called extensions to use SIP or analog phones which are able to automatically go off-hook. For **Paging** service supported on IP phones, refer to the "**Epygi IP PBX Features on Epygi Supported IP phones**" document on the Epygi's Web portal.

The **Paging Group** list is used to define the extensions that will be paged. They will automatically go off-hook when the paging call comes in.

The **Access List** is used to define PBX, SIP or PSTN users that are explicitly allowed/forbidden to activate the call paging using the corresponding extension.

When calling to the **Paging Group** extension, the call will be forwarded to the extensions listed in the **Paging Group** table. The phones of the called extensions will automatically go off-hook (the phone speaker automatically becomes activated) and the caller will be able to make his announcement. Since the paging call opens one-way communication, the called extensions will not be able to give an answer to the caller. To terminate the paging call, caller should simply hang up.

Attention: Call paging will not work if the called extension is in call.

When caller not listed in the **Access List** calls the **Paging Group** extension, password authorization (using the password of the **Paging Group** extension) will be required to start the call paging. When a denied user tries to call the **Paging Group** extension, "Party does not accept your call" message will be played to the caller. When caller dials the **Paging Group** extension with empty Paging Group table, "Number dialed temporarily unavailable" message will be played to the caller.

For **Paging Group** extensions, **Extensions Management - Edit Entry** page consists of **General Settings, SIP Settings** and **Advanced SIP Settings** pages. The **SIP Settings** and **Advanced SIP Settings** pages are the same as for the regular extensions (see User Extension Settings), while **General Settings** page has a different content:

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

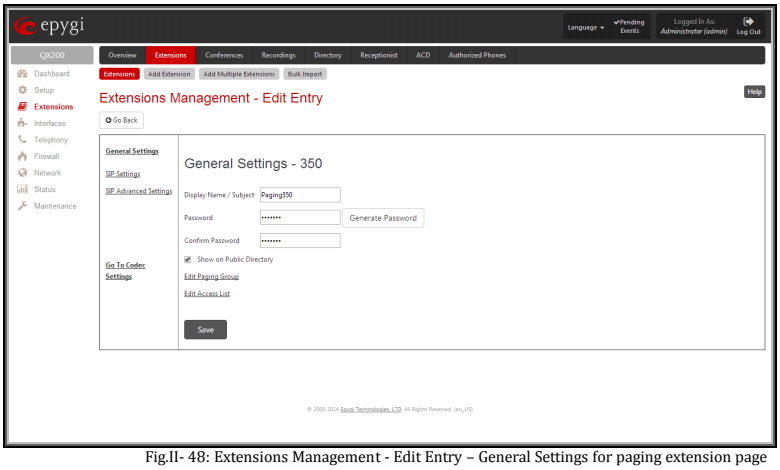


Fig.II- 48: Extensions Management - Edit Entry – General Settings for paging extension page

Display Name is an optional parameter used to recognize the caller. Usually the display name appears on the called party's phone display whenever a call is performed.

Password requires a password for the new extension.

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

If you are unable to define a strong password, press **Choose Generated 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 error will appear: "Incorrect Password confirm".

The **Edit Paging Group** link leads to the page where a list of extensions to be paged can be selected.

The **Paging Group of Extension** page lists all available regular and virtual extensions on the QX IP PBX and allows you to manage the Paging Group.

The **Enable** functional button is used to include the selected extension(s) to the Paging Group of the corresponding extension. Once the call to the paging group comes in, all the extensions in that group will be paged, i.e. will automatically go off-hook (by automatic activation of the phone's speaker).

The **Disable** functional button is used to exclude the selected extension(s) from the Paging Group of the corresponding extension.

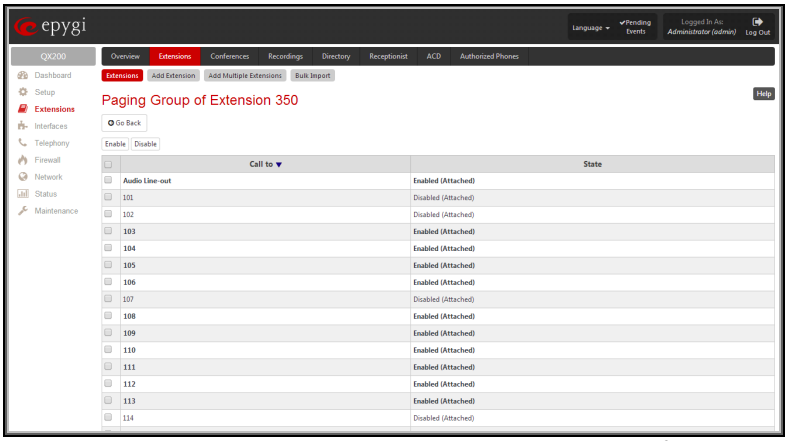


Fig.II- 49: Paging Group of Extension page

The **Edit Access List** link leads to the page where permissions for users to use the Paging Group service can be defined.

The **Access List of Extension** page lists all users (or a group of users if a wildcard is used) and the appropriate permissions to use the Paging Group through the corresponding extension.

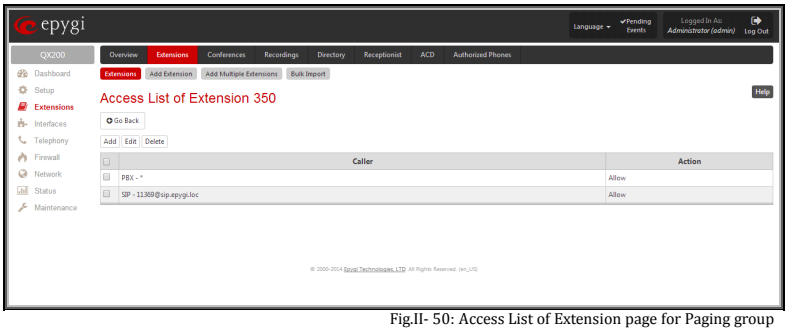


Fig.II- 50: Access List of Extension page for Paging group

The **Add** functional button opens an **Add Entry** page where a new user with corresponding permissions might be created. This page consists of the following components:

Call Type lists the available call types:

- **PBX** - local calls from QX IP PBX's extensions
- **SIP** – calls through a SIP server
- **PSTN** – calls from global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through Call Routing Table.

Fig.II- 51: Access List of Extension –Add Entry page for Paging Group

The **Address** text field is used to define the address to be included in the Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here.

The **Action** drop down list is used to select the defined user's permissions (allow or deny) to use the Paging Group service for the extensions included in the Paging Group table.

ACD Group Extension Settings

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

1. **General Settings** (for ACD Group extension)

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

Display Name is an optional parameter used to recognize the ACD Group. Usually the display name appears on the called party's phone display when a call is made or a voice mail is sent. This information is also displayed in the ACD Management Groups table.

Password requires a password for the ACD Group extension.

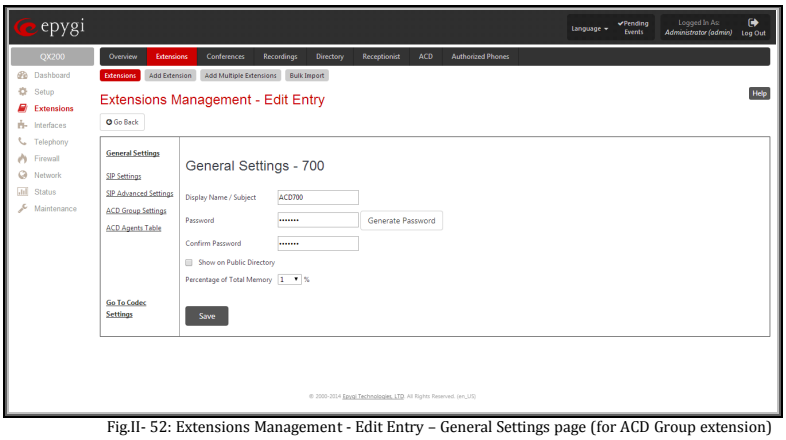


Fig.II- 52: Extensions Management - Edit Entry – General Settings page (for ACD Group extension)

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

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

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

The **Percentage of Total Memory** drop down list allows you to select the space for the uploaded custom messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX IP PBX.

2. ACD Group Settings

This group is used to adjust the ACD group settings and has the following components:

Max Queue Size defines the maximum number of calls waiting in the queue. If all positions of the queue are busy and a new call arrives, it will be rejected by the Agents Group.

Agent Ring Timeout defines the maximum ringing time of the agent's phone. If the call is not answered before this timer expires, the system will try to connect the call to another agent in that group.

Group Ring Timeout defines the maximum waiting time of the calls in the queue including connection time (when the call is extracted from the queue and rings on the agent's phone until it is answered). If this value for some call in the queue is exceeded then the call is being disconnected unless the call redirection is enabled from this page. In that case the call will be redirected to another destination as defined here.

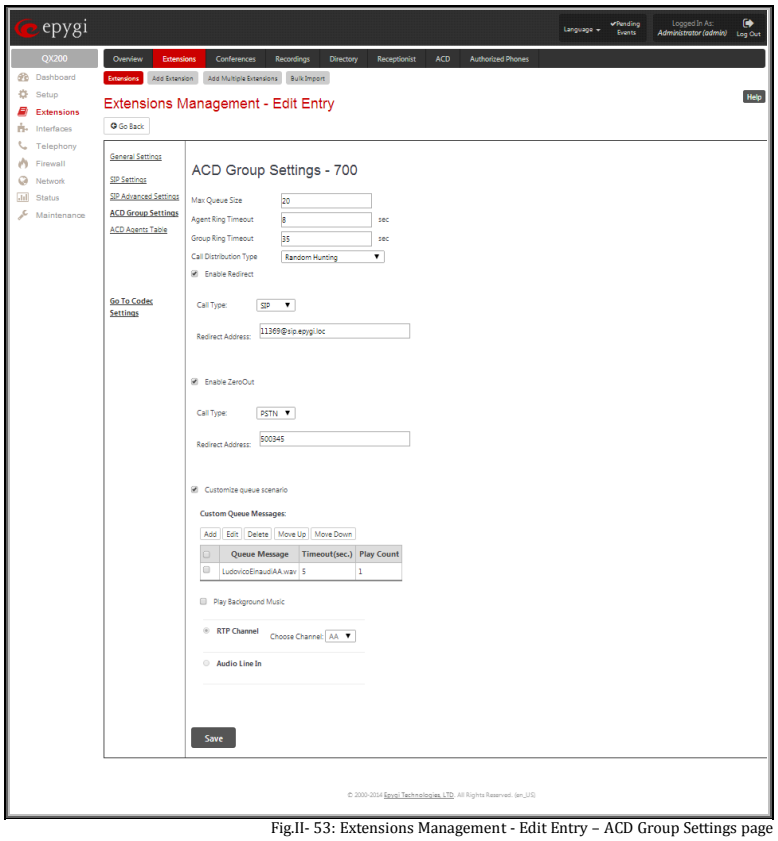


Fig.II- 53: Extensions Management - Edit Entry – ACD Group Settings page

Call Distribution Type defines the method of choosing the agents within the group for connecting the call. The following distribution types are available:

- **All Agents Ringing** – the system tries to reach all available agents in the group ringing their phones. As soon as the first answers, it cancels the calls to other agents (similar to Many Extension Ringing on the QX IP PBX, see Manual III – Extension User's Guide). If no one answers within **Common Timeout**, the system either disconnects or redirects the call.
- **Round Robin** – the system calls to the first available agent in the list of agents configured with AG. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next agent in the list, etc. Reaching the end of the list it starts from the beginning again. If the call is not answered and the **Common Timeout** has expired, the system either disconnects or redirects the call.
- **Longest Idle** – the system calls to the first available agent who was longest idle after the last call. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach another agent who was longest idle, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Less Busy During Last Hour** - the system calls to the first available agent who was least busy during the last hour (in average). If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next least busy agent, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Random Hunting** – the system calls to the first available agent selected randomly from the list of agents configured with Agents Group. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach another agent selected randomly from the list, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Skills** - the system calls to the first available agent with the highest composite skill's grade in the group. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next agent with the highest composite skill, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.

Enable Redirect checkbox is used to enable the call redirection to the other destination after some time spent in the queue. This will avoid the caller to wait in the queue for too long. This checkbox selection enables the following components:

Call Type lists the available call types:

- **PBX** - local calls to QX IP PBX's extensions
- **SIP** – calls through a SIP server
- **PSTN** – calls to a global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

The Redirect **Address** text field is used to define the address where the call will be redirected. It might be within the scope of ACD, like the address of another ACD agent, or out of scope, like the address of some voice mailbox. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address (see chapter Entering SIP Addresses Correctly) should be defined, for the **PSTN** call type, the PSTN user number should be defined here. For the **Auto** call type, a routing pattern needs to be defined.

Enable ZeroOut checkbox enables the ZeroOut feature. When this feature is enabled, callers that have reached the ACD Group extension may accelerate the automatic redirection instead of holding in the extension's queue. To activate this feature, caller should dial **0** digit (see Feature Codes) while in the

queue of ACD Group extension. The caller will then be automatically transferred to the destination specified in this page. This selection activates the following fields to be inserted:

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

- **PBX** - local calls between QX IP PBX 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.

Upload new call queue welcome message allows updating the active call queue welcome message for the agents group (played when a caller joins the agents group call queue), downloading it to the PC, or restoring the default one.

The **Remove call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Customize Queue Scenario settings are used to define a custom scenario for audio files played in the ACD queue. Here you may upload custom audio files and to define the sequence in which they will be played for the person in the queue. By selecting this option, the default ACD queue messages will be replaced with the scenario defined below.

Custom Queue Messages table lists all audio files in the custom queue scenario and allows you to add new field. Each audio file is characterized by the number of repeats and the timeout when it should start. The audio files may be ordered in the list with **Move Up** and **Move Down** functional buttons. The custom queue will start with the first audio file in this list and will be played in the loop in the order audio files are listed.

The **Add** functional button opens an **Add Entry** page where a new audio file can be defined. This page consists of the manipulation radio buttons selection to allow upload a new audio file or to select an already uploaded one.

- **Existing File** – this selection is used to choose one of the already uploaded custom queue messages to include in the scenario. The same file may appear in the different instances of the queue music.
- **Upload New File** – used to upload a new audio file. The uploaded files should to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message.

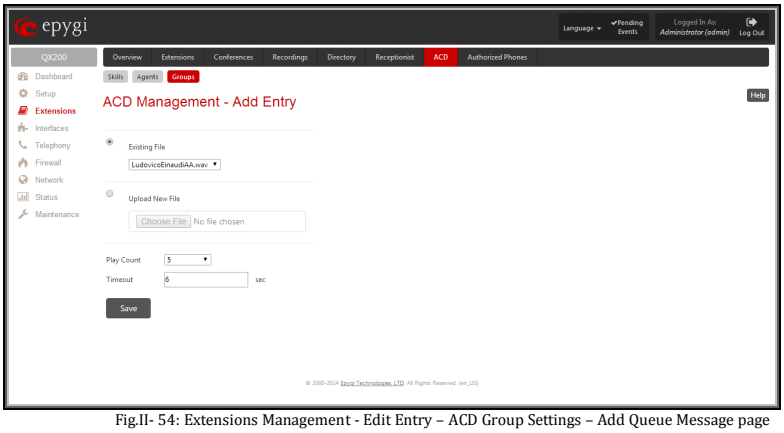


Fig.II- 54: Extensions Management - Edit Entry – ACD Group Settings – Add Queue Message page

Please Note: The file name can contain only alphanumerical characters and '_', '-', '.' symbols.

Attention: You should have enough memory allocated to the corresponding extension (from General Settings) in order to be able to upload audio files; otherwise error message prevents uploading new files.

Play Count indicates the number of times the corresponding audio file will be played continuously in the queue.

Timeout indicates the timeout (in seconds) between the end of the previous queue audio file in the scenario (if any) and the beginning of the current audio file. For the first audio file in the list, this timeout indicates the interval between the beginning of the queue and the beginning of the current audio file's playback.

Play Background Music checkbox is used to fill in the timeout intervals between the audio files in the scenario with the background music. This option requires you to choose the **Audio Line-in** or **RTP Channel** of broadcast streaming. The RTP channels are created from RTP Streaming Channels page.

3. ACD Agents Table Settings

This group is used to configure agents in the ACD group and has the following components:

The **ACD Agents Table** lists all agents in the corresponding ACD group and their statuses.

Add opens the **Add Entry** page where a new agent may be added to the group. The **Add Entry** page contains the following components:

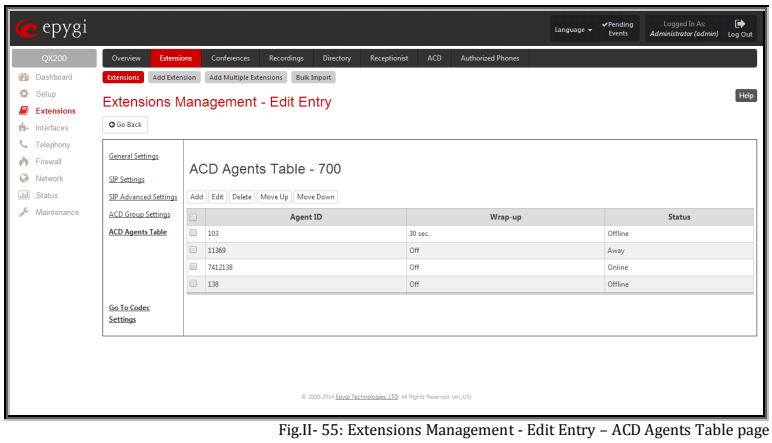


Fig.II- 55: Extensions Management - Edit Entry – ACD Agents Table page

ACD Agent ID text field requires the name of the agent previously created from the Agents table of ACD Management.

Agent Status drop down list requires the actual status of the agent. The following values are available in this list:

- **Online** – the agent is logged into agent group and available for receiving the calls from that group.
- **Offline** – the agent is not logged into the agent group and cannot receive the calls from that group. The same agent still can receive the calls from the other groups where he/she is online.
- **Away** – the agent is logged in but temporarily unavailable for a short time by some reason.

Fig.II- 56: Agents Table of Group – Add Entry page

- **DND** (Do Not Disturb) – agent is busy by some other activity not related to conversation on the phone. For example, agent can be busy by updating the customer's record after the call or entering some data into database. Versus to **Away** status, the **DND** state of the agent changes automatically to **Online** when the preconfigured DND timeout expires (it is now 30 seconds by default).

Please Note: The state of the Agent can also be modified from the handset by calling the predefined Auto Attendant (see Attendant Extension Settings and ACD Management).

Enable wrap-up – if enabled, the current Group doesn't send new calls to the Agent within the wrap-up **Timeout** after closing the active call. Versus DND, the agent's status doesn't change during **Timeout** period, which activates automatically every time when the agent finishes the call. That period is used, for example, by the agent for updating the customer's records after the call.

Move Up and **Move Down** buttons are used to move the selected entry one level up or down within the **Agents Table**. The sequence of Agents is important when **Round Robin** call distribution is selected in the **ACD Group Settings** page (see above). Agents will be called in the order selected in the Agents table.

Recording Box Extension Settings

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

1. **General Settings** (for Recording Box extension)

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

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

Password requires a password for the Recording Box extension.

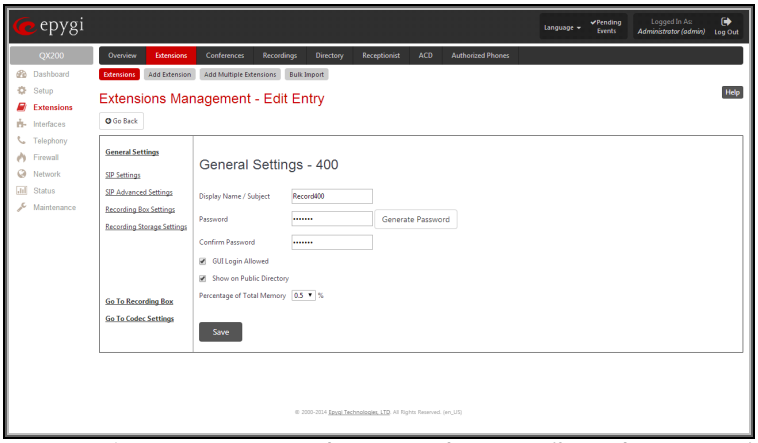


Fig.II- 57: Extensions Management - Edit Entry – General Settings page (for Recording Box extension)

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

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

GUI Login Allowed checkbox enables the current extension to be used to access the QX IP PBX via WEB interface by extension name and password.

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

The **Percentage of Total Memory** drop down list allows you to select the space for call recordings and the uploaded custom messages of Recording Box extension. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX IP PBX.

2. **Recording Box Settings**

This group contains Recording Box settings and has the following components:

Ask Password on Local Access checkbox selection enables the password protection for local PBX callers when entering Recording Box.

Ask Password on Remote Access checkbox selection enables the password protection for remote SIP or PSTN callers when entering Recording Box.

Play Welcome Message checkbox is used to enable/disable the welcome message played when entering the Recording Box.

Maximum recording count drop down list indicates the maximum number of call recordings allowed to be stored in the corresponding extension's Recording Box. If the limit is reached, some call recordings should be deleted from the Recording Box to be able to make more recordings.

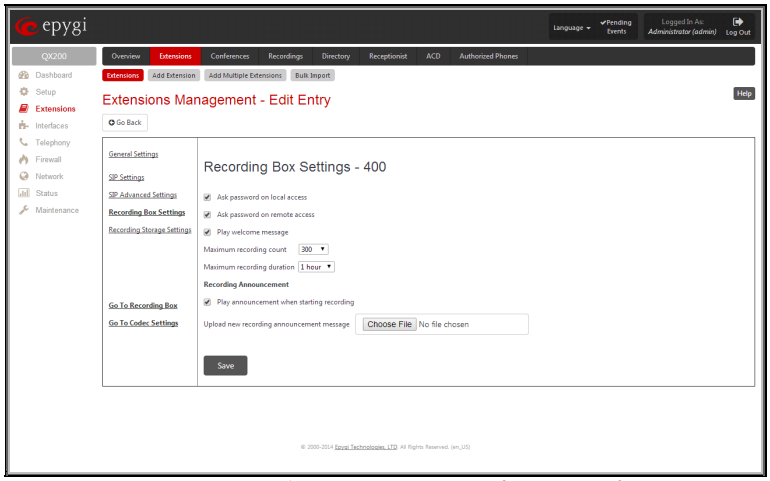


Fig.II- 58: Extensions Management - Edit Entry – Recording Box Settings page

Maximum Recording Duration drop down list is used to select the maximum duration of the single call recording for the selected Recording Box extension. When the call reaches the selected duration, the recording will be automatically stopped, while the call will stay active.

Recording Announcement group allows updating the active recording announcement (played in the call when call recording starts), downloading it to the PC, or restoring the default one. The group offers the following components:

Play Announcement When Starting Recording checkbox is used to enable/disable the announcement played during the call saying that the call recording starts. When this checkbox is not selected, the call recording will start silently, without any notification.

Upload new recording announcement message indicates the file name used to upload a new recording announcement 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 recording announcement message file.

The **Download Recording Announcement Message** and **Remove Recording Announcement Message** links appear only if a file has been uploaded previously. The **Download Recording Announcement 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 Recording Announcement Message** link is used to restore the default recording announcement message.

3. Recording Storage Settings

This group contains recording storage settings and is divided into two groups:

The **Modes** radio buttons selection is used to choose the storage option once the call recording is done. Following options are available:

- **FTP Mode** - this option will send immediately recordings to the FTP server and delete from device. This option will keep your device memory the most free.
- **Simple Local Mode** - this option will keep recordings locally. Stop recording when local space is full and generate an event.
- **Cyclic Local Mode** - this option will keep recordings locally. When local space is full, delete the oldest recordings.
- **Mixed Mode** - this option will keep recordings locally. When local space is full or when **Maximum recording count** is reached, move the oldest recording to FTP server.

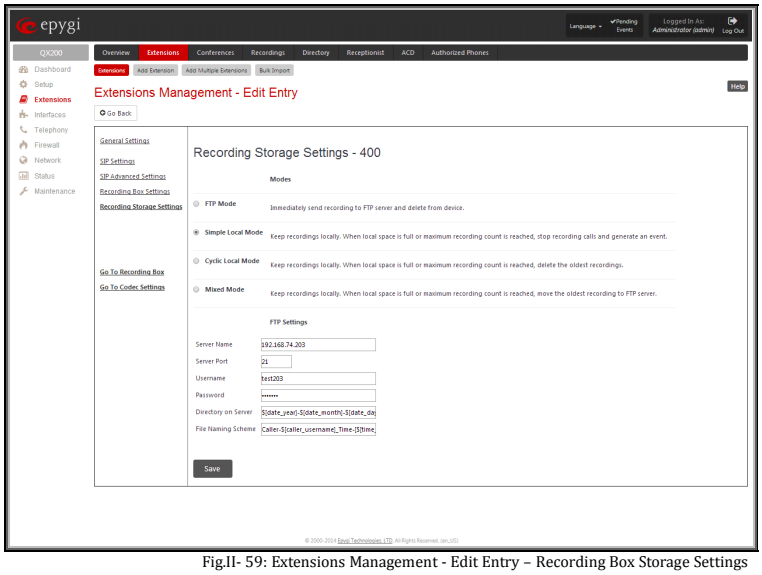


Fig.II- 59: Extensions Management - Edit Entry – Recording Box Storage Settings

The **FTP Settings** group is used to define the FTP server settings where the recordings will be uploaded, if configured accordingly.

Server Name text field requires the FTP server name.

Server Port text field requires the FTP server port number.

Username and **Password** text fields require the FTP server authentication parameters.

Path on Server text field requires the location on the server where the recordings will be stored.

Naming Scheme text field requires the naming scheme of the files to be uploaded to the FTP server. This scheme helps to distinguish files among others and to avoid possible overwriting of the files. This text field may contain any distinctive text and also offers a list of variables:

- caller_dispname – caller's display name
- caller_username – caller's username
- caller_fullname – caller's full name in the username@host[:port] format
- callee_dispname – called user's display name
- callee_username – called user's username
- callee_fullname – called user's full name in the username@host[:port] format
- duration – duration of the call
- time_hour – hour when the call recording started
- time_min – minute when the call recording started
- time_sec – second when the call recording started
- date_year – year when the call recording started
- date_month – month when the call recording started
- date_day – day when the call recording started
- extension – recording box extension
- hostname – QX hostname

Any combination of above variables can be used in the **Naming Scheme** text field along with the manually text inserted. The following syntax applies:

Example: MyQX-$[caller_dispname]-$[duration]-$[time_hour]-$[time_min]_business

In case if the caller's display name was Andrew, the call lasted 15 seconds and it took place on 14:10 the files stored on the FTP server for this Recording Box extension will have the name:

MyQX-Andrew-15 sec-14-10-business.wav

Attention: Make sure **Naming Scheme** text field contains symbols that your FTP server allows. For example, symbols :, /, \, *, ?, ", <, >, | are not allowed by the MS Windows Operation System running servers.

Retry Count text field indicates the number of retries to access the server, in case of networking problems.

Retry Timeout text field timeout between retries to access the server.
The **Go to Recording Box** link moves to the recording box of the corresponding extension's Recording Box where all recorded calls are locally stored. The Recording Box is also accessible from Extensions Management table, by clicking on the corresponding Recording Box extension.

Recording Box

Recorded calls on the QX IP PBX can either be stored locally in the Recording Box or be uploaded to the remote FTP server. The **Recording Box** is used to locally store the recorded calls. The Recording Box can be accessible online from Web Management or from handset by calling the corresponding Recording Box extension. With both options, the user can play and delete the recorded calls located in the Recording Box.

Please Note: When using **Call Recording** on the QX50/QX200 it is advisable to use an SD memory card to expand the system memory.

When accessing the Recording Box through the handset, all recording box functionality settings, such as enabling the welcome message, adjusting the maximal call recording duration, recording box access security, etc. are configurable from Recording Box Extension Settings page.

Instructions on accessing and navigating within the Recording Box via the phone handset are described in the Feature Codes.

Please Note: When playing a new call recording (via a phone handset or with the use of the **Play** button in this page) will deprive the "New" state of the recorded call.

The **Recording Box** can hold **New** (not yet played) and **Old** (already played) call recordings. The **Status** column in the Recording Box table indicates the current state of the call recordings. All new recordings in the table are displayed in bold font. Playing a call recording cancels both the **New** status and bold font. Call recording can be selected to be played or deleted. The following information is available on this page:

Recording free space provides information on the number of minutes/seconds of free recording box space.

Refresh functional button is used to refresh the Recording Box for any latest recordings or status changes.

Send to FTP functional button is used to move one or more selected recordings to the FTP server configured from **Recording Storage Settings** in Recording Box Extension Settings page.

New recordings field shows the number of newly done call recordings since the user's last access to the voice mailbox.

All recordings field shows the number of all recordings existing in the Recording Box.

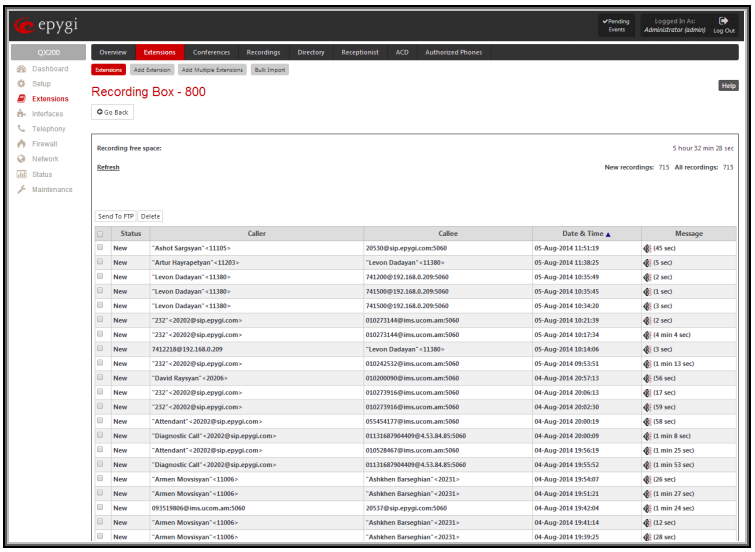


Fig.II- 60: Extension's Recording Box

Recording Box table displays the following information:

Status - indicates whether the call recording is **New** and not yet played. New recordings are displayed in bold font.

Caller – is the address of the caller of the recorded call.

Callee – is the address of the called party of the recorded call.

Date & Time – is the call recording start date and time.

Message – indicates call recording duration (in minutes/seconds) and a speaker sign used to play (using any available media player supported by your Operation System) the recording or to download the audio file to the PC.

The column headings of the voice mail tables are created as a link. By clicking on the column heading the table will be sorted by the selected column. Upon sorting (ascending, descending) arrows will be displayed next to the column heading. Each row in the Voice Mailbox tables can be selected by a checkbox for editing, deleting or marking.

To Play a Call Recording

1. Click on the speaker icon of the corresponding recorded call.
2. Depending on you browser's settings the .wav file will be played directly or an application will ask you to save the .wav file on the local PC. In the second option, please specify the path and run the media file from the specified location to play it.

To Delete a Call Recording

1. Select the checkbox of the corresponding record(s) in the **Recording Box** table that should to be deleted.
2. Select the **Delete** button.
3. Confirm the deletion with **Yes**. The selected recordings will be deleted. To abort the deletion and keep the recordings in the inbox, select **No**.

Attendant Extension Settings

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

1. **General Settings** (for attendant extension)

This group requires 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.

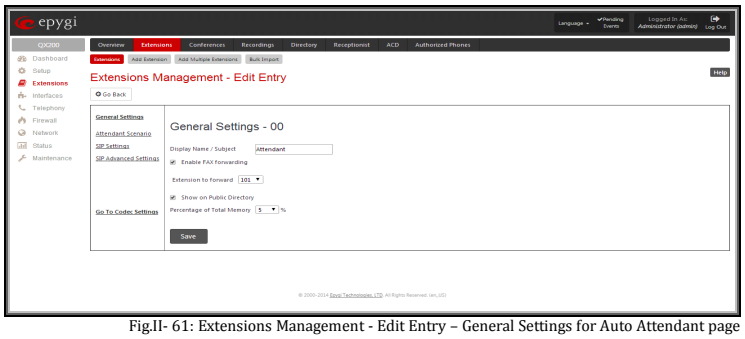


Fig.II- 61: Extensions Management - Edit Entry – General Settings for Auto Attendant page

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

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

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

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

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 IP PBX.

- **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 (see Feature Codes) during the Auto Attendant welcome message. The caller will then be automatically transferred to the destination specified in this page.

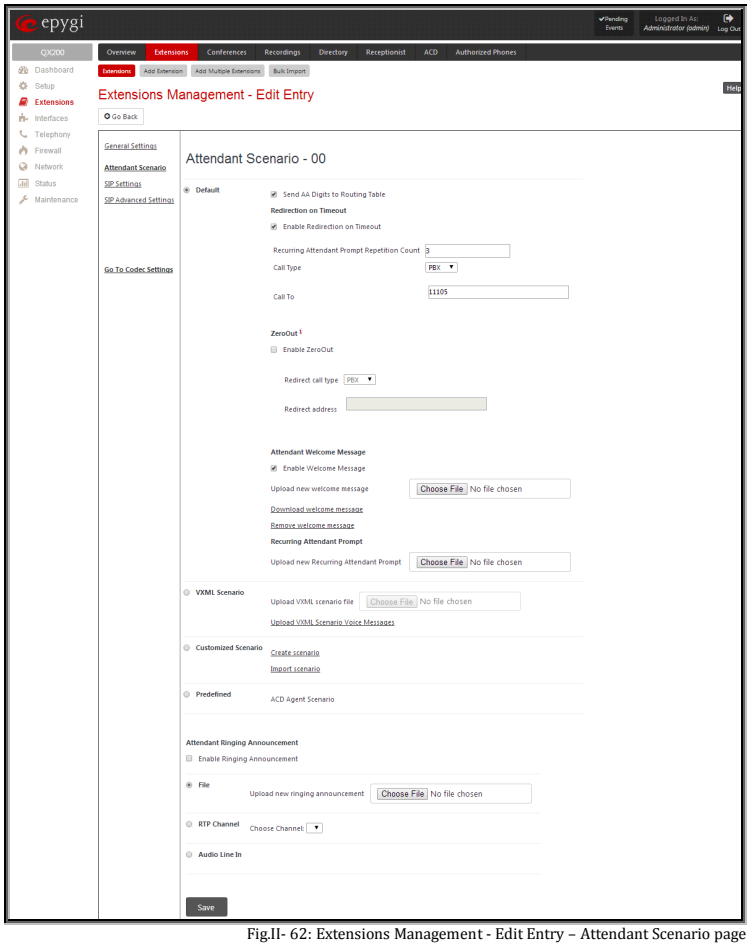


Fig.II- 62: Extensions Management - Edit Entry – Attendant Scenario page

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

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

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

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

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

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

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

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

  Upload new Recurring Attendant Prompt indicates the file name used to upload a new recurring auto attendant prompt. The uploaded file needs to be in PCMU (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.

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

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

- **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 IP PBX 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. **Browse** opens the file chooser window to browse for a custom scenario file.

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

The **Customized Scenario** radio button selection allows you to switch the Attendant to the customized Attendant scenario. The **Customized Scenario** radio button selection enables the following components:

- The **Create Scenario** link refers to the **Edit Scenario** page where a new scenario for a current Auto Attendant might be created.

The **Edit Scenario** page consists of two pages for menu configurations: The **Main menu** configuration page and the **Submenus** configuration page.

The **Main menu** is the menu where all incoming calls to the certain Auto Attendant will be placed first. The **Submenus** are the supplementary menus which can be called from the other menus.

Both the **Main menu** and all **Submenus** can call each other. This allows the opportunity to have several index levels for the Auto Attendant. There are no limitations on the depth and nesting levels of menus.

The **Main menu** page consists of the following components:

Welcome message indicates the file name used to upload a new custom Auto Attendant welcome message. The Auto Attendant **Welcome message** will play only once when callers enter the Customized Auto Attendant.

Delay after message requires the delay (in seconds) after which the **Recurring message** will be played.

Recurring message indicates the file name used to upload a new custom Auto Attendant recurring message. The Auto Attendant **Recurring message** will play after the Attendant **Welcome message** (if it is uploaded).

Play Count text field indicates the number of times the corresponding **Recurring message** will be consecutively played to the caller.

Interval requires the time period (in seconds) between consecutively played **Recurring messages**.

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

Press the **Save** button to submit the changes or use **Go Back** to keep the initial data.

Attention: 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.

The **Download** and **Remove** links appear only if a file has been uploaded previously. The **Download** 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** link is used to restore the default welcome message.

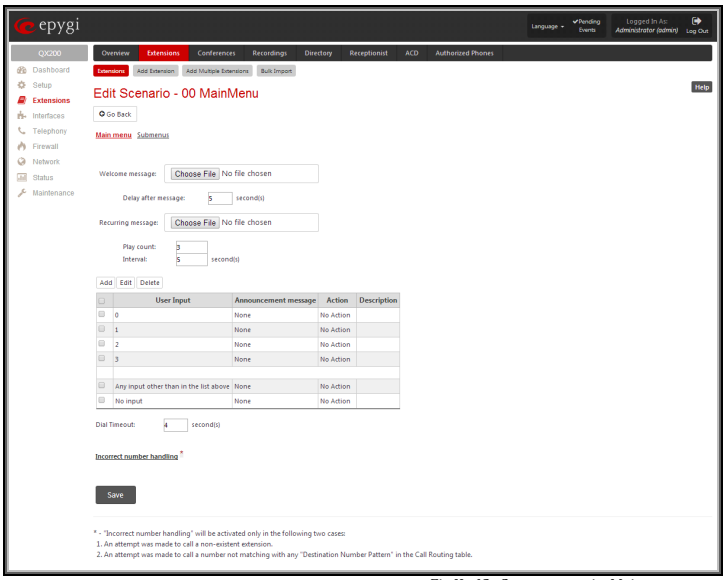


Fig.II- 63: Create scenario-Main menu page

The **User Input Options** table is for configuring the action to be taken based on one of the following user choices:

- **User Input**
- **Any input other than in the list above**
- **No input**

The user will press one of the following input options on the phone to activate the corresponding action. The option can be selected after reaching the Auto Attendant Service and after the **Welcome** and/or **Recurring messages** have been played.

The **User Input** table consists of the following functional buttons:

Add opens the **Add Option** page where the actions for previously unspecified inputs can be configured.

Add link opens the **Add Option** page where the actions for previously unspecified inputs can be configured.

Edit link opens the **Edit Option** page where the actions of previously configured **User Input** options can be adjusted.

The **Add/Edit Option** page offers the following components:

Description – text field for an optional description of the option.

Option is used for choosing the user input for which some announcement and/or action should be configured. The following input options are available in the list to configure the **Customized Scenario**:

- Digits (in a range from **0** to **9**)
- Signs ("*****" and "**#**")

Announcement indicates the file name used to upload a new custom message. When the caller selects the option configured in the **Option** drop down list, this message will be played once before the **Action** will be activated.

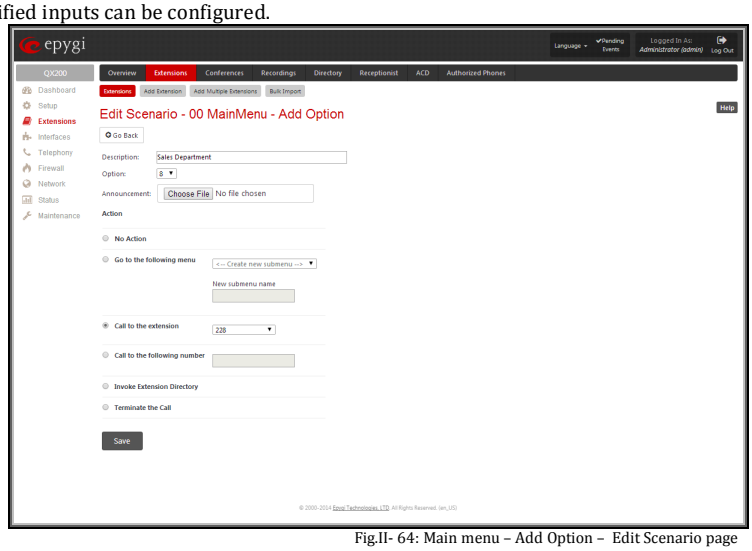


Fig.II- 64: Main menu – Add Option – Edit Scenario page

Attention: 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.

The **Download** and **Remove** links appear only if a file has been uploaded previously. The **Download** 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** link is used to restore the default welcome message.

Action is used to configure the action based on the caller's selection.

The **Action** radio buttons allows you to configure the action type after playing the **Announcement** message (if configured):

- **No Action** the Auto Attendant will continue to play the **Recurring message** (if configured) of the current menu.
- **Go to the following menu** will go to the specified submenu and take actions defined in that submenu. The drop down list allows the selection of a previously created submenu or to create a new submenu by choosing the **Create New Submenu** item. The **New submenu name** text field requires the new submenu name.
- **Call To the following extension** will call to the extension number specified in the extensions drop-down list.
- **Call to the following number** will call the specified phone number via the Call Routing Table**.**
- **Call to the number dialed** will send the user inputs to Call Routing table and if there is a matching with any Call Routing rule the call will be made with the conditions of Call Routing rule (available only in case when the **Any input other than in the list above** input is edited).
- **Invoke Extensions Directory** will connect the caller to Extensions Directory.
- **Terminate the call** will exit from this Customized Scenario and disconnect the call.

The following options can be configured too:

- **Any input other than in the list above -** allows configuring the action taken when the caller makes a selection other than options listed in the **User Input** table. If it is configured to **No Action** then the timer for No Input will reset and it will be counting the No Input time again.
- **No input** – allows configuring the action taken when the caller doesn't enter anything during the certain period. The **No Input** timeout is equal to [*Welcome message duration*] + **Delay after message** + [*Recurring message duration*] * **Play Count** + **Play Count** * **Interval**. If there is no input during that time, the action specified for **No input** will take effect.

The **Dial Timeout** specifies the period of time to determine when the user has completed dialing and to begin to process the call. The timer will start after the last digit or symbol is entered. If the (#) key has been pressed then the call will be processed immediately.

Incorrect number handling link opens the **Edit Incorrect Number Handling** page which is similar to **Edit Option** page to configure the action taken when the user has selected a destination that resulted in a failed call, such as an invalid extension number.

Incorrect number handling link will open the page to configure the action taken when the user has selected a destination that resulted in a failed call, such as an invalid extension number.

Please Note: The **Incorrect number handling** will be activated only in the following two cases:

- An attempt was made to call a non-existent extension,
- An attempt was made to call a number not matching with any "Destination Number Pattern" in the Call Routing table.

Attention: If a file with the same name is uploaded for other options, the previous file will be replaced.

The **Submenus** page consists of the following functional buttons:

Add opens the **Edit Scenario - Add menu** page where a new **Menu name** may be defined.

Edit opens the **Edit Scenario** page where a newly created submenu scenario settings might be adjusted.

Fig.II- 65: Create scenario-Submenus page

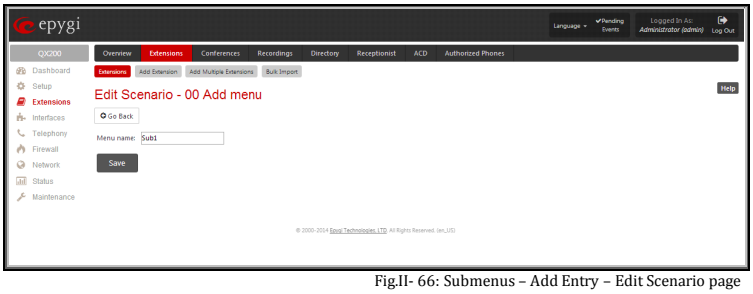


Fig.II- 66: Submenus – Add Entry – Edit Scenario page

- The **Edit Scenario** link appears only if a new scenario has been created previously. The **Edit Scenario** link opens the **Edit Scenario** page, where a previously created scenario can be changed.
- The **Import/Export scenario** link leads to the page where a new scenario file can be imported or exported.

The **Import/Export Scenario** page offers the following components:

Import scenario is used for uploading the previously downloaded scenario and custom messages file.

Export scenario appears when the **Customized Scenario** was previously configured for the current Auto Attendant. The **Download scenario** link is used to download the scenario and voice message files to the PC and opens the file-chooser window where the saving location may be specified.

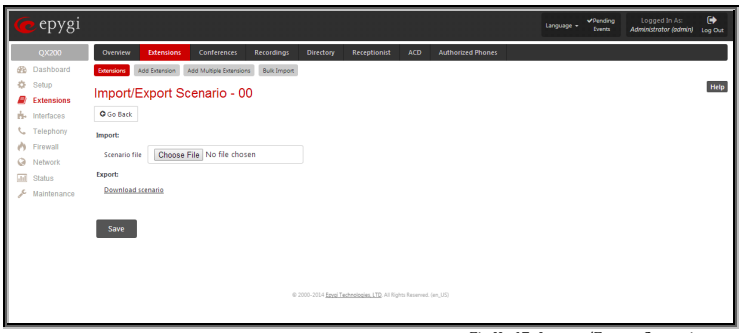


Fig.II- 67: Import/Export Scenario page

- The **Remove Scenario** link removes the current **Customized Scenario**. After pressing the **Remove scenario** link all configurations and uploaded voice messages will be deleted from the system.
- The **View/Download VXML Scenario** link appears only when a customized scenario has been created and is used to view or download the generated script in a VXML file format.

The **Predefined** manipulation radio button selection allows you to switch the Attendant to the ACD Agent Scenario (see ACD Management).

Attention: This selection is only available if the ACD feature is previously activated from the Feature Keys page.

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

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

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

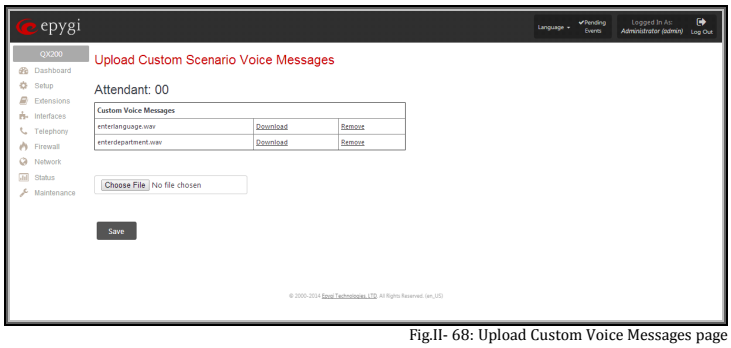


Fig.II- 68: Upload Custom Voice Messages page

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.

- **Audio Line In** (available only for QX50/QX200) selection uses the external radio broadcasting or any other audio resource as the hold music. When selecting this option, check with your system administrator if there is an external audio resource connected to the QX IP PBX.

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

Delete removes the selected extensions. If no records are selected an error message occurs. Deleting an extension from the Extensions Table will automatically remove the name attached to the deleted extension in Extensions Directory.

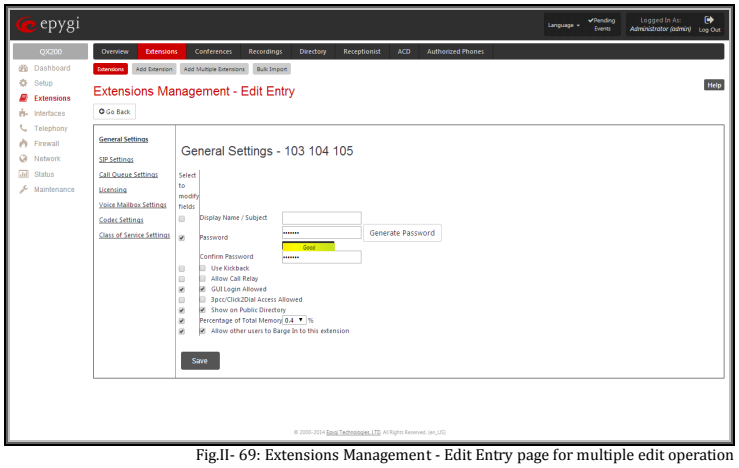


Fig.II- 69: Extensions Management - Edit Entry page for multiple edit operation

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 IP PBX. 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/conference. 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/conference will be impossible.

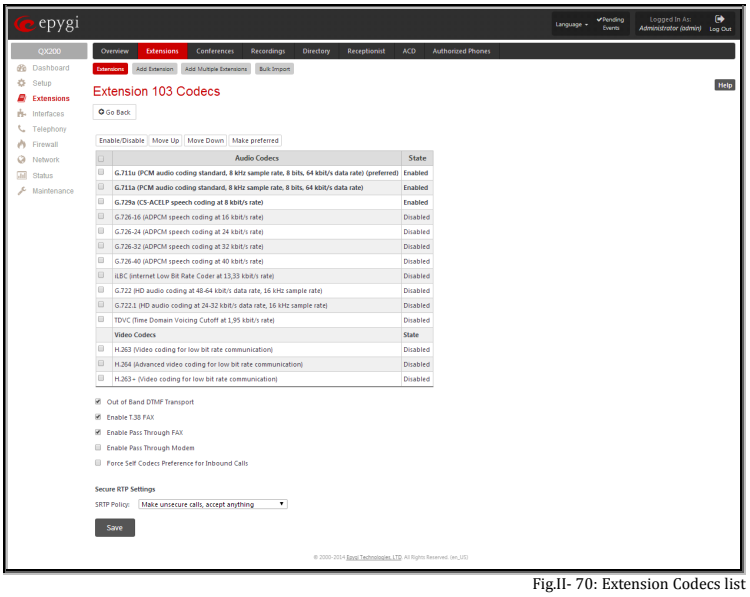


Fig.II- 70: Extension Codecs list

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 (fax to mailbox) 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. For virtual extensions, the incoming FAX can only be stored in the extension's voice mailbox. To allow FAX to be stored in the voice mailbox, the extension's user should not answer the incoming calls, so that they are forwarded to the voice mailbox.

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

Enable Pass Through Modem checkbox is 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 IP PBX. 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.

Call Park and Directed Call Park Service

The **Call Park** and **Directed Call Park** services are used to store a call on a specific number so that any other user on the system can retrieve it. For example, a user receives a call but wants to take it in a conference room where it is possible to speak privately. Transferring the call to the conference room is not an option because the conference room it is transferred to might be in use, or the user is unable to walk to the conference room in time to answer the call. The user can use **Call Park** and **Directed Call Park** to place the call at a specific number and then retrieve when they reach the conference room.
To use the **Call Park** or the **Directed Call Park** features, at least one Call Park extension should be created in the Extensions Management table. Additionally, two lists should be defined for the call park extension: **Park Access List** for users that might park a call to the corresponding Call Park extension and **Retrieve Access List** for the users that can pick up calls parked to that extension. By default, both of these lists have entries so any PBX extension on the QX IP PBX can park the call, and any destination can retrieve the parked call. Any limitations to these settings should be done individually for each call park extension.

To make a Call Park

To make a Call Park, the QX IP PBX user which has been previously added to the **Park Access List** for at least one of the available Call Park extension on the QX IP PBX should dial the appropriate digit combination (see Feature Codes in Manual III - Extension User's Guide) during the call. The active call will go on hold, while the PBX number and the SIP username (if it is registered on the SIP server) of the first available call park extension where the user is added will be played to him/her.

The pickup user will be able to pick up the parked call from any destination by calling the extension where the call has been parked (either by its PBX number or SIP address). The authentication password will be prompted (if configured) of the call park extension in order to retrieve the parked call.

For example, the Call Park extension 77 is created which has been registered on the SIP Server under the 892220 registration username. The QX IP PBX user is added to the Park Access List, while the phone at the remote location is added to the Park Access List of that call park extension.
While being on a call with user A, the QX IP PBX user dials the appropriate calling code. As a reply, QX IP PBX will play the extension 77 and SIP username 892220 to the QX IP PBX user. The user A goes on hold. The QX IP PBX user moves to a remote location and makes a call to the call park extension. The QX IP PBX user enters call park extension's password and resumes the conversation with user A.

To make a Directed Call Park

To make a Directed Call Park, the QX IP PBX user, which has been previously added to the Park Access List for at least one of the available Call Park extension on the QX IP PBX, should place the current call on hold and then dial the Call Park extension number within the five second timeout (see Feature Codes in Manual III - Extension User's Guide).

Attention: If the five second timeout is exceeded, then the QX IP PBX will consider it as an attempt for retrieving the parked call.

The Call Park extensions can be mapped directly to IP phones or simply announced via paging through the IP phones or analog paging system. Calls can be easily parked by placing the current call on hold and then pressing the park button followed by the desired extension. This can be further simplified if the desired Call Park extension is already mapped to the phone, then the user will just press that specific park key and the call will automatically be parked to that extension.

The pickup user will be able to pick up the parked call from any destination by calling the extension where the call has been parked (either by its PBX number or SIP address). The authentication password will be prompted (if configured) of the call park extension in order to retrieve the parked call.

Please Note: The Call Parking is valid for the period defined in the Call Park Extension Settings. By default it is 15 minutes. During that time hold music (if configured) will be played to the parked party. When the **Retrieve Timeout** expires, the phone that initiated the call parking will start to ring. If no one picks up the parked call, or if the phone is off hook, the parked call will be automatically disconnected.

Please Note: Anyone who wishes to retrieve the parked call will be requested to pass a password authentication (if the password is defined for the call park extension) to resume the parked call. The parked call will be disconnected if an incorrect password has been inserted and authentication has been rejected. To avoid unexpected calls received on the extension used for call parking, it is recommended to use virtual extensions for the **Call Park** service.

Barge In Service

Attention: The **Barge In** service is an optional feature and can be activated with a feature key from the Feature Keys page.

The **Barge In** service on the QX IP PBX allows the PBX users to participate to the third party's calls while remaining imperceptible. With the special feature codes (for details, see Feature Codes in the Manual III – Extension User's Guide), you may dial in to the active calls between the other local PBX user and his call partner and depending on the configuration and the feature code used you may listen to the call, additionally be able to speak to the extension user only or to all participants.
This service offers three options:

- **Listen in** – with this option you may only listen to the third party's call without being able to speak in the call. No sound notification will be heard in the third party's call when you dial in.
- **Whisper –** with this option you may listen to the third party's call and speak to the extension to which you have barged in. Only that extension will hear a sound notification when you dial in.
- **Barge in –** with this option you may listen to the third party's call and speak to all participants in the call. All participants of the call will hear a sound notification when you dial in.

To use the **Barge In** service options, the **Barge In** feature should be enabled and configured on the extension (from User Extension Settings) to which you wish to barge in the call.
Attention: **Barge In** service calls are not displayed in **Active Calls** table on the Administrator's Main Page, nor are registered in the Call History.

Add Multiple Extensions

The **Add Multiple Extensions** tab is used to add multiple extensions to the Extensions Management table at once. The page consists of the following components:

Type checkbox is used to select the type of the extensions (User Extension, Pickup Group, Call Park, Paging Group, ACD group, Recording Box or Attendant) to be created.

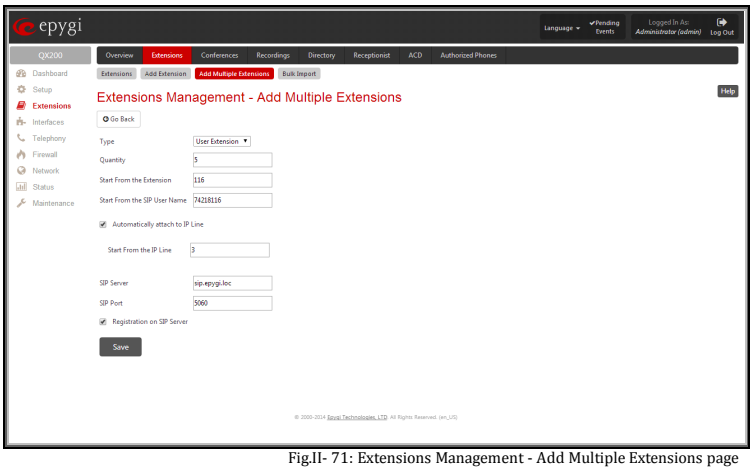


Fig.II- 71: Extensions Management - Add Multiple Extensions page

Quantity text field requires the number of extensions to be created at once. For example, inserting 5 in this text field will add 5 new extensions to the Extensions Management table.

Start from the Extension text field requires the number of the first new extension to be created. Depending on the value in the **Quantity** text field, the next extensions to be created will have subsequent numbers. For example, if you have inserted 41 in this text field and the **Quantity** text field contains the value "5", then extensions 41, 42, 43, 44 and 45 will be added to the Extensions Management table. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" will appear. If an extension with the given numbers already exists in the Extensions Management table, a next subsequent not used extension number will be used instead.
Please Note: Extension cannot start with the digit 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.

Start from the SIP User Name text field requires the SIP server registration user name for the first extension to be created. Depending on the value in the **Quantity** text field, the next extensions to be created will have subsequent SIP user names. For example, if you have inserted 30201 in this text field and the **Quantity** text field contains the value "5", then the 5 newly created extensions will correspondingly have the following registration SIP user names: 30201, 30202, 30203, 30204 and 30205. This user name is used for the registration on the SIP Server and should be unique on the SIP server. This field length is limited by 20 symbols and is not limited regarding the use of symbols. If an extension with the given SIP user name already exists in the Extensions Management table, a next subsequent not used SIP user name will be used instead.

The **Automatically attach to IP Line** checkbox selection is used to automatically attach extensions to IP Lines.

Start From the IP Line text field requires the number of the new IP Line to be created. The error message "One or more IP Lines in the specified range are already attached to existing extensions" appears if an IP line with the given numbers already exists in the Extensions Management table.

SIP Server text field requires the address of the SIP server. The field is not limited regarding symbol usage and length as it can be either an IP address or a host address (e.g. sip.epygi.com).

SIP Port text field requires the port number to connect to the SIP server. The SIP Port may only contain digit values, otherwise an error message "SIP Port is incorrect" will appear. If the SIP server port is not specified, QX IP PBX will access the SIP server via the default 5060 port.

Registration on SIP Server checkbox enables the SIP server registration option on the newly created extensions.

User Extension Bulk Import

The **Extensions Template Management** feature and the PC-based **Bulk User Extensions Importer** tool are used to create and update multiple user-type extensions.

The user extension settings can be divided into two groups - common settings of extensions groups (for example, SIP server name, SIP port, etc.) and settings, which are different for each extension of these groups (for example, Display Name, Extension Password, etc.). Based on this, the following three steps can be used to **Add/Modify** a group of extensions:

- Configure the common settings for a group of extensions, using the QX IP PBX Extension Template Management feature.
- Based on the common settings of these groups, configure the extensions specific settings using the Epygi **Bulk User Extensions Importer** tool. The tool will save the settings in a bulk User Extension configuration file that will be ready to upload to the QX IP PBX.
- Import the configuration file to the QX IP PBX, using the Extension Import feature.

Please Note: The **Bulk User Extensions Importer** tool is applicable only for **Adding** and **Modifying** the extensions of User Extension type. The extension types other than User Extension (such as Auto Attendant, Pickup Group, etc.) currently are not supported by this tool.

To configure the Extension Templates on the QX IP PBX, select the **Extension Template Management** tab from this page.
The **Extension Template Management** page is used to configure different sets of user extension settings. The **Extension Template Management** offers the following components:

- **Add** opens the **Extension Template Management- Add Entry** page, where a new template can be created.
- **Edit** opens the **Extension Template Management - Edit Entry** page, where the settings of the user extension template can be configured.

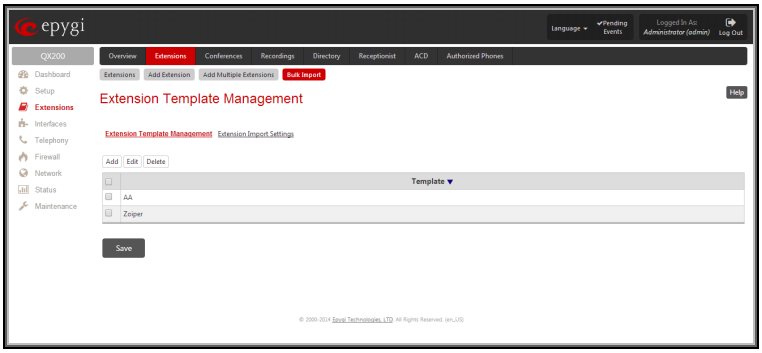


Fig.II- 72: Extension Template Management page

The template file contains the common settings for user extensions, which can be the same for a group of extensions. The other settings which have to be different for each extension (such as SIP username or IP Line configuration) should be specified by the Epygi's Bulk User Extensions Importer configuration tool and imported later from the appropriate configuration file. These settings are marked with "variable" sign in the extensions configuration page (see User Extension Settings).

The Epygi **Bulk User Extensions Importer** configuration tool is a MS Excel based form, which allows a configuration file to be created (based on the configured templates) for **Add/Modify** type of files.

When your configuration file is ready, select the **Extension Import Settings** tab to upload the Bulk User Extensions Importer configuration file to the QX IP PBX.

Browse opens the file selection window to browse for a new user bulk extension configuration file.

The **Override Existing Extension** indicates whether the settings of the imported file should change the settings of existing extensions if the imported file is of the **Add** type. It can also contain the settings for extensions which already exist on the QX IP PBX. When the **Override Existing Extension** is unchecked and the uploaded **Add** type CSV configuration file contains extensions which already exist on the QX IP PBX, an error will appear and the conflicting extensions will be highlighted. If the uploaded file is of the **Add** type and the intent is to modify existing extensions, then the **Override Existing Extension** should be enabled, otherwise the file must be of the **Modify** type.

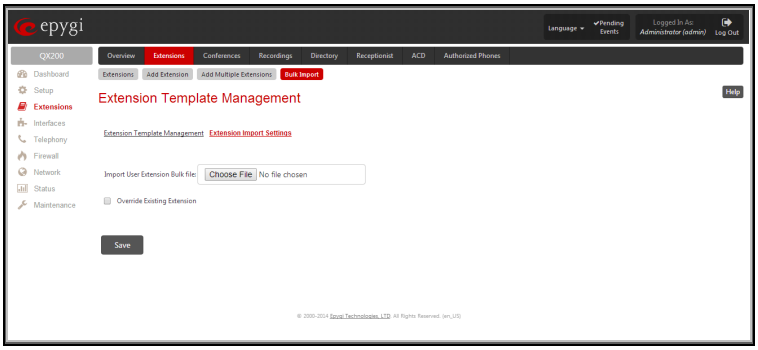


Fig.II- 73: Extension Import Settings page

When you upload the Bulk User Extensions Importer configuration file, the system will check the entire file before applying the uploaded configurations. If there are some incorrectly configured settings in the file, the system will return a table with all uploaded configurations and highlight the parameters which have an error.

If the uploaded file passed and did not give any error message, the system will start to **Add/Modify** all specified extensions. As a result, the system will **Add/Modify** the specified extensions. In addition, for any settings that need to be updated in the IP phone, (e.g Display Name), a new IP phone configuration file will be created and ready for sending to the phone the next time it is rebooted.

Conferences

Please Note: The **Conference Server** and the **Video Conferencing** are optional features and can be activated with a feature key from the Feature Keys page.

Conference users with video will be able to see the current speaker and either manually or automatically switch between participants. This gives the user power over which person they get to view or allows the video conference server to rotate the video feed to the person currently speaking.

After activating Video Conferencing feature from the **Setup - Licensed Features** GUI page, the video codecs will be available on the QX IP PBX's Conference Codecs GUI page.

Please Note: Administrator should enable only one codec at a time, either **H.263** or **H.264**.

Video Conferencing provides possibility to view particular participant based on switching modes.
In general there are two switching modes for each phone:

- **Manual -** allows participant to switch between video capable participants manually, by dialing *50 or *51, a participant will see the next or previous participant who has video capability enabled. In the context of manual switching "**next**" and "**previous**" means the order of entrance to the conference bridge, so the first caller will be the first video- capable participant connected to conference.

- **Automatic –** In this mode QX IP PBX determines the speaker (or loudest participant), and will automatically switch the video stream to show that speaker. As a result all the video phones, which are in automatic mode, will see the speaking participant. If participant does not have a video phone, then the other participants will see a black screen.

Please Note: Users can switch between manual and automatic mode by using *50/*51 and *52.

By default, **Automatic Speaker Detection** is switched off. From the Conference Settings page administrator can enable or disable the default mode for video conferencing (see Automatic Speaker Detection).

Conferences Management

The **Conferences** page displays a table with the existing conferences on the system. This page allows you to create new conferences and manage the existing ones.

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

- **Conference ID** - indicates the unique ID of the conference. This number is used from Auto Attendant to reach the conference. The Conference ID is also used as the username for the moderator when logging into the QX IP PBX.
- **Display Name** – any optional information about the conference.
- **Description** – any descriptive information about the conference.
- **SIP Address** - displays the SIP address of the conference.
- **Status** - indicates the status of the conference (Active, Non Active or Waiting). Clicking on the conference status link will display the **Conference Progress** page with detailed information about the conference status, participants in the conference and description of each participant. This page additionally allows the administrator to drop a participant from the conference or invite new participants. It also allows the moderator to start/stop/resume/pause the conference recording and to terminate the conference.
- **Percentage of System Memory** - indicates the conference related memory space (in percents) dedicated to conference recordings and the conference specific custom system messages.
- **Codecs** - column lists the short information (full information is seen in the tool tip) about conference specific voice Codecs. Conference codec's can be accessed and modified by clicking on the link of the corresponding conference's Codecs. The Link moves to the Conference Codecs page.

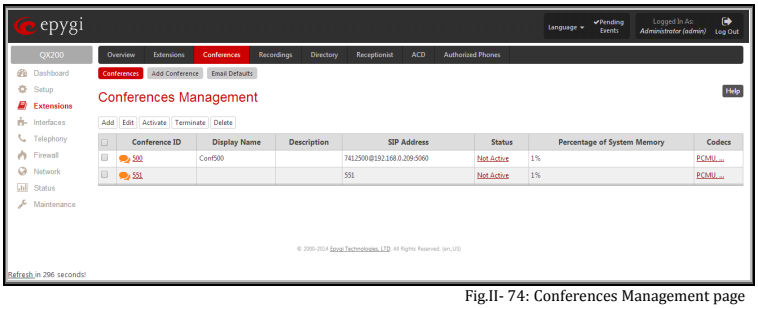


Fig.II- 74: Conferences Management page

Clicking on the corresponding conference ID will move to the Moderator's page where call general settings can be configured.

The page **Conference** consists of the following functional buttons:

Add opens the Conferences Management - Add Entry page where a new conference can be created.

Edit opens the **Conferences Mangement - Edit Entry** page where the settings of a newly created conference might be adjusted. The system provides the possibility of editing multiple conferences at the same time.

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 Entry** - **General Settings** page allows the administrator to edit the following conference settings:

- **Display Name** is any optional information about the subject of the conference.
- The **Show on Public Directory** checkbox is selected, the details of the selected conference will be displayed in the User Settings table on the **Main Page** of the Extension's Web Management. Besides this, the details of the conference will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the conference is reserved or not used.
- The **Percentage of System Memory** drop-down list is used to select the memory space (in percents) that can be used for storing conference recordings.

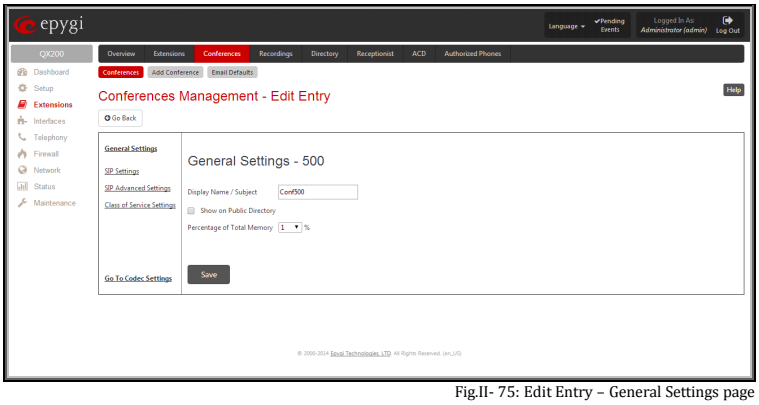


Fig.II- 75: Edit Entry – General Settings page

The **Edit Entry - SIP Settings, Edit Entry – SIP Advanced Settings** and **Edit Entry – Class of Service Settings** pages are used to configure the conference's SIP basic registration, advanced settings and assign the defined classes to the conference extensions respectively. The descriptions of the settings can be found in the User Extension Settings section.

Activate is used to activate the selected conferences.

Terminate is used to stop the selected conferences.

Add Conference

Add Conference tab opens the **Conferences Management - Add Entry** page where a new conference can be created.

The page consists of the **Conference ID** text field that requires a unique ID for the call conference.

Please Note: The length of the Conference ID is limited to 20 digits. The Conference ID cannot start with the digit 0, which is a reserved character.

The Conference IDs can be used in Auto Attendant to reach a conference on the system. To join a conference using its ID, dial the **Conference ID** when in Auto Attendant.

To add a conference, specify the Conference ID and click on **Save**. This will open the Edit Entry page (see below).

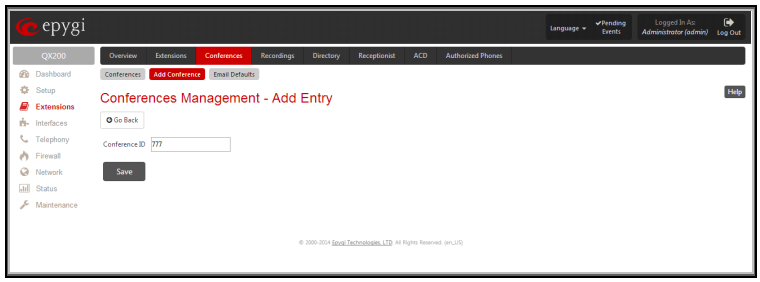


Fig.II- 76: Conferences Management – Add Entry page

Email Default Settings

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

- **Conference Notification Default Mail** - delivered when the moderator chooses the Send Notification Mail menu option.
- **Conference Activation Default Mail** - delivered by the conference Scheduling system, if the **Send Mail before Conference Activation** option is enabled.

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

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

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

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

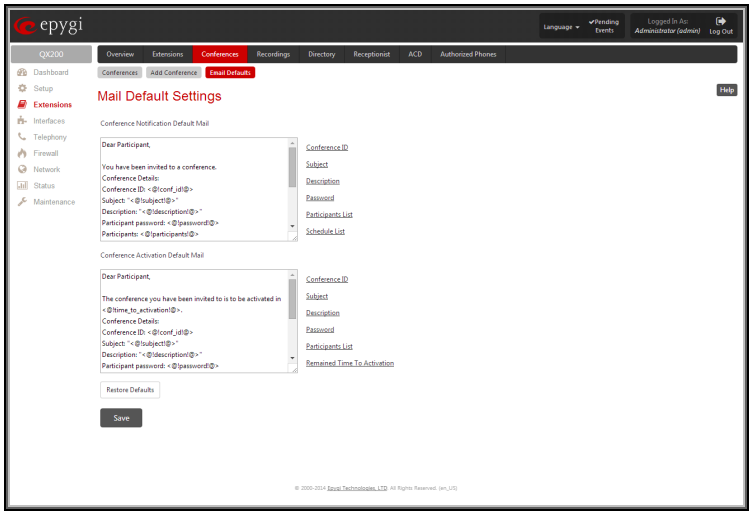


Fig.II- 77: Conferences- Mail Default Settings page

Upload Universal Extension Recordings

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

The following system messages can be uploaded from this page:

- **Hold Music** – played to the held user. The **Edit** link is used to select the way custom hold music will be provided.
- **Voice Mail Regular Greeting** – played when a caller reaches the extension's voice mailbox
- **Voice Mail Out-of-Office Greeting** – played when a caller reaches the extension's voice mailbox if the Out-of-office greeting is enabled
- **Incoming call blocking** - played when a blocked user calls the extension
- **Outgoing call blocking** – played when the extension dials a blocked destination
- **Call Queue Welcome Message** - played when a caller joins the extension's call queue
- **Call Queue Message** - played when a caller is being held in the queue

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 IP PBX.

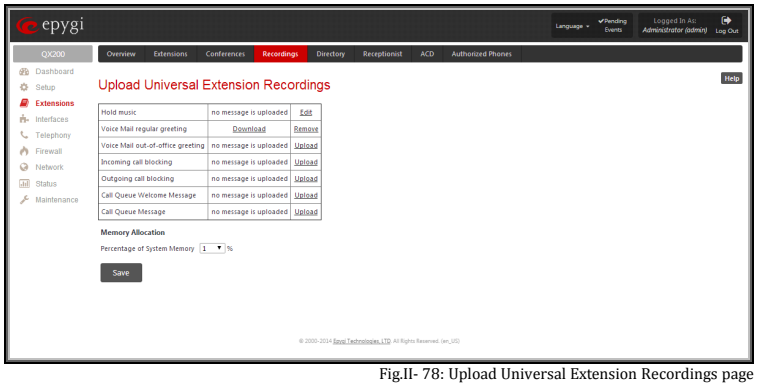


Fig.II- 78: Upload Universal Extension Recordings page

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

Upload Universal Extension Recordings - Hold music

The manipulation radio buttons on this page allows you to select the way custom hold music will be provided.

- **Default Music** enables the default music. If the option is selected, the text field **Upload Recording** will be disabled.
- **File** selection is used to upload the hold music file. The following option is available under this selection:

  Upload Recording text field can be used to type the path where hold music file is located. If hold music file is browsed with the help of file-chooser, this field displays the path of the browsed file. **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 display the warning message "Invalid audio file or format is not supported". The system will refuse uploading also if there is not enough memory available for the corresponding extension and will then announce "You do not have enough space".

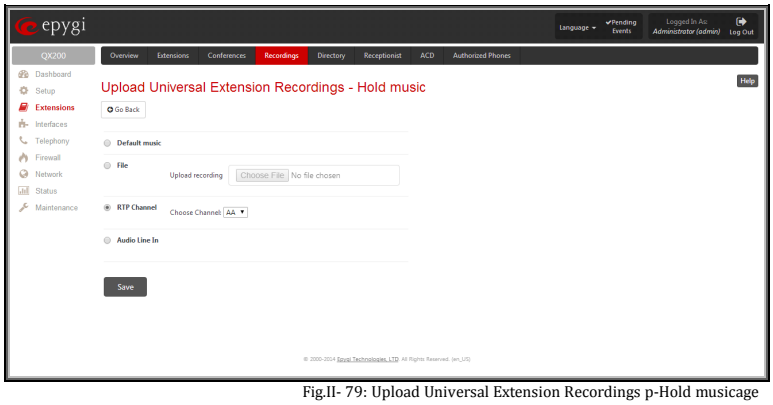


Fig.II- 79: Upload Universal Extension Recordings p-Hold musicage

  Please Note: It is recommended to use a piece of music not longer than one minute in order to leave enough space for user defined messages and voice mails.

- **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.
- **Audio Line In** (available only for QX50/QX200) selection uses the external radio broadcasting or any other audio resource as the hold music. When selecting this option, check with your system administrator if there is an external audio resource connected to the QX IP PBX.

Extensions Directory

The **Extensions Directory** is a useful tool for callers to get direct access to the QX IP PBX extensions by spelling the username with the help of the phone keypad. The Extensions Directory can be accessed through QX IP PBX Auto Attendant Services and it has its own manipulation buttons to browse the directory.

The **Extensions Directory Settings** page allows you to make a list of names assigned to the extensions on the QX IP PBX. If the name spelled by the caller matches the one(s) listed in the Extensions Directory, the corresponding extension user name(s) will be played to the caller for verifying the input and selecting the user to connect. Each extension's user should record their name with the help of the handset, or they can upload a wave file from the extension's Account Settings page (see Manual III: Extension User's Guide).

The **Custom Greeting** column in the Extensions Directory table displays whether or not a custom greeting (user's name) is recorded or uploaded. Users cannot be accessed through the Extensions Directory and it is implied as being an inactive entry in the event a custom greeting is not recorded or uploaded. Warnings will be seen in the Extensions Directory table for inactive entries. Extension numbers in the Extensions Directory table are made as a link to move to the corresponding extension's Account Settings page (see Manual III: Extension User's Guide). This helps the administrator access the extension's settings page where a custom greeting can be manually uploaded.

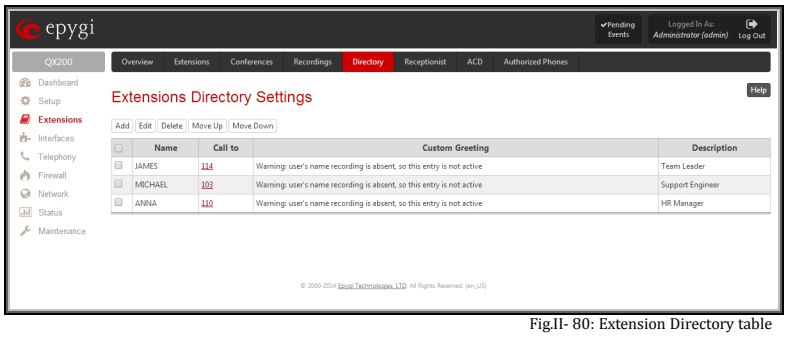


Fig.II- 80: Extension Directory table

Move Up and **Move Down** are used to move the selected record one level up or down in the Extensions Directory table. The sequence of the entries in the Extensions Directory is important if several records match the same spelled name. The Extensions Directory table is parsed from the top down and the matched entries will be played according to their position in the table.

Add opens the **Add Entry** page where a new name may be assigned to the extension. An error message appears and prevents adding a new entry to the Extensions Directory if no extensions are available in the Extensions Management table.

Fig.II- 81: Extensions Directory - Add Entry page

The **Add Entry** page offers the following components:

Name requires the name of the extension owner. Several extensions can have the same name and a single extension may have several names. User's Name is the identification parameter being searched within the Extensions Directory. You should use uppercases letters in this field, otherwise the name will automatically be changed to uppercase when saving it to the Extensions Directory table.

Call to drop down list contains all extensions on the QX IP PBX that should ring when selecting the specified Name.

Description can be used for any optional information requiring entry in the Extensions Directory.

Please Note: The entries in the Extensions Directory can automatically be deleted if the extensions assigned to the entries are removed from the Extensions Management table.

Receptionist Management

The receptionist feature on the QX IP PBX offers a variety of services to manipulate with multiple calls, to keep the calls in the queue with the perspective to be answered by the receptionist and finally to be forwarded to the corresponding destination, if needed.
The **Receptionist** service requires called extensions to use one of the following SIP Phones.

- Aastra 6730i
- Aastra 6731i
- Aastra 6735i
- Aastra 6737i
- Aastra 6739i
- Aastra 6755i (55i)
- Aastra 6757iCT (57iCT)
- Aastra 6757i (57i)
- Aastra 9133i
- Aastra 9143i (33i)
- Aastra 9480i (35i)
- Aastra 9480iCT (35iCT)
- Aastra 480i
- Aastra 480iCT
- snom 320
- snom 360
- snom 370
- snom 720
- snom 760
- snom 820
- snom 821
- snom 870
- Grandstream GXP 2000
- Grandstream GXP 2100
- Grandstream GXP 2110
- Grandstream GXP 2120
- Grandstream GXP 2124
- Grandstream GXP 2160

- Polycom SoundPoint IP 650
- Polycom SoundPoint IP 650 Pre - 3.3.0
- Polycom SoundPoint IP 670
- Polycom SoundPoint IP 670 Pre - 3.3.0
- snom 190
- snom 200
- Grandstream GXP 2200
- Yealink SIP T-26P
- Yealink SIP T-28P
- Yealink SIP T-38G
- Yealink SIP T-46G
- Alcatel Temporis IP800

The following services are available to the receptionist:

- Call Queue
- Extension Status
- Call Interception
- Voicemail Transfer
- Multi-Company Receptionist

Call Queue

This feature allows keeping multiple incoming calls in the queue when being on the line and to answer calls in the order they have been received. The usage of this service is not limited to receptionist only and can also be used by the extension user, if configured correspondingly.

The configuration of the Call Queue feature is done from the Extensions Management - Edit Entry page where the length of the call queue and the call queue appearance is defined. When the Call Queue service is enabled, the second arriving call to the receptionist/extension user will be either set into the queue (if call queue appearance is 1) or will be ringing in the background of the active call (if call waiting is enabled for the user and the call queue appearance value is greater than 1). If the call ringing in the background isn't answered, it will be transferred to the user's voice mailbox or, if no answer forwarding is enabled, it will be forwarded to the corresponding destination.

If the call is set into the queue, the caller will hear a message asking them to wait until the call will be answered. Once the receptionist or extension user terminates the call, the next call in the queue will ring to the user.

For regular FXS users, indication about the callers in the queue is through the Call Waiting service (see Manual III-Extension Users Guide). When a new caller arrives to the call queue, the phone display (if available) of the phone connected to the FXS will display the total number of callers in the queue along with the name/phone number of the last caller.

Extension Status

QX IP PBX provides the possibility of controlling and determining the actual state of the managers phones' through the receptionist's IP phone (configuration of the IP phone is done automatically by QX IP PBX through the Receptionist Phone Configuration Wizard). A programmable key on the receptionist's IP phone that is assigned to the corresponding manager will blink when an incoming call to the manager's phone is currently ringing. The key lamp will be ON when manager is on a call and will be OFF if the manager's phone is in the idle state. The extension status can be watched (viewed) by the receptionist to determine the availability of managers for incoming call transfers to them.

Call Interception

To use Call Interception service, the managers' phones watch option should be enabled and each manager should have a programmable key assigned on the receptionist's IP phone. This is performed automatically by QX IP PBX through the Receptionist Phone Configuration Wizard.

When an incoming call addressed to the certain manager comes in, the receptionist can see the corresponding programmable key blinking and the caller's ID on the phone's display. The receptionist is able to intercept the incoming call by pressing the blinking key. The caller will then be connected to the receptionist. If the receptionist does not answer the call addressed to the manager, and if the manager does not answer it either, the call will be directed to the manager's voice mailbox if it is enabled. If the manager's voice mailbox is not enabled, the call will be disconnected.

Kickback

QX IP PBX allows the receptionist to forward the incoming calls to the manager's extension and if there is no answer or if the called extension is busy on another call, the call is returned to the receptionist's phone, instead of getting into Voice Mail Service or being disconnected. To use this service, receptionist should simply transfer the incoming call to the local extension. In case of no answer or busy, the call will automatically get back to the receptionist.

Voicemail Transfer

QX IP PBX allows the receptionist or extension user to forward incoming calls directly to the voice mail of the other attached extension. To do so, an appropriate routing pattern should be added to the Call Routing table. Hence, when transferring a call to the assigned extension, incoming call will directly go to the extension's voice mailbox.

Multi-Company Receptionist

QX IP PBX provides the possibility to use a single IP phone to manage the receptionist's features for multiple companies at the same time. To do so, the incoming line appearance for the phone should be created, attached to the IP line of the IP phone and be labeled to the corresponding company name. Being busy with a call related to one company, the receptionist is able to also receive the calls related to other companies. While calls are ringing in the background, the receptionist can switch between the incoming calls. If the receptionist does not answer the incoming calls, and if the Call Queue service is enabled on the extensions, the incoming calls will be stored in the queue specific for each company line.

The **Receptionist Management** page allows you to configure IP phones to be used as a receptionist on the QX IP PBX. This page contains the list of configured receptionists with information about the attached IP lines and watched extensions.

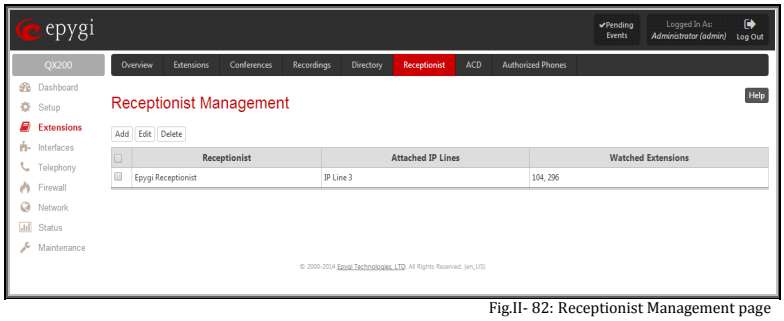


Fig.II- 82: Receptionist Management page

Add opens the **Receptionist Phone Configuration Wizard** where the new receptionist phone can be created and configured. The wizard consists of several pages.

The **Receptionist Phone Configuration Wizard – IP Phone Model** page has the following components:

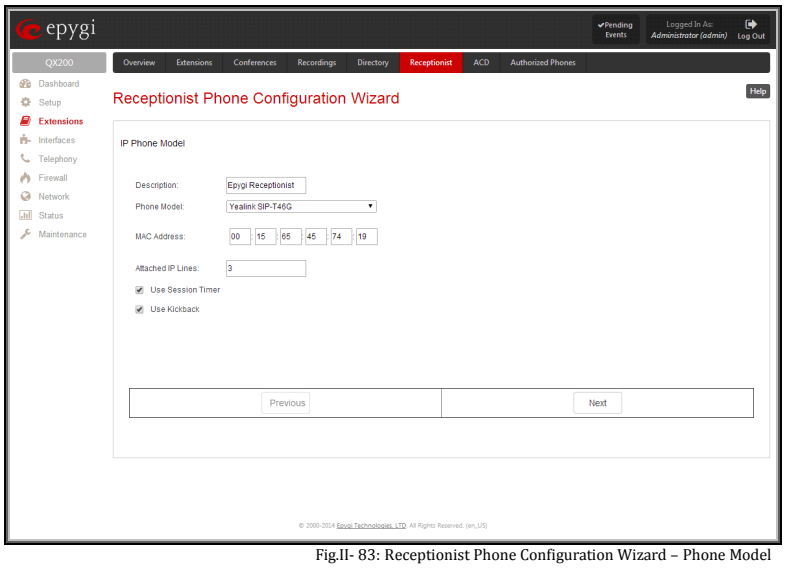


Fig.II- 83: Receptionist Phone Configuration Wizard – Phone Model

The **Description** text field requires the description of the receptionist to be configured.

The **Phone Model** drop down list is used to select the IP phone model to be used by the receptionist.

The **MAC Address** text fields require the MAC Address of the corresponding IP phone.

Based on the selected IP phone model and the inserted MAC Address, the IP phone can be automatically configured by simple reset/reboot (for more information about IP phone configuration, refer to the corresponding IP phone's users manual).

The **Attached IP Lines** text field requires the numbers of QX IP PBX's IP lines used by the receptionist. The IP lines should be separated by commas.

The **Use Session Timer** enables the SIP session timer for the IP lines specified in the **Attached IP Lines** text field. This checkbox 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 **Use Kickback** checkbox enables the kickback service on the corresponding receptionist. When this service is enabled, if receptionist transfers the incoming calls to the extension and if there is no answer or if the called extension is busy on another call, the call is returned to the receptionist's phone, instead of getting into Voice Mail Service or being disconnected. To use this service, receptionist should simply transfer the incoming call to the local extension. In case of no answer or busy, the call will automatically get back to the receptionist. When this service is not enabled, the incoming call will reach the Voice Mail Service or the call queue of the called extension, depending on the extension user's configuration.

If you have selected the snom 320/360/370/720/760/820/821/870, Grandstream GXP 2000/2100/2110/2120/2124, Yealink SIP-T28P/SIP-T26P/SIP-T38G/SIP-T46G IP phones from the **Phone Model** drop down list, the next page in the wizard will be the **Receptionist Phone Configuration Wizard – Hardware Modules**. For all other phone models, this page is skipped.
For Grandstream GXP 2000/2100/2110/2120/2124 IP phones, this page contains a single checkbox only:

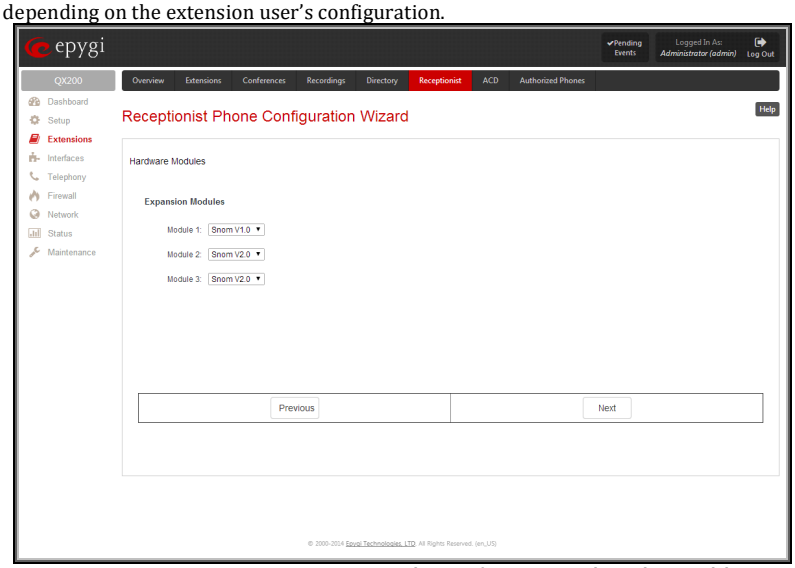


Fig.II- 84: Receptionist Phone Configuration Wizard – Hardware Modules page

The **Enable Expansion Module** checkbox is used to enable the supplementary module attached to the IP phone. The **Expansion Modules Count** drop down list allows you to select how many additional expansion modules will be connected to the IP phone. When the module is selected, the number of programmable keys on the next page of the wizard is multiplied accordingly.

For Aastra 6737i, 6739i, 6755i and 6757i IP phones, **Receptionist Phone Configuration Wizard – Hardware Modules** page contains a number of drop down lists to select the types of the expansion modules and the sequence in which they are connected to the IP phone.

The **Receptionist Phone Configuration Wizard – Programmable Keys Configuration** page is used to set the correspondence between the selected **Functions** and the available Programmable keys on the IP Phone. To do so, assign a Function to each programmable key from the drop down list on this page.

The following options are available in the **Functions** list:

- **Watch Ext. #** - watch the extension on the QX IP PBX and a possibility to pickup the call addressed to that extension.
- **Call Park Ext #** - watch the calls parked to the corresponding extensions and a possibility to retrieve the calls parked to that extension.

This list also contains a number of PBX services available on the QX IP PBX and accessible with the * key combination (see QX IP PBX's Feature Codes). When configured from this page, the key combinations become transparent for the IP phones too.

- **Vmail** – accesses the voice mailbox of the extension to which the receptionist IP line is attached to.
- **DND** – enables the Do Not Disturb service on the extension to which the receptionist IP line is attached to.
- **CallFwd** – accessed Forwarding Management of the extension to which the receptionist IP line is attached to.
- **AutoReDI** – auto redials the last dialed call.
- **CallBack** – calls back to the last caller.
- **LineInfo** – gets the IP line information from the QX IP PBX.
- **CallBlk** – blocks the last caller.
- **Record** – records the call (in case if the manual call recording is allowed for the call, configured from
- **Call Recording**– used for configuring the call recording rules
- **ACD Login/Logout** – allows the corresponding ACD agent to login to all groups it is involved in, if previously logged in, to log out from those groups. For details on ACD functionality, see ACD Management.

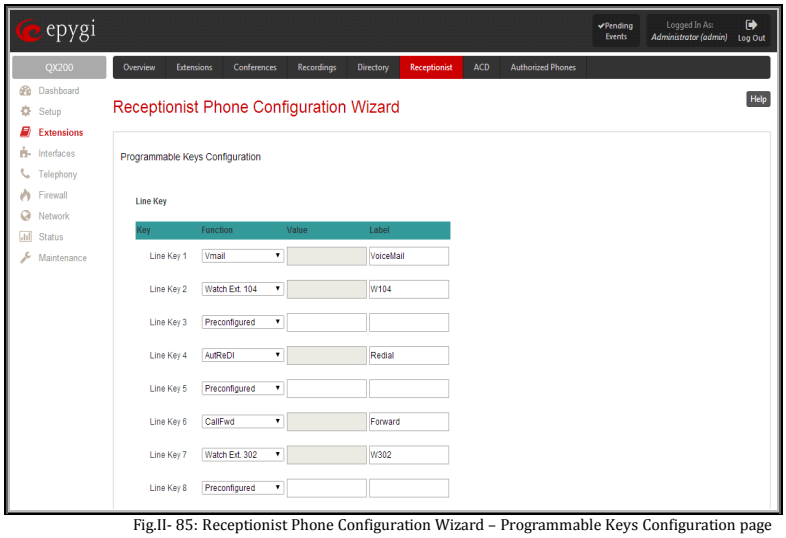


Fig.II- 85: Receptionist Phone Configuration Wizard – Programmable Keys Configuration page

Please Note: Once a new receptionist is created, the **Call Queue** feature will be automatically enabled with the corresponding **Call Queue Size** and **Max Call Queue Appearance** settings on all extensions attached to the IP lines defined in the **Attached IP Lines** text field.

The next page of the wizard is a **Receptionist Phone Configuration Wizard - Summary** where the configured settings for the receptionist should be verified. Additionally, this page contains a **Reboot IP Phone now** checkbox which should be selected if you wish to have your IP phone rebooted once the corresponding receptionist is created. Reboot is needed for a proper functionality of the IP phone. However, if you wish to reboot the IP phone later, leave this checkbox unselected.

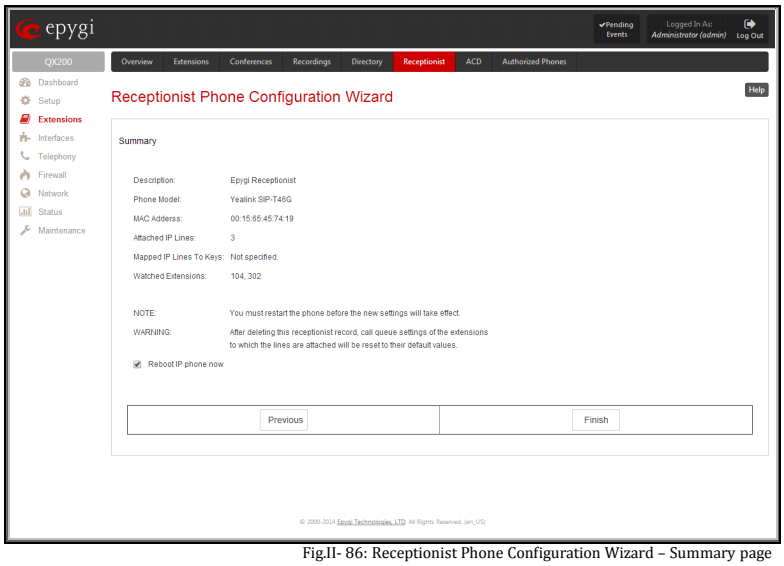


Fig.II- 86: Receptionist Phone Configuration Wizard – Summary page

ACD Management

Attention: The **Automatic Call Distribution** is an optional feature and can be activated with a feature key from the Feature Keys page.

Automatic Call Distribution (ACD) is the contact center solution designed for queuing and automatic distribution of the calls between contact center agents.

ACD concept and the contact center solution are based on the following building blocks:

- **Agent** – a call center user reachable via QX IP PBX.
- **Agent Group** (AG) – comprises the call queue, collection of agents (call center users), and call distribution mechanism between its agents.

- **Interactive Voice Response system** (IVR) – a custom Auto Attendant on QX IP PBX, answering the calls from remote callers/customers, collecting information from callers in the form of DTMF digits and, based on that, making the routing decision on delivering the call to proper Agent Group.
- **Predefined ACD Agent Auto Attendant** - used for agent login/logout and updating the current status of the agent from the phone.

To monitor ACD processes on the QX IP PBX, Epygi provides a **Statistics, Monitoring and Reporting (SMR)** application, running on MS Windows PC. SMSR doesn't require the 3PCC license (see Feature Keys section) to be installed on the QX IP PBX. It displays the current status and statistics on Agent Groups and Agents, builds the statistical reports and sends notifications and alerts to ACD supervisor/administrator. For more details and requests for this applications, contact Epygi sales division (www.epygi.com).

Agent

Agent is the call center user answering the customers' calls and reachable via QX IP PBX due to ACD. To receive the calls, agent needs to be logged into some Agent Group (AG). Agent is characterized by the agent ID, password, skills' levels and termination phone number. Agent can be logged into several agent groups at the same time and receive the calls distributed by those agent groups. For easy login/logout to all groups where the agent is subscribed, agent should use the ***83** feature code from the handset.

ACD allows the system administrator to define the set of skills adequate to call center profile and grade the professional capabilities of each agent according to each defined skill. The skill grading range starts from 0 and goes up to 10; with 0 meaning the absence of that specific skill and 10 meaning the highest level.

The termination phone number defines the phone assigned to agent. In other words, the calls on some termination number assigned to agent should be answered by that agent. The agent may have only one termination number and changing that number will result in answering the calls to that agent in different location.

Agents are being managed from **ACD Agents Table** (see ACD Group Extension Settings).

Agent Group

Agent Group (AG) is actually a QX IP PBX extension with enhanced capabilities. The type of that extension in QX IP PBX configuration is **ACD Group** (see ACD Group Extension Settings). Except for regular attributes intrinsic to extension (like extension number, SIP user name, etc.), it is characterized also by the collection of agents included into that group, call queue and the call distribution mechanism. These agent group specific parameters of extension are being configured from **ACD Group Settings** or **ACD Agents Table** accessible from ACD Group Extension Settings.

Call Queue of Agent Group

Agent Group receives the calls from customers via means existing currently on QX IP PBX. For example, it may receive the direct call through ITSP on SIP number (DID number) assigned to AG, receive a call through ACD's IVR on AG's extension number, external call through Call Routing Table on QX IP PBX, etc.

Arrived call is being added to the end of the AG queue if there are no available (online) agents to answer the call immediately. For connecting to the agents always the call at the top of the queue is being selected. The call queue settings are configured from the **ACD Group Settings** (see ACD Group Extension Settings).

Each agent can have of the following states: online, offline, away, busy or DND (Do not Disturb) (for details see **ACD Agents Table** accessible from ACD Group Extension Settings). If the same agent is logged into different agent groups, he/she may have different states in different groups except for DND status. If the agent has DND state in some group then his state will be the same for all other groups.

The state of the agent can be updated either by administrator from the **ACD Agents Table** (with the exception of "DND" and "busy" states) or by agent from the handset (except for "busy" state). The agent, for changing the state to "online", "offline", "away" from the handset needs to call the predefined Auto Attendant (see Attendant Extension Settings) and on attendant's prompt enter the agent ID, password and the status code. The state changes from "online" to "busy" or vice versa automatically when the agent starts or finishes conversation.

Calculation of Composite Skill Grade

Usually, before the call arrives to the agent group, it is first answered by ACD specific IVR. The main function of IVR is follows: via short questions to calling customer determine the set of skills required from the agent for best serving the customer. On IVR's questions, the customer answers by phone keystrokes (DTMF digits), each keystroke corresponding to some required skill. After finishing the quiz, IVR routs the call to AG along with information about the required skills set.

To calculate the agent's composite skill grade, AG sums up the grades of those skills of the agent that are included into the required skill set received from IVR. The grades of the non required skills are not considered.

The composite skill grade of AG is the sum of composite grades of the online agents of that group.

Interactive Voice Response system

ACD IVR is a custom Auto Attendant (see Attendant Extension Settings) configured on QX IP PBX with VoXML script and voice prompts designed for quizzing the customers, determining the set of required skills as described above and routing the call to the agent group having the maximum current value of the composite skill grade for required set. Since the general skill set is configured by ACD administrator and is application specific (call center specific), the VoXML script and voice prompts of IVR should be built taking into account the skill set configured by administrator.

ACD IVR is needed mainly in case if there are Agent Groups that are configured to do skills based call distribution between agents. In such circumstances the IVR is quizzing the calling customer to determine the set of required skills and when handing over the call to ACD module it passes the set of skills required by calling customer. Having that set the ACD module calculated the composite skill grade of each AG in the system and sends the call to AG having the highest value of composite skill grade. The call in AG is handled according to call distribution type configured with that AG.

For example, if the call distribution type of AG is "skills based" then AG will try to connect the call to the agent having the highest composite skill grade and if it is not answered within timeout the AG will try to connect to the next agent with the highest grade, etc. If the call distribution type is something else then AG will distribute the calls according to that distribution type don't taking into account the skill grades of the agents.

In case if the call is received on agent group bypassing ACD's IVR and the skills based call distribution is selected for that agent group, the agent group will consider the full set of skills when making decision on which agent to make a call first. In other words, since there is no required set of skills received from IVR, then the agent group will consider the full set of skills summing up all skill grades of agent.

To simplest way to build the VoXML script for IVR is using the text of the Epygi's sample VoXML script modify that and customize for your application. The IVR voice prompts should be recorded and uploaded as usual.

The **ACD Management** page consists of 3 sub-pages: **Skills**, **Agents** and **Groups**.

The **Skills** page contains a list of all available skills and their descriptions. The skills defined in this page are then used in the agent management (see above) to assign the skill level to the agents.

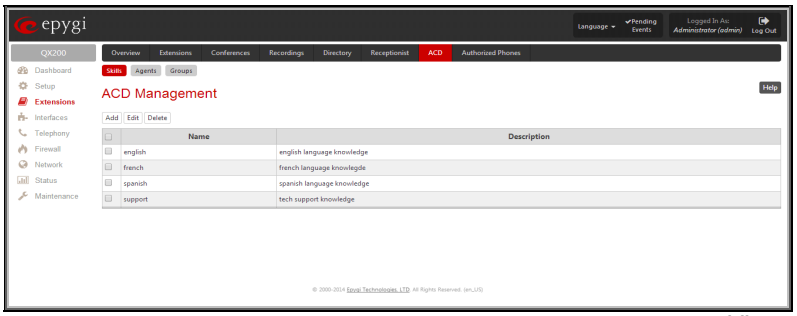


Fig.II- 87: ACD Management - Skills page

Add opens the **Add Skill** page where a new skill may be defined. The **Add Skill** page contains the **Skill** text field to define the skill name and an optional **Description** field for the description of the skill.

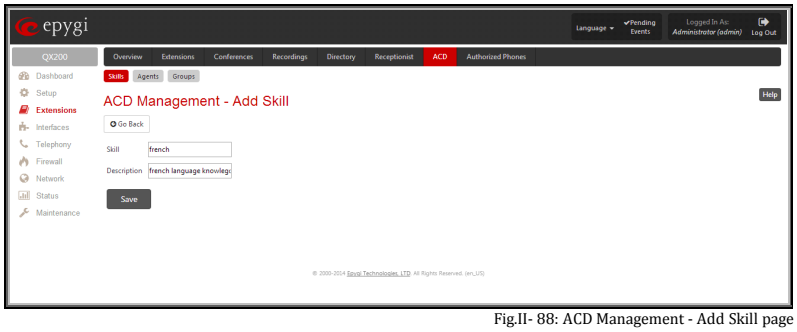


Fig.II- 88: ACD Management - Add Skill page

The **Agents** page of **ACD Management** contains a list of agents and the skill set corresponding to each agent. Every agent is characterized by an **Agent ID** which should be unique in the system. Agent IDs and passwords are used by the agents for logging into Agents Group (see description above).

Add opens the **Add Agent** page where a new agent may be created.

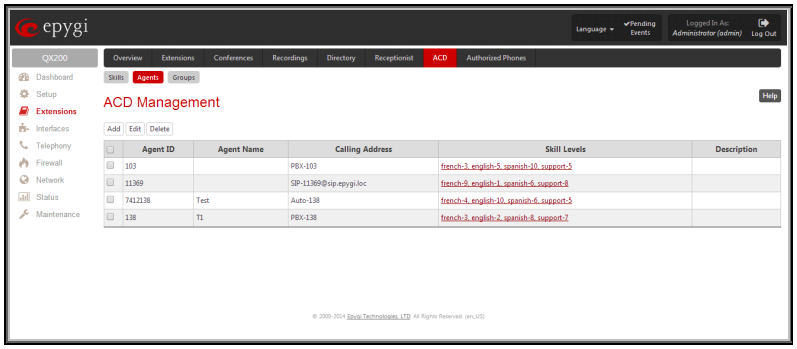


Fig.II- 89: ACD Management page-Agents page

The **Add Agent** page contains the following components:

ACD Agent ID requires the number of the agent. Digits are only accepted for this field. The Agent ID should be unique in the system.

Password requires a password of the agent. The agent password may only contain digits. If non-numeric symbols are entered, the "Incorrect Password: no symbol characters allowed" error will prevent creating the agent.

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

Description requires an optional description of the agent.

Call Type lists the available call types:

- **PBX** - extensions on the QX IP PBX
- **SIP** – calls through a SIP server
- **PSTN** – calls to a global telephone network
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

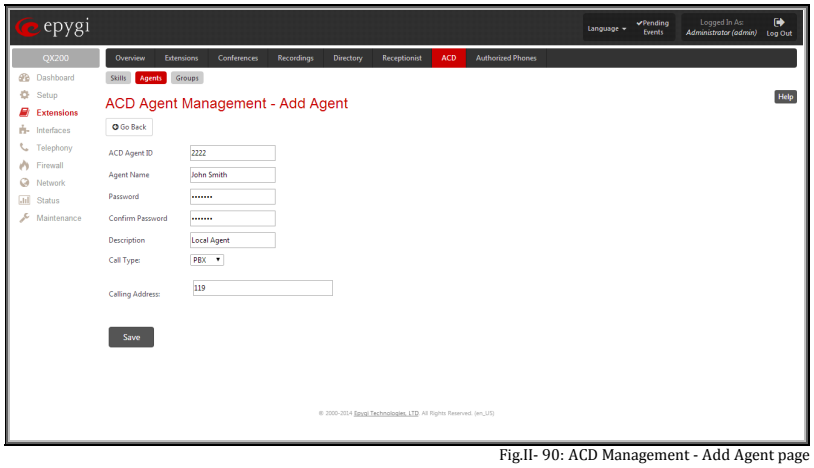


Fig.II- 90: ACD Management - Add Agent page

The **Calling Address** text field is used to define the address by which the agent can be contacted. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list.

If the **PBX** call type is selected, the **Calling Address** field should contain the extension number on QX IP PBX and the corresponding agent can be reached by calling on extension number located on the same QX IP PBX. However, it doesn't necessarily mean that the agent shall be located at that QX IP PBX – if the extension is remote extension then agent's location might be far from QX IP PBX.

For the **SIP** call type, the **Calling Address** field should contain the SIP address (see chapter Entering SIP Addresses Correctly) and the corresponding agent can be reached by calling on SIP address. The agent with that kind of termination number might be located either at the same QX IP PBX or anywhere else in the SIP network.

For the **PSTN** call type, the **Calling Address** field should contain the PSTN number and the corresponding agent can be reached by calling on PSTN number via some PSTN interface on QX IP PBX (FXO). The agent with that kind of termination number is located in the PSTN network, fixed or cellular.

For the **Auto** call type, the **Calling Address** field should contain the phone number routable through Call Routing Table on QX IP PBX. The agent with that kind of termination number might be positioned in any of the above mentioned locations.

Pressing on the **Skill Value** column of the **Agent Management** table will lead you to the **Agent - Skill Levels** page where the skill levels for the corresponding agent should be configured.

The **Agent - Skill Levels** page consists as many drop down lists as Skills created in the Skills page (see below). For each available Skill you should select the skill level (from 0 to 10, with 0 meaning the absence of that specific skill and 10 meaning the highest level) matching to the corresponding agent.

Fig.II- 91: ACD Management – Agent Skills page

The **Groups** page of **ACD Management** contains a list of ACD Group type extensions filtered from the Extensions Management table. This page allows you to configure the ACD Group specific parameters, i.e. a collection of agents included to the group, call queue and the call distribution mechanism. Any new ACD Group created in this page will automatically be displayed in the Extensions Management table.

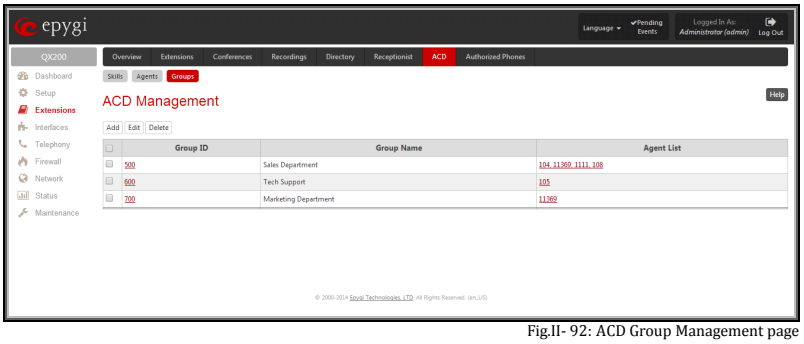


Fig.II- 92: ACD Group Management page

Add opens the **Add Group** page where a new ACD Group may be created. The **Add Group** page includes the only **ACD Group ID** text field which requires the ACD Group number (extension). The ACD Group ID should not match any existing extension in the Extensions Management table. Any newly created ACD Group will automatically appear in the Extensions Management table.

Edit opens ACD Group Extension Settings in the Extensions Management.

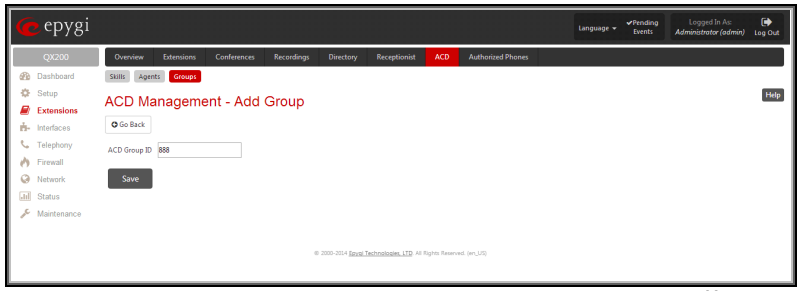


Fig.II- 93: ACD Group Management - Add Entry page

Pressing on the links in the **Group ID** and **Agents List** columns of the **Groups** table will lead you to the ACD Group Extension Settings where group settings and the list of group's agents may be adjusted correspondingly.

Authorized Phones Database

The **Authorized Phones Database** page is used to create a list of trusted external phones. If they are part of the QX IP PBX Authorized Phones database, external SIP or PSTN, then users are free to access the QX IP PBX 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 IP PBX 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.

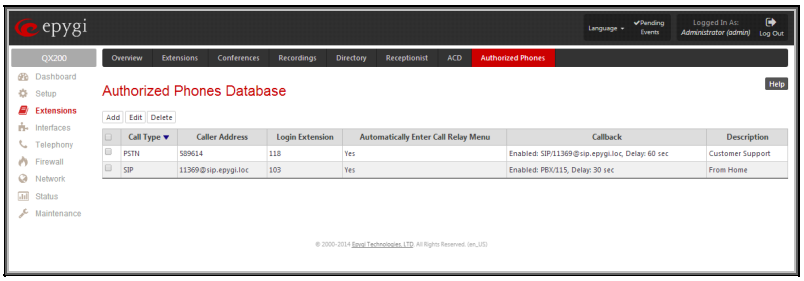


Fig.II- 94: Authorized Phones Database

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

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

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

Caller Settings

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

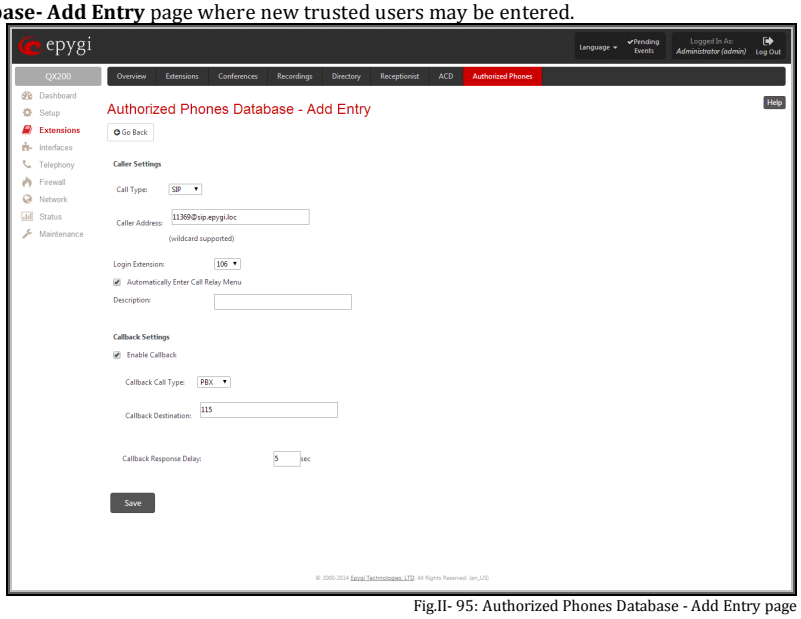


Fig.II- 95: Authorized Phones Database - Add Entry page

The **Login Extension** drop down list provides all existing extensions on the QX IP PBX. When calling the QX IP PBX 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 IP PBX system. The trusted user will directly access the QX IP PBX 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 IP PBX Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but will still be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

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

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

Callback Settings

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

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

The **Callback Destination** text field requires the destination number where QX IP PBX 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 IP PBX. QX IP PBX provides the possibility of creating a list of those trusted callers that are allowed to make free of charge calls to QX IP PBX'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 IP PBX: **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 IP PBX'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 IP PBX'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 IP PBX 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 routed to the Auto Attendant (from the FXO 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 IP PBX. Remote Call Back Configuration is divided into two modes accessible from the QX IP PBX'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 IP PBX's Auto Attendant and entering the Auto

Attendant menu, the caller can use the * 6 code (see Feature Codes) 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 IP PBX'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 IP PBX's Auto Attendant and the defined Call Back destination will receive a call from the QX IP PBX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX IP PBX'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 IP PBX. 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 IP PBX's Auto Attendant and entering the Auto Attendant menu, the caller can use * 5 menu (see Feature Codes) 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 IP PBX'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 IP PBX's Auto Attendant and the defined Call Back destination will receive a call from the QX IP PBX within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX IP PBX'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 IP PBX. There must be network connectivity and the destination must be reachable.

Interfaces Menu

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

- **IP Lines**
  - IP Line Settings
  - IP Phone Templates
  - IP Phones Logo
  - FXS Gateways
- **FXS Lines**
  - FXS (On-board) Line Settings
  - Diagnostic Loopback
- **FXO Settings**
- **E1/T1 Trunk Settings**
- **ISDN Trunk Settings**
- **External PSTN Gateways**
  - Authorization Parameters

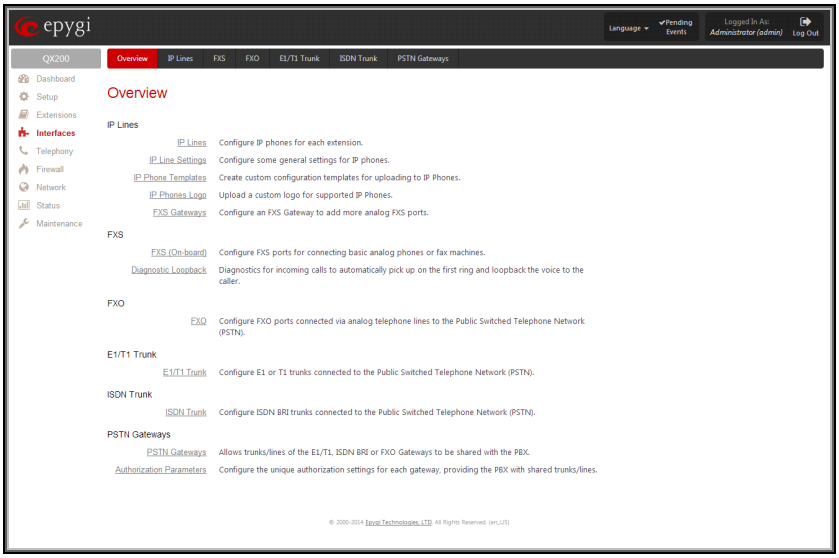


Fig.II- 96: Interfaces Menu page

IP Lines

The **IP Lines** page is used to configure IP lines for IP phones to be connected to the QX IP PBX. QX IP PBX provides the options to connect SIP phones to its LAN side, assign the corresponding IP line to an active extension, and use SIP phones as a simple phone with all telephony services of the QX IP PBX (for example, call hold, waiting, transfer, etc).

By default, 16 IP lines are available on QX50, 24 IP lines are available for QX200 and 200 IP lines are available on QX2000. The **IP Lines** page displays a table with the available IP lines on the QX IP PBX. Entering the feature key in the Feature Keys page can enable more IP lines.

The **IP Lines** table lists all available IP lines with additional information about each of them: number of the extension attached to it, information about the phone type and the configuration details.

Each column heading in the tables is 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 alternating **Hide disabled IP lines** and **Show disabled IP lines** buttons are used to respectively hide or show the IP lines that have not been activated with a feature key. To enable the lines, install a feature key from the Feature Keys page.

By pressing on the **IP line#** link in the **Available IP Lines** column, the **IP Line Settings** page specific for the current IP line is opened. This page offers a group of manipulation radio buttons that allows you to enable the IP line and to configure it to for use by the SIP phones.

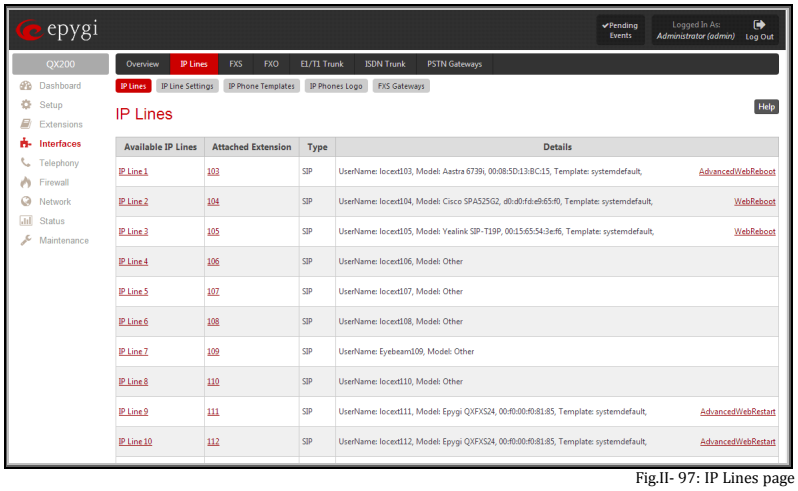


Fig.II- 97: IP Lines page

Inactive – this selection disables the corresponding IP line.

SIP Phone – this selection configures the IP line for a SIP phone to be connected to the QX IP PBX's.

- **Phone Model** drop down list is used to select the IP phone model to be used by the receptionist. The drop down list, excluding **Other** selection, enables the MAC address text fields used to insert the **MAC Address** of the corresponding SIP phone. Use **Other** selection if your SIP phone is not in this list.
- **Line Appearance** text field requires a number of simultaneous calls supported by the SIP phone.
- **Username** and **Password** are required for this selection. They should match on both the QX IP PBX and the SIP phone for a successful connection. The **Password** field is checked against its strength and you may see how strong is your inserted password right below that field.To achieve the well protected strong password minimum 8 characters of letters in upper and lower case, symbols and numbers should be used. If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.
- **Transport** drop down list is used to select the SIP protocol transport layer - UDP, TCP or TLS. For TLS you may activate the TLS certificate update mechanism from IP Phone to obtain the latest certificate generated by the QX IP PBX.

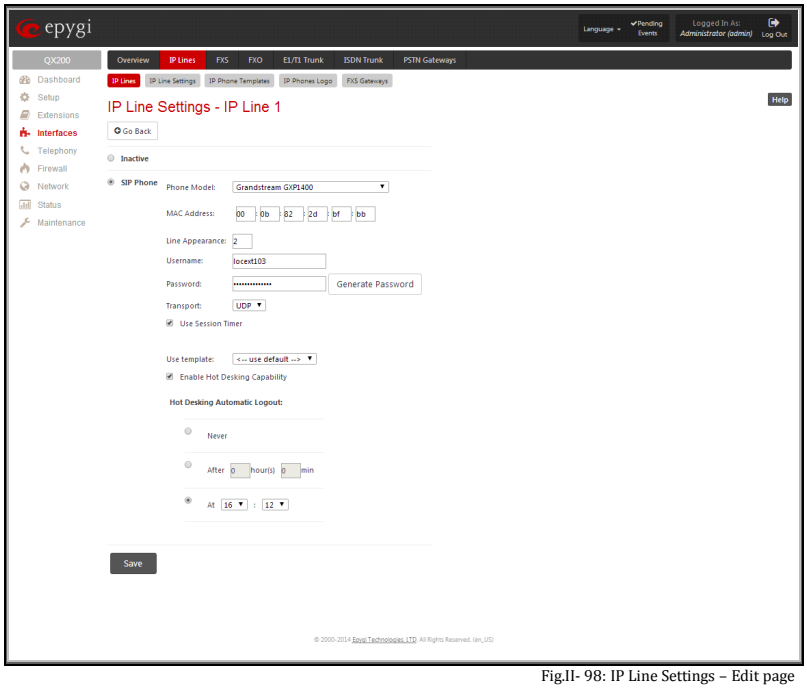


Fig.II- 98: IP Line Settings – Edit page

For automatic SIP phone configuration, the SIP phone should be reset/rebooted. The appropriate configuration will then be automatically downloaded from QX IP PBX to the SIP Phone.

Please Note: For automatic configuration, some SIP phones may require additional actions to follow the restart. For example, by default the IP Dialog SIP Tone II is in a non-auto-provisioning mode, so it should be manually enabled on the phone. Refer to the user's manual of the corresponding SIP phone for instructions on performing a factory reset or reboot on any of the supported phones, what additional configurations are required for a specific SIP phone, and how to manipulate with the GUI.

- The **Use Session Timer** enables the SIP session timer for the corresponding IP line. This checkbox 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 **Use Template** drop down list is used select a preconfigured custom template for the IP phone. When the "Use default" is selected in this drop down list, the template selected on the IP Line Settings page will be used.

- The **Enable Hot Desking Capability** checkbox is used to enable the Hot Desking feature on the corresponding IP line.
- The **Hot Desking Automatic Logout** section is used to configure Hot Desking functionality expiration on the corresponding IP line. This may be useful when someone who logged in to the public phone with the extension attached to this line forgot to log out after using it. With this option enabled, once the expiration time arrives, the extension will automatically log out from the public phone.

The following options are available:

- **Never** – the extension will never expire and will remain logged in to the public phone.
- **After the defined period of time** – requires the period after which the extension will automatically log out from the public phone.
- **At the certain moment** – requires the moment (hour and minute) when the extension will automatically log out from the public phone.

By pressing the **Web** link in the **Details** column for each configured SIP phone will lead you to the Web configuration page of the corresponding SIP phone.

Please Note: This link only works from the LAN side of the QX IP PBX, i.e. when the QX IP PBX's GUI is accessed from a PC located in the QX IP PBX's LAN. If you wish to connect the SIP phone's GUI through the WAN, an appropriate Incoming Traffic/Port Forwarding filtering rule should be added on the QX IP PBX.

The **Advanced** link in the **Details** column takes you to the Programmable Keys Configuration page where programmable keys for the corresponding IP phone can be configured.

The **Reboot** link in the **Details** column appears for supported IP phones and is used to remotely initiate a reboot of an IP phone attached to the line.

IP Line Settings

Enable PnP to IP lines checkbox is used to setup the SIP phones connected to the QX IP PBX via Plug and Play automatic configuration service. To use this service, this checkbox needs to be selected. The SIP phone should be reset then. After a clean boot-up of the SIP phone, QX IP PBX will detect the SIP phone and all its characteristics, generate the automatic configuration file and will upload it to the SIP phone. The SIP phone will be then configured on the first available IP line of the QX IP PBX and will become completely functional.

Please Note: The Plug and Play service is only available for the supported SIP phones (see the list below). This service will not work in case the SIP phone is already manually configured or if it is not reset after enabling the **Enable PnP to IP lines** checkbox.

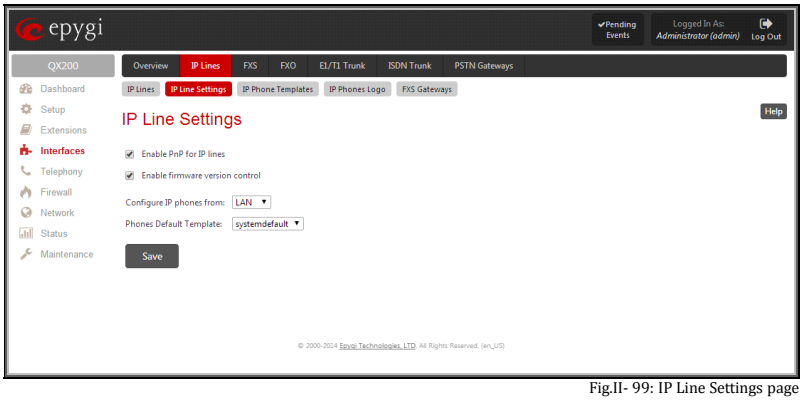


Fig.II- 99: IP Line Settings page

Enable Firmware Version Control checkbox is used to control the firmware version running on the SIP Phone attached to the QX IP PBX. This service also allows you to have the new firmware automatically downloaded and installed on your SIP Phone (in case your SIP phone was running an old firmware upon connecting to the QX IP PBX or when the QX IP PBX's firmware has been updated and the compatibility was changed to the higher firmware version of the SIP phone). Every new firmware of QX IP PBX is compatible to a certain firmware version of each supported SIP phone. If you are running older firmware on your SIP phone, this service will automatically download and install the newer firmware on your SIP phone.

Please Note: The Firmware Version Control service is only available for snom and Aastra SIP phones.

Attention: Do not select this checkbox if you wish to run other firmware version on your SIP phone than the one compatible with the QX IP PBX.

The **Configure IP phones from** drop down list is used to select the QX IP PBX's interface where the IP phones are connected. Besides LAN and WAN, this list also includes all defined VLAN interfaces.

Plesae Note: For QX2000 the **Configure IP phones from** drop down list appears only if VLAN is configured on the QX2000.

The **Phones Default Template** drop down list is used to select the QX IP PBX default template for the IP Phone which will be used if not selected otherwise on the particular line (see IP Phone Templates).

Supported SIP Phones

Below is the list of IP phones supported by QX IP PBX and officially compatible with it. The **Plug-and-Play (PnP)** and/or auto configuration feature is working for all IP phones listed below.

- Aastra 9112i
- Aastra 9133i
- Aastra 480i
- Aastra 480iCT
- Aastra 9143i(33i)
- Grandstream GXP2000
- Grandstream GXP2100
- Grandstream GXP2110
- Grandstream GXP2120
- Grandstream GXP2124
- SIPUra SPA 841
- snom 190
- snom 200
- snom 220
- snom 300

- Aastra 9480i(35i)
- Aastra 9480iCT
- Aastra 6751i
- Aastra 6753i
- Aastra 6755i
- Aastra 6757i(57i)
- Aastra 6757iCT (57iCT)
- Aastra 6730i
- Aastra 6731i
- Aastra 6735i
- Aastra 6737i
- Aastra 6739i
- Aastra MBU400
- Akuvox SP-R53P
- Alcatel Temporis IP200
- Alcatel Temporis IP600
- Alcatel Temporis IP800
- AudioCodes 310HD
- AudioCodes 320HD
- Berkshire (ATL) 5000
- CISCO 7960
- CISCO SPA525G2
- CISCO SPA303
- CISCO SPA501G
- CISCO SPA509G
- Fanvil C58/C58P
- Fanvil C62/C62P
- Fanvil F52/F52P
- Grandstream BT100
- Grandstream BT200
- Grandstream GXP1400
- Grandstream GXP1405
- Grandstream GXP1450
- Grandstream GXP2140
- Grandstream GXP2160
- Grandstream GXP2200
- Grandstream GXV3140
- Grandstream GXV3175
- Grandstream HT286
- Grandstream HT386
- IpDialog SipTone II
- Linksys SPA921
- Linksys SPA922
- Linksys SPA941
- Linksys SPA942
- Linksys SPA2002
- Linksys PAP2T
- Panasonic KX-UT136
- Panasonic KX-UT123
- Panasonic KX-TGP550T04
- Polycom SoundPoint IP 300SIP
- Polycom SoundPoint IP 330SIP*
- Polycom SoundPoint IP 331SIP*
- Polycom SoundPoint IP 335SIP*
- Polycom SoundPoint IP 450SIP*
- Polycom SoundPoint IP 501SIP
- Polycom SoundPoint IP 550SIP*
- Polycom SoundPoint IP 601SIP
- Polycom SoundPoint IP 650SIP*
- Polycom SoundStation IP 5000*
- Polycom SoundStation IP 6000*
- POLYCOM VVX 1500*
- Polycom VVX 300/310*
- Polycom VVX 400/410*
- POLYCOM KIRK wireless server 6000
- POLYCOM KIRK wireless server 300
- snom 320
- snom 360
- snom 370
- snom 710
- snom 720
- snom 760
- snom 820
- snom 821
- snom 870
- snom M3
- snom PA1
- snom m9
- snom MeetingPoint
- Swissvoice IP 10S
- Telematrix IP550 Spectrum Plus
- Telematrix IP 3300
- Telematrix IP9600 MWD5
- Thomson ST2030S
- Yealink SIP-T19P
- Yealink SIP-T20P
- Yealink SIP-T21P
- Yealink SIP-T22P
- Yealink SIP-T26P
- Yealink SIP-T28P
- Yealink SIP-T41P
- Yealink SIP-T32G
- Yealink SIP-T38G
- Yealink SIP-T42G
- Yealink SIP-T46G
- Yealink W52P
- Yealink VP-2009/VP-2009P
- Yealink VP530

Please Note: In the model's list the Polycom phones with (*) sign are also presented as **Polycom-xx-Pre-3.3.0** due to backward incompability of UCSoftware 3.1.1 configuration. It is recommended to use **Pre-3.3.0** models with Application SIP software 3.2.2.0477.

Programmable Keys Configuration

The **Programmable Keys Configuration page** is used to assign a function to the programmable keys of the IP phone. The design of this page depends on the IP phone model. However, independently on the IP phone model, this page contains a number of the **Programmable Keys** and **Functionality** drop down list assigned to each of them.

The following options are available in the **Functionality** drop down list:

- **Watch Ext. #** - watch the extension on the QX IP PBX and a possibility to pickup the call addressed to that extension.
- **Park Answer Ext #** (on the phone can be visible as PkA Ext. #, PrkA Ext. #, PrkAn Ext. # or PrkAns Ext. #) - watch the calls parked to the corresponding extensions and a possibility to retrieve the calls parked to that extension.

This list also contains a number of PBX services available on the QX IP PBX and accessible with the * key combination (see QX IP PBX's Feature Codes). When configured from this page, the key combinations become transparent for the IP phones too.

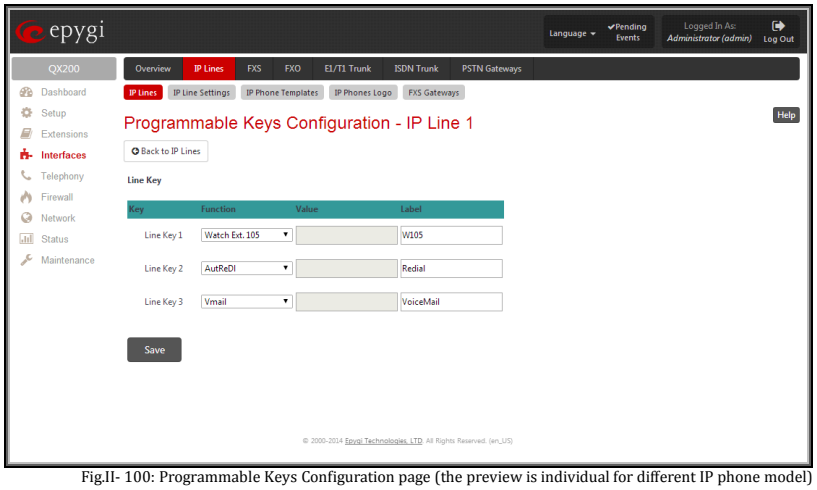


Fig.II- 100: Programmable Keys Configuration page (the preview is individual for different IP phone model)

- **Vmail** - accesses the voice mailbox of the extension to which the receptionist IP line is attached to.
- **DND** - enables the Do Not Disturb service on the extension to which the receptionist IP line is attached to.
- **CallFwd** - accessed Forwarding Management of the extension to which the receptionist IP line is attached to.
- **AutoReDI** - auto redials the last dialed call.
- **CallBack** - calls back to the last caller.
- **LineInfo** - gets the IP line information from the QX IP PBX.
- **CallBlk** - blocks the last caller.
- **Record** – records the call (in case if the manual call recording is allowed for the call, configured from Call Recording Settings).
- **ACD Login/Logout** – allows the corresponding ACD agent to login to all groups it is involved in, if previously logged in, to log out from those groups. For details on ACD functionality, see ACD Management.

Please Note: When saving changes on this page, the system asks for a confirmation to remotely reboot the IP phone. It is recommended to reboot the IP phone after configuration changes on this page in order to make the new configuration effective on the IP phone.

IP Phone Templates

The **Manage IP Phone Templates** page is used to create custom templates for the IP Phones. The templates contain a set of configuration settings that are uploaded to the IP phone once it is registered on the QX IP PBX. With the custom templates the most popular configuration settings may be adjusted accordingly. The saved custom templates can be then configured from the **Edit IP Line Settings** page to be used on the particular IP phone.

The **Manage IP Phone Templates** page consists of a table where the available IP phone templates are listed. The **systemdefault** template in this table indicates the QX IP PBX default template for all IP phones. This template cannot be edited or deleted.

Add opens the **Add Entry** page where an IP phone template can be created.

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

- **Template Name** text field indicates the name of the template. This name will be visible in the **Edit IP Line Settings** page when defining the template for the IP phone.
- **Description** text field requires optional information about the template.

Edit opens the **Manage IP Phone Templates - Edit Entry** page where the selected template's settings can be adjusted.

The **Manage IP Phone Templates - Edit Entry** page allows configuration of multiple IP phones. The IP phones templates help you manage the settings for group of IP phones, which saves your time and ensures consistency.

This page allows you to adjust the IP phone's template general settings and define options for advanced configuration of the IP phones models, which can be common for group of IP phones.

The subpages for each supported IP phone model allows you to define a set of extensions mapped to keys on IP phones (see Programmable Keys Configuration).

For **Aastra** models the **General Settings** page contains the following components:

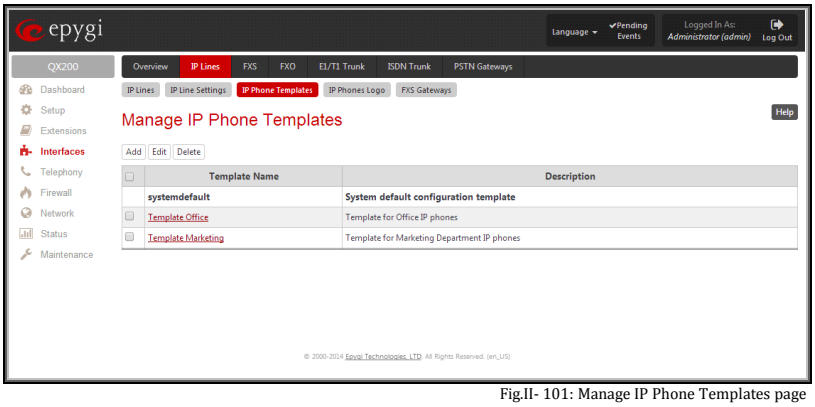


Fig.II- 101: Manage IP Phone Templates page

- **Local Dial Plan** – indicates the number and pattern of digits dialed by the user in order to reach a particular destination.
- **Send Dial Plan Terminator** – is used to switch a dial plan terminator or timeout. When the IP phone is configured to use a dial plan terminator (such as the pound sign (#)), the phone waits for 4 or 5 seconds after the handset is picked up or a key is pressed to place a call.

Play a Ring Splash - is used to switch a "call waiting tone" when there is an incoming call on the BLF (Busy Lamp Field) monitored extension. If the host tone is idle, the tone plays a "ring splash".

Fig.II- 102: Manage IP Phone Templates – Add Entry page

For **snom** models the **General Settings** page contains the following components:

- **Dial-Plan String** – indicates a dial plan string used to match dialed digits from the handset to the certain actions, e.g. dialing.

  Dialog-Info Call Pickup - is used to switch a subscription to the status information of SIP URLs mapped as "Destination/Extension" on the programmable keys.
- **Transfer on Onhook** - is used to switch the call transfer when the handset is placed on hook.
- **Call join on Xfer (2 calls)** - when this option is enabled, you will connect the newly arrived incoming call to the call on hold by pressing Xfer button. When this option is disabled and you press the Xfer button, you will have an option to choose the call on hold to transfer the newly arrived incoming call to, or to dial a new destination manually.
- **Message LED for Dialog State/Missed Calls** – when this option is enabled, the phone will indicate missed calls and changing dialog states using the message LED.
- **Dialtone during Hold** - when this option is enabled and the call is held the caller gets dial tone. Otherwise there will be no dial tone after pressing **Hold**.
- **Do not Disturb** – this selection allows you to manipulate with the IP phone DND service. When the ***72** is selected from this list, the DND service of the IP Phone and the DND service of the QX IP PBX for the corresponding extension will be activated when enabling the DND service from IP Phone. This option is recommended. When **keyeventF_DND** is selected only DND service of the phone will be activated when enabling the DND.
- **Record Missed Calls** – when this option is selected, the information about the missed calls will be displayed on the IP Phone.

Any parameters not listed above or parameters defined in this page for other IP phone models can be found in the user's manual of the corresponding IP phone.

Please Note: Save changes before moving among the configuration pages.

IP Phones Logo

The **IP Phones Logo** page is used to upload a custom logo for the IP Phones. This page contains only those IP phones for which QX IP PBX supports the custom logo upload. The uploaded custom logo will be visible on the display of the IP phone.

The **Enable** checkbox is used to enable the custom logo for the selected IP phone model(s).

The **Choose File** button opens the file-chooser to select the custom logo file.

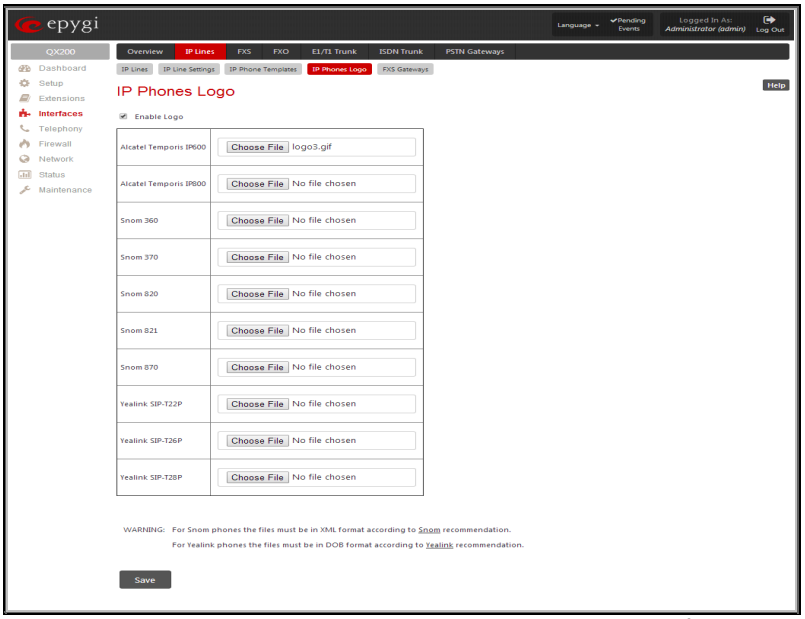


Fig.II- 103: IP Phones Logo page

FXS Gateways

The QX FXS Gateway is an analog Gateway that allows connecting analogue phones to a VoIP network. The device can be used with QX IP PBXs to emulate additional FXS ports. Both QX IP PBX and the FXS Gateway should be located in the same network. QX IP PBX is connected to the QX FXS gateway through its MAC address.

The **FXS Gateway Management** page is used to define QX FXS Gateway devices in your network that can serve as FXS expansion modules for your QX IP PBX. Additional FXS lines provided by the FXS Gateway can be connected to the IP lines on the QX IP PBX.

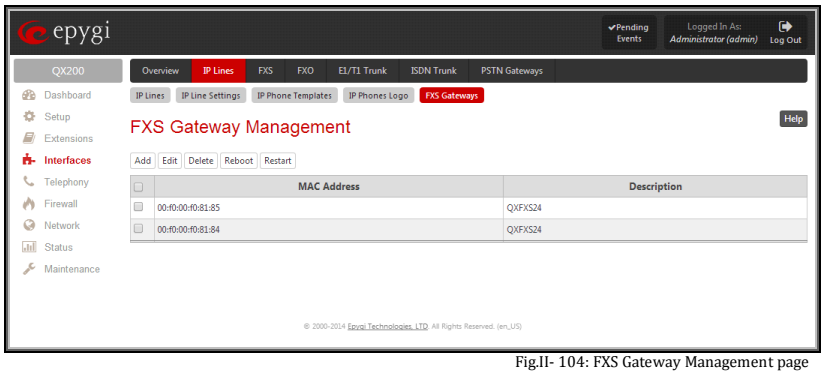


Fig.II- 104: FXS Gateway Management page

Add functional button opens **FXS Gateway Management Wizard** where new FXS Gateway should be defined.

The **FXS Gateway Configuration Wizard - FXS Gateway Model** page contains following components:

- The **FXS Gateway Model** drop down list is used to select the FXS Gateway model to be used as an FXS expansion device.
- The **MAC Address** text fields require the MAC Address of the FXS Gateway. Based on the selected FXS Gateway model and the inserted MAC Address, the FXS Gateway can be automatically configured by simple reset/reboot.
- The **Description** text field requires the description of the FXS Gateway to be configured.

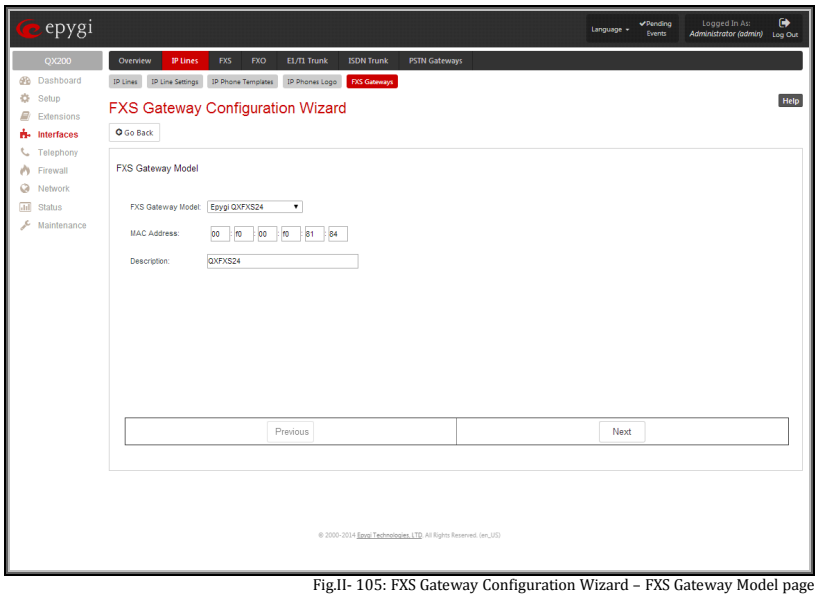


Fig.II- 105: FXS Gateway Configuration Wizard – FXS Gateway Model page

The next page of the wizard is **FXS Gateway Configuration Wizard - FXS Gateway Lines**. This page displays a list of FXS lines provided by the FXS Gateway and is used to assign each FXS line to an IP line on the QX IP PBX. System will automatically assign the provided FXS lines to the first available IP lines on the QX IP PBX. You may adjust the configuration from this page.

Please Note: The FXS lines can be assigned only to inactive IP lines on the QX IP PBX. If there are no enough free IP lines available on the QX IP PBX, you should first deactivate the IP line from the IP Line Settings page to use it in the FXS Gateway Configuration Wizard.

The next page of the wizard is **FXS Gateway Configuration Wizard - Summary** where the configured settings should be verified.

Once FXS Gateway Configuration Wizard terminates, a new entry is added to the table and the corresponding FXS Gateway's configuration gets updated according to the settings defined in the wizard, i.e. corresponding routing rules will be added to the Call Routing table of the FXS Gateway. If you need to reboot the FXS gateway, use the Reboot functional button in the **FXS Gateway Management** page.

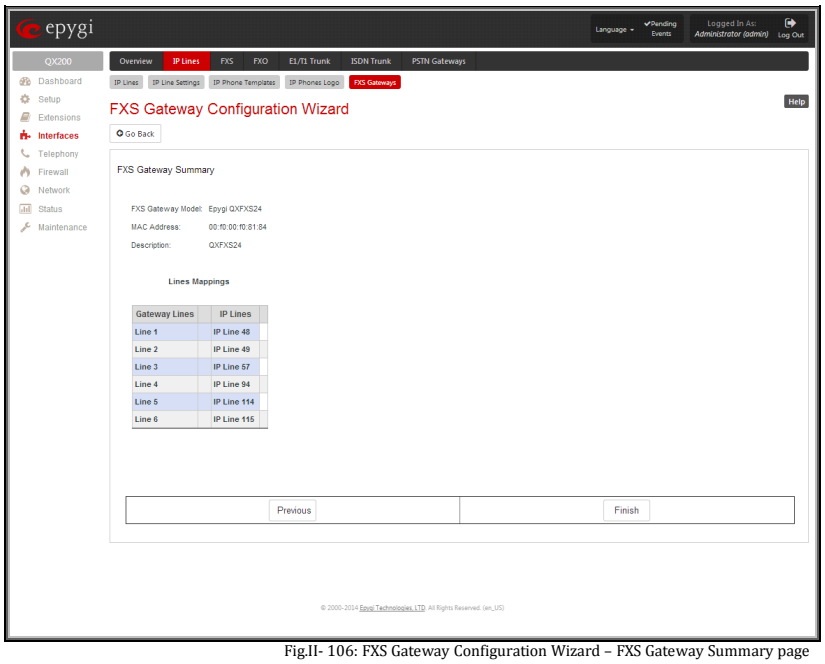


Fig.II- 106: FXS Gateway Configuration Wizard – FXS Gateway Summary page

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 IP PBX are listed 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.

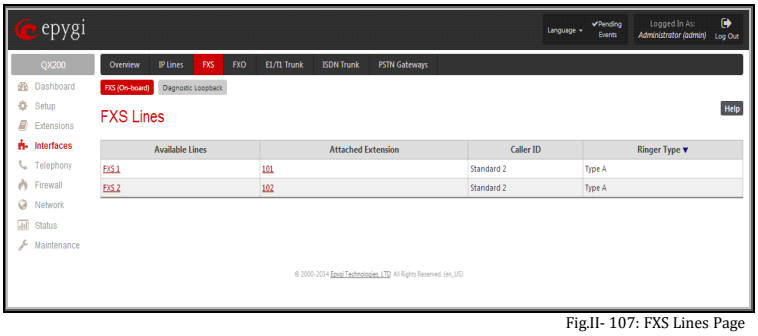


Fig.II- 107: FXS Lines Page

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:

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

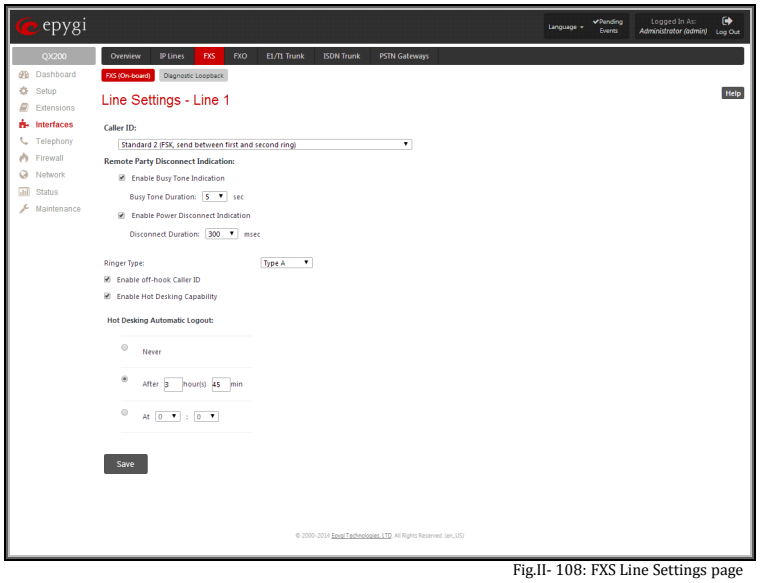


Fig.II- 108: FXS Line Settings page

A group of **Remote Party Disconnect Indication** parameters are used to configure the private PBX attached to the QX IP PBX 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.

The **Enable Hot Desking Capability** checkbox is used to enable the Hot Desking feature on the corresponding onboard analogue FXS line.

Please Note: When this option is enabled or the analogue FXS lines are attached to the corresponding extension, the caller gets dial tone. Otherwise there will be no dial tone for FXS lines.

The **Hot Desking Automatic Logout** section is used to configure Hot Desking functionality expiration on the corresponding FXS line. This may be useful when someone who logged in to the public phone with the extension attached to this line forgot to log out after using it. With this option enabled, once the expiration time arrives, the extension will automatically log out from the public phone.

The following options are available:

- **Never** – the extension will never expire and will remain logged in to the public phone.
- **After the defined period of time** – requires the period after which the extension will automatically log out from the public phone.
- **At the certain moment** – requires the moment (hour and minute) when the extension will automatically log out from the public phone.

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 IP PBX: 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 Line Settings

1. Select the line number that should to be configured from the **Active Lines** column in the **Lines** table on the **Line Settings** page.
2. Press on the line number link in the **Line Settings** table. The **Line Settings - Line#** page will appear in the browser window.
3. Use the **Caller ID** drop down list to select the caller ID detection system mode corresponding to the phone type.
4. Enable the **Dialing Prefix With Caller ID** checkbox if needed.
5. Configure the **Remote Party Disconnect Indication** parameters by selecting the corresponding checkboxes.
6. Define a **Ringer Type** from the corresponding drop down list.
7. Enable **Off-hook Caller ID** if needed.
8. 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 IP PBX when the **Loopback Timeout** expires.

The **FXS Lines Loopback Settings** page shows the only table where all FXS lines of the QX IP PBX 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 IP PBX 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).

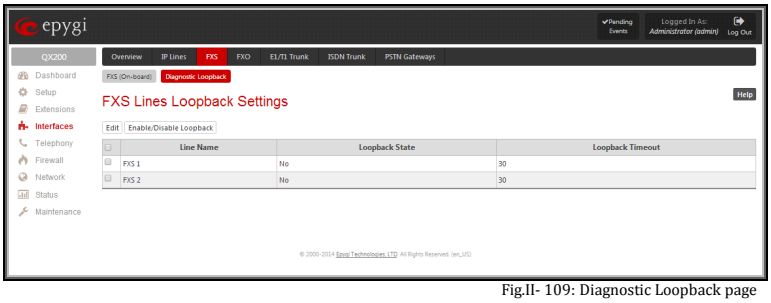


Fig.II- 109: Diagnostic Loopback page

Hot Desking

If QX IP PBX has limited number of analogue and IP phones connected and much more users wishing to make and receive calls through the QX IP PBX, some of the connected phones can be announced as public. Public phones have no static owners; they are just connected to the analogue or IP lines. Each user that accesses the public phone should first login with the previously created virtual extension and the corresponding password in order to make the phone assigned to the certain extension. From that point forward and unless the user with log off the phone, he may place and receive calls and use all the supplementary PBX services of the QX IP PBX.

The **Hot Desking** feature is used to organize the user login/logout on the public phones. Each user should have a virtual extension configured in the Extensions Management table. The virtual extensions can be configured as needed to use all the available supplementary PBX features when the user will log in from the phone with that extension. The **Hot Desking** option should be enabled on the corresponding analog or IP lines from the IP Lines or FXS Lines page accordingly.

To login to the phone, use the *78 feature code (for more details see Feature Codes chapter). You will be prompted for the extension and the password. When you login to the phone with your extension, the phone becomes a fully featured phone connected to the QX IP PBX. You may place and received calls with the SIP address configured in the Extensions Management page, use Voice Mail services, etc. When you have finished using the phone, logout with the *78 feature code. From that moment forward, your extension becomes again virtual and is not connected to any analogue or IP line but it still can handle calls (using Call Forwarding, Many Extension Ringing, Hunt Grouping, etc. services) and voice mails according to the supplementary service configured on that virtual extension. The phone becomes no more assigned to your extension and is now available for other users to login and use it.

FXO Settings

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

The number of available FXO ports is dependent on the type of your QX IP PBX. **QX50** has two FXO lines and the **QX200** has four FXO lines available. The **QX2000** has no own FXO lines, only shared FXO lines are displayed in this page

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 QX IP PBXs, 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 IP PBX "default users". If the QX IP PBX 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:

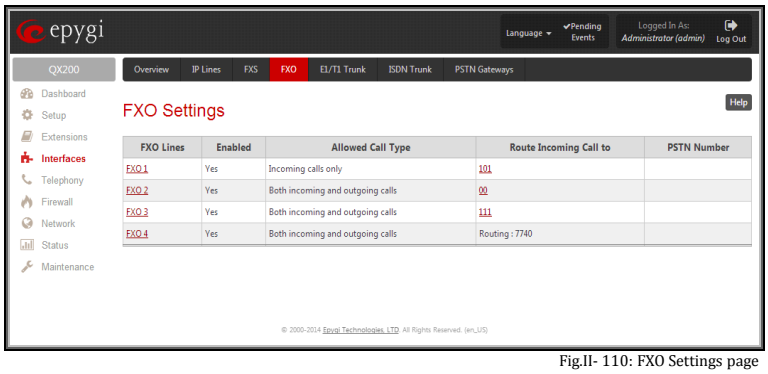


Fig.II- 110: FXO Settings page

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 incoming and outgoing calls** for the selected FXO line.

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

- **Extension** – this selection allows you to choose the local PBX user or auto attendant extension to forward calls. If an inactive extension is chosen from this list, the voice mail system will answer the call addressed to the corresponding FXO line. If the Auto Attendant extension is chosen, it will become the "default user" for the corresponding FXO line on the QX IP PBX.
- **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.

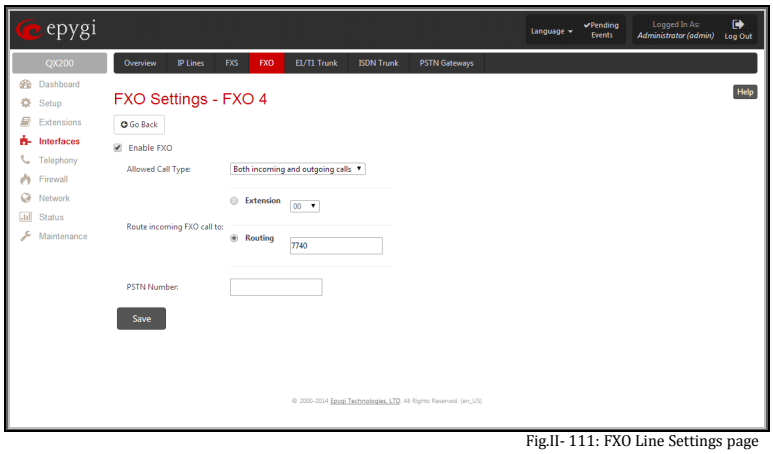


Fig.II- 111: FXO Line Settings page

By choosing a destination, the QX IP PBX administrator virtually assigns a default number that will start ringing when a call is initiated to the QX IP PBX'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 IP PBX 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 QX50/QX200/QX2000 has no own E1/T1 trunks, only shared E1/T1 trunks are displayed in this page, if available. The shared trunks/lines can be edited from this page. Any changes applied in this page will be automatically reflected on the QX E1/T1 gateway(s) that share its E1/T1 trunks.

E1/T1 service allows QXE1/T1 Gateway to be connected to a PBX or to the CO (Central Office) via E1/T1 lines, using E1/T1 CAS/CCS signaling. QXE1/T1 Gateway can be connected to act as a **User** (if connected to a CO) or as **Network** (if connected to a PBX). If a private PBX is connected to QX E1/T1 Gateway, it should be configured in network mode, if the E1/T1 line from a CO is connected to QXE1/T1 Gateway, it should be configured as a User. The **E1/T1 Trunk Settings** page is used to configure the E1/T1 trunk and the timeslots settings.

The **Trunk Settings** table lists the available E1/T1 trunks on the QX IP PBX 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.

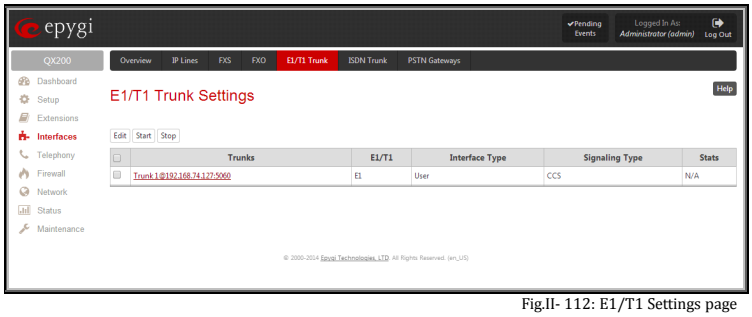


Fig.II- 112: E1/T1 Settings page

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.

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.

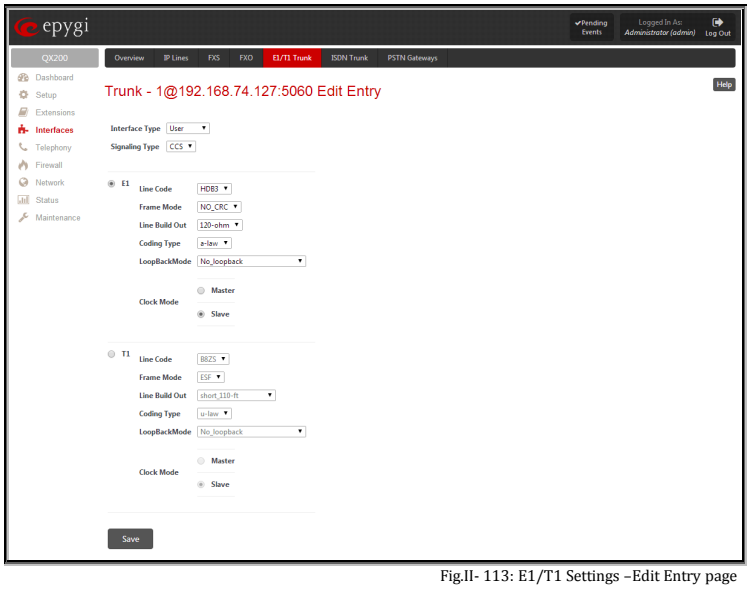


Fig.II- 113: E1/T1 Settings –Edit Entry page

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 IP PBX 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 IP PBX 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.

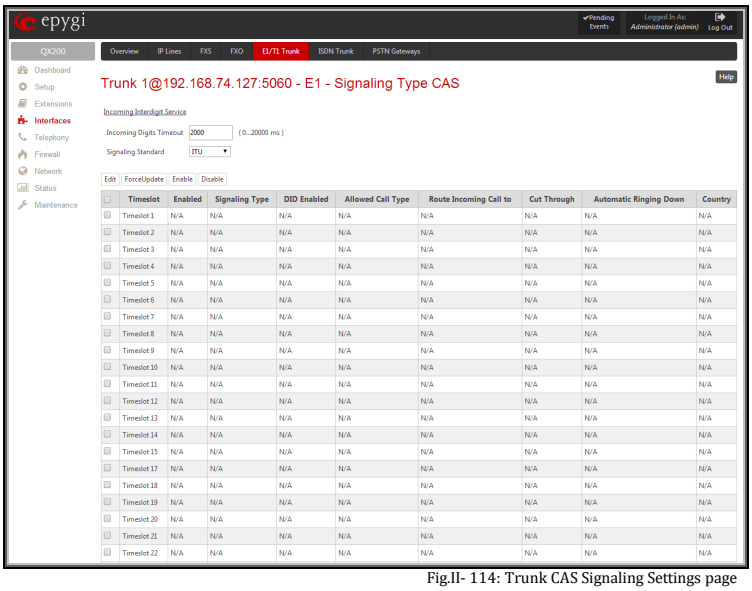


Fig.II- 114: Trunk CAS Signaling Settings page

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 IP PBX 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.

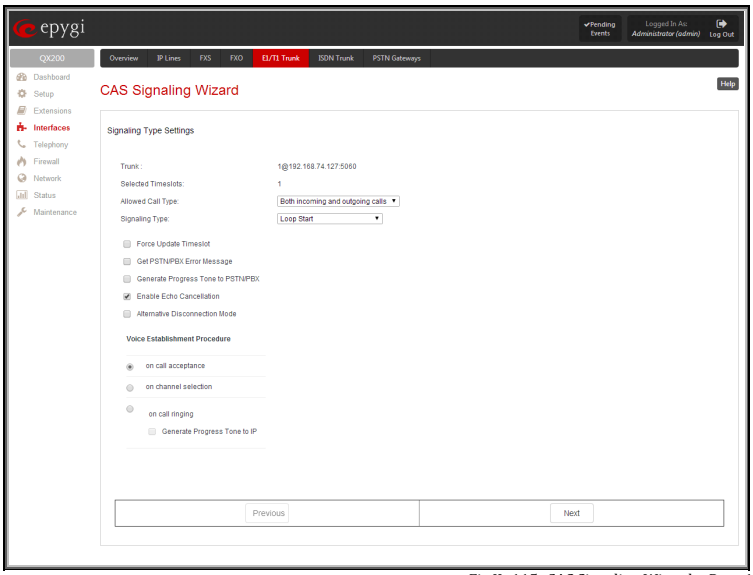


Fig.II- 115: CAS Signaling Wizard – Page 1

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).

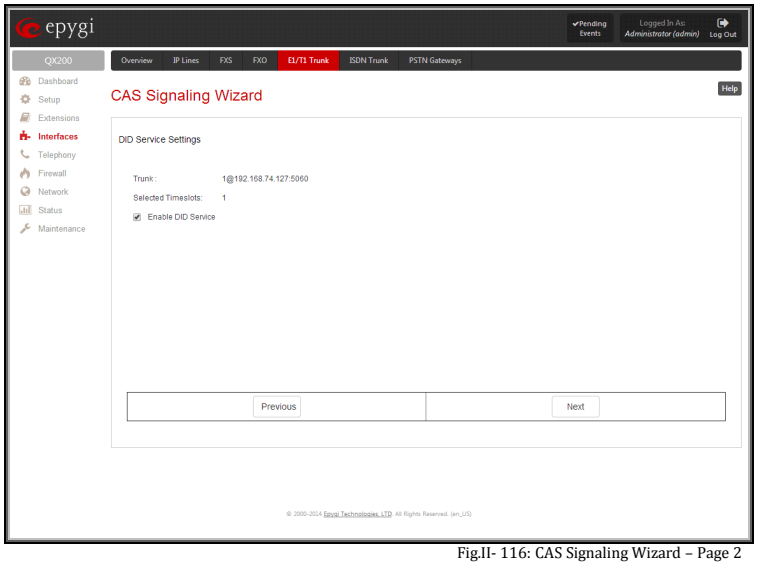


Fig.II- 116: CAS Signaling Wizard – Page 2

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.

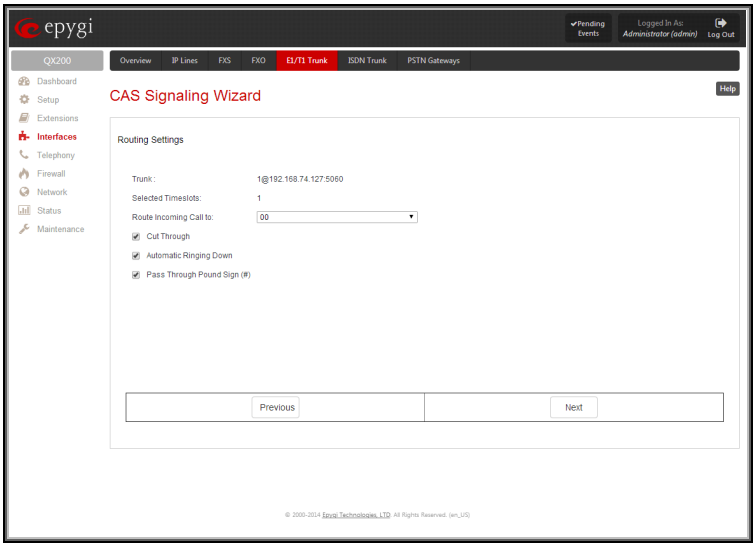


Fig.II- 117: CAS Signaling Wizard – Page 3

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 IP PBX'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.

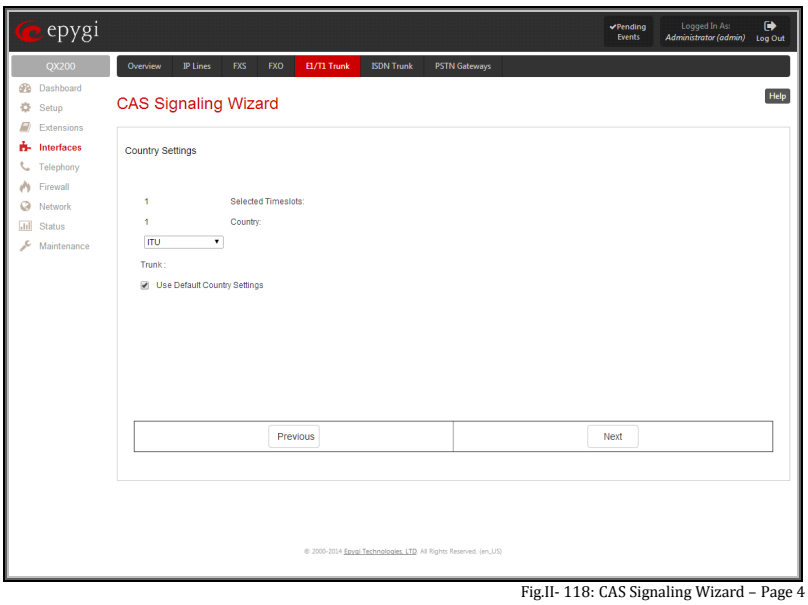


Fig.II- 118: CAS Signaling Wizard – Page 4

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.

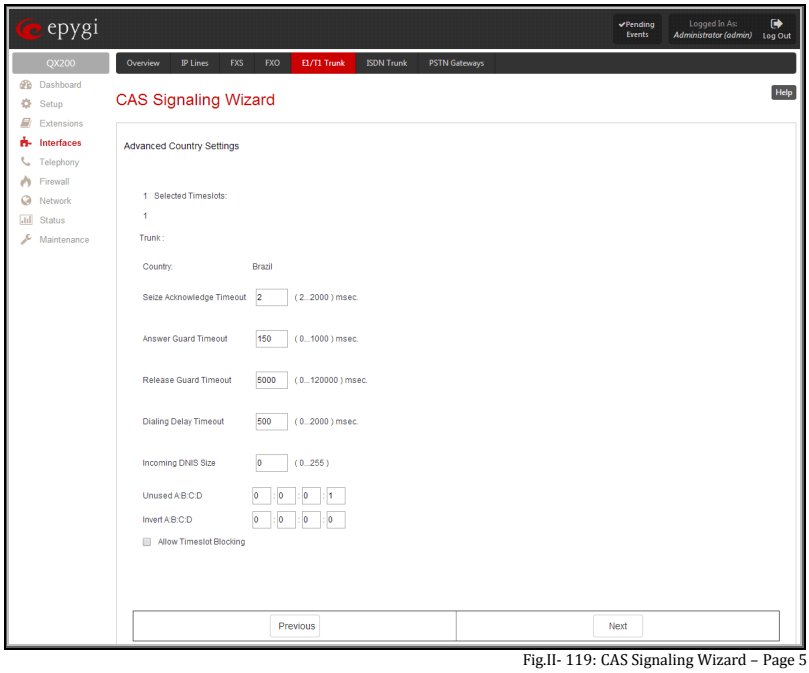


Fig.II- 119: CAS Signaling Wizard – Page 5

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.

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.

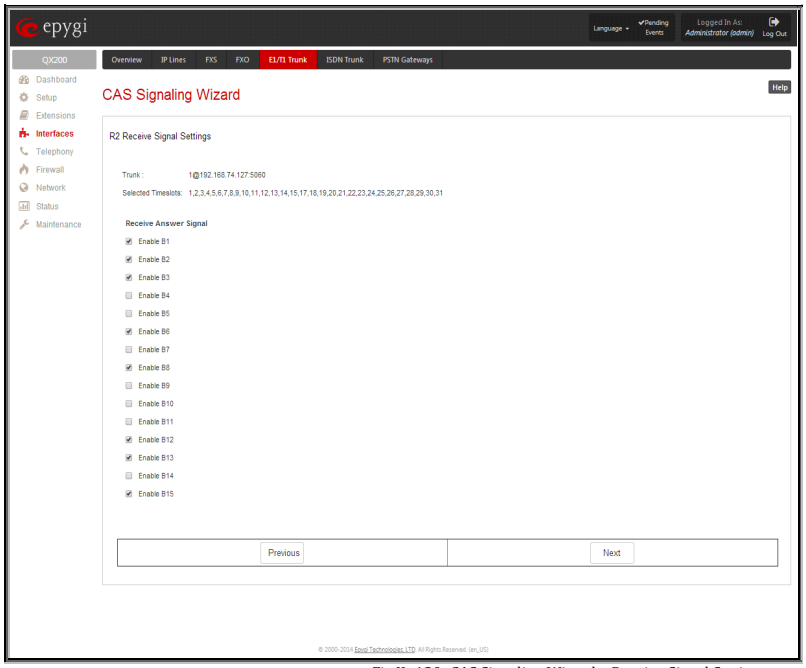


Fig.II- 120: CAS Signaling Wizard – Receive Signal Settings page

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 IP PBX will disconnect the call as soon as disconnect message has been received from the peer, otherwise, when checkbox is selected, QX IP PBX'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 IP PBX 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.

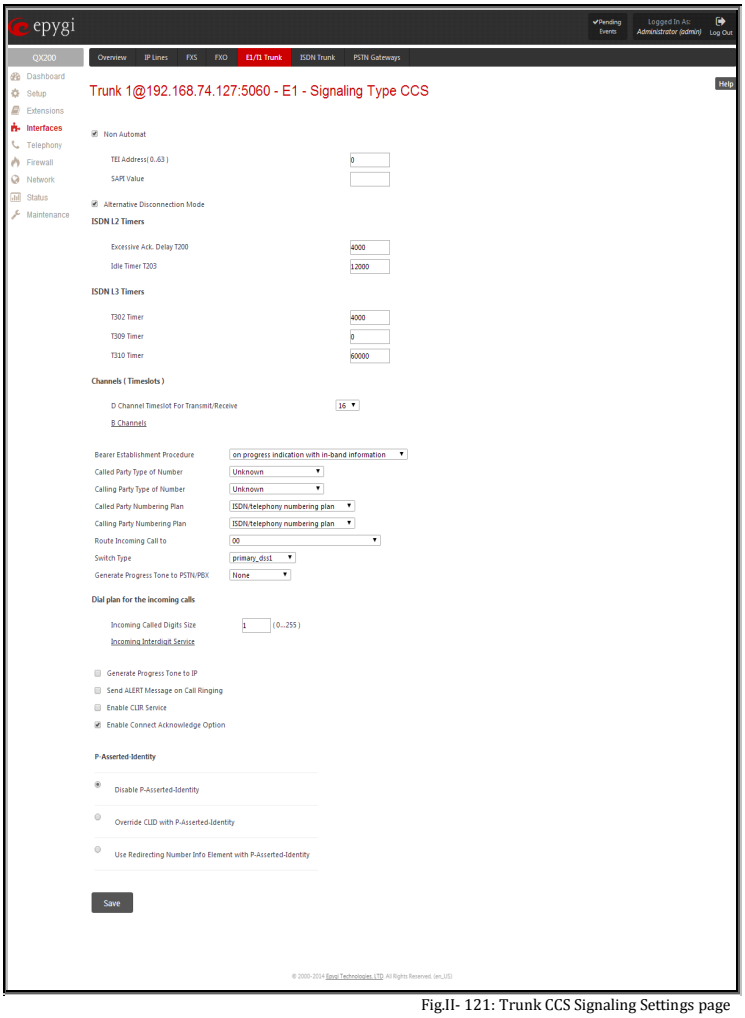


Fig.II- 121: Trunk CCS Signaling Settings page

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 No Answer Disconnect Timer text field requires the value for the No Answer Disconnect Timer (digit values from 0 to 200000) which is used in certain types of PBXs. The value 0 indicates that the timer is disabled. When time expires, QX will play a busy tone towards the PBX if the call has been disconnected by the peer.

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.

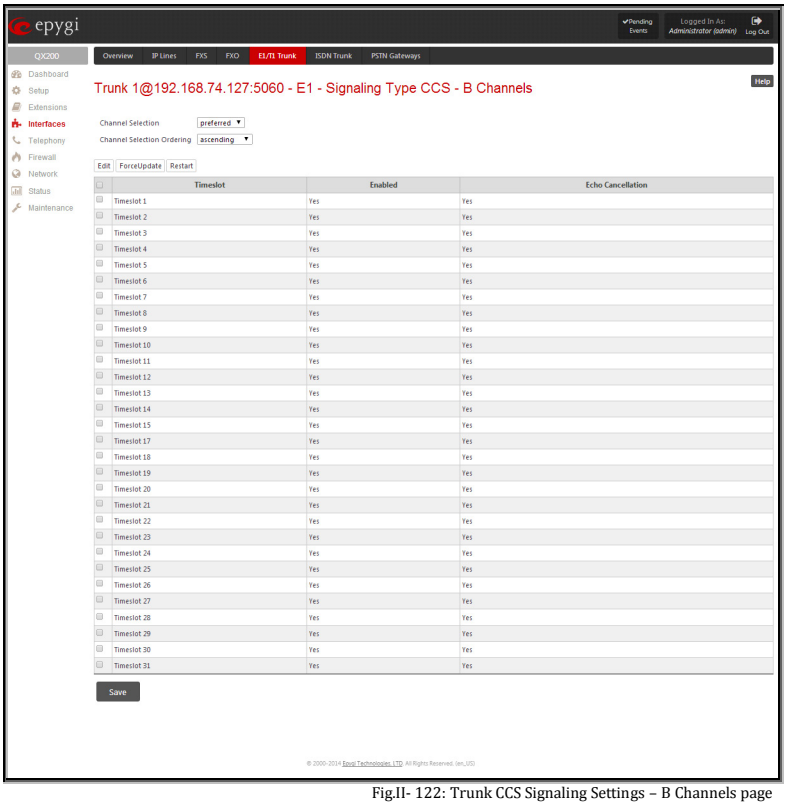


Fig.II- 122: Trunk CCS Signaling Settings – B Channels page

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).

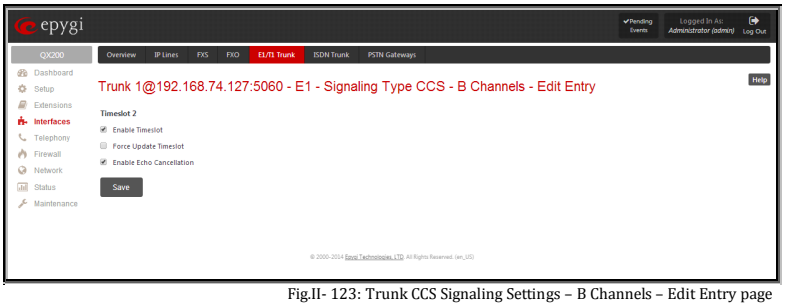


Fig.II- 123: Trunk CCS Signaling Settings – B Channels – Edit Entry page

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 IP PBX'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.

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

If the **Send ALERT Message on Call Ringing** checkbox is selected, the system will send ALERT messages to callers from the PSTN/PBX on call ringing. If not, the system will send a PROGRESS message on receiving early media from the called party if the **Generate Progress Tone to PSTN/PBX** setting is not set to **None**.

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

When the **Enable Connect Acknowledge Option** checkbox is selected, QX will stop the T303 and T310 timers upon receiving the CONNECT message, will send a CONNECT ACKNOWLEDGE message to the remote side and enter the active state. When this checkbox is not selected, QX will stop the T303 and T310 timers upon receiving the CONNECT message and will enter the active state without sending the CONNECT ACKNOWLEDGE message to the remote side.

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 Stats** are not available in shared mode.

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.

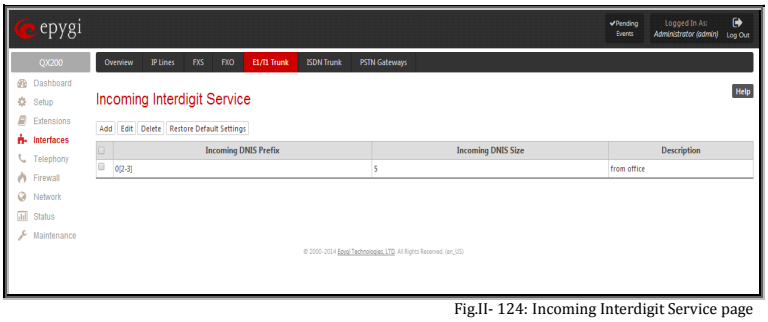


Fig.II- 124: Incoming Interdigit Service page

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.

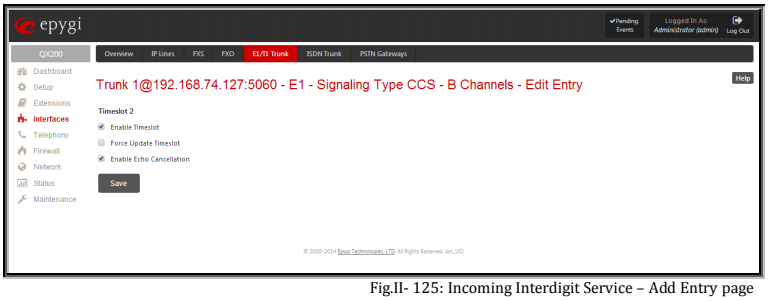


Fig.II- 125: Incoming Interdigit Service – Add Entry page

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 Trunk 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 QX ISDN Gateway act as a user or as a network. If connected to a private PBX, the QX ISDN Gateway should be configured in the network mode. If an ISDN trunk from the CO (Central Office) is connected to the QX ISDN Gateway, it should be configured as a user. QX 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 QX50/QX200/QX2000 has no own ISDN trunks, only shared ISDN trunks are displayed in this page, if available. The shared trunks/lines can be edited from this page. Any changes applied in this page will be automatically reflected on the QX ISDN gateway(s) that share its ISDN trunks.

The **ISDN Trunk Settings** page is used to configure the ISDN trunk and their signaling. This page offers the following input options:

The **Trunk Settings** table lists the available ISDN trunks on the QX ISDN Gateway(s) 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).

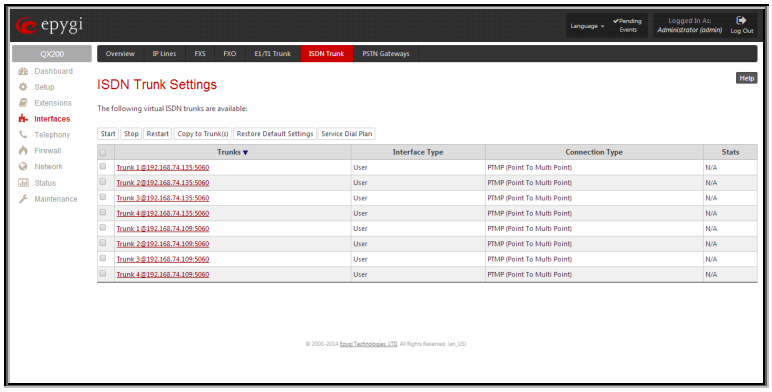


Fig.II- 126: ISDN Settings page

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 ISDN Gateway is connected to the CO then **User** interface type should be selected. If the ISDN port of the QX ISDN Gateway is connected to the PBX then **Network** interface type should be selected (in that case QX ISDN Gateway 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 IP PBX) 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 ISDN Gateway (no other ISDN devices are connected to the particular ISDN trunk from the QX ISDN Gateway).
  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.
- **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 IP PBX.
  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 ISDN Gateway except for the PBX.
  In both cases, with this selection QX sets the TEI to automatic mode.

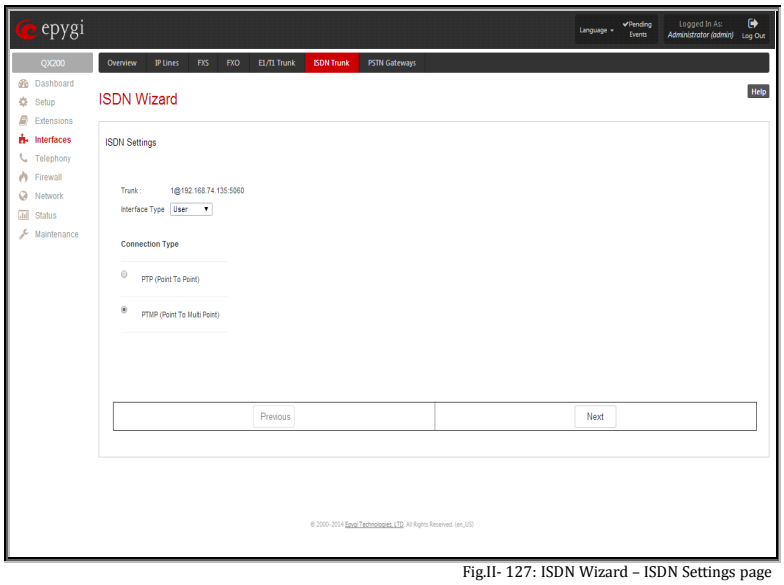


Fig.II- 127: ISDN Wizard – ISDN Settings page

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.

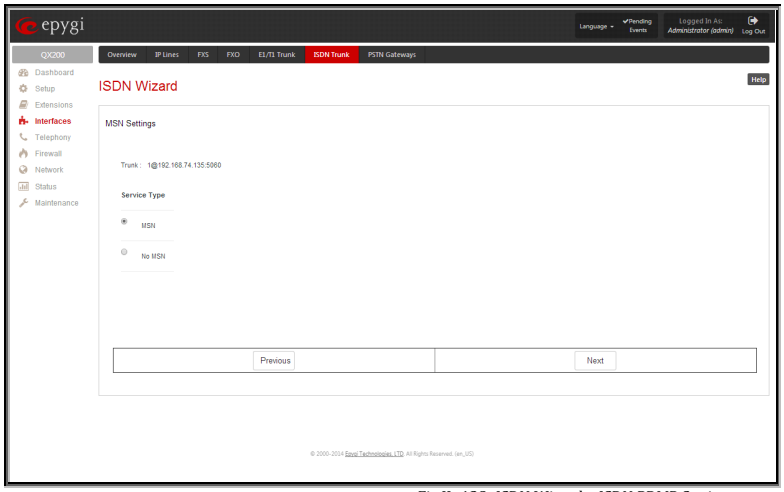


Fig.II- 128: ISDN Wizard – ISDN PRMP Settings page

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 IP PBX'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.

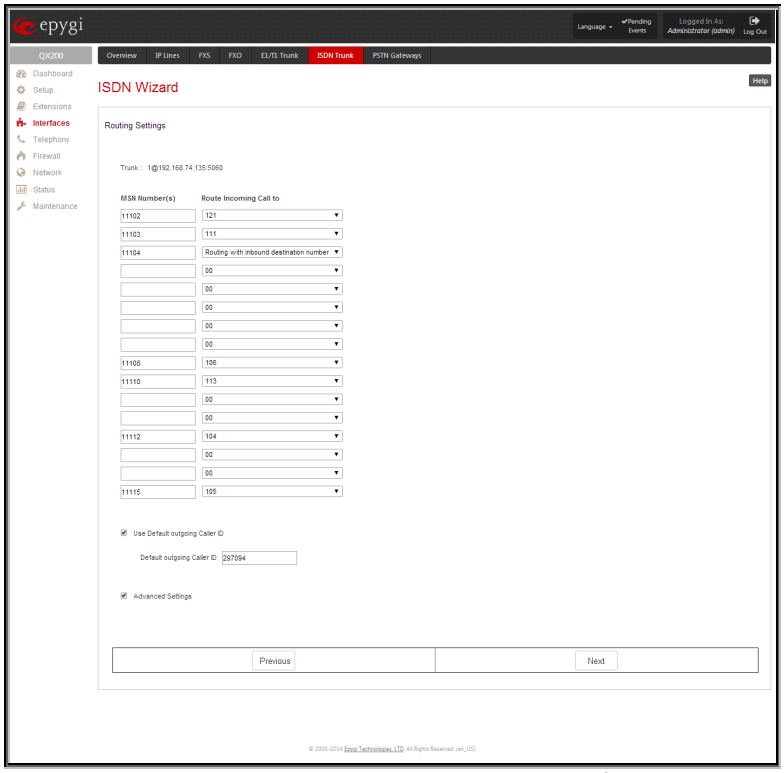


Fig.II- 129: ISDN Wizard – Routing Settings page

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- 130: 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.

The **ISDN Stats** are not available in shared mode.

External PSTN Gateways

The **External PSTN Gateways** page allows QX IP PBX to use the PSTN lines (FXO lines, E1/T1 and/or ISDN trunks) on other QX. 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 IP PBX 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 **Use PSTN lines of the other device** checkbox is used to enable QX IP PBX to use the shared PSTN lines on a remote device. This selection requires you to configure the Authorization Parameters.

Fig.II- 131: External PSTN Gateways page

Authorization Parameters

The **Authorization Parameters** page is used to create accounts for the remote QX Gateway allowing them to connect the QX and share the available PSTN lines. The table on this page lists all registered accounts and account information. It will show the corresponding authentication parameters (username and password) and date/time of the last registration.

The **Add** functional button opens an **Add Entry** page where a new account can be configured. A **Username** and a **Password** is required for a new account on this page.

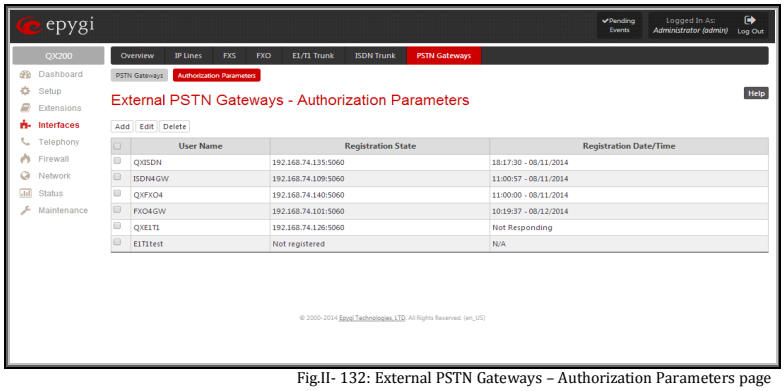


Fig.II- 132: External PSTN Gateways – Authorization Parameters page

To use the shared remote PSTN lines

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

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
  - Class of Service
- **Call Recording Settings**
- **NAT Traversal Settings**
  - General Settings
  - SIP Parameters
  - RTP Parameters
  - STUN Parameters
  - NAT Exclusion
- **RTP Settings**
- **SIP Settings**
  - SIP Aliases
  - TLS Certificates
- **Advanced Settings**
  - Voice Mail Common Settings
  - RTP Streaming Channels
  - Gain Control
  - 3PCC Settings
  - RADIUS Client Settings
  - Dial Timeout
  - Call Quality Notification

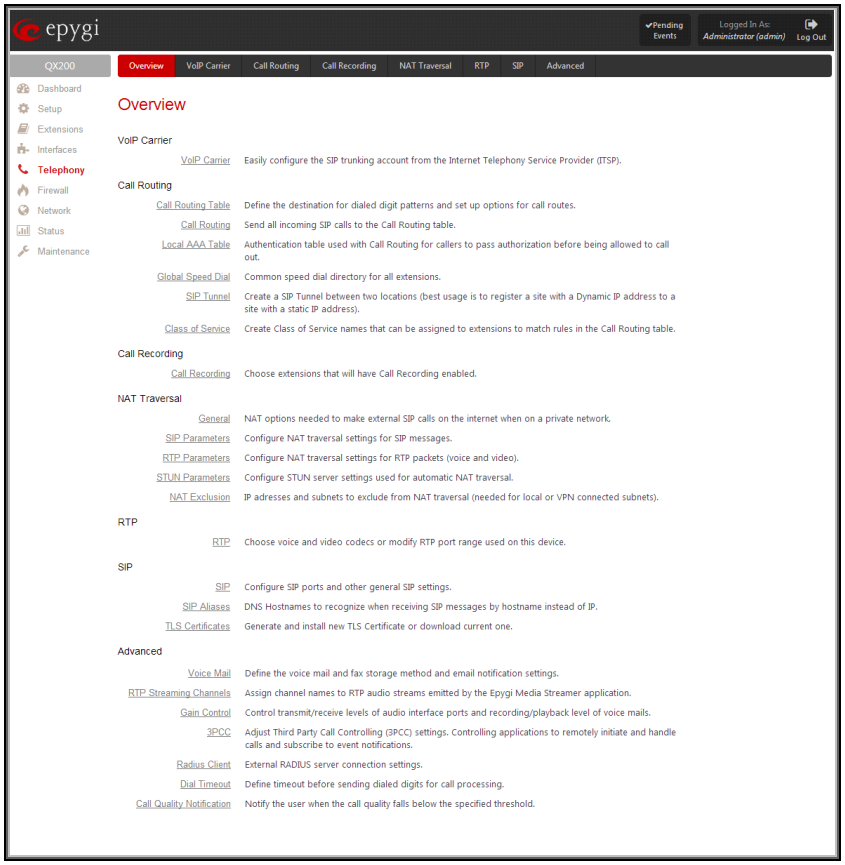


Fig.II- 133: Telephony Menu page

VoIP Carrier Wizard

The **VoIP Carrier Wizard** is used to define access codes for available VoIP Carrier accounts which will particularly allow you to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

For each configured VoIP carrier, the wizard creates a specific IP-PSTN routing rule in the Call Routing Table. 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 IP PBX'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.

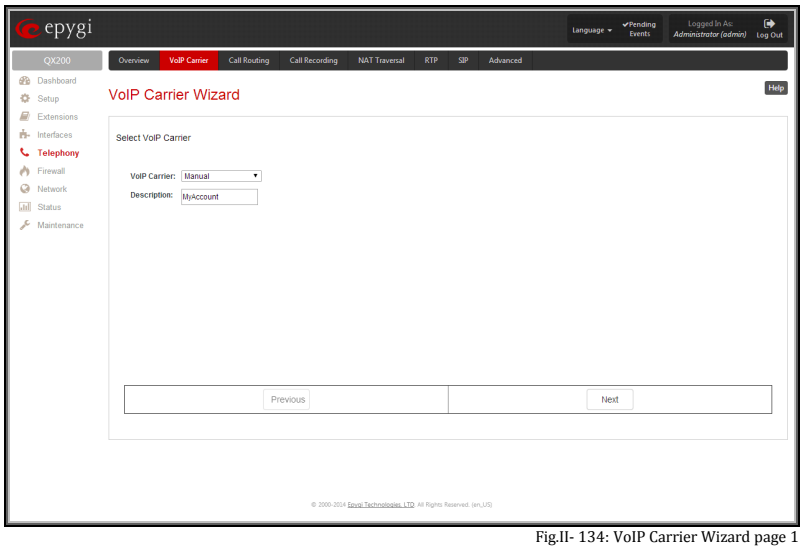


Fig.II- 134: VoIP Carrier Wizard page 1

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.

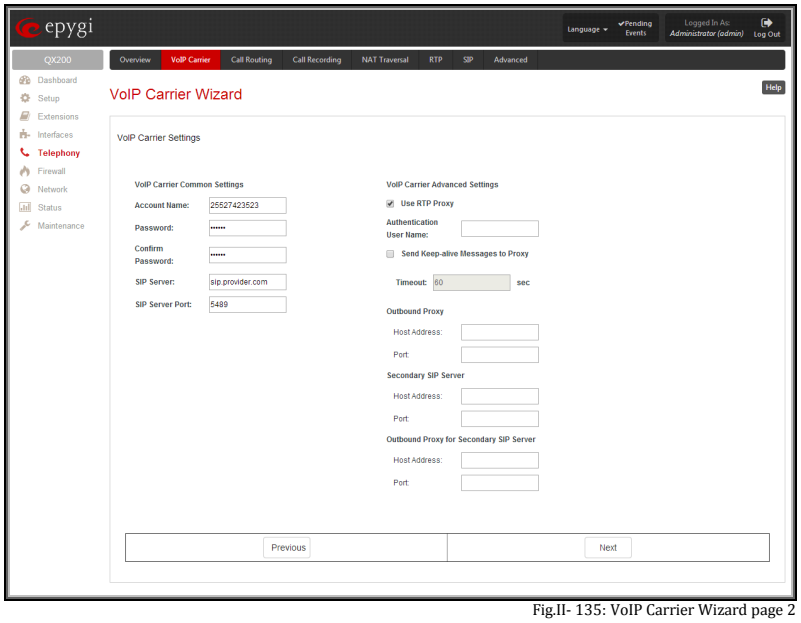


Fig.II- 135: VoIP Carrier Wizard page 2

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 IP PBX. When this checkbox is selected, the RTP streams between external users will be routed through QX IP PBX. When the checkbox is not selected, RTP packets will move directly between peers.

User Name 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 IP PBX 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 IP PBX 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.

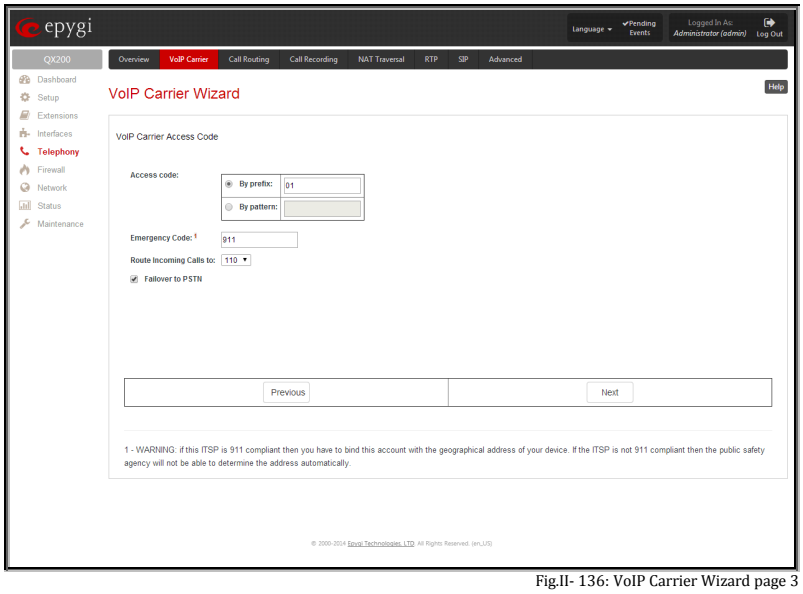


Fig.II- 136: VoIP Carrier Wizard page 3

The **Emergency Code** text field requires the emergency code supported by the specified ITSP. By default this field is filled with the information defined in the QX IP PBX's System Configuration Wizard, but this field also allows to define an ITSP specific emergency codes. In case your system has both local PSTN emergency codes and ITSP codes configured, when dialing the certain emergency code, QX IP PBX will first try to reach the local PSTN allocated emergency destination, and if failed will dial the ITSP emergency destination.

Please Note: If the defined ITSP is 911 compliant then you have to bind this account with the geographical address of your device. If the ITSP is not 911 compliant then the public safety agency will not be able to determine the address automatically.

The **Failover to PSTN** checkbox selection will route the call to the PSTN through the local FXO line in case if the VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the Call Routing Table. This maintains digit transmission to the local PSTN when an IP call towards the configured VoIP Carrier cannot be established.

Please Note: A warning message will appear when the defined **Access Code** already exists in the Call Routing Table or causes a conflict with entries already in the Call Routing table. In this case, when continuing through the VoIP Carrier Wizard, the existing entry in the Call Routing table will automatically be overwritten by the new settings.

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.

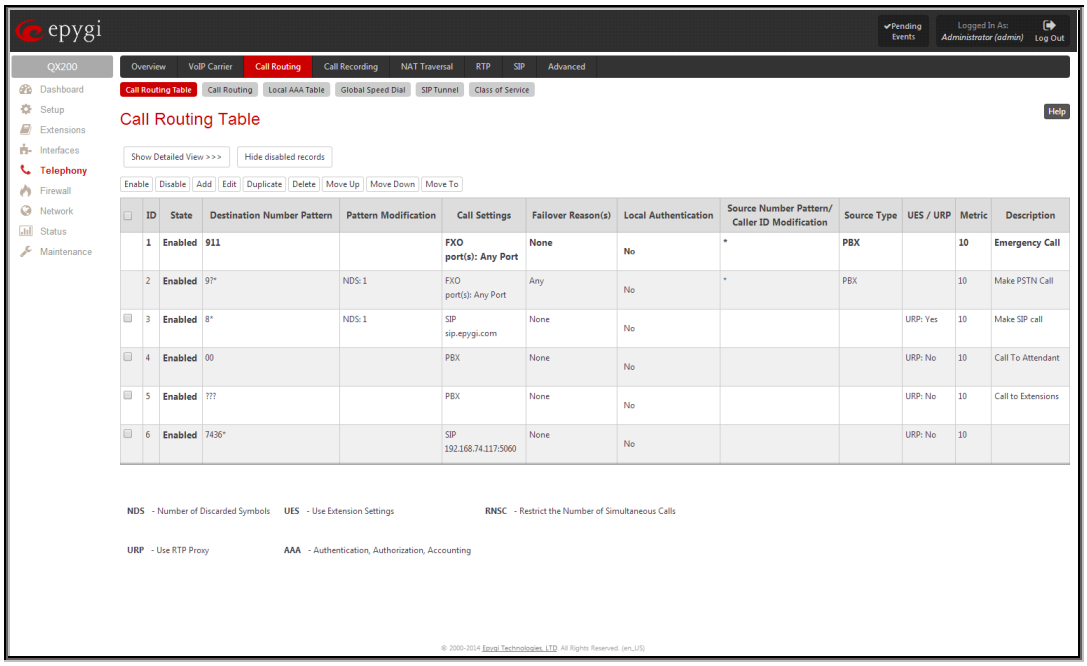


Fig.II- 137: Call Routing table – brief preview

Defining patterns in the **Call Routing Table** avoids registering QX IP PBX 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:

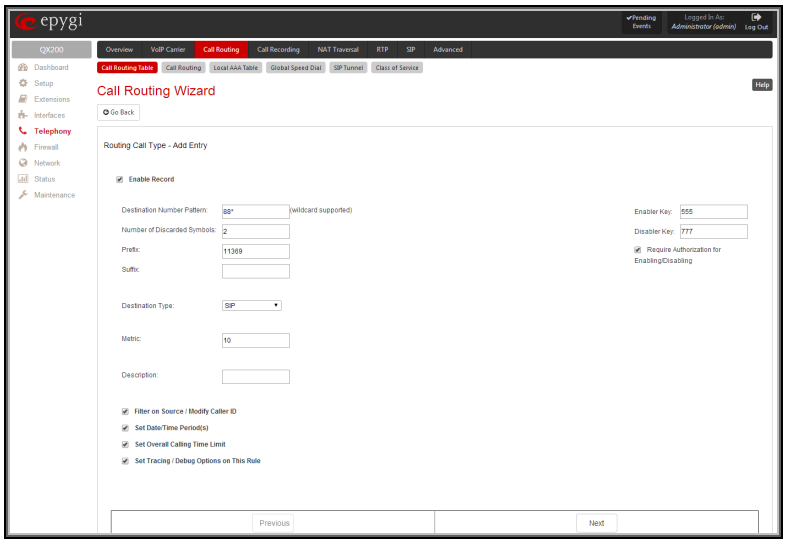


Fig.II- 138: Call Routing Wizard - page 1

- <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 IP PBX's extensions
- PBX-Voicemail **-** calls directly to the voice mailbox of the local PBX extension
- PBX-Intercom - local calls to PBX extensions with the request of Intercom service (see Manual III – Extension Users Guide)
- 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. Calls to the FXO global telephone network through shared FXO lines are also present if available.
- ISDN – calls to the PSTN global telephone network through shared ISDN trunk (this option is only present when there are shared ISDN trunks available on the QX IP PBX)
- E1/T1 – calls to the PSTN global telephone network through shared E1/T1trunk (this option is only present when there are shared E1/T1 trunks available on the QX IP PBX)

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**, **PBX-Voicemail** and **PBX-Intercom** 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 is used to enable administrator's password authentication when enabler/disabler keys are configured for the routing rule. The service can be used locally from the handset (see Feature Codes in Manual III - Extension Users Guide) or remotely from Auto Attendant (see Auto Attendant Services in Manual III - Extension Users Guide). When this checkbox is selected, administrator's password will be requested to enable/disable the certain routing rule(s). If the administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.
Enabler Key and **Disabler Key** text fields request digit combination which should be dialed from the handset or Auto Attendant to enable or disable the certain routing rules in the Call Routing Table. You can set the same Enabler/Disabler Key for multiple routing rules (the same key may be used as enabler for one routing rule, and as disabler for another one) - this will allow managing several routing rules with the single key.

The second page of the **Call Routing Wizard** offers different components depending on the **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 IP PBX.

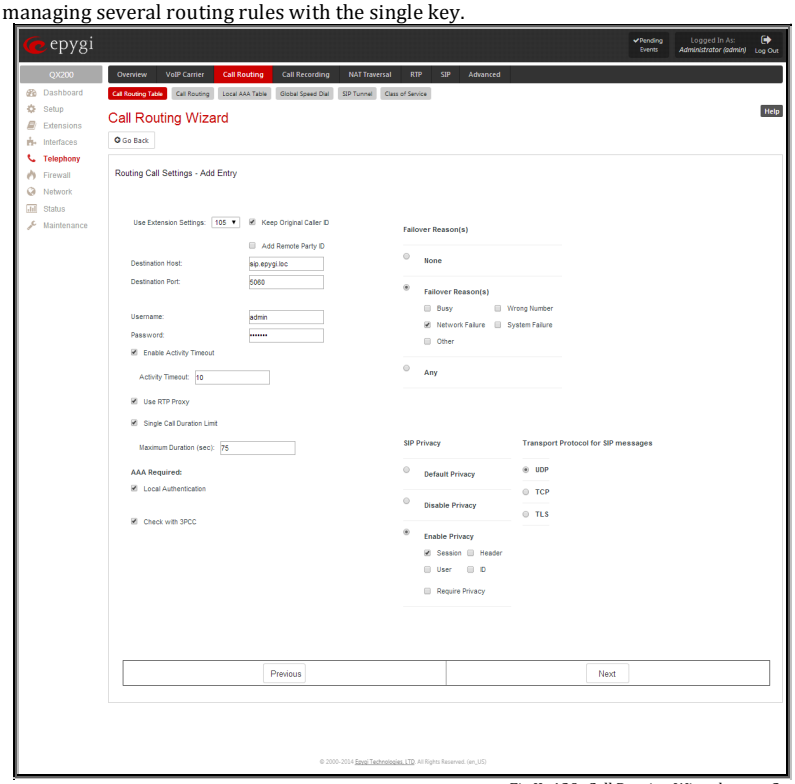


Fig.II- 139: Call Routing Wizard - page 2

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 IP PBX between peers that are both located outside the QX IP PBX. When this checkbox is selected, RTP streams between external users will be routed through QX IP PBX. 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 **Play audible signal before Intercom activation** checkbox is appeared only if **PBX Intercom** is selected as **Destination Type** (see Manual III – Extension User's Guide-Intercom Service).

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

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

- **None** - indicates that matching patterns should not be used regardless of the failover reason.
- **Failover Reason(s)** - indicates possible failure reasons. Failure reasons vary depending on the 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.

The **Custom Profile** text field is present if the **PBX-Voicemail** destination type has been selected on the first page of the Call Routing Wizard. This field requires the **Voice Mail Profile** name to activate the custom voice mail settings (see Manual III: Extension User's Guide) on the extension when the corresponding routing rule will be used.

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 IP PBX 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 IP PBX.

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**.

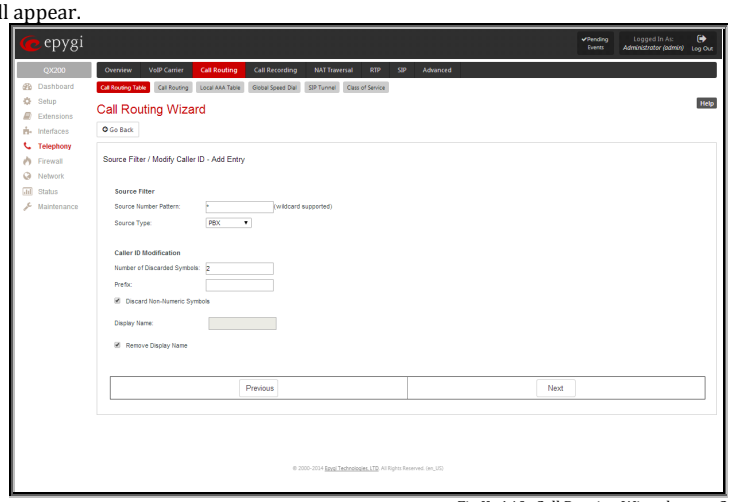


Fig.II- 140: Call Routing Wizard - page 3

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 or ISDN/E1T1 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).

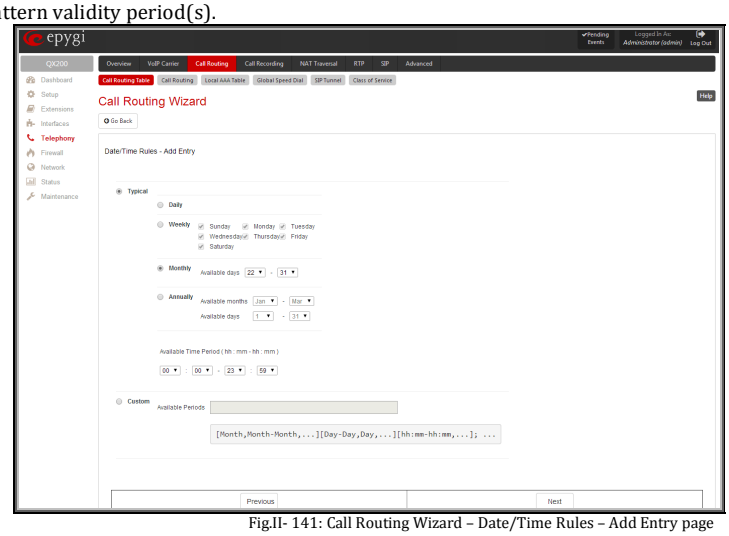


Fig.II- 141: Call Routing Wizard – Date/Time Rules – Add Entry page

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 IP PBX's 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,...]; ...

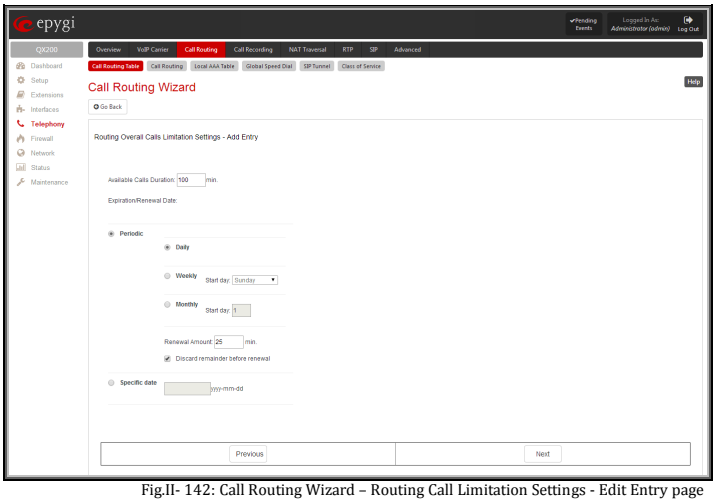


Fig.II- 142: Call Routing Wizard – Routing Call Limitation Settings - Edit Entry page

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**.

  - 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 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.

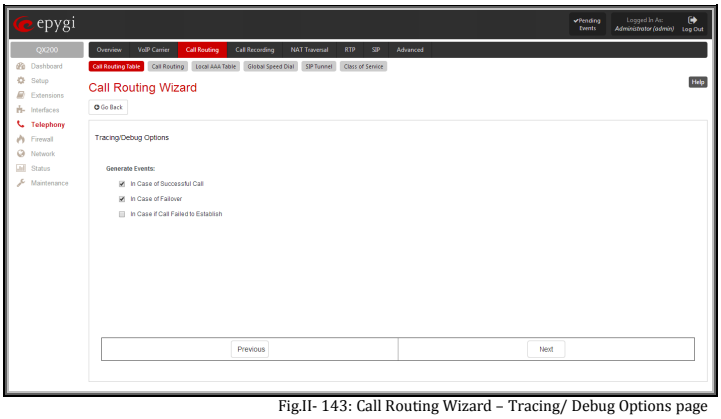


Fig.II- 143: Call Routing Wizard – Tracing/ Debug Options page

The **Call Routing Wizard - Class of Services - Edit Entry** page is used to assign the defined class of services to a certain call routing pattern. To use **Class of Service** feature for the corresponding routing rule, it should be enabled from the Class of Service page.

The **Class of Service**(CoS) functionality allows to permit or deny the attempt of extensions to use certain types of call routing rules.

Suppose you want for a certain group of PBX/Conference extensions to deny the right to make international calls, but allow them to make local and long distance calls and for another group of PBX/Conference extensions give a permission to make international calls only.

The classes defined in the Class of Service page will appear on this page to assign the corresponding routing rule to a certain class of service(s).

Please Note: The **Class of Service** feature is applicable only for **PBX** source type routing rules.

Please Note: The **Filter on Source/Modify Caller ID** option should be selected on the first page of the Call Routing Wizard to have a possibility to select the source caller type as a PBX.

Each routing rule can be attached to a several class of service(s).

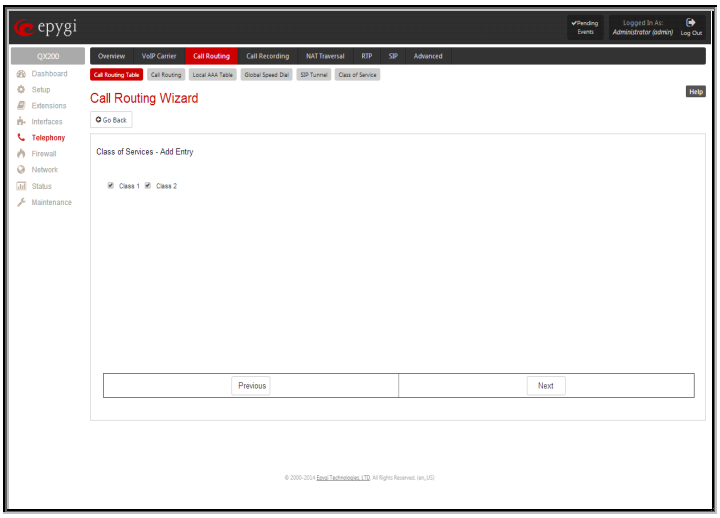


Fig.II- 144: Call Routing Wizard – Class of Services – Edit Entry page

Please Note: Established patterns based on the **Emergency Codes and PSTN Access Codes Settings** in the System Configuration Wizard will be marked in bold and will be placed in the first position in the Call Routing Table. Additionally, they cannot be modified and deleted from the Call Routing Table.

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

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

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 IP PBX 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 IP PBX 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 IP PBX will directly look for a matching routing rule in Call Routing Table and will ignore the possible matches in the Extensions Management table.

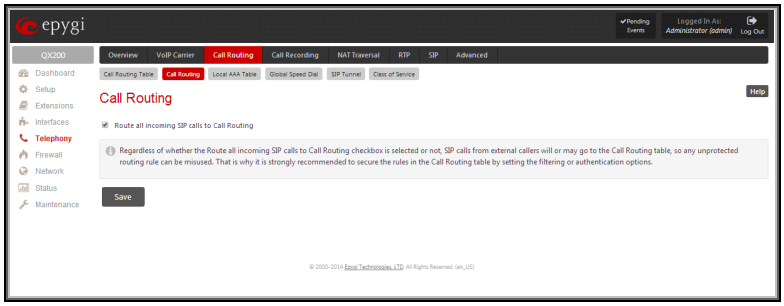


Fig.II- 145: Call Routing page

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.

Fig.II- 146: Call Routing - Local AAA Table page

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:

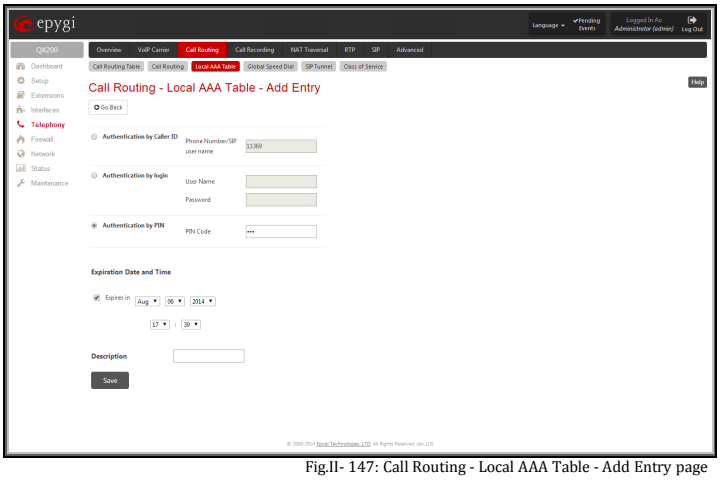


Fig.II- 147: Call Routing - Local AAA Table - Add Entry page

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller's phone number (which is considered to be automatically detected). The **Phone Number/SIP User Name** text field requires the caller's phone number or the SIP username. Only numeric and wildcard characters (see chapter Entering SIP Addresses Correctly) are allowed for this field. '[' , ']' , ',', '-', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number. The {11, 15, 23, 38, 45} pattern means that the dialed number may be 11, 15, 23, 38 or 45 to match the pattern.
- **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- 148: 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 IP PBX 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 / E1/T1 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. If the **Class of Service** feature is enabled, assign the defined classes to the selected routing rule.
26. 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 IP PBX 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 IP PBX 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 IP PBX 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] 1231 {100-150, asd, *\?}1	4 4 4
123?	3
??1	2
[1-3]???	1
12*31	4
123* {11-15}3*	3 3
*2*1	2
1 [1-3]*	1 1
*	0

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

Criterion 3

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

The list of patterns	Matching digits
1231 1[1-3]3[0-8] {100-150, asd, *\?}1	4 2 1
123?	-
??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?
??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 IP PBX. 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 **Supplementary Addresses** table that are used by **Outgoing Call Blocking** and **Hiding Caller Information Settings** services. 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 QX IP PBXs and to use that tunnel for routing the SIP calls through the remote QX IP PBXs. When this service is enabled, slave QX IP PBXs should be registered on the master QX IP PBX with the corresponding username/password. With the appropriate configuration done on the master QX IP PBX, the master device can use the slave QX IP PBXs for routing the SIP calls through them and accessing peers located behind the slave QX IP PBX or recognized by it. This enables the master QX IP PBXo to locate the slave, even when the network settings, like IP address, SIP port and other settings are changed on the slave QX IP PBX.

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 QX IP PBXs allowing to route SIP calls back and forth. A QX IP PBX 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 IP PBX can act as a master for the master device it is registered on. For example, the QX IP PBX-1 can act as a slave for the QX IP PBX-2. In its turn, the QX IP PBX-2 can act as a slave for the QX IP PBX-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 IP PBX-1 to QX IP PBX-2 and vice versa.

The **SIP Tunnel Settings** page is used to enable the QX IP PBX 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 IP PBX as a master device and allows you to configure the SIP tunnels to the slave QX IP PBXs. 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.

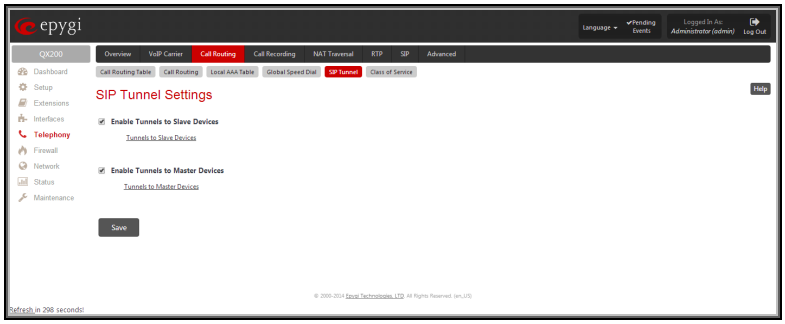


Fig.II- 149: SIP Tunnel Settings page

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:

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 IP PBX, 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_".

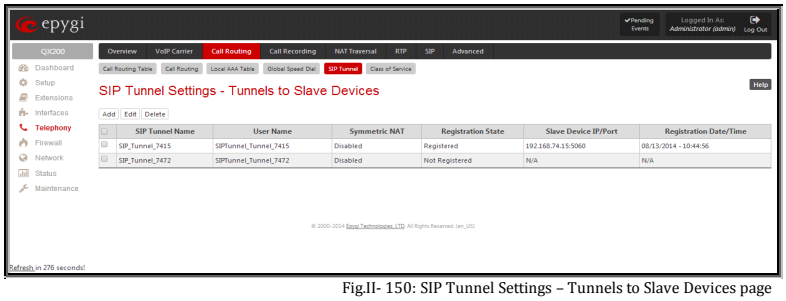


Fig.II- 150: SIP Tunnel Settings – Tunnels to Slave Devices page

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

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

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

Fig.II- 151: SIP Tunnel Settings – Tunnels to Slave Devices – Add Entry page

The **Enable Tunnels to Master Devices** checkbox enables the QX IP PBX as a slave device and allows connecting to the master QX IP PBX 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.

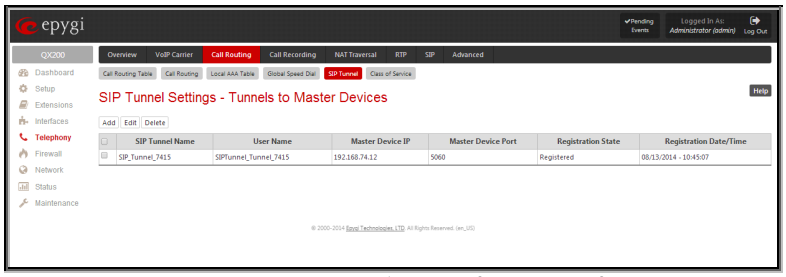


Fig.II- 152: SIP Tunnel Settings – Tunnels to Master Devices page

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 IP PBX, 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 QX IP PBXs for the successful SIP tunnel establishment.

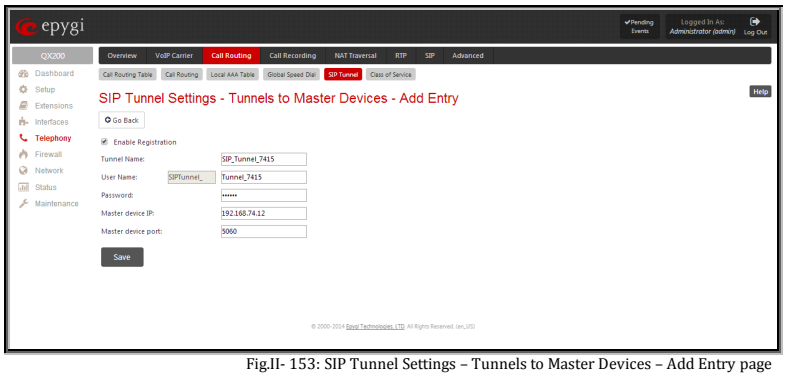


Fig.II- 153: SIP Tunnel Settings – Tunnels to Master Devices – Add Entry page

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.

Class of Service

The current implementation of **Class of Service** (CoS) on QX IP PBX is used to define the permissions that PBX and Conference extensions will have when using call routing rules to make a call.

The **Class of Service** feature provides the ability to set restrictions on the call routing rules for each extension. The **Class of Service** functionality allows to permit or deny the attempt of extensions to use certain types of call routing rules.

Suppose you want for a certain group of PBX/Conference extensions to deny the right to make international calls, but allow them to make local and long distance calls and for another group of PBX/Conference extensions give a permission to make international calls only.

Class of Service allows to specify which extensions can use which routing rules to make a call.

For example, if an extension is not assigned to a certain class of service and an attempt is made to place a call from that extension using routing rule with the Class of Service enabled, then "**Number dialed does not exist**" message will be played to the caller.

The permissions for a group of PBX extensions can be changed easily by modifying the CoS variable for each PBX extension.

On QX IP PBX the defined CoS variables are associated with PBX/Conference extensions and call routing rules in the Call Routing Table.

In order to configure CoS feature, follow the steps below:

- At first assign the specified CoS(s) to a certain routing rule(s).
- Assign the specified CoS(s) to the PBX/Conference extension(s).

If there is no CoS assigned to the call routing rule, that rule will be generally available for any PBX extension whether it is attached to a CoS or not.

Please Note: If the **Enable Class of Service** option is disabled, call routing rule(s) that are assigned to a certain CoS(s) will be available for any PBX extension, if there are no any other filtering limitations.

The **Class of Service** page offers the following components:

Enable Class of Service checkbox is used to enable the Class of Service functionality on the QX IP PBX and consists of the following components:

Add opens the **Class of Services - Add Entry** page where a new class of service can be created.

Edit opens the Class of Services - **Edit Entry** page where the selected class of service's settings can be modified. This page includes the same components as the **Class of Services - Add Entry** page does.

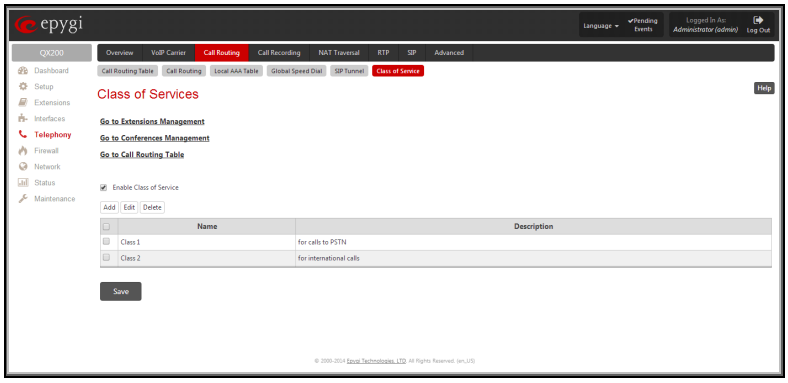


Fig.II- 154: Class of Services page

The Go to Extensions Management link leads to the Extensions Management page where the extensions can be assigned to use certain class of service from the **Extensions Management – Edit Entry – Class of Service Settings** page.

The Go to Conferences Management link appears only if the **Conference** feature is activated from the Feature Keys page and leads to the Conferences Management page where the conference extensions can be assigned to use certain class of service.

The Go to Call Routing Table link leads to the Call Routing Table page where the call routing rules can be assigned to a certain class of service.

The **Class of Service – Add Entry** page is used to create a new **Class of Service** and contains the following components:

- **Name** text field indicates the name of the class of service. This name will be visible in the **Extensions Management – Class of Service Settings** page, in the **Conferences Management – Class of Service Settings** page and in the **Call Routing Wizard** when assigning the classes for the extensions.
- **Description** text field requires optional information about the Class of Service.

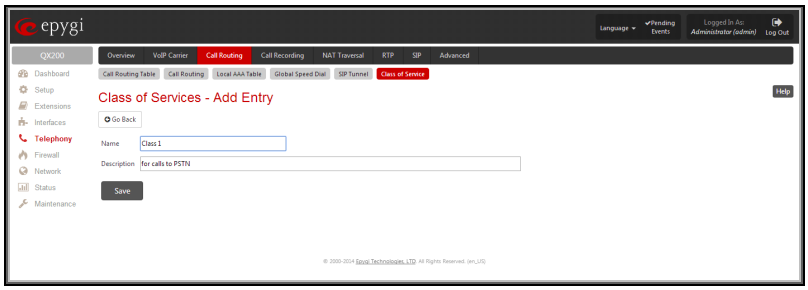


Fig. II-1: Class of Services - Add Entry page

Call Recording Settings

The **Call Recording** service is optional on the QX IP PBX and is activated from Feature page by inserting a feature key.

The **Call Recording** is used to record PBX, SIP or PSTN calls on the QX IP PBX and store the recorded calls either in the local Recording Box or upload them to the remote server. From Call Recording Settings page the call recording can be configured to be started automatically once the call starts or to be started manually from Administrator's Main Page of the QX IP PBX's Web Management or by pressing the **Record** button on the IP phone during the call. If no such button exists on IP phone, the functional key can be configured from QX IP PBX to handle the recording functionality (see Programmable Keys Configuration).

To configure Call Recording, an extension of the Recording Box type should be created first. The memory allocated to that extension will be used for storing the recorded calls. There are two ways to access the recorded calls in the Recording Box: through handset and through Web Management. Through

handset, Recording Box is accessible by calling the Recording Box extension. On QX IP PBX's Web Management, call recordings are available from Extensions Management page by clicking on the Recording Box extension.

Attention: Following limitations apply to the call recording on the QX IP PBX:

- Calls to Auto Attendant or Voicemail cannot be recorded.

The **Call Recording Settings** page is used for configuring the call recording rules. It has two view modes - the **Basic View** and **Advanced View**, which can be switched by appropriate button.

The **Basic View** displays the table with the list of all active extensions, recording states of those extensions and recording parameters.

The **Advanced View displays** the table with all existing call recording rules. Click on the recording box extension number in the **Recorded To** column will move to the corresponding Recording Box.

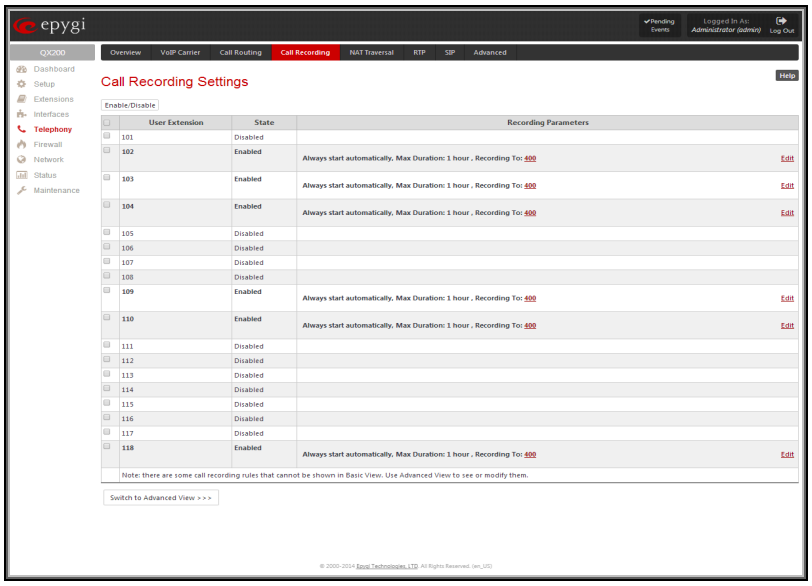


Fig.II- 155: Call Recording Basic View Settings page

The **Call Recording Settings** table offers the following functions:

Enable and **Disable** functional buttons are used to activate and deactivate the selected call recording rule(s). At least one rule should be selected in order to use these functions, otherwise the following error message will appear: "No record(s) selected."

Add functional button opens the **Add Entry** page where a new call recording rule is being configured. The **Add Entry** page consists of the following components:

The **Caller Information** requires the **Call Type** and the caller's **Address**.

The **Called Party Information** consisting of the **Call Type** and the called party's **Address**.

The **Call Type** lists the available call types:

PBX - indicates that the calling or called party is QX IP PBX extension

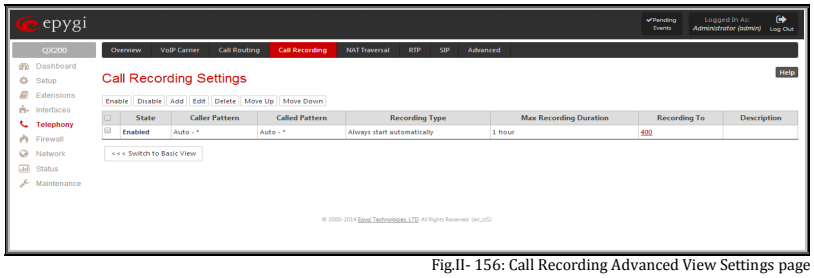


Fig.II- 156: Call Recording Advanced View Settings page

SIP - indicates that the calling or called party is located in SIP network external to QX IP PBX.

PSTN - indicates that the calling or called party is located in PSTN network external to QX IP PBX.

Auto - indicates any of the types listed above.

The value in the **Address** text field is dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX IP PBX extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here. In case of **Auto** call type, any of the addresses listed above are allowed. Wildcards are applicable for this field.

The **Recording Type** drop down list allows you to select whether the recording will start automatically as soon as the call is established, or whether it will be activated manually by pressing the button on the phone during the call.

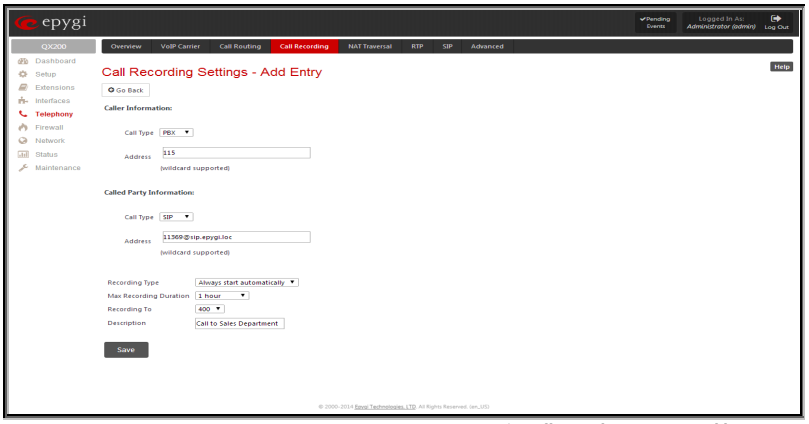


Fig.II- 157: Call Recording Settings – Add Entry page

The **Maximum Recording Duration** drop down list is used to select the maximum duration when the call between the defined caller and called parties will be recorded. When the call recording duration expires, it will be silently stopped while the call will stay active.

The **Recording To** drop down list is for selecting the Recording Box extension Extensions Management) to be used for storing the recordings.

The **Description** text field should contain some descriptive text related to recording rule.

Edit opens the **Edit Entry** page to modify the selected entry. This page contains all the same components as the **Add Entry** page does.

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 IP PBX will be routed through the NAT router).

- **Automatic** – with this selection, system will analyze the QX IP PBX'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 IP PBX'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- 158: 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.

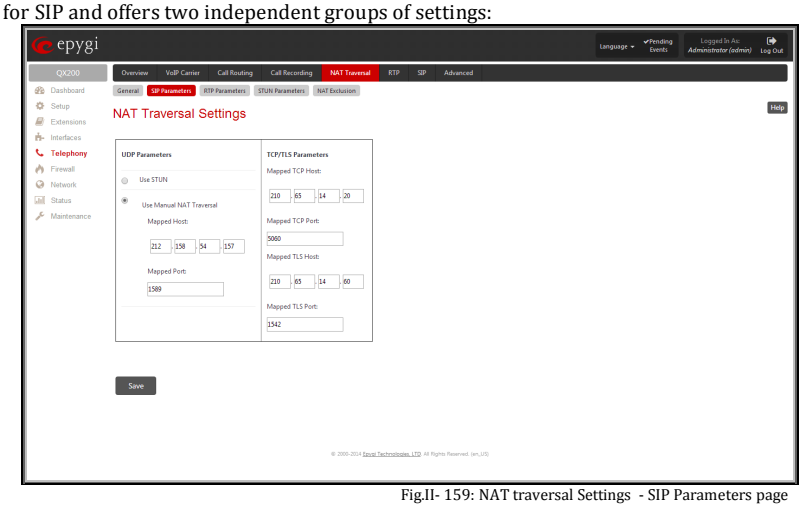


Fig.II- 159: NAT traversal Settings - SIP Parameters page

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.

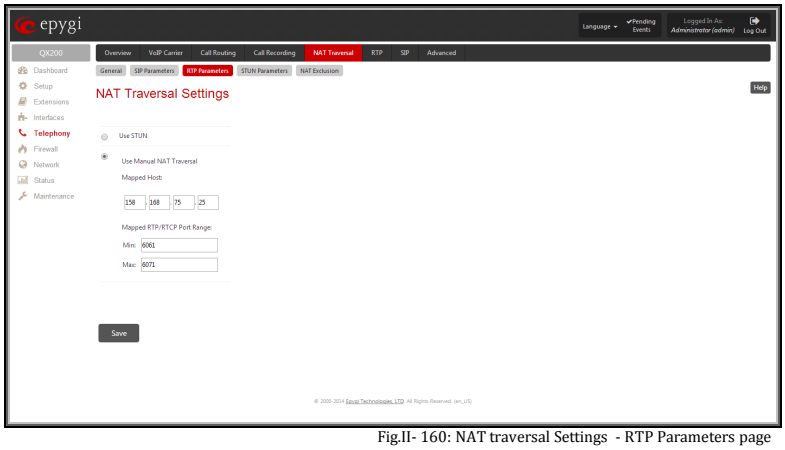


Fig.II- 160: NAT traversal Settings - RTP Parameters page

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 IP PBX. 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.

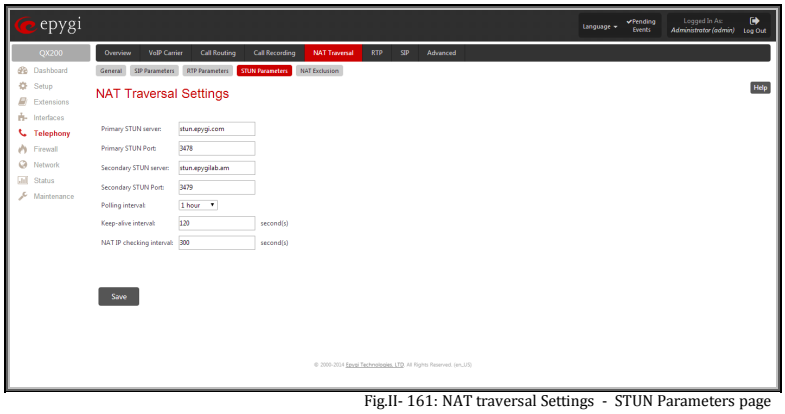


Fig.II- 161: NAT traversal Settings - STUN Parameters page

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 IP PBX 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.

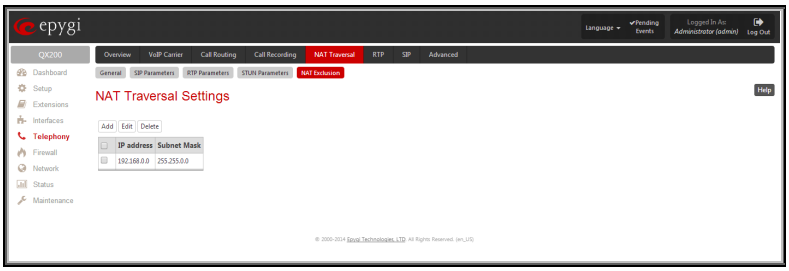


Fig.II- 162: NAT traversal Settings - NAT Exclusion Table page

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.

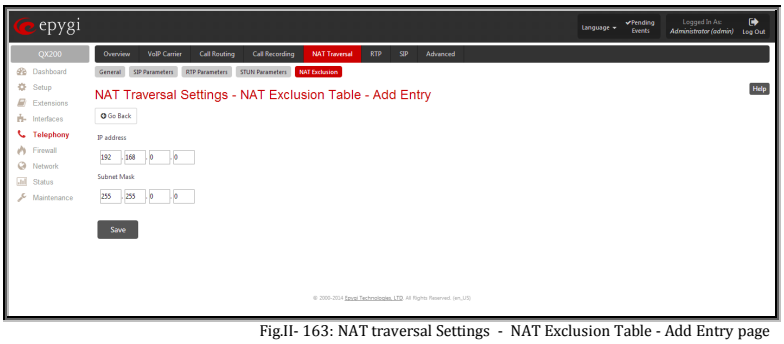


Fig.II- 163: NAT traversal Settings - NAT Exclusion Table - Add Entry page

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.

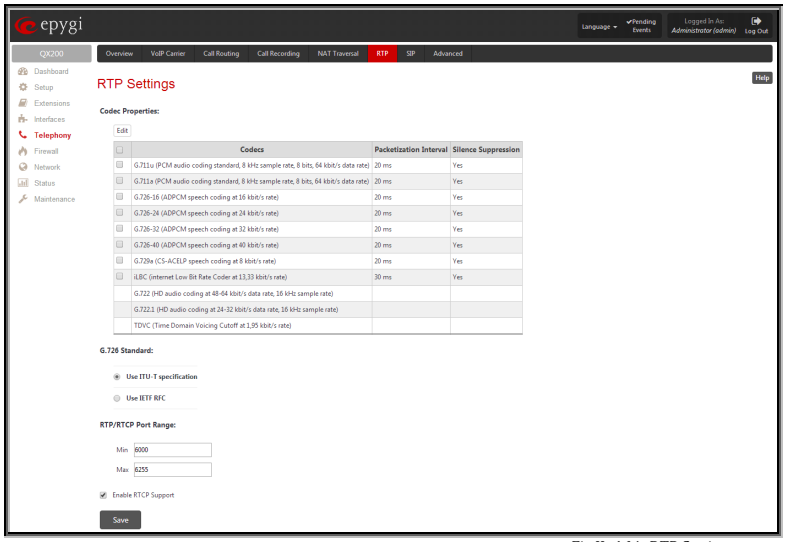


Fig.II- 164: RTP Settings page

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.

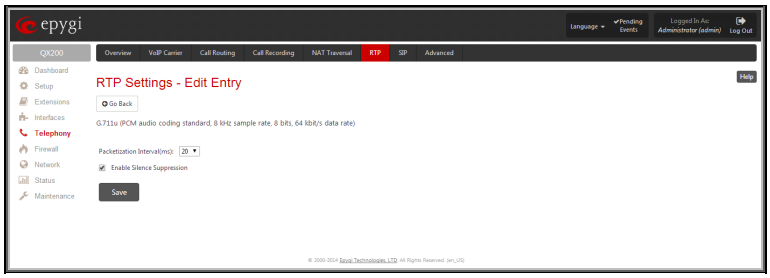


Fig.II- 165: RTP Settings - Edit Entry

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 IP PBX 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 IP PBX. This information might be used by remote side for authentication purposes.

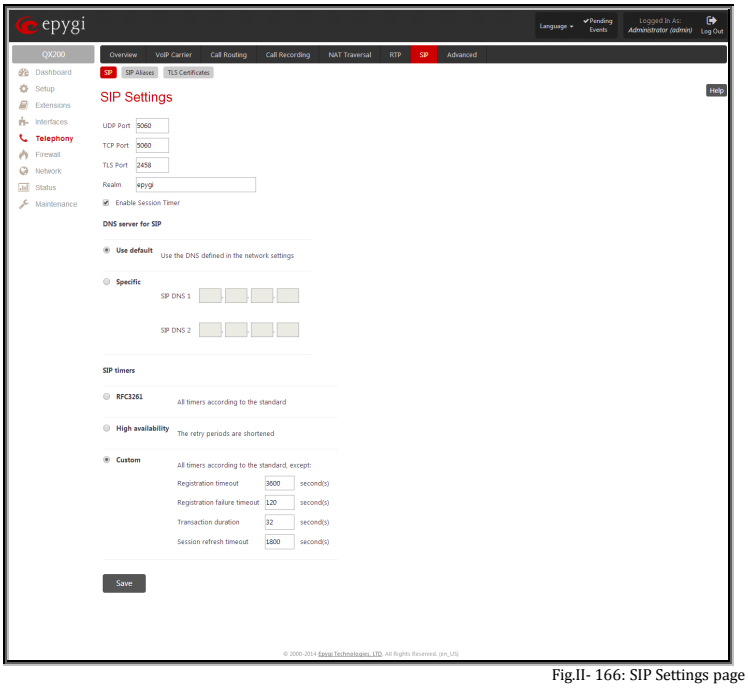


Fig.II- 166: SIP Settings page

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 IP PBX.

- **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 IP PBX's hostnames register on remote DNS servers. This list will be used to identify SIP packets received from remote servers where QX IP PBX is registered with different names.

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

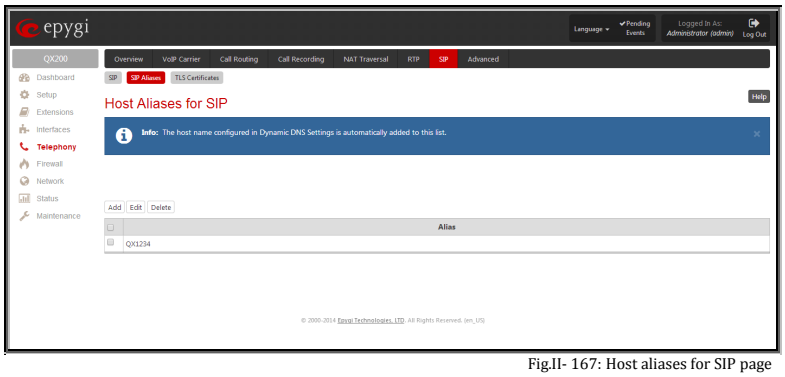


Fig.II- 167: Host aliases for SIP page

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 IP PBX. QX IP PBX 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 IP PBX'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 IP PBX. If the end user is a server or other device, you may download the certificate from the QX IP PBX 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.

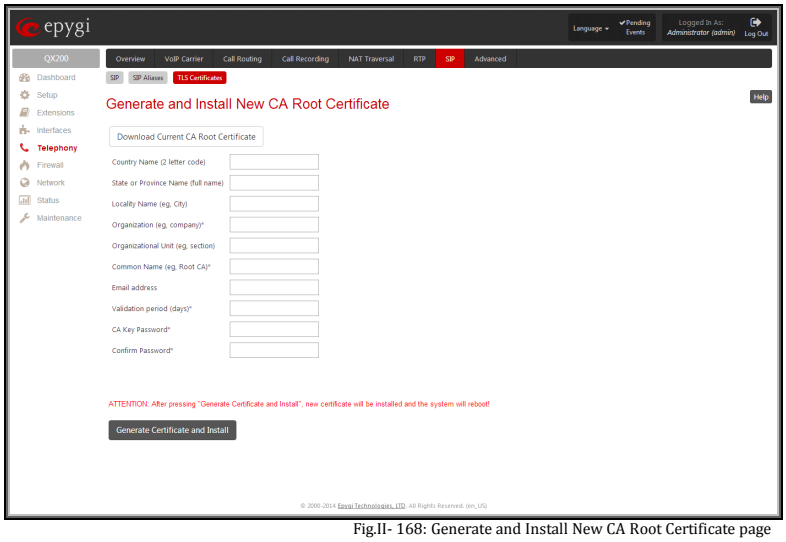


Fig.II- 168: Generate and Install New CA Root Certificate page

Advanced Settings

The **Advanced Settings** page allows you to configure the following settings: Voice Mail Common Settings, RTP Streaming Channels, Gain Control, 3PCC Settings, RADIUS Client Settings, Dial Timeout and Call Quality Notification.

Voice Mail Common Settings

The **Voice Mail Recording Codec** page is used to configure the codec for the Voice Mail recording and other settings related to the voicemail to email and FAX to email sending. It offers the following components:

The **Recording Codec** drop down list contains the existing codecs for voice mail compression. Changing the Voice Mail recording codec will directly affect the allocated memory size for users.

Email Subject for voice field is used to when user enables **Send new voice messages via e-mail** option from his personal **Voice Mail Settings**. In this field you may define a flexible subject for all emails sent from the QX IP PBX and carrying the voice mails.

Besides using static text in the subject line, you may want to use the predefined tags to combine the needed subject:

- **Hostname** - the hostname of the QX IP PBX.
- **Displayname** - the caller's display name. This value is not displayed for PSTN callers.
- **Username** - the caller's SIP username. For PBX caller this is the caller's PBX number, for PSTN callers this is the caller's PSTN number.
- **Full name** - the caller's full SIP address (SIP username and the SIP server). For PBX caller this is the caller's PBX number, for PSTN callers this is the caller's PSTN number.
- **Duration** - the voice mail duration.
- **Date** - the date the voice mail was received.

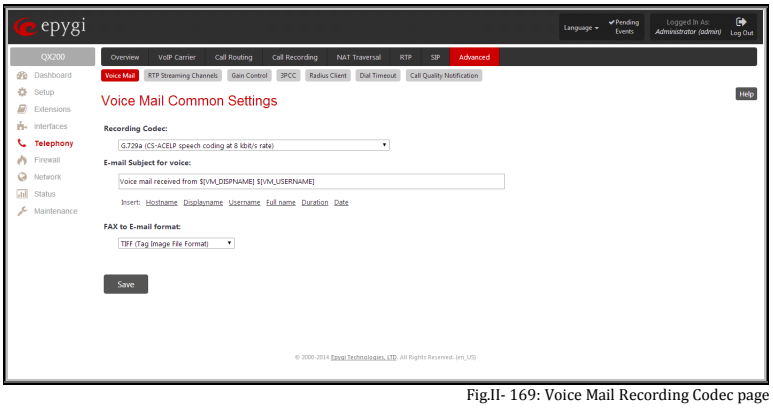


Fig.II- 169: Voice Mail Recording Codec page

To insert the predefined tag to the subject line, you should simply click on the corresponding tag. The following format should be maintained to create a flexible subject:

Example: Voice mail received from $[VM_DISPNAME] $[VM_DATE]

In this example, all email subjects will contain a static text "Voice mail received from" following by the display name of the caller and the date voice mail is received.

FAX to E-mail format drop down list is used to define the format of the FAX document received in the voice mail and to be attached to the email, in case user has enabled **Send new voice messages via e-mail** option from his personal **Voice Mail Settings**. TIFF or PDF formats may be selected here.

RTP Streaming Channels

The **RTP Streaming Channels** page is used to configure channels where the broadcast RTP streams are transmitted. These channels may be then configured to be used as hold music (see Manual III – Extension User's Guide) or any other type of music played to the caller.

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

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

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

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

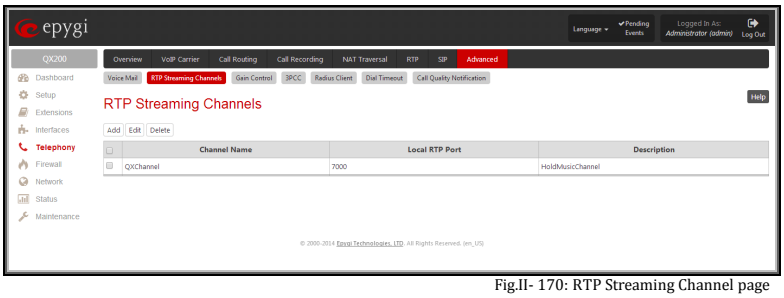


Fig.II- 170: RTP Streaming Channel page

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

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

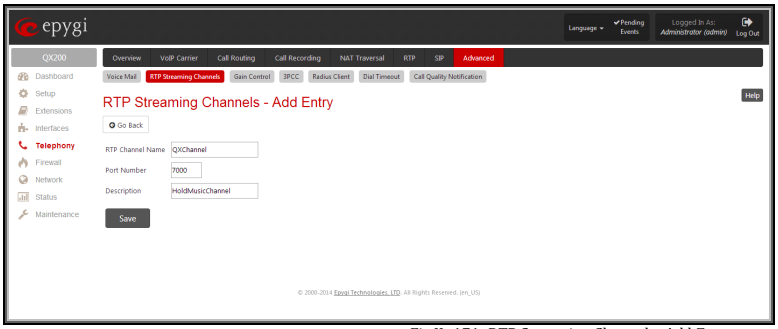


Fig.II- 171: RTP Streaming Channel – Add Entry page

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 IP PBX to the FXO network.

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

For **Voice Mail**:

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

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

For **Audio Lines**:

Transmit Gain (Line Out) defines the level of voice transmitted from QX IP PBX to the Audio Line Out port.

Receive Gain (Line In) defines the volume of voice received by QX IP PBX from the Audio Line In port.

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

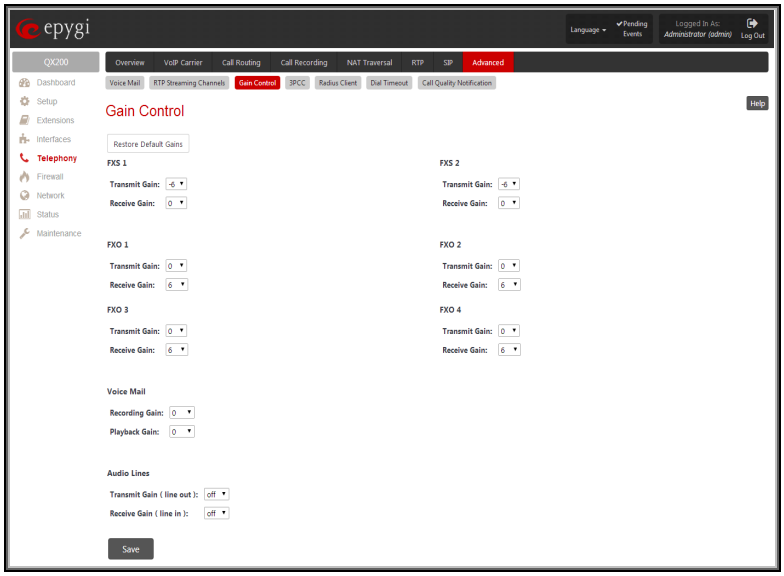


Fig.II- 172: Gain Control page

3PCC Settings

The **3PCC Settings** page is used to adjust the third party call controlling settings. 3PCC service on the QX IP PBX allows call controlling applications to remotely initiate and handle calls on the QX IP PBX and to subscribe for certain event notifications from the QX IP PBX.

This page consists of the following components:

The **Secure Connection** checkbox is used enable a secure encrypted connection between the call controlling application and the QX IP PBX.

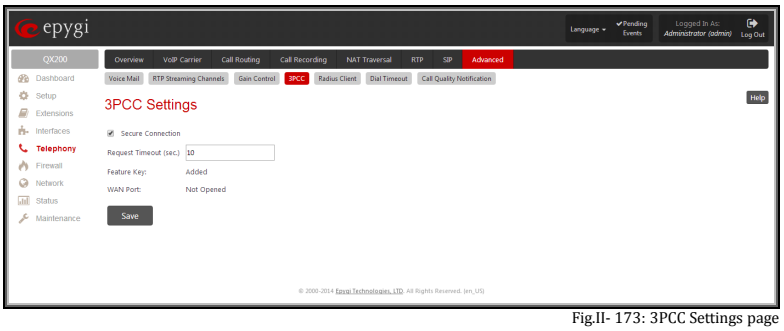


Fig.II- 173: 3PCC Settings page

Please Note: For successful connection, this option should be set up in the same way on both sides (enabled or disabled on both sides).

The **Request Timeout** text field requires the timeout (in seconds) during which the QX IP PBX should receive a response to the request from the call controlling application. If the response is not received during this timeout, QX IP PBX will perform a request dependent default action. For example, if the call controlling application is configured to handle incoming calls on the QX IP PBX. Once the incoming call occurs, QX IP PBX is trying to transfer the call to the call controlling application. If the call controlling application does not response within the mentioned timeout, QX IP PBX will answer the call or perform an action configured for unanswered incoming calls. This setting is dependent on the network conditions therefore consult with your network administrator before changing the default value.

The read-only **Feature Key** text field indicates whether the feature key for the 3PCC Support is installed on the system. The system will not accept connections from 3PCC applications if no key is found. The 3PCC support is an optional feature and can be activated with a feature key from the Feature Keys page.

The read-only **WAN Port** text field indicates whether there is a filtering rule specified for the Call Control Access. If a third-party call control application connects to the QX IP PBX from the WAN interface, a filtering rule for the corresponding host should be created on the Call Control Access page to allow the application a remote access. Creating a filtering rule is not required if the firewall is not setup on the QX IP PBX. The field shows **Opened** if there is at least one enabled filtering rule for the Call Control Access.

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 IP PBX to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the QX IP PBX, and according to the configuration of **AAA Required** option, 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 IP PBX Network.

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

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 IP PBX, 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 IP PBX'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 IP PBX.

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 IP PBX is to send the authentication requests.

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

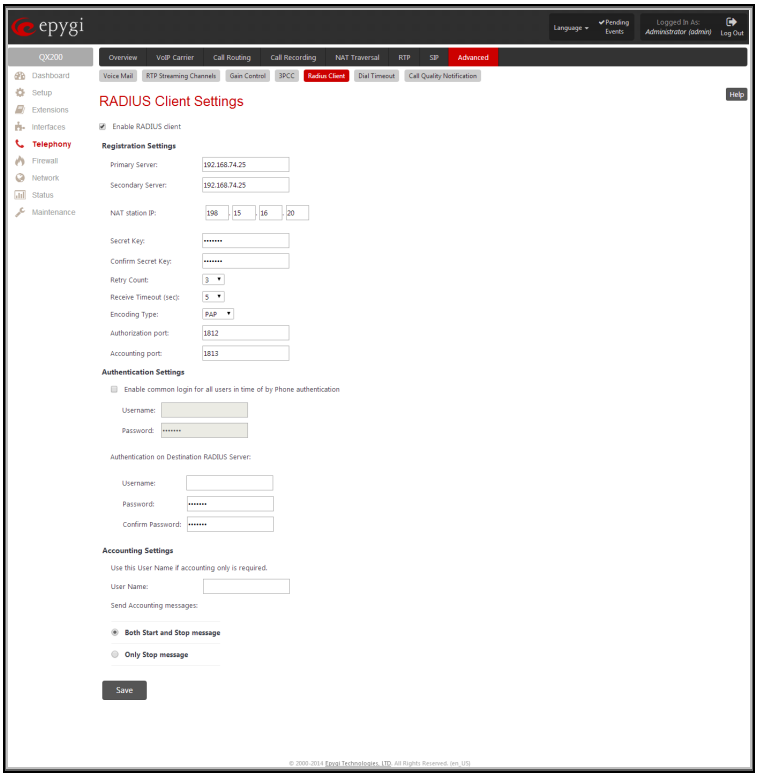


Fig.II- 174: Radius Client Settings page

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 IP PBX. 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 IP PBX. 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 IP PBX 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.

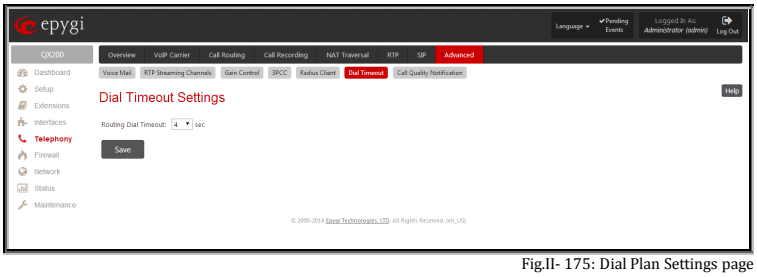


Fig.II- 175: Dial Plan Settings page

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 IP PBX, an event notification will appear. When the **Notify** checkbox is disabled, no Call Quality events will occur on the QX IP PBX.

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

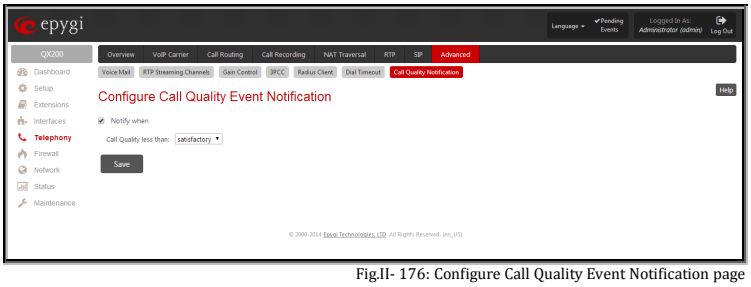


Fig.II- 176: Configure Call Quality Event Notification page

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
  - Call Control Access
  - SIP Access
  - Blocked IPs
  - Allowed IPs
- **Custom Services**
  - Service Pool Configuration
- **IP Groups**
  - IP Pool Configuration
- **SIP IDS Settings**

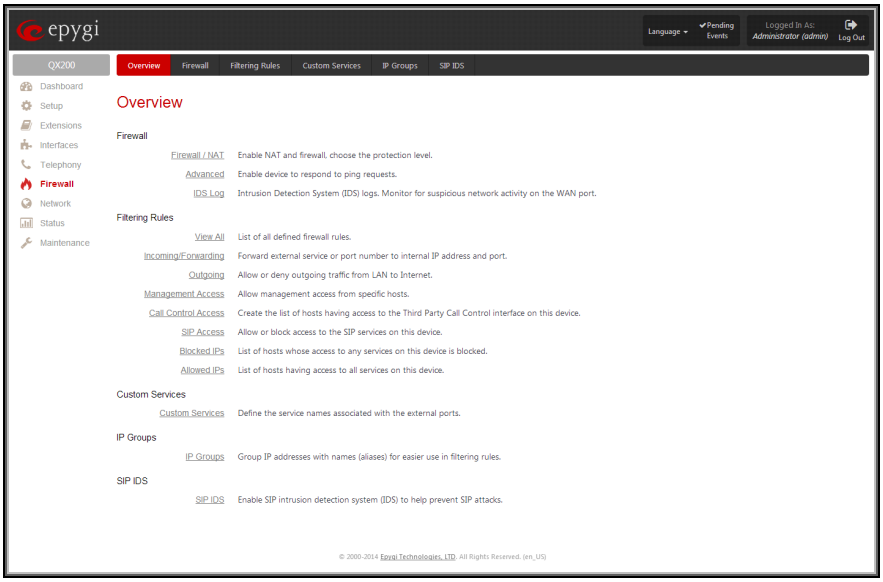


Fig.II- 177: Firewall Menu page

Firewall

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

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

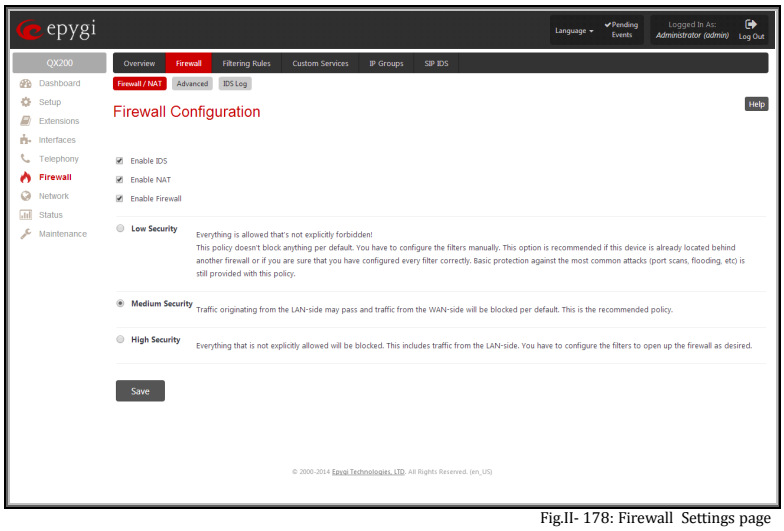


Fig.II- 178: Firewall Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed towards the device. With these features enabled, QX IP PBX 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 IP PBX from its WAN.

The **Fool Portscanner** checkbox (available only for QX50/QX200) selection prohibits QX IP PBX portscanning from its WAN. As a reply to a Portscanning operation, "network unreachable" or "host unreachable" feedback messages will be sent.

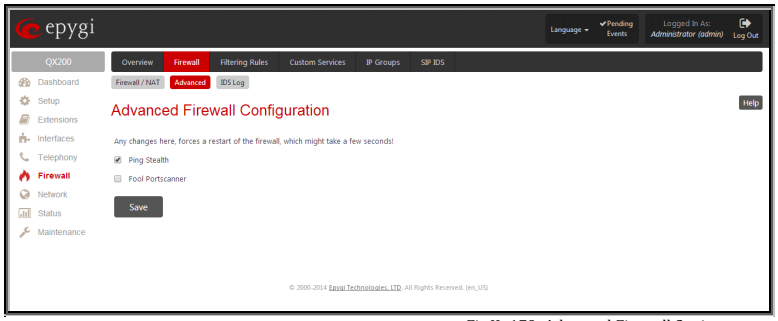


Fig.II- 179: Advanced Firewall Settings page

IDS Log

The **IDS logging** page (available only for QX50/QX200) 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.

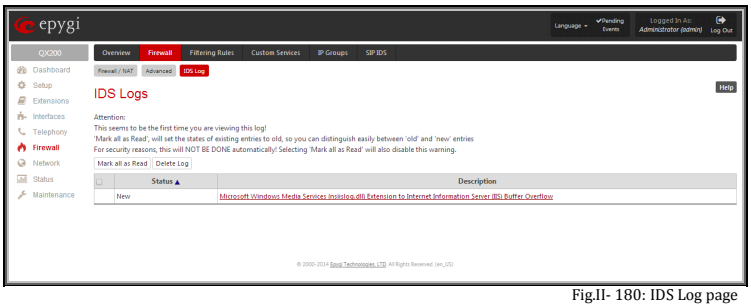


Fig.II- 180: IDS Log page

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.

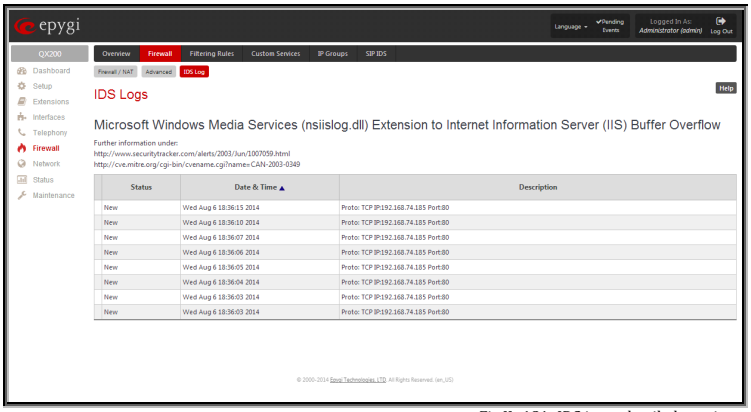


Fig.II- 181: IDS issue detailed preview

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 IP PBX to make the newly created blocking rule effective immediately. However, if you are unable to restart the QX IP PBX, 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.

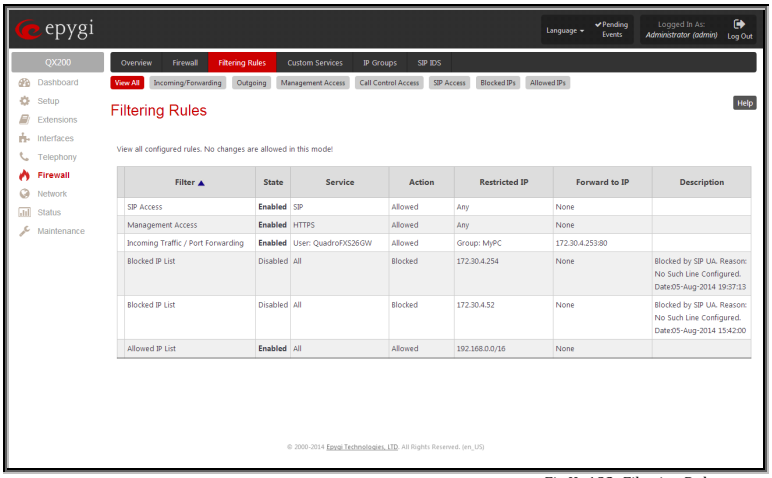


Fig.II- 182: Filtering Rules page

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 IP PBX's LAN. The NAT service should be enabled on the QX IP PBX 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.

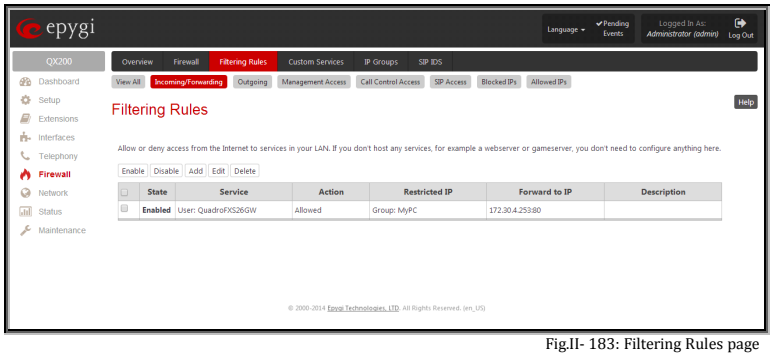


Fig.II- 183: Filtering Rules page

Outgoing Traffic

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

Fig.II-184: Filtering Rules page

Management Access

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

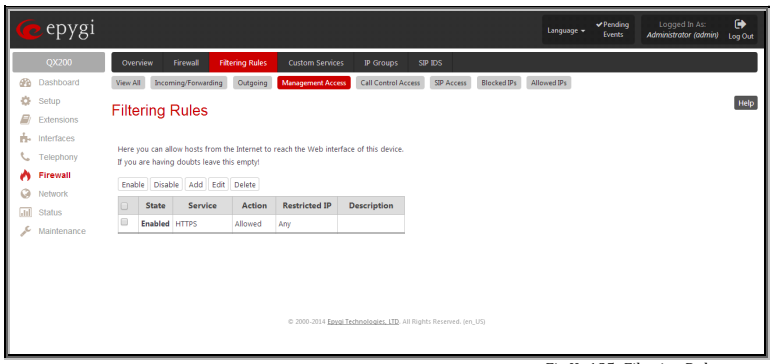


Fig.II- 185: Filtering Rules page

Call Control Access

Call Control Access is used to enable the access from the call controlling application from the Internet to the QX IP PBX. The call controlling applications can be used to remotely initiate and handle calls on the QX IP PBX and to subscribe for certain event notifications from the QX IP PBX.

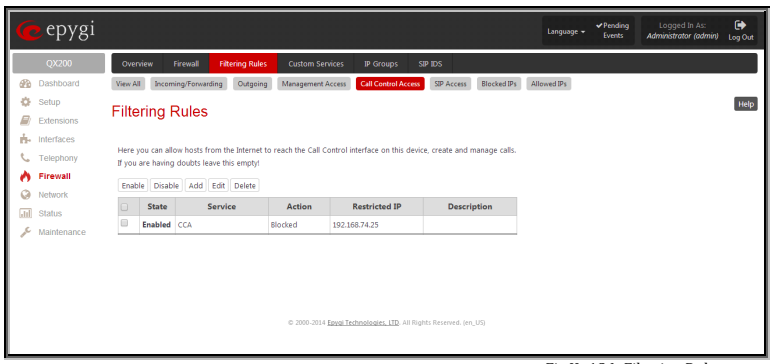


Fig.II- 186: Filtering Rules page

SIP Access

SIP Access is used 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).

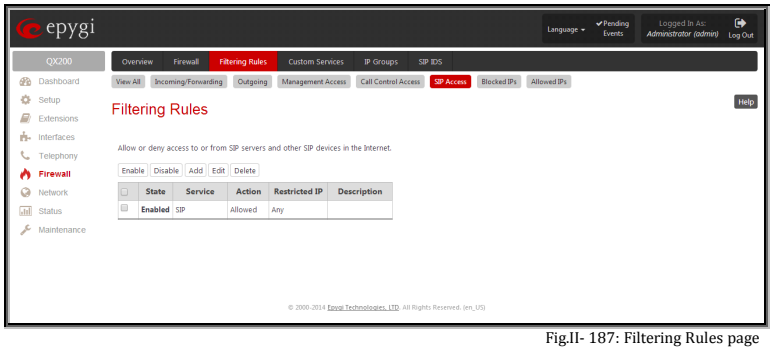


Fig.II- 187: Filtering Rules page

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.

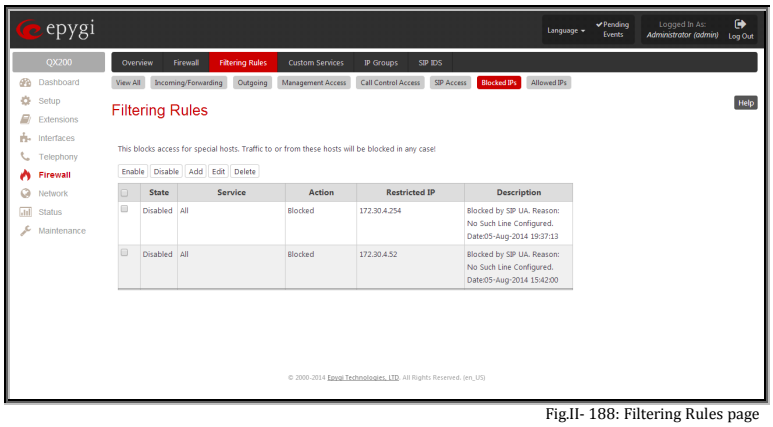


Fig.II- 188: Filtering Rules page

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.

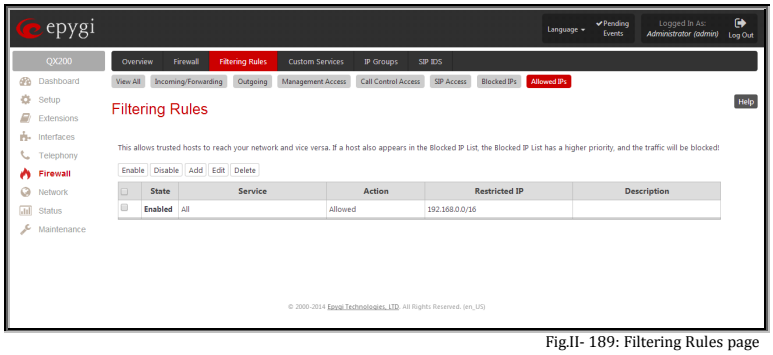


Fig.II- 189: Filtering Rules page

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 custom 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 IP PBX.

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.

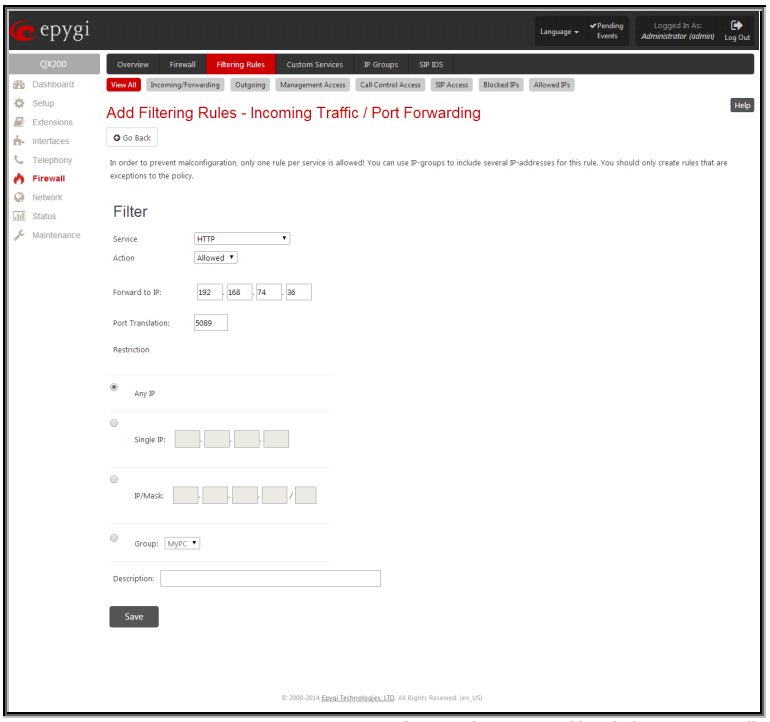


Fig.II- 190: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filtering Rule** (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, Call Control 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, Call Control 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.

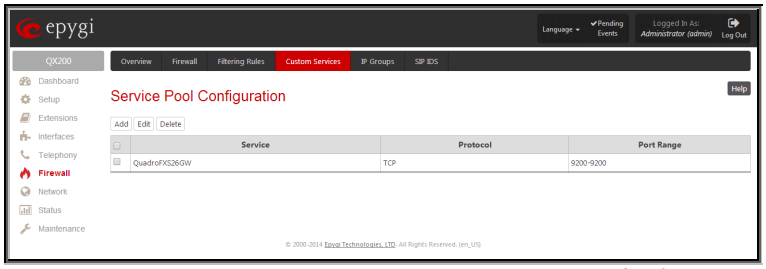


Fig.II- 191: Service Pool Configuration page

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.

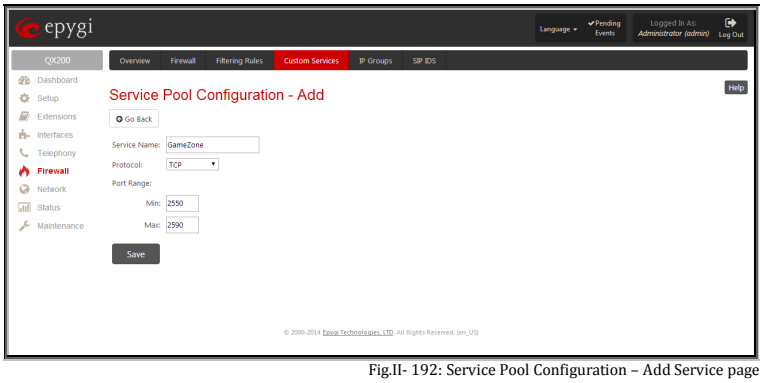


Fig.II- 192: Service Pool Configuration – Add Service page

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.

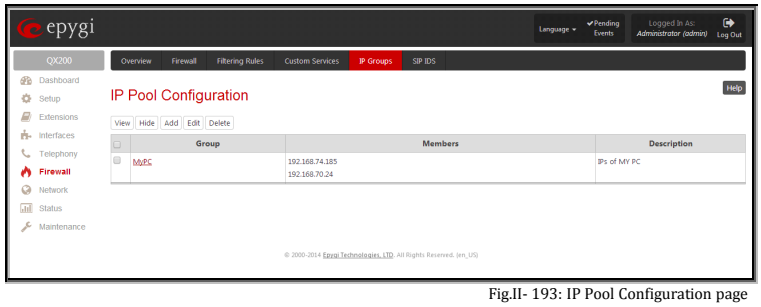


Fig.II- 193: IP Pool Configuration page

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.

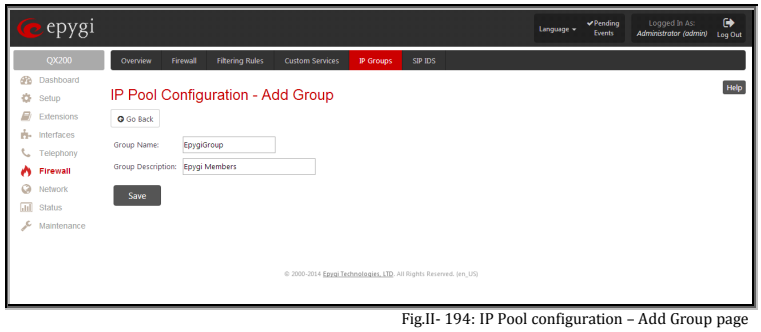


Fig.II- 194: IP Pool configuration – Add Group page

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- 195: 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.

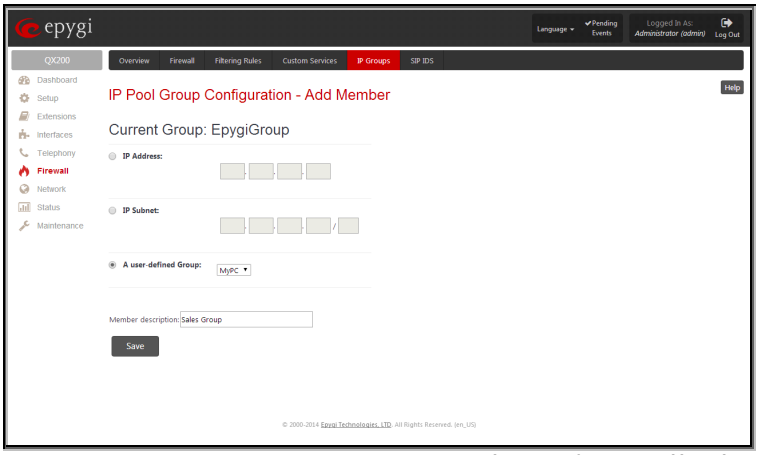


Fig.II- 196: IP Pool Group Configuration – Add Member

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 IP PBX 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 IP PBX SIP cash after defined timeout (default timeout value of "Discard SIP messages from IP address for" service is 32 seconds).

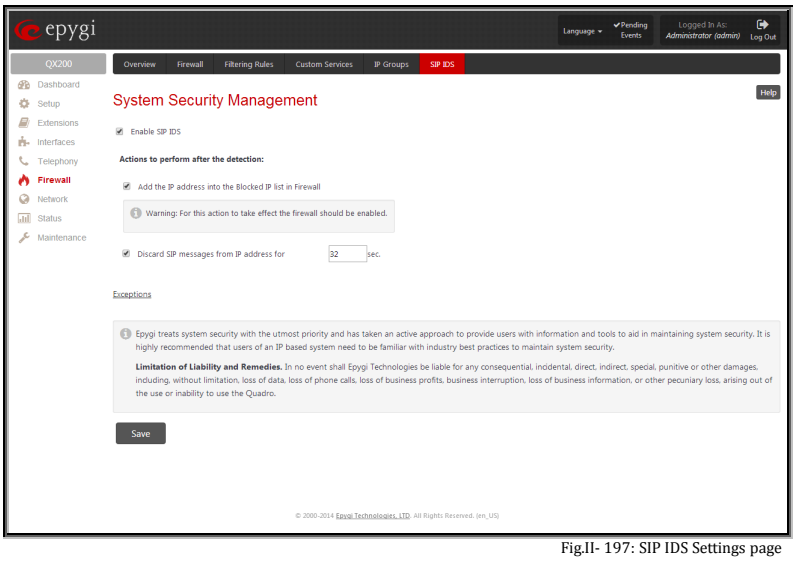


Fig.II- 197: SIP IDS Settings page

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.

Delete removes the selected exceptions from the **Exceptions for SIP IDS** table.

Fig.II- 198: 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

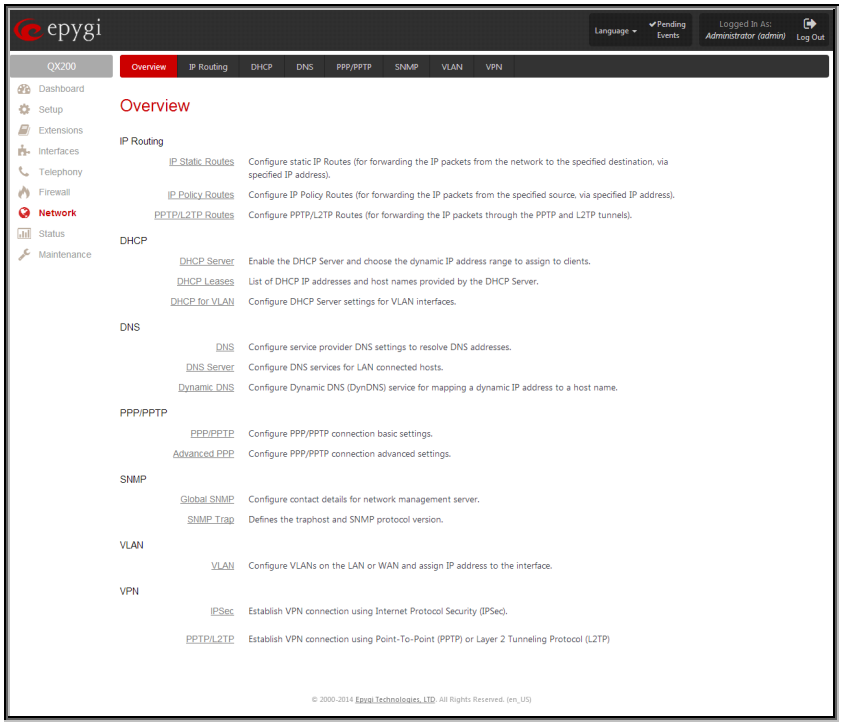


Fig.II- 199: Network Menu page

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

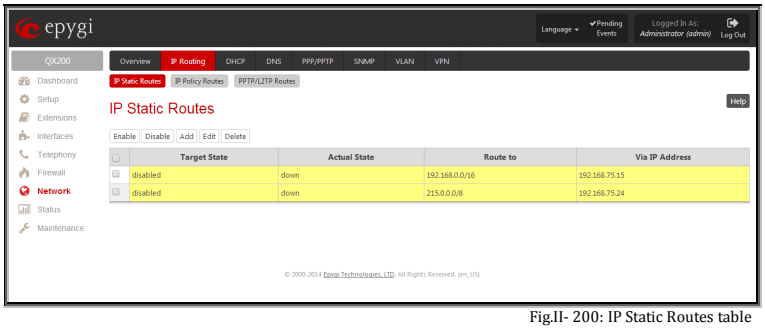


Fig.II- 200: IP Static Routes table

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.

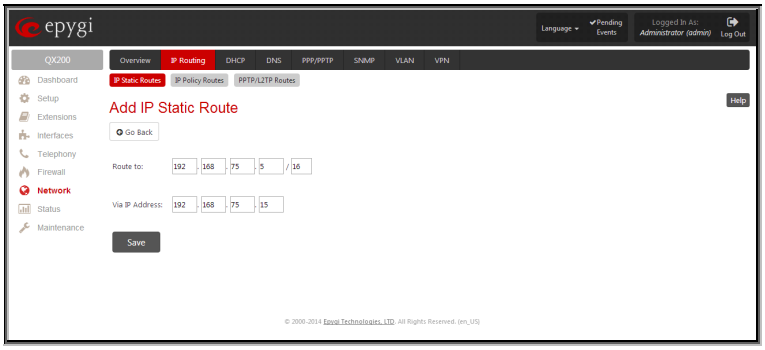


Fig.II- 201: Add IP Static Route page

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).

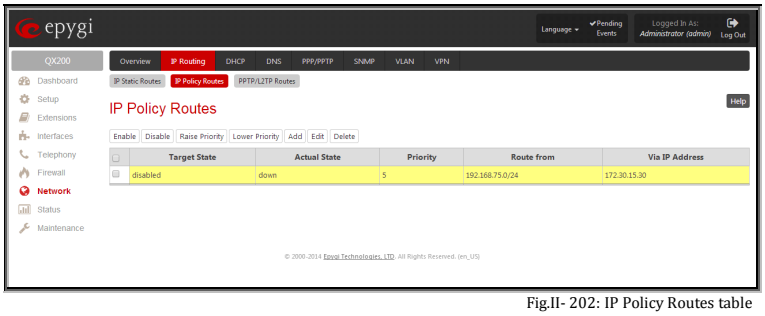


Fig.II- 202: IP Policy Routes table

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.

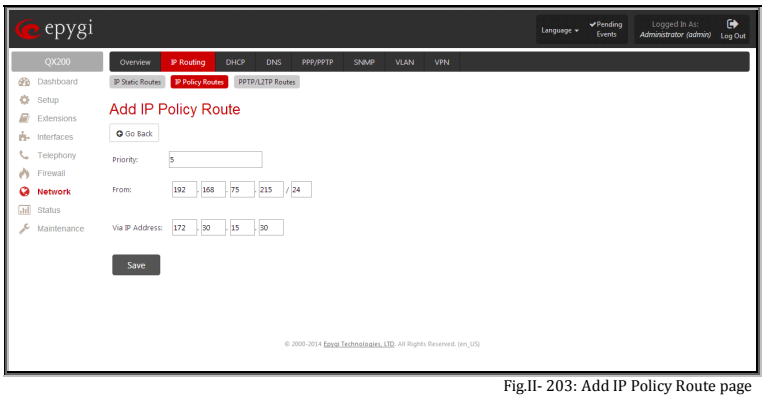


Fig.II- 203: Add IP Policy Route page

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.

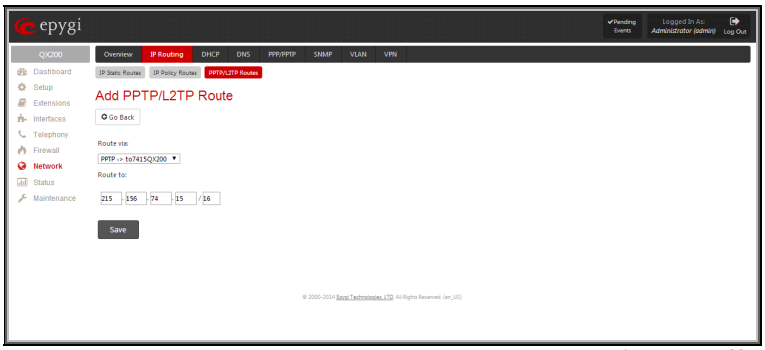


Fig.II- 204: PPTP/L2TP Routes table

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 IP PBX'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.

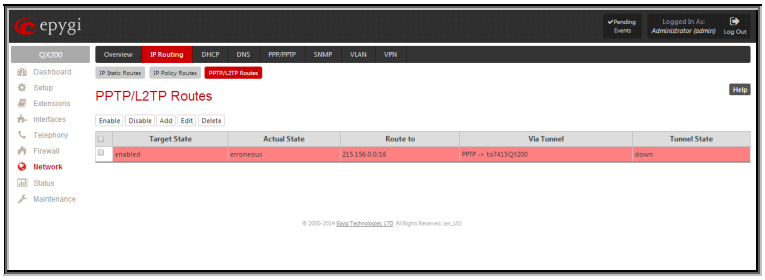


Fig.II- 205: Add PPTP/L2TP Route page

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 IP PBX user's LAN settings. Therefore, QX IP PBX LAN users will automatically be provided with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the QX IP PBX's IP address)
- WINS server
- Nameserver (corresponds to the QX IP PBX'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 IP PBX. With this checkbox enabled, QX IP PBX 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.

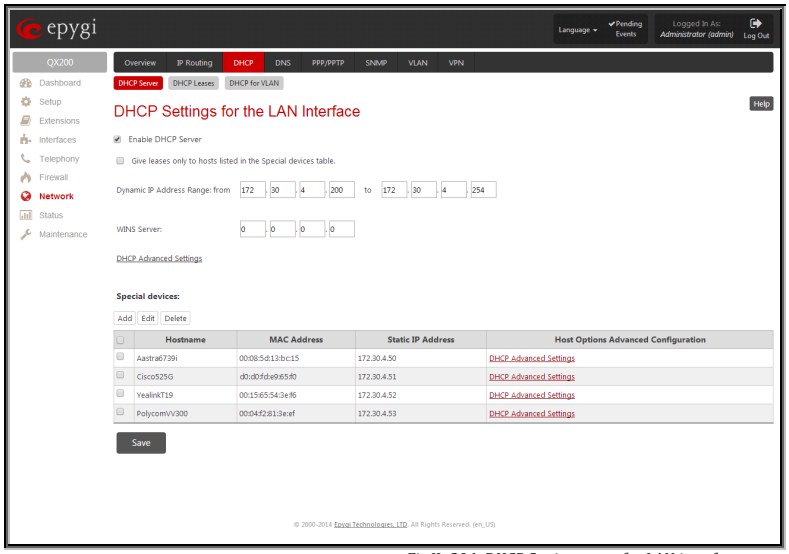


Fig.II- 206: DHCP Settings page for LAN interface page

IP Address Range defines a range of IP addresses that will be assigned to the QX IP PBX 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 IP PBX LAN users.

DHCP Advanced Settings link leads to the page where the advanced options of the QX IP PBX'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 IP PBX'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 IP PBX'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 IP PBX's LAN.

Please Note: If you leave this field empty, the device in the QX IP PBX's LAN will get the first available IP address from range defined in the **DHCP Settings** page (see above).

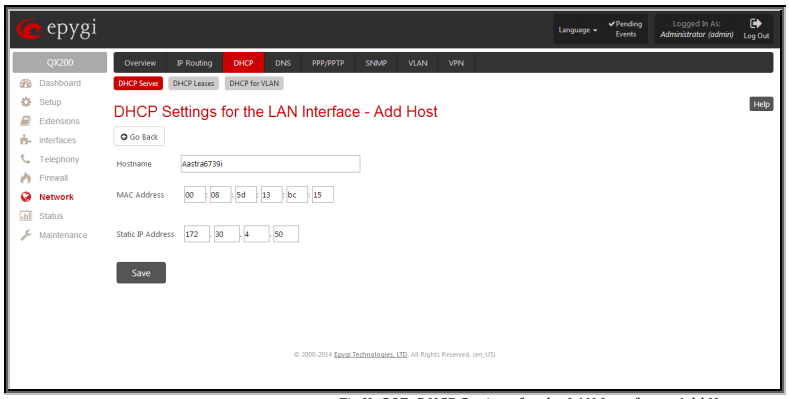


Fig.II- 207: DHCP Settings for the LAN Interface – Add Host page

DHCP Advanced Settings

The **DHCP Advanced Settings** page is used to modify the advanced options of the DHCP server on the QX IP PBX. 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.

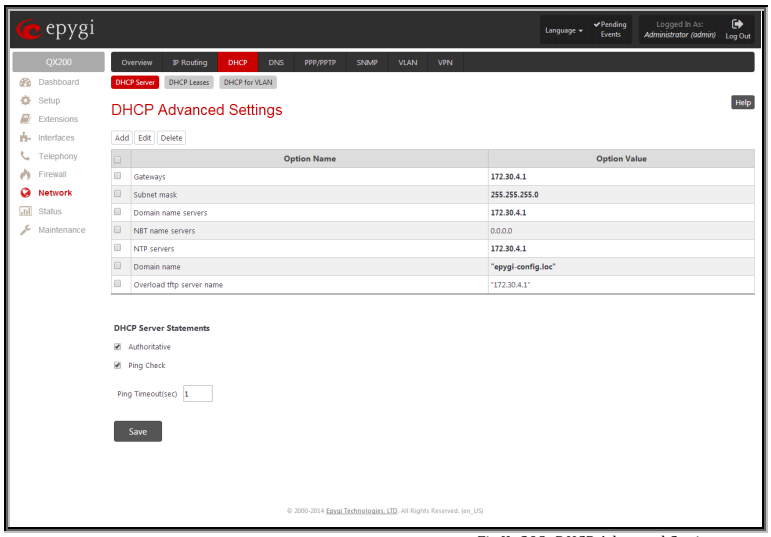


Fig.II- 208: DHCP Advanced Settings page

- The **Authoritative** checkbox is used to enable/disable authoritative mode on the QX IP PBX DHCP server. Disabling the checkbox is recommended if several DHCP servers are used on the network and the QX IP PBX 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 IP PBX 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:

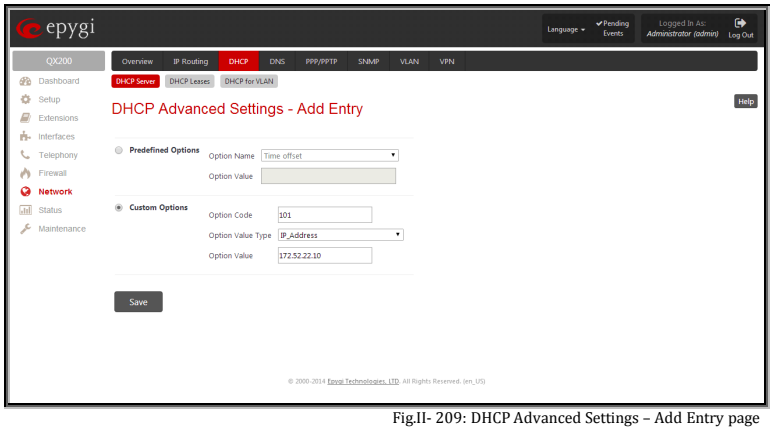


Fig.II- 209: DHCP Advanced Settings – Add Entry page

- **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 IP PBX's LAN. For these hosts, QX IP PBX 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:

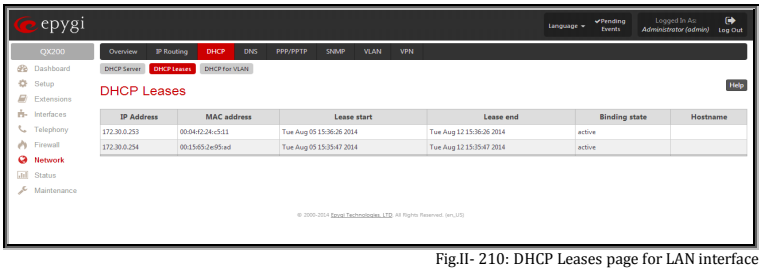


Fig.II- 210: DHCP Leases page for LAN interface

IP address - host IP address, assigned by QX IP PBX.

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 IP PBX's LAN or to integrate the QX IP PBX 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 IP PBX s 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 IP PBX.

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:

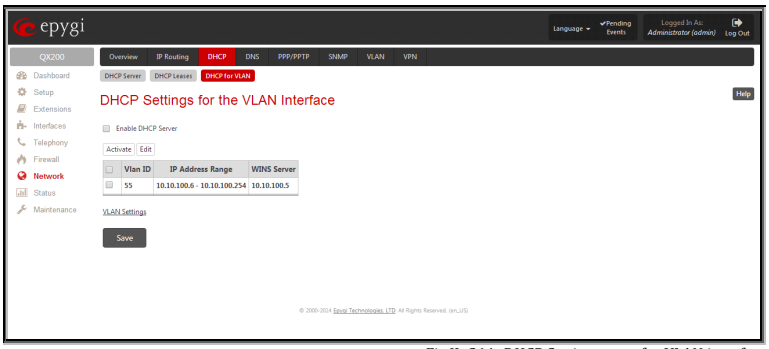


Fig.II- 211: DHCP Settings page for VLAN interface

Enable DHCP Server checkbox activates the DHCP server on QX IP PBX for VLAN. With this checkbox enabled, QX IP PBX 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 IP PBX. 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.

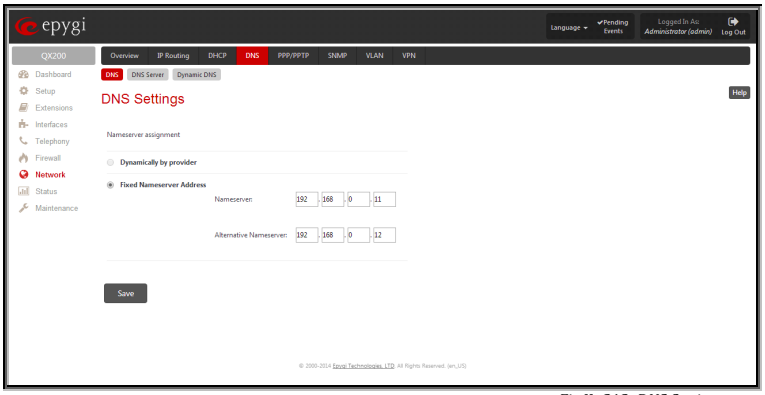


Fig.II- 212: DNS Settings page

DNS Server Settings

The **DNS Server** on the QX IP PBX provides the services to the hosts in the QX IP PBX's LAN. With this service, QX IP PBX 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 IP PBX and to define a list of aliases for the devices in the QX IP PBX'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 IP PBX.

The table on this page lists aliases for each of the device in the QX IP PBX's LAN to be resolves through the DNS server.

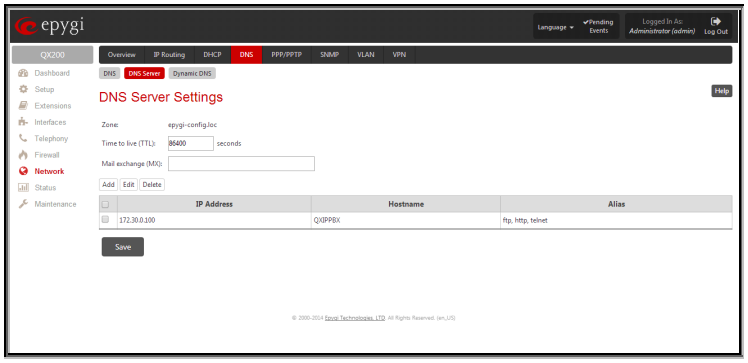


Fig.II- 213: DNS Server Settings page

Add functional link opens the page **Add Host** where a list of aliased can be defined for the certain device in the QX IP PBX's LAN. The page contains the following components:

IP Address text fields require the IP address of the device in the QX IP PBX's LAN.

Hostname text field requires the hostname of the device in the QX IP PBX's LAN.

Alias text fields are used to enter up to 5 alias names by which the device in the QX IP PBX's LAN will be resolved.

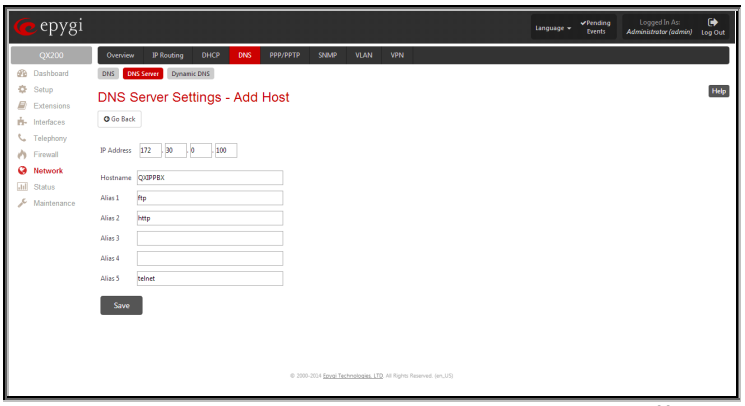


Fig.II- 214: DNS Server Settings – Add Host page

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 IP PBX, you first have to choose a DynDNS provider and register at their website.

The **Dynamic DNS Settings** page provides the following components:

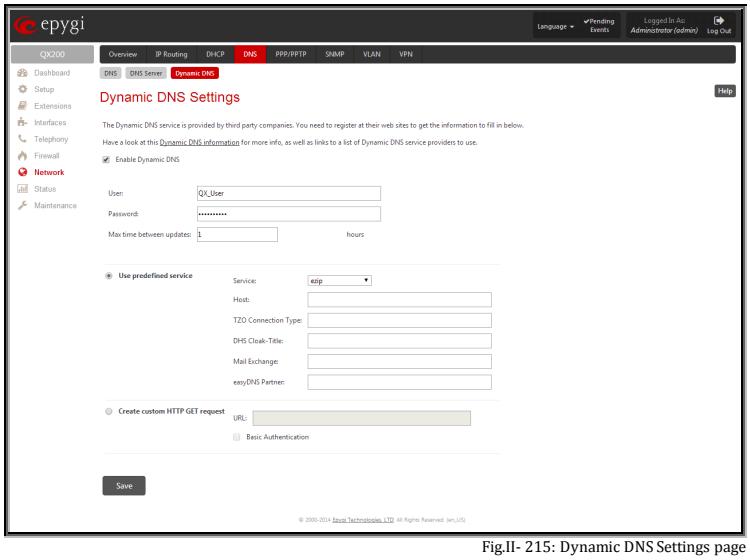


Fig.II- 215: Dynamic DNS Settings page

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 (available only for QX50/QX200) 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 IP PBX and the provider, QX IP PBX 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 IP PBX 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 IP PBX 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 IP PBX first.
- **Always connected** - QX IP PBX 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.

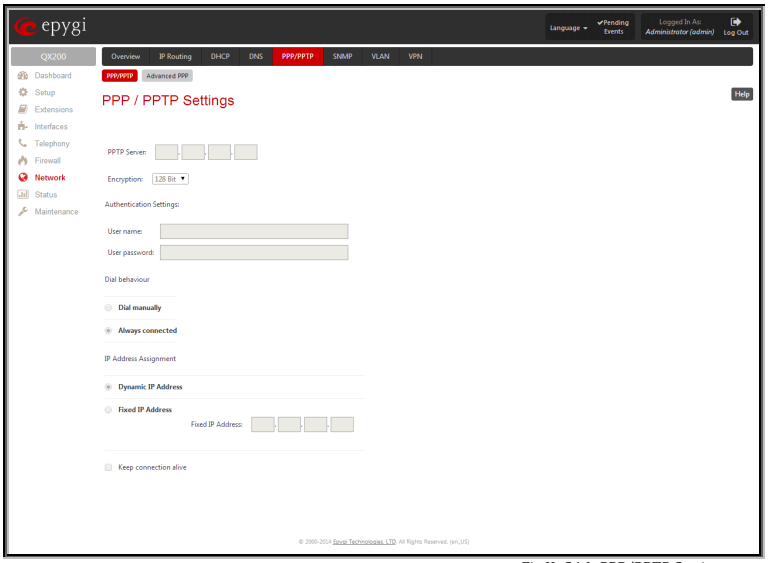


Fig.II- 216: PPP/PPTP Settings page

Advanced PPP Settings

The **Advanced PPP Settings** page (available only for QX50/QX200) 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.

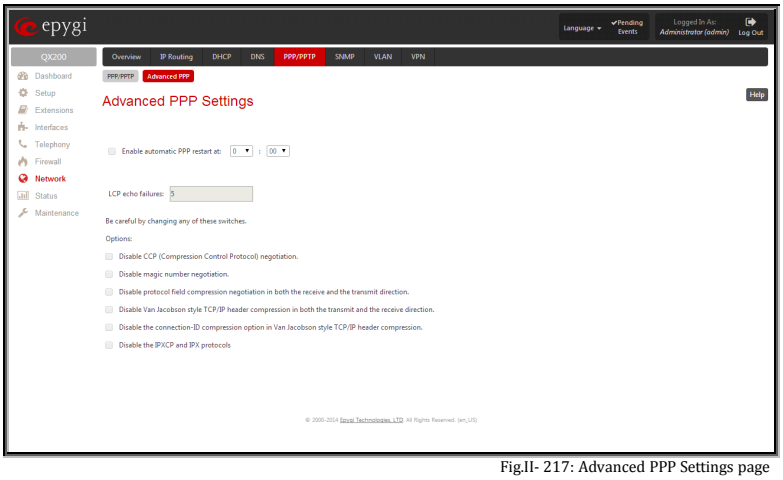


Fig.II- 217: Advanced PPP Settings page

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 IP PBX, SNMP agent is running to allow administrators to remotely manage QX IP PBX'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 IP PBX or remotely modify QX IP PBX'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 IP PBX.

Global SNMP Settings

Enable SNMP checkbox is used to enable SNMP agent on the QX IP PBX.

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 IP PBX s SNMP agent and the administrating application. If this checkbox is not selected, **SNMP v1** will be implied.

SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about QX IP PBX's). Field may contain some kind of password which should be matching both on QX IP PBX 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 IP PBX for the SNMP monitoring application. With this checkbox enabled, administrator will be able to remotely configure the QX IP PBX via SNMP administrating program.

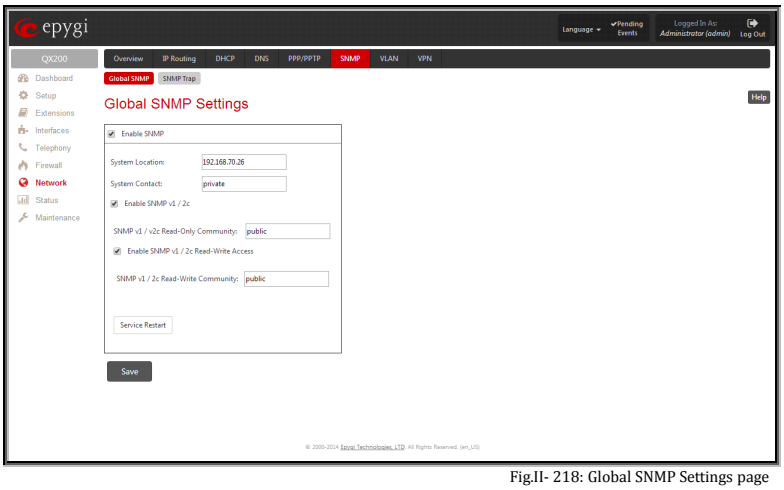


Fig.II- 218: Global SNMP Settings page

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 IP PBX's and remotely changing QX IP PBX's configuration). Field may contain some kind of password which should be matching both on QX IP PBX and on the administrating application for successful SNMP management.
The **Service Restart** button restarts the SNMP sub-system on the QX IP PBX. 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 IP PBX. For the listed traphosts to be informed about the events on the QX IP PBX, **Send SNMP Trap** action should be configured for the corresponding event(s) from the Events page.

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

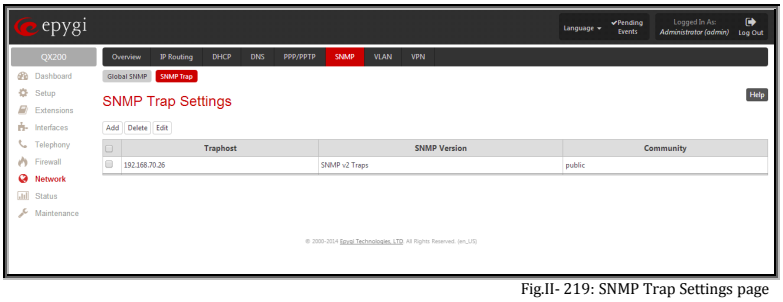


Fig.II- 219: SNMP Trap Settings page

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 IP PBX. Field may contain some kind of password which should be the same both on QX IP PBX 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 IP PBX to the administrating application.

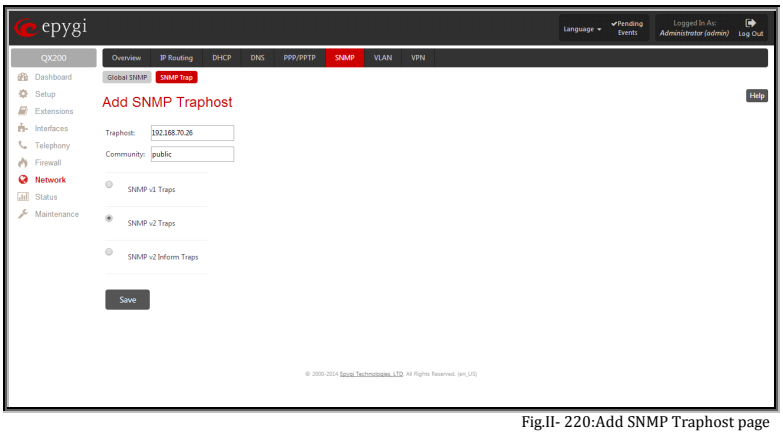


Fig.II- 220:Add SNMP Traphost page

VLAN Configuration

VLAN Settings page lists all existing virtual interfaces created on the QX IP PBX and allows you to create new interfaces.
Enable and **Disable** functional buttons are used to correspondingly enable and disable the selected virtual interface(s).

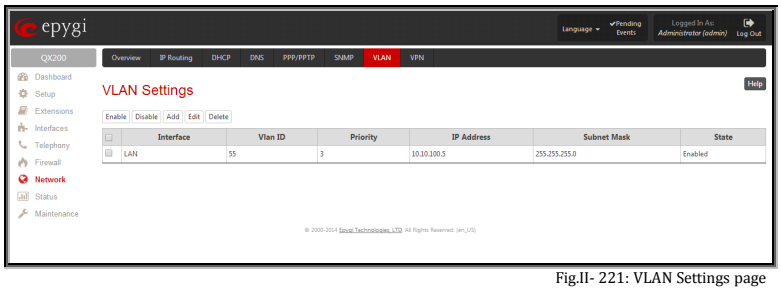


Fig.II- 221: VLAN Settings page

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 (available only for QX50/QX200) 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.

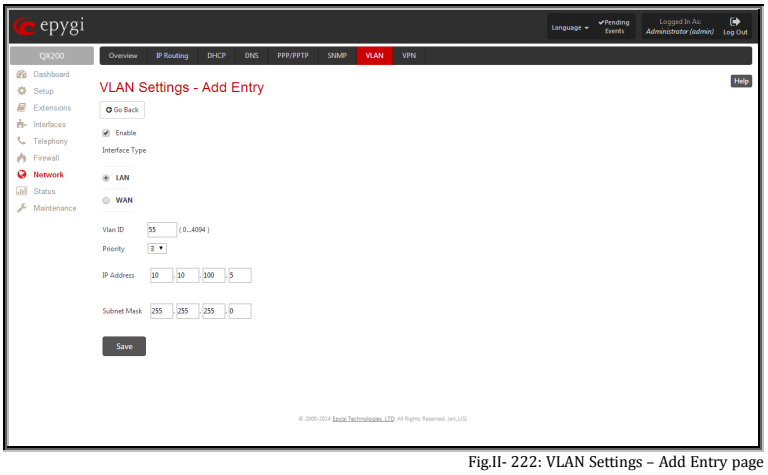


Fig.II- 222: VLAN Settings – Add Entry page

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.

The **VPN Configuration** page is not available for QX2000.

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 IP PBX 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 IP PBX 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 IP PBX 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 IP PBX, 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 IP PBX is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. QX IP PBX 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 IP PBX can also be set up to act as a Road Warrior. If a home office is connected to the Internet via QX IP PBX with PPPoE (Point-to-Point Protocol) and dynamic IP addressing, setting up QX IP PBX 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 IP PBX 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 IP PBX's public key can be decrypted with QX IP PBX'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.

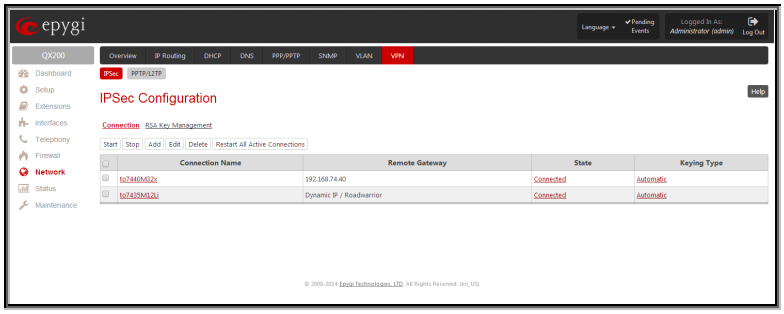
Please Note: A pair of keys will always be generated, a public one and a private one. The previously generated pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

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 stopped.

Fig.II- 223: IPSec Configuration - Connection Settings page

Add leads to the **Add IPSec Connection** wizard where a new IPSec connection can be defined and specified. The wizard provides several pages.

Edit leads to a set of **IPSec Connection Properties** pages to modify the parameters of the selected IPSec connection. The page includes the same components as the **Add IPSec Connection** page. To operate with **Edit**, only one record may be selected, otherwise an error message "One row must be selected" appears.

Restart All 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 IP PBX and a peer.
- This device <>[Internet]<>Peer – connection between QX IP PBX and peer over Internet.
- This device <>NAT<>[Internet]<>Peer – connection between QX IP PBX and peer over Internet through QX IP PBX provider's NAT.
- This device <>[Internet]<>NAT<>Peer – connection between QX IP PBX and peer over Internet through peer provider's NAT.

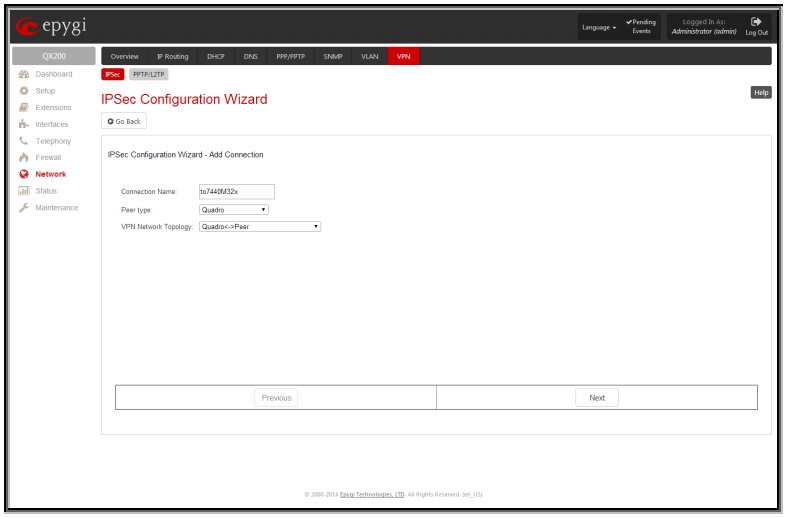


Fig.II- 224: IPSec Connection Wizard - Add IPSec Connection page

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.

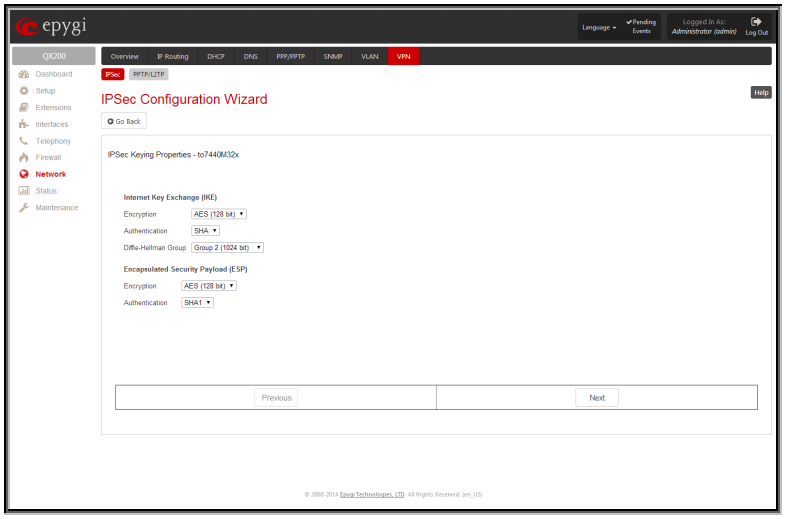


Fig.II- 225: IPSec Connection Wizard -IPSec Keying Properties page

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 IP PBX 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.

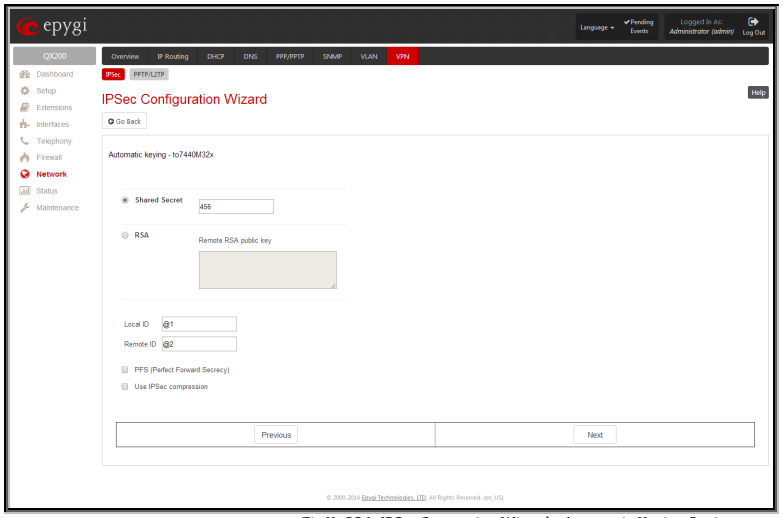


Fig.II- 226: IPSec Connection Wizard - Automatic Keying Settings page

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 IP PBX (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.

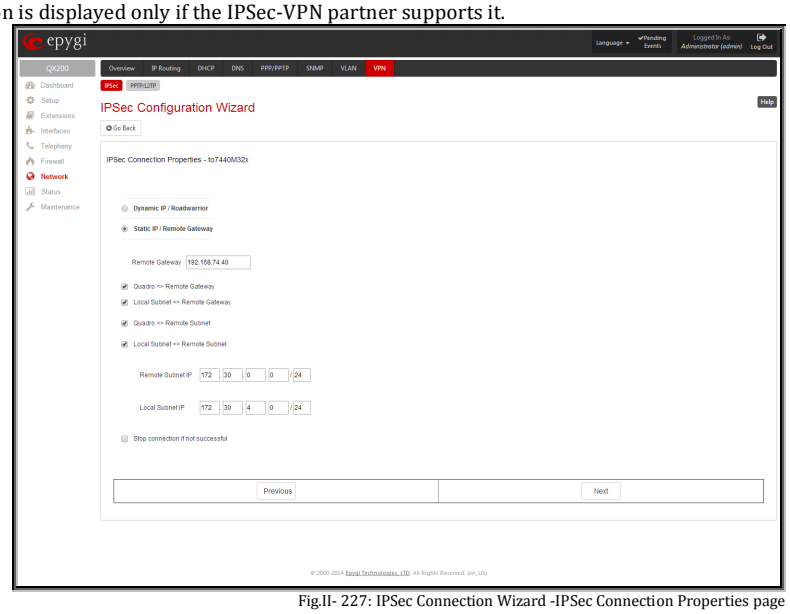


Fig.II- 227: IPSec Connection Wizard -IPSec Connection Properties page

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 IP PBX 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 IP PBX 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 IP PBX's public RSA key into an e-mail and send it to the IPSec connection partner.

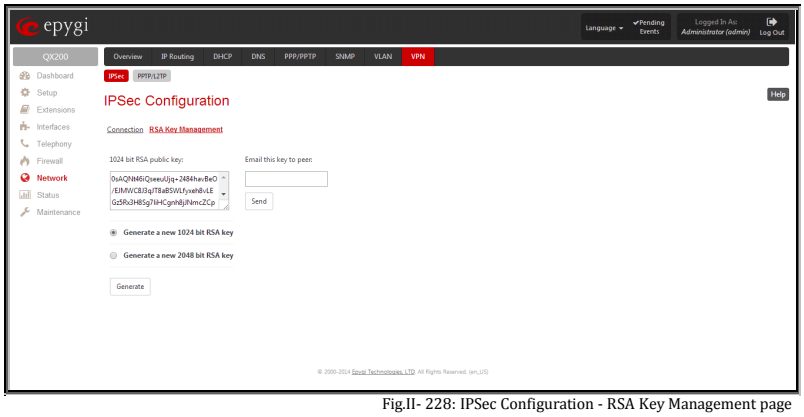


Fig.II- 228: IPSec Configuration - RSA Key Management page

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 (the QX IP PBX 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- 229: 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 IP PBX 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).

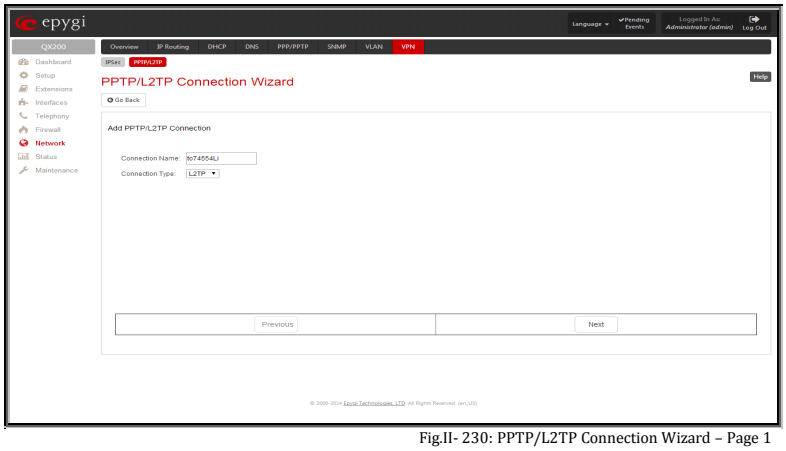


Fig.II- 230: PPTP/L2TP Connection Wizard – Page 1

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 IP PBX'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

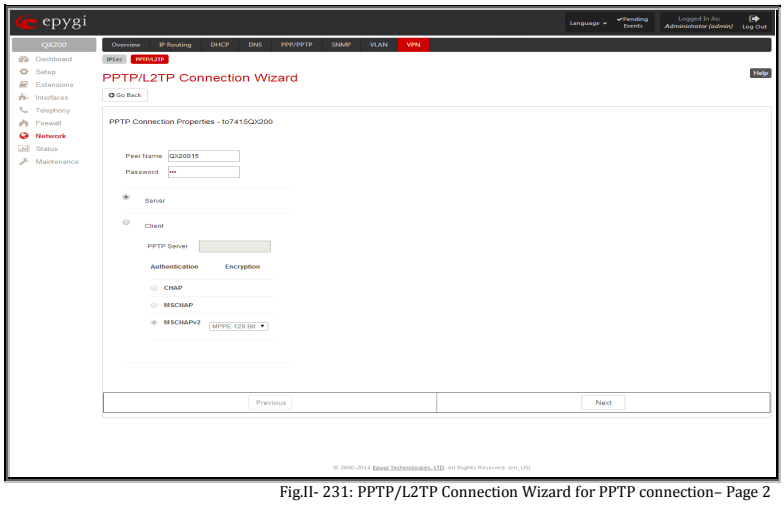


Fig.II- 231: PPTP/L2TP Connection Wizard for PPTP connection– Page 2

establishment.

The manipulation radio buttons selection on this page allows you to choose whether the new connection will be a client or a server. For the **Client** radio button selection, no further details need to be provided. For the **Server** radio button selection, the following information needs to be provided:

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.

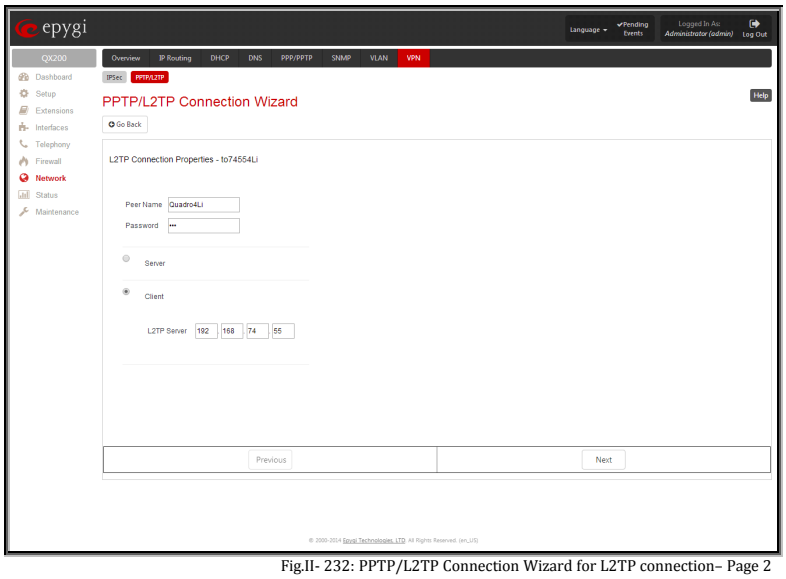


Fig.II- 232: PPTP/L2TP Connection Wizard for L2TP connection– Page 2

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.

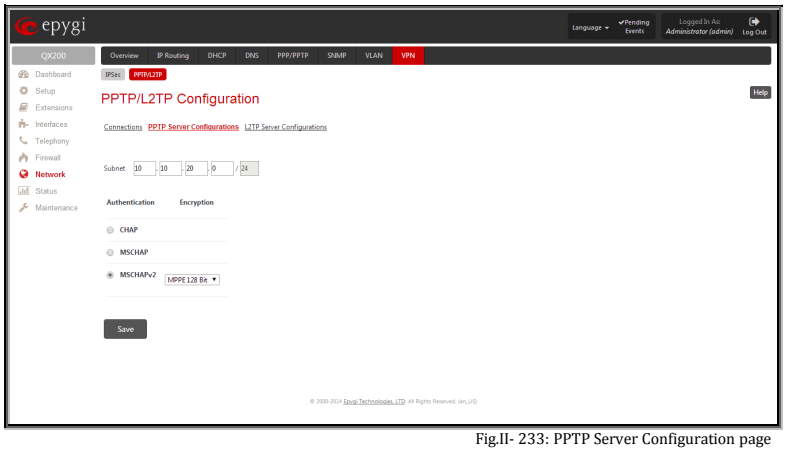


Fig.II- 233: PPTP Server Configuration page

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.

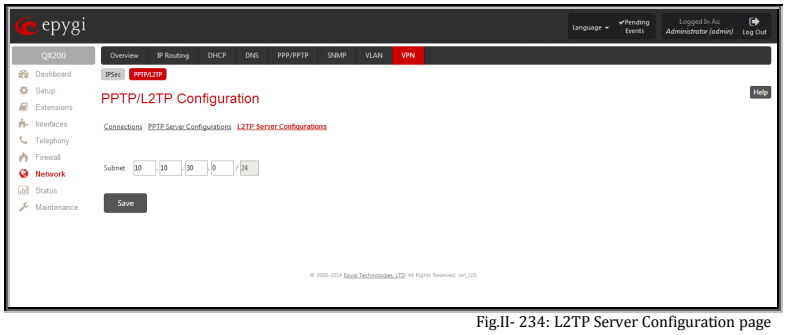


Fig.II- 234: L2TP Server Configuration page

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 **Status Menu** consists of the following sections:

- **System Status**
  - General Information
  - Network Status
  - Lines Status
  - Memory Status
  - Hardware Status
  - SIP Registration Status
  - IP Lines Registration Status
  - License Status
- **Events**
  - System Events
  - Event Settings
- **Call History**
  - Successful, Missed and Unsuccessful Calls
  - Call History Settings
  - CDR Archive
  - Archiving Settings
- **Conference History**
  - Conferences
  - Successful Calls and Unsuccessful Outgoing Calls
  - CDR Settings
- **LAN/WAN**
  - LAN and WAN Interface Statistics
- **Statistics**
  - Network Transfer
  - PSTN Channel Usage

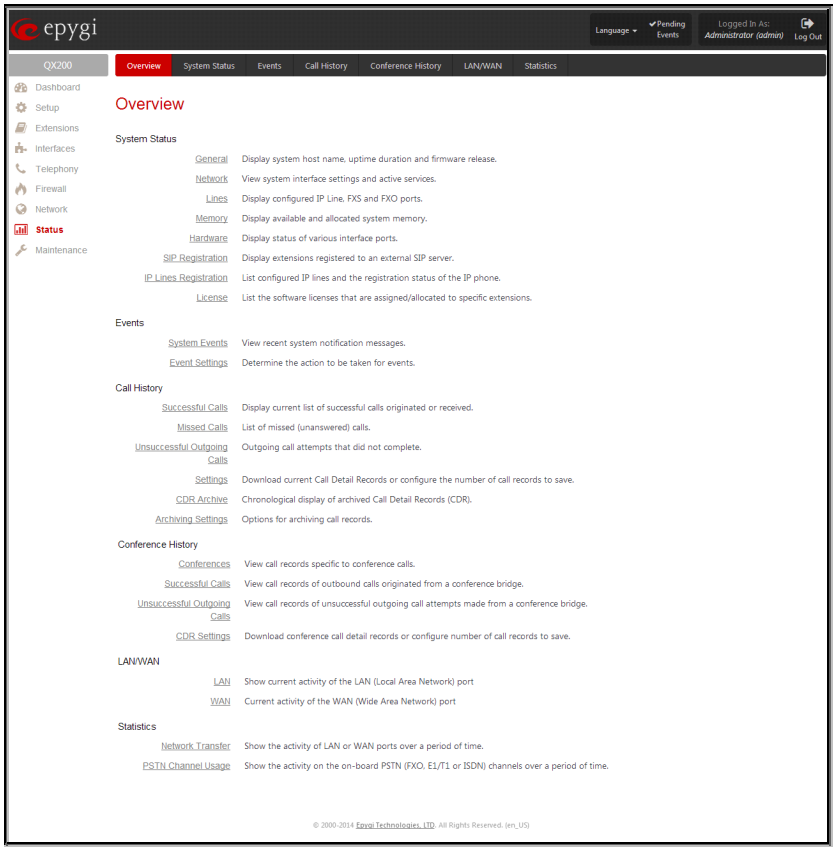


Fig.II- 235: Status Menu page

System Status

General Information

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

- **Uptime duration -** Period QX IP PBX is running since last reboot.
- **Device hostname -** QX IP PBX device host name.
- **Application Software -** Software and file system versions of the QX IP PBX.
- **Language Pack** – this field is present only when the custom language pack is uploaded and it indicates the version.

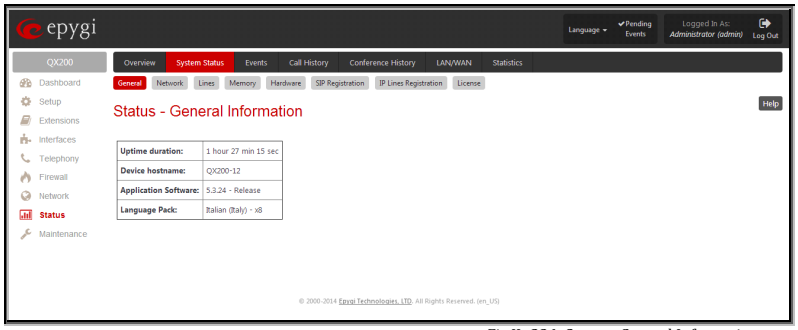


Fig.II- 236: Status - General Information page

Network Status

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

Interface Name lists the Network interfaces available on the QX IP PBX (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 IP PBX.

Monitor includes links to survey LAN, VLAN, WAN (For QX50/QX200) and PPP (for QX50/QX200) 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:

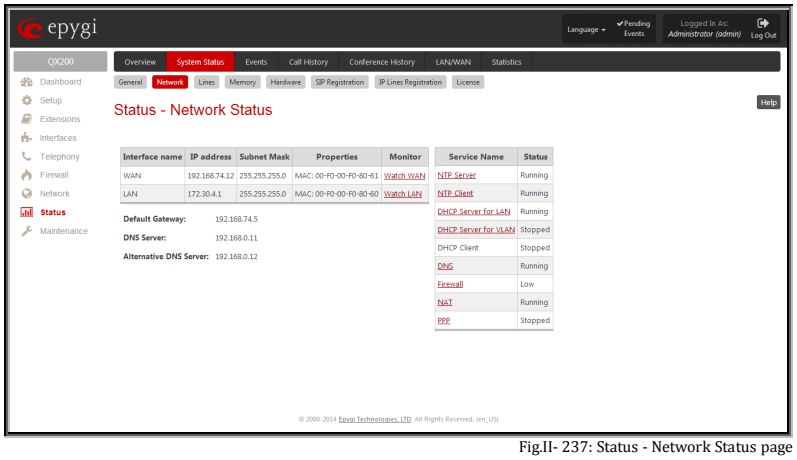


Fig.II- 237: Status - Network Status page

- 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

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 IP PBX 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 **Status** - **Lines Status** page shows the current status of each of the FXS, IP and FXO lines or shared FXO/ISDN/E1T1 lines including details of the attached extension. Since only one line of information can be displayed at a time, the **Line, IP Line** and **FXO** line, **ISDN** or **E1/T1 Trunk** functional buttons are used to navigate through the information regarding other lines.

The **Lines Status** table displayed for **FXS** and **IP** lines includes a group of static and dynamic parameters. Static parameters are always displayed. Dynamic parameters only appear when an event takes place on the extension.

Static Parameters:

Extension shows the extension number of the selected telephone line.

Display Name shows the corresponding name.

Phone State may have the value **On Hook** or **Off Hook**. For IP Line Status, this field may additionally have **Not Configured** and **Temporary Offline** values.

Number of Active Calls shows the number of calls that are currently present on the phone.

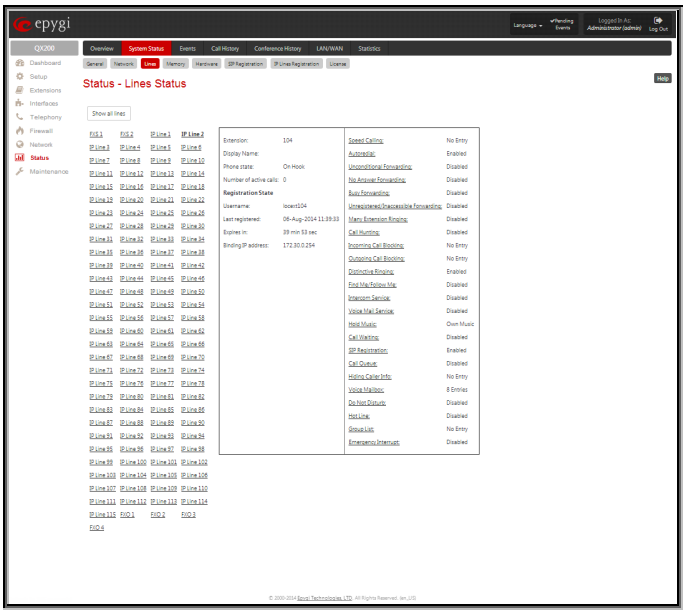


Fig.II- 238: Status - Lines Status page

Dynamic Parameters:

Call State shows the current state of the extension (in voice mail, in call, waiting, busy, call out, ring in, etc.).

Caller Party appears when a call is received and indicates the caller extension and the IP address or a phone number, depending on type of call.

Called Party appears when a call is placed and indicates the destination extension and the IP address or a phone number, depending on type of call.

Call Type shows whether the call is **Internal** or **External** and whether it is a **PSTN** call, **PBX** call or **IP** call.

Call Start Time shows the call start date and time.

Call Duration shows the current call duration.

RX Codec shows the codec used to encrypt the incoming packets. **TX Codec** shows the codec used to encrypt the outgoing packets. If RX and TX codecs are the same, only one **Codec** field will be displayed.

For IP Line Status, the following dynamical parameters appear on this page:

Username shows the IP phone's client name registered on the QX IP PBX.

Last Registered shows the date and time, the corresponding IP phone has been last registered on the QX IP PBX.

Expires In shows when the last registration of the IP phone will expire.

Binding IP Address shows the IP address of the IP phone within the QX IP PBX's LAN network.

The list of supplementary services provides the following additional status information for each telephone line: **Enabled** or **Disabled**.

For **Incoming** and **Outgoing Call Blocking**, **Speed Calling, Hiding Caller Info**, **Voice Mailbox** and **Group List** services, the number of **Entries** will be displayed in the corresponding service table. For **Voice Mail Service**, the voice mailbox configuration mode is displayed here.

This allows administrator to view the status and to be notified about services running on QX IP PBX for every line. The services are designed as links that guide the administrator to the corresponding service page of the selected user.

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

Static Parameters:

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

Dynamic Parameters:

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

The **Line Status** for shared **E1/T1 Trunk** displays the list of available timeslots (in E1 mode, 30 active timeslots both for CAS and CCS signaling types; in T1 mode, 24 timeslots for CAS signaling and 23 timeslots for CCS signaling type) and their settings (**Route Incoming Call to**, **Allowed Call Type** and **Timeslot State**). When Timeslot is in the call, information about call direction (incoming or outgoing), **Caller Party**, **Called Party** and **Call Duration** is displayed.

Memory Status

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

Memory Size shows total memory space (counted in minutes/seconds) available on the QX IP PBX 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.

CDR Archive field displays the total and used size of archived call statistics of Archiving Settings and links to it.

The **Conference Memory Status** shows total memory space (counted in minutes/seconds) available on the QX IP PBX. The table's links lead the administrator to the Conferences Management page where Total Space for the corresponding conference extension may be altered.

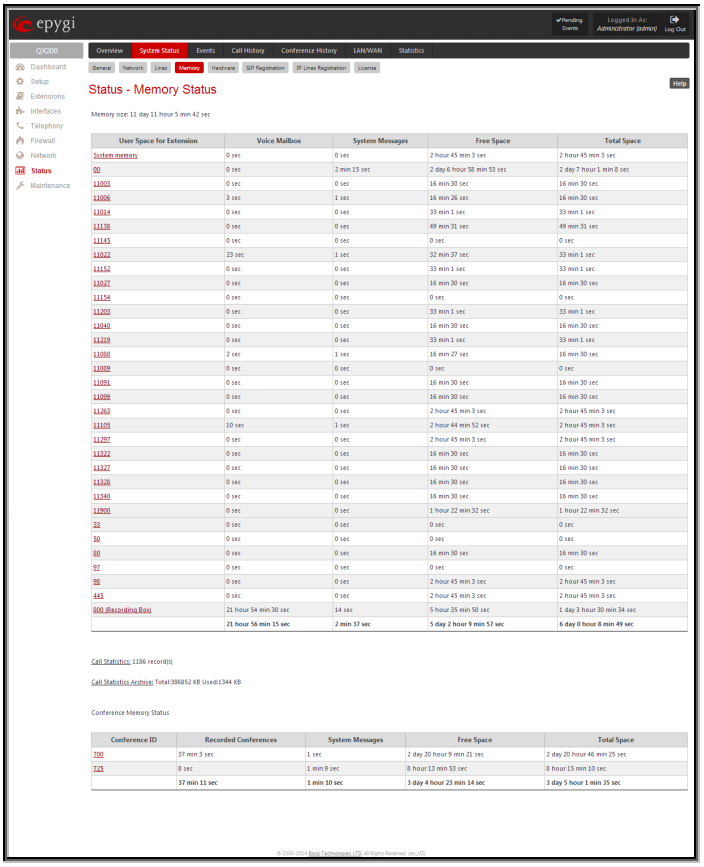


Fig.II- 239: Status - Memory Status page

Hardware Status

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

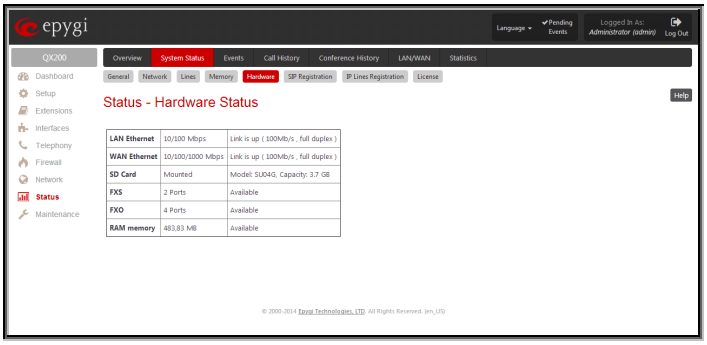


Fig.II- 240: Status -Hardware Status page

SIP Registration Status

The **SIP Registration Status** is a table displaying the SIP registration information of the QX IP PBX extensions.

The table contains a list of all the registered extensions of the QX IP PBX , 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 **Detected Connection Type** field displays the connection type QX IP PBX currently is acting in (direct connection or behind NAT). If QX IP PBX is acting behind NAT, the NAT machine IP address is also displayed.

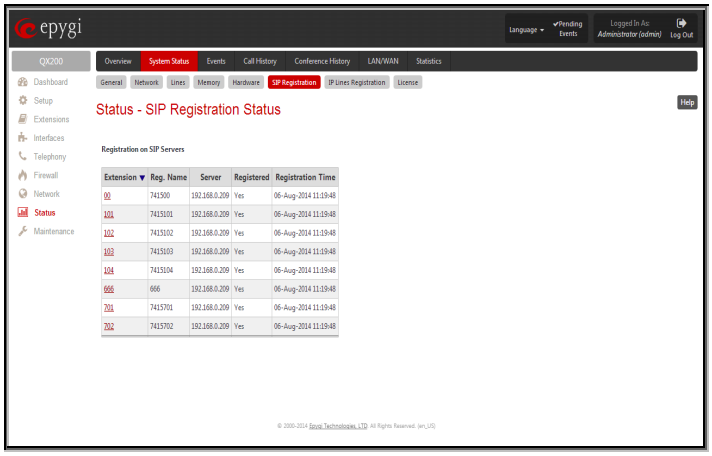


Fig.II- 241: Status -SIP Registration Status page

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

IP Lines Registration Status

The **IP Lines Registration Status** displays a table with the IP Lines registration information on the QX IP PBX.

The table lists the IP lines and remote extensions registered on the QX IP PBX. The table indicates the actual IP addresses of the remote devices, the usernames by which the devices have been registered on the QX IP PBX, as well as the registration status information.

Subscription Count field indicates used and allowed number of subscriptions for all IP phones registered on the QX IP PBX. Subscriptions are events originated by IP phones when watching other extensions on the QX IP PBX and when monitoring voice mailbox for new received voice mails.

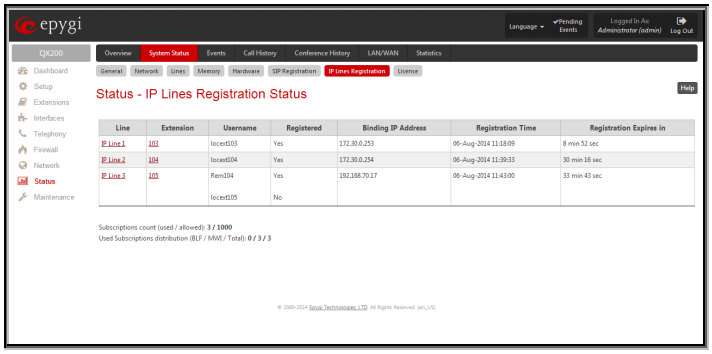


Fig.II- 242: Status –IP Lines Registration Status page

When the allowed number of subscriptions is reached, no new subscriptions are possible. Typically the number of subscription should be keep reasonably below the maximum allowed number, to avoid losing subscriptions. Thus, in case the actual subscription number is close to the limit, configuration of IP phones should be adjusted to decrease the number of total subscriptions on the QX IP PBX.

Used Subscription Distribution field indicates IP phone's subscriptions distribution among BLF (Busy Lamp Field) subscriptions, which are used for watching extensions on IP phones, and MWI (Message Waiting Indication) subscriptions, which are used for voice mailbox status indication on the phone.

License Status

The **License Status** page displays a table with all available licenses on the QX IP PBX and the corresponding settings for each license. (Currently only iQall and DCC Pro/Basic Level license statuses are displayed.)

This page includes the following information:

Type indicates the type of the license available on the QX IP PBX.

Count indicates the number of the corresponding licenses available on the QX IP PBX.

In Use indicates the number of used licensed from the total available licenses.

Extension lists the extensions that are using the corresponding license. Links in this column move to the corresponding service configuration page for the extension.

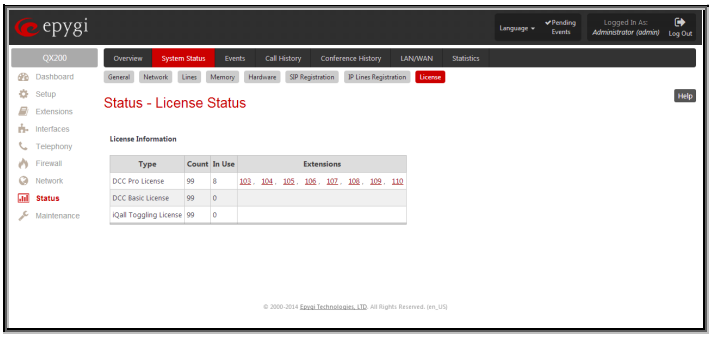


Fig.II- 243: Status -License Status page

Events

System Events

The **System Events** page lists information about system events that have occurred on QX IP PBX. 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 (available only for QX50/QX200) 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:

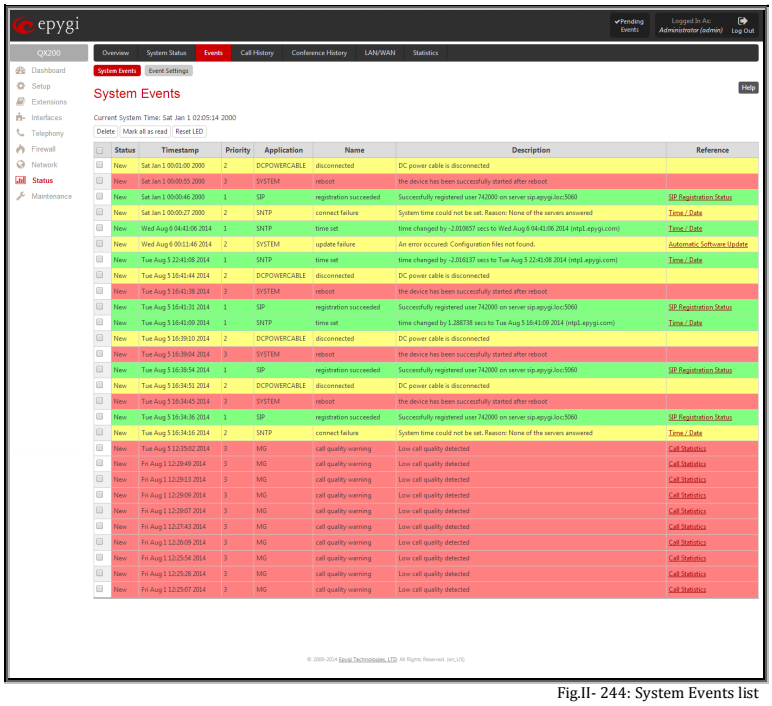


Fig.II- 244: System Events list

Current System Time displays the local date and time on QX IP PBX.

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 IP PBX to flag an event.

Event Settings

The **Event Settings** page lists all possible events on the QX IP PBX 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.

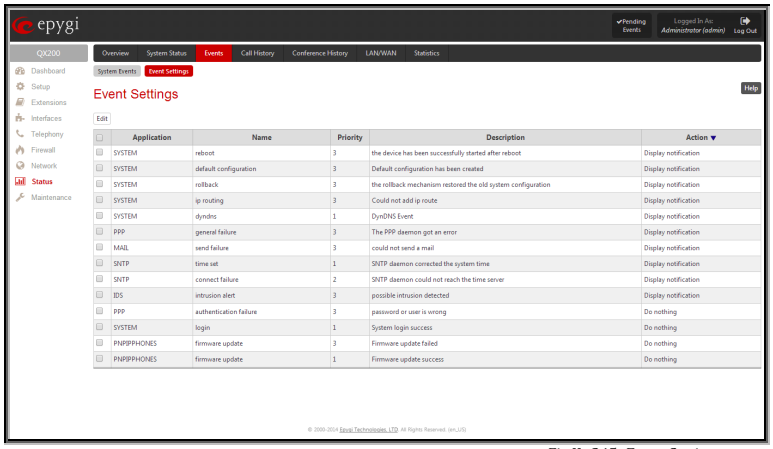


Fig.II- 245: Event Settings page

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 IP PBX administrator when an event(s) takes place. The following actions can be available:

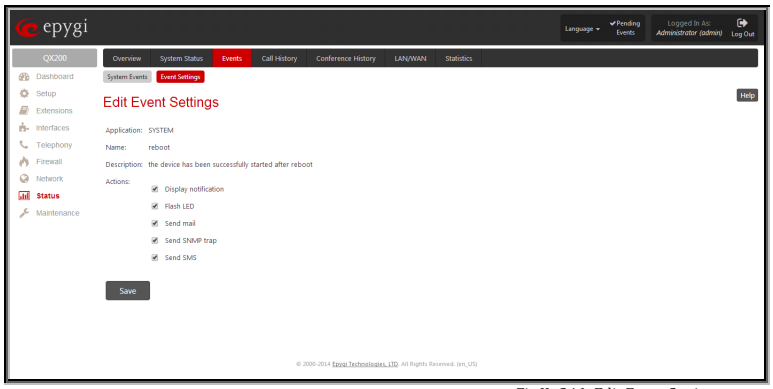


Fig.II- 246: Edit Event Settings page

- **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** (available only for QX50/QX200) - 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 e-mail notification about the new event on the QX IP PBX 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 about the new event on the QX IP PBX 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 IP PBX 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 IP PBX 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 **Go Back** button to abort the selected action.

Call History

The **Call History** page provides information on Successful, Missed, Unsuccessful Outgoing Calls, Call History Settings, CDR Archive and Archiving Settings. Call History allows the collecting of call events on the QX IP PBX 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.
- 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.

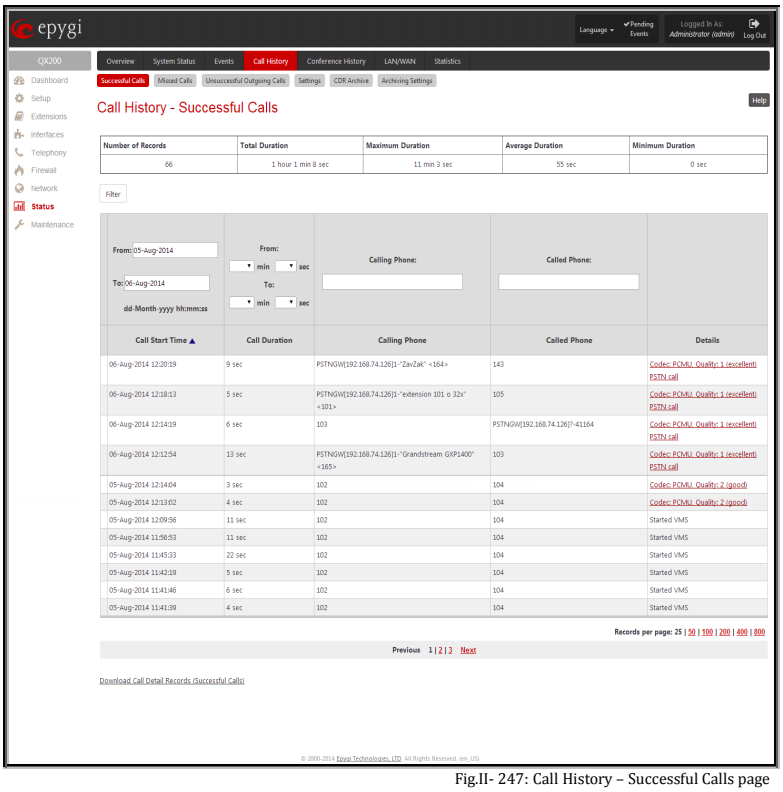


Fig.II- 247: Call History – Successful Calls page

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 IP PBX 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.

Call History 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.

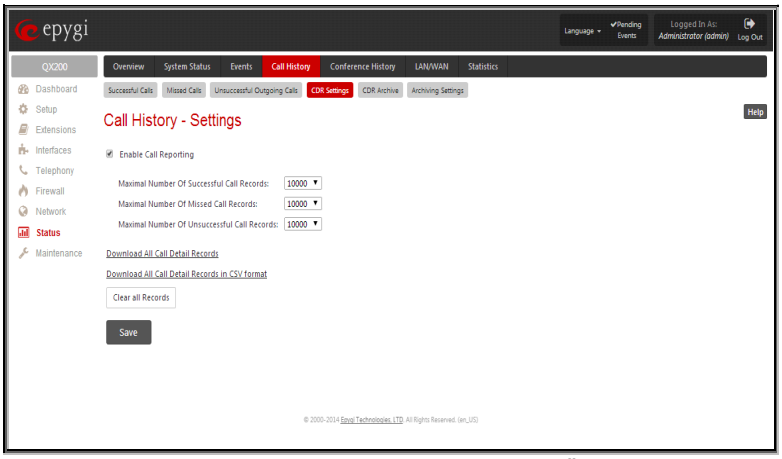


Fig.II- 248: Call History – CDR Settings page

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

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 Archiving Settings service of the Call History.

CDR Archive

In the table on this page all available Call History archived files are listed.

The **Archive Record** field shows the time when the Call History was archived.

The **[csv]** and **[log]** links in this field allows you to download the archived Call History file to the PC in a Comma Separated Values (.csv) or Tab Delimited Text (.log) file formats and opens the file-chooser window where the saving location can be specified.

The **Number of Call Records** field shows the number of records in particular Call History archive file.

The **External Backup Status** shows the status of the backup.

The following functional buttons are available on this page:

- **Delete** removes the selected record(s) from the system and **Call Statistics Archive** table.
- The **Clear all Records** button is used to clear all statistics records.

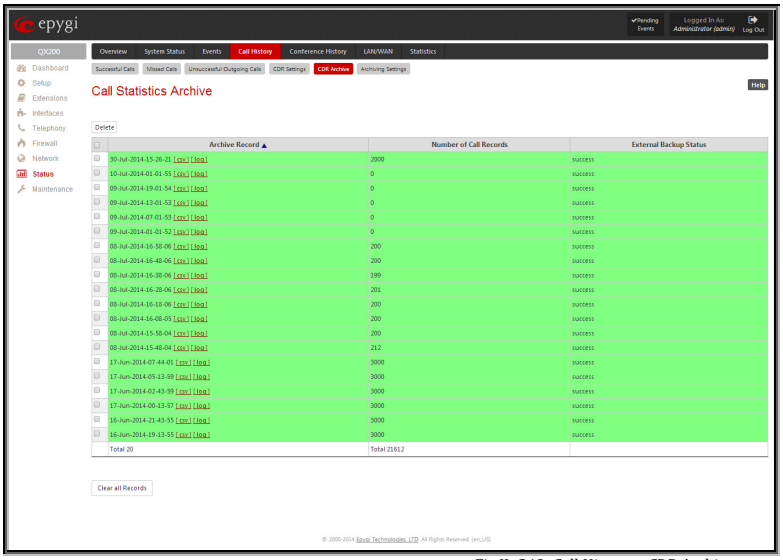


Fig.II- 249: Call History – CDR Archive page

Archiving Settings

The **Archiving Settings** page is used to configure the automatic archiving of the Call History.

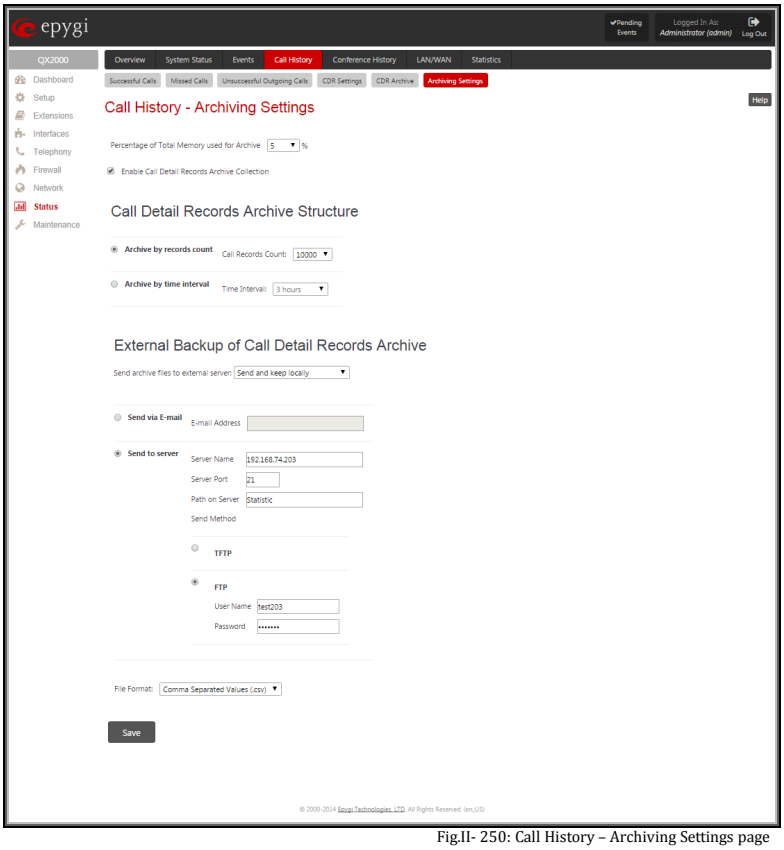


Fig.II- 250: Call History – Archiving Settings page

The **Percentage of Total Memory used for Archive** drop-down list is used to select the internal memory space (in percents) that can be used for storing the archived Call History. When the required memory exceeds the size entered, the oldest entries are being automatically deleted.

The **Enable Call Detail Records Archive Collection** checkbox enables automatic downloading mechanism of the Call History.
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 **Call Detail Records Archive Structure** is used to configure the intervals for archiving the Call History. The archiving structure allows to archive the Call History either by time intervals or per statistics record count:

The **Call Records Count** drop down list is used to select the portion size of the Call History (including all types of call statistic, i.e. successful, missed and unsuccessful outgoing Call History) which will be archived locally. The number selected in this drop down list indicates the number of entries in the single archived Call History file. If there are no enough entries in the Call History table on the QX IP PBX, the system will wait until the necessary number of entries will be collected and then will archive the statistics file.

The **Time Interval** drop down list is used to select the time interval by which the Call History will be archived locally. After each time interval the system will archive the Call History (including all types of call statistic, i.e. successful, missed and unsuccessful outgoing Call History). If there are no any record made during last time interval the black file is archived.

The **External Backup of Call Detail Records Archive** is used for configuring the Call History backup service.

The **Send archive files to external server** is used to enable/disable the backup service and configuring whether the statistics should be kept locally after backing up them.

Two options of the Call History backup are available: uploading the Call History file to the server or sending it to the mailing address.

The following group of manipulation radio buttons allows you to select whether the Call History 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 History files via email. The selection enables **Email Address** text field that requires the email address of the administrating person to receive the Call History files.
- The **Send to Server** radio button is used to store the Call History files on a remote server. This selection enables the following fields to be inserted:
  - The **Server Name** requires the IP address or the host name of the remote server.
  - The **Server Port** requires the port number of the remote server.
  - The **Path on Server** requires the path on the server to store the Call History files in.

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

The **File Format** drop down list is used to select the format in which Call History will be saved. This list offers to choose between Tab Delimited Text (.log) and Comma Separated Values (.csv) file formats.

To Enable/Disable the Call History

1. Enter the **Call History 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 **Call History 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 IP PBX 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 IP PBX's IP line to an external SIP destination or from one external SIP destination to another through the QX IP PBX'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 IP PBX and the other leg describes the RTP stream from QX IP PBX 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

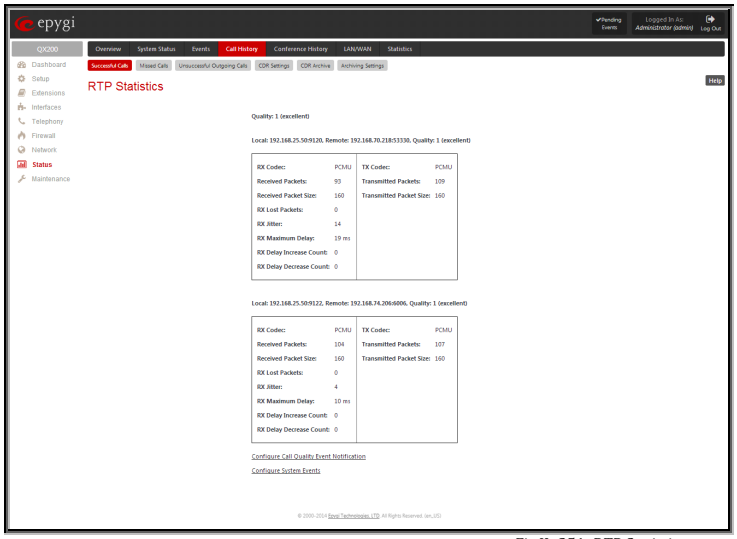


Fig.II- 251: RTP Statistics page

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 IP PBX. 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 IP PBX'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 IP PBX'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.

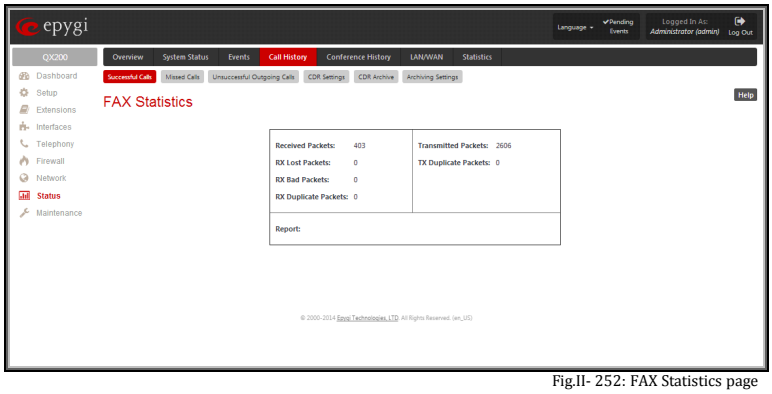


Fig.II- 252: FAX Statistics page

Conference History

In the **Conference History** page, the calls are classified by conferences. The Conference Call History (sent via 3PCC, Radius, email or FTP) is the same as is - it shows only the PBX calls not sorted out by the conference.

The **Conference History** page consists of four tables. They provide information on Conferencess, Successful, Unsuccessful Outgoing Conference Calls and CDR Settings. Conference History allows the collecting of conference call events on the QX IP PBX with their parameters and to search them by various criteria. Only the administrator is allowed to enable or disable the conference statistic services.

Conferences

The **Conferences** page lists all Conference Calls and their parameters (**ConfID- Activation Time**, **Conference Duration**, **Participant Count**, **Activation Reason** and **Activation Details**). 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 **Activation Reason** column indicates whether the participant is a key member to start the conference, i.e. when participant dials into the conference, the conference is getting automatically activated and the dial out participants (if any) are called to join the conference (see Conference Progress).

The **Activation Details** column provides information about how the conference call is activated.

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:

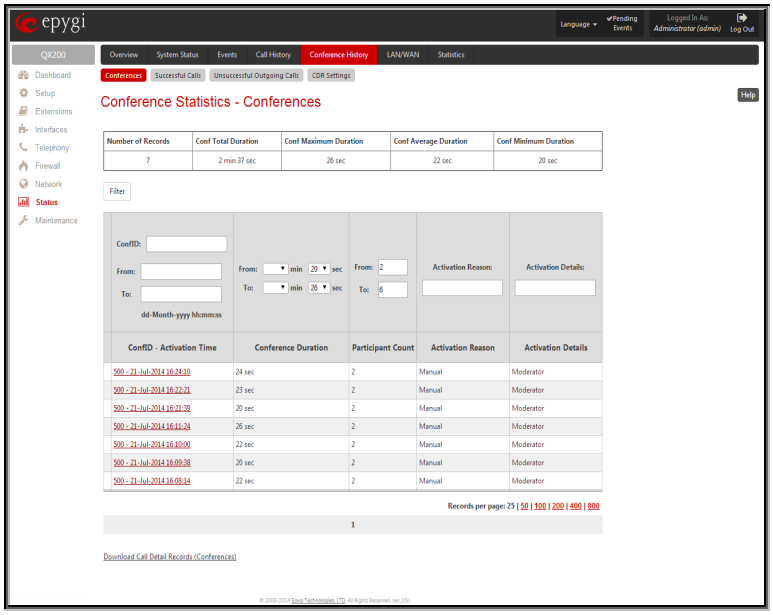


Fig.II- 253: Conference History-Conferences page

- The text fields **ConfID**, **From** and **To** are used for the search by **ConfID-Activation Time**. **ConfID** requires the unique ID of the conference. For **From** and **To** fields 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 **Conference 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.
- The **From** and **To** drop down lists offer a search by the **Participant Count**, specified by the list of values. The field **From** must indicate a shorter count than the field **To**. Otherwise the error message "Minimal count should be less than maximal count" prevents statistics filtering.
- The text fields **Activation Reason** and **Activation Details** require the reason and the details of the conference call activation to be defined.

Number of Records displays the current amount of conference Call History entries in the table. For **Conferences** and **Successful Calls** pages **Total Duration**, **Maximum Duration**, **Conf Average Duration** and **Minimum Duration** statistics are organized at the top of the table.
The **Records per page** are used to select the number of displayed conference call statistic records per page. The **Previous** and **Next** can be utilized to switch between these pages.
The **Download Call Detail Records (Conferences)** links are available below for all Conference Call History tables and allows you to download the displayed conference Call History in a text file.

Successful Calls and Unsuccessful Outgoing Calls

The pages **Successful Calls** and **Unsuccessful Outgoing Calls** lists successful and unsuccessful outgoing calls and their parameters (**ConfID- Activation Time**, **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 **Details** column is only present in **Successful Calls** table and provides the following information:

- Brief information about the call quality, voice codec used to receive and transmit packets and the close conference call reason. The close conference call reason appears to provide more information about the call termination reason which can be a network problem, termination by one of the conference call parties, voice mail service activation, etc. Clicking on the details information will open the RTP Statistics page where all RTP parameters of established conference call are provided.
- **Authenticated By** information details the conference participants that passed an authentication on the QX IP PBX as configured in the Local AAA Table.

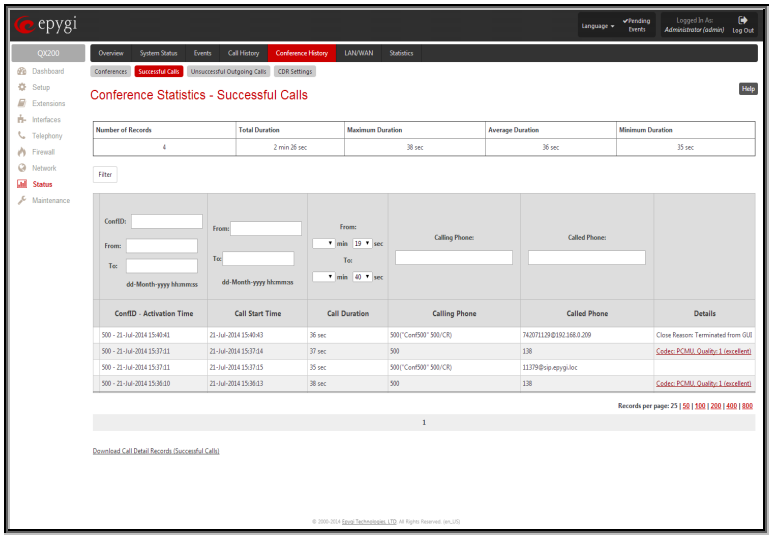


Fig.II- 254: Conference History-Successful Calls page

The **Call Detail** column is present only in the **Unsuccessful Outgoing Calls** table and indicates the reason why the call was unsuccessful.
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 **ConfID**, **From** and **To** are used for the search by **ConfID- Activation Time**. **ConfID** requires the unique ID of the conference. For **From** and **To** fields 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 text fields **From** and **To** drop down lists offer a search by the **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.
- The text fields **Calling Phone** and **Called Phone** require the calling and called conference party's SIP address, extension number or PSTN number as search criterion. Wildcard symbols are allowed here.

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 Conference Call History tables and allows you to download the displayed Call History in a text file.

CDR Settings

The **CDR Settings** page is only displayed when an administrator is logged in. The conference **CDR Settings** page offers the following input options:

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

The **Maximal Number of Displayed Conference Call Records** drop down lists are used to select the number of Conference Call, Successful and Unsuccessful statistics entries to be displayed in the corresponding Conference 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 conference Call History file is easy-to-read and can be displayed in a spreadsheet.

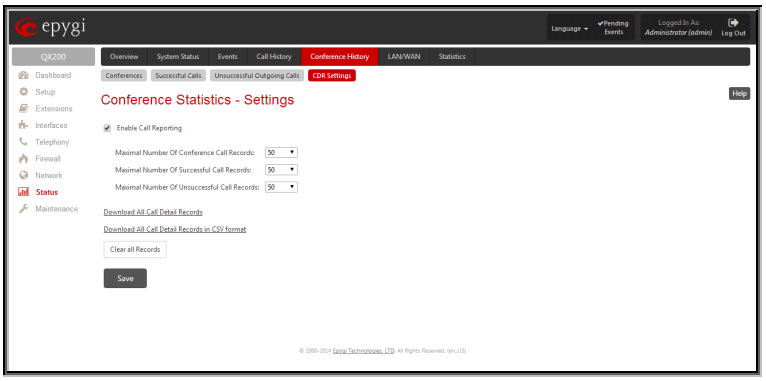


Fig.II- 255: Conference History - CDR Settings page

The **Download All Call Detail Records (CSV format)** link is used to download the entire displayed conference Call History in a CSV (Comma-Separated Values) formatted file.
The **Clear all Records** button is used to clear all conference Call History records.
When the number of Conference Call History entries exceeds the numbers specified in the **CDR Settings** page, the oldest entries are being automatically deleted.

LAN/WAN

LAN and WAN Interface Statistics

The LAN and WAN Interface Statistics pages display the LAN and WAN statistics (LAN Interface Statistics page is not available for Qx2000). 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.

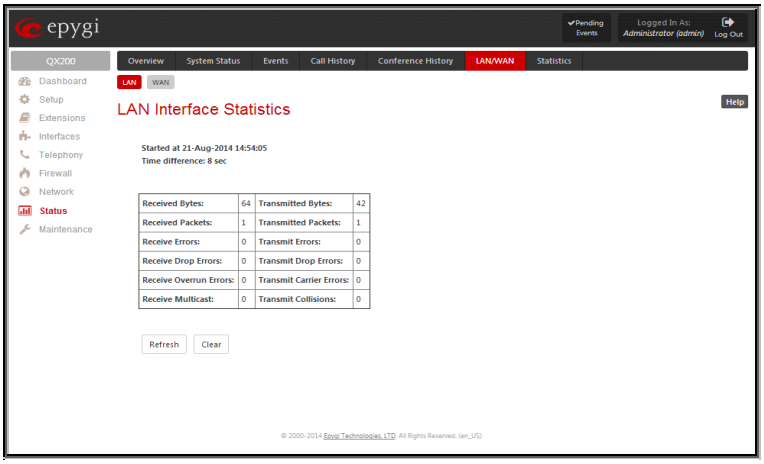


Fig.II- 256: lAN Interface Statistics page

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.

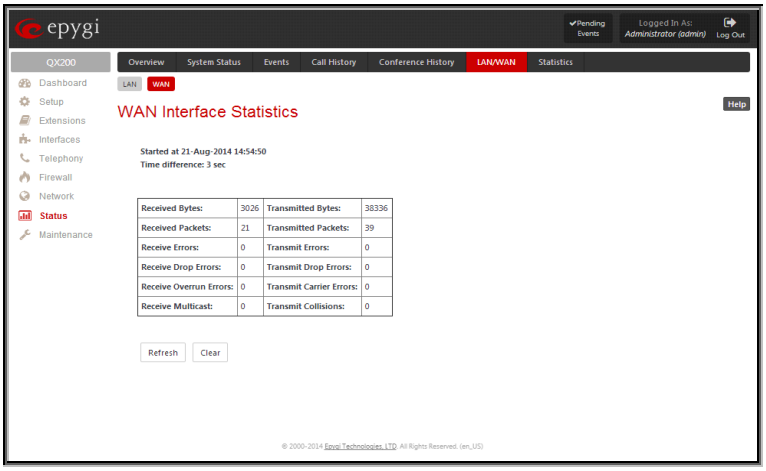


Fig.II- 257: WAN Interface Statistics page

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 drop-down list (available only for QX50/QX200) 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.

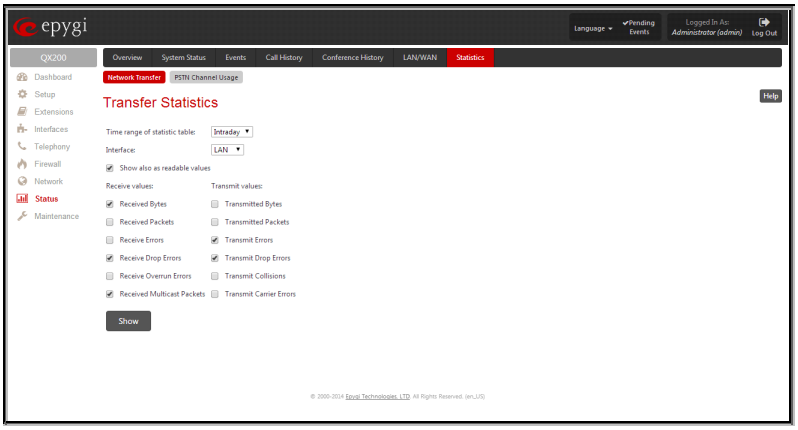


Fig.II- 258: Transfer Statistics page

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

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

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

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

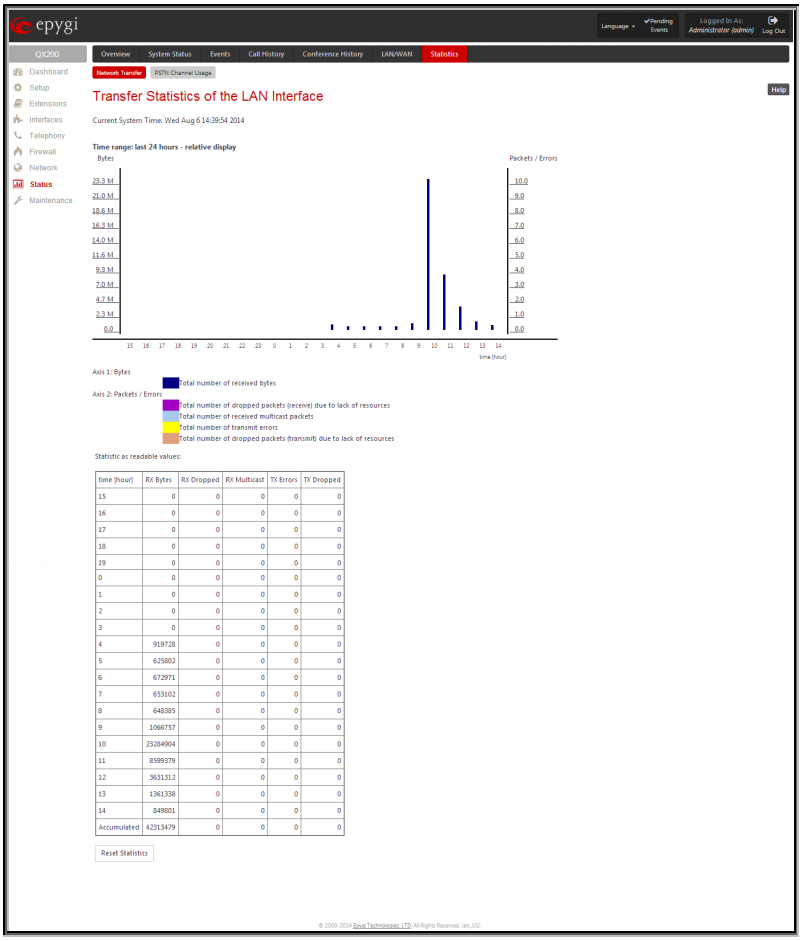


Fig.II- 259: Transfer Statistics Diagram Chart

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 traffic chart will be built. At least one **Trunk** checkbox should be selected, otherwise error message appears.

Please Note: The **PSTN Channel Usage** page is not available for QX2000.

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

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

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

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

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

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

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

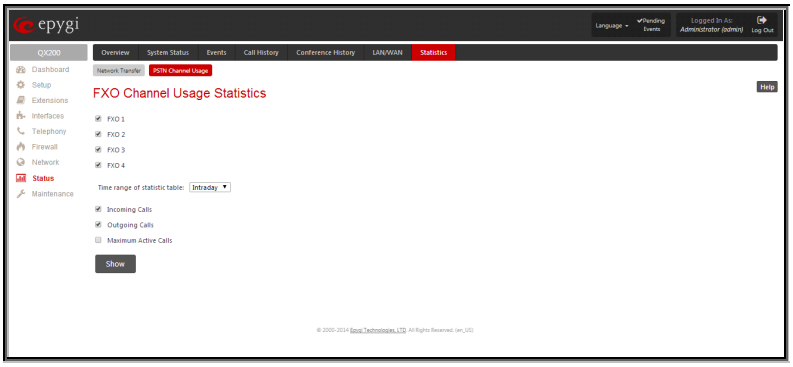


Fig.II- 260: FXO Channel Usage Statistics page

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

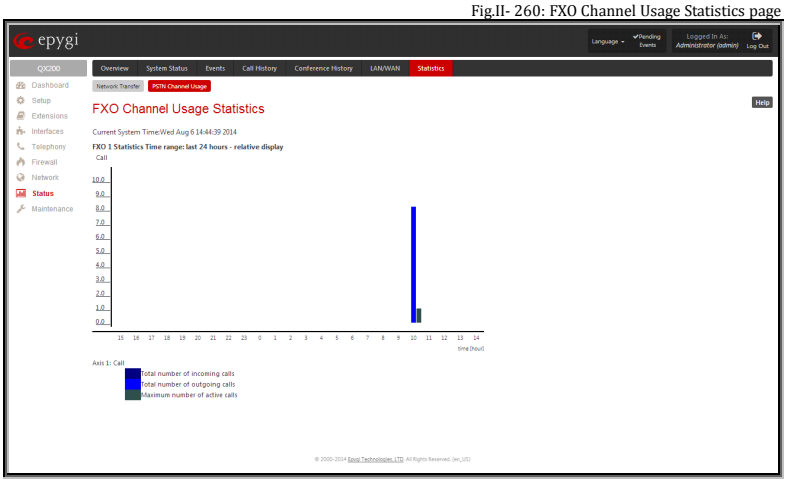


Fig.II- 261: FXO Channel Usage Statistics page

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
  - Logs Archive
- **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**

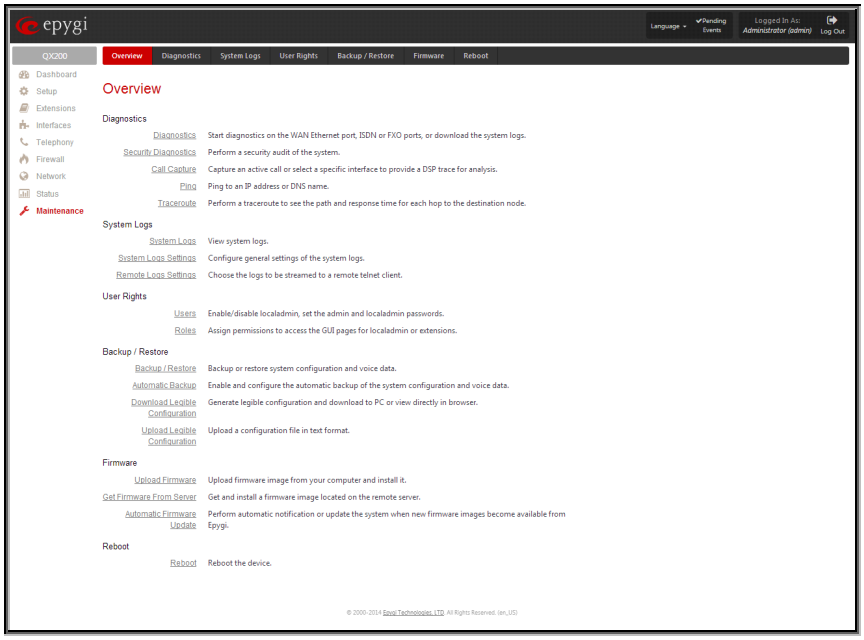


Fig.II- 262: Maintenance Menu page

Diagnostics

The **Diagnostics** page gives a possibility of running Network protocol diagnostics to verify QX IP PBX'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 QX50/QX200) 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 **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 IP PBX.

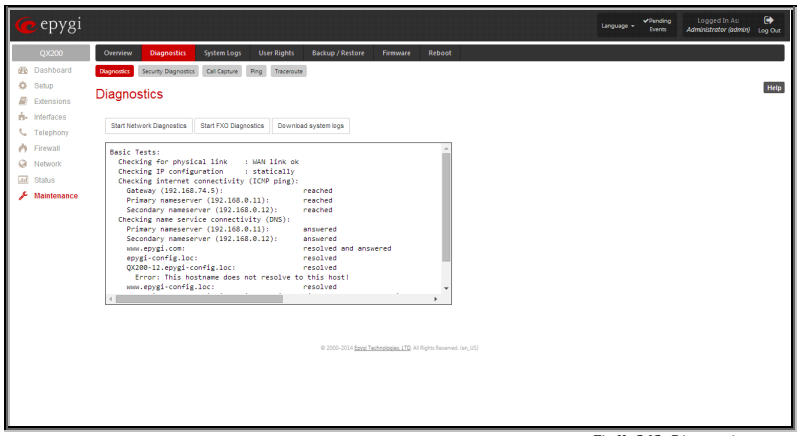


Fig.II- 263: Diagnostics page

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 IP PBX Security Audit is a security reporting system, which generates the warnings regarding the QX IP PBX'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, IP Line passwords, Call Routing and extension settings.

The output of Security Audit may look as follows:

Start security audit ...

Checking ...
Firewall ... done
IP Lines ... 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.

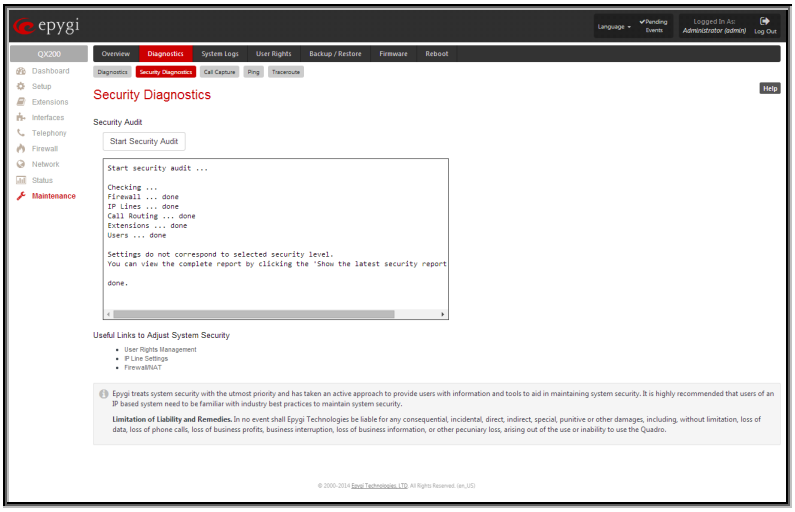


Fig.II- 264: Security Diagnostics page

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
- IP Line Settings
- 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 IP PBX (FXS and FXO). This page consists of two sub-pages:

The **Active Calls** sub-page lists all FXO/FXS active calls on the QX IP PBX 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.

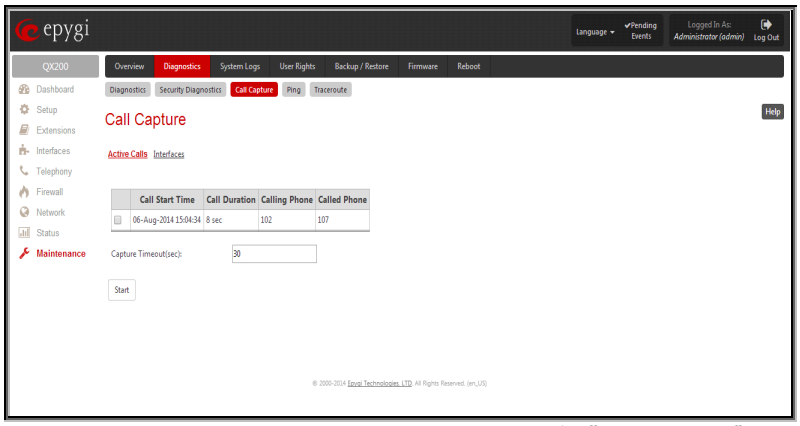


Fig.II- 265: Call Capture – Active Calls page

The **Interfaces** sub-page lists all available interfaces on the QX IP PBX. 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.

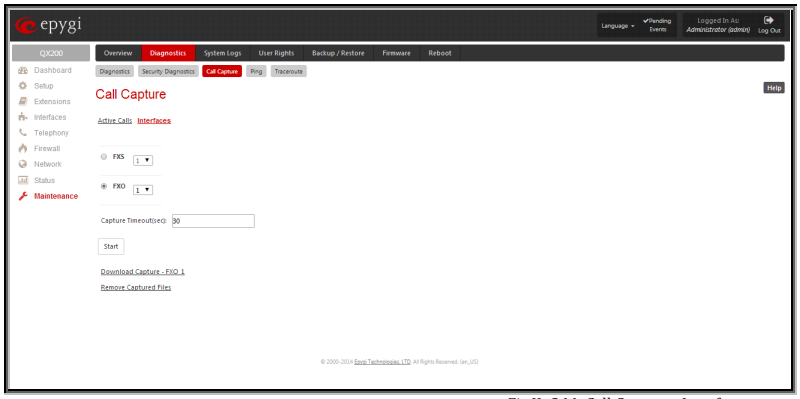


Fig.II- 266: Call Capture - Interfaces page

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.

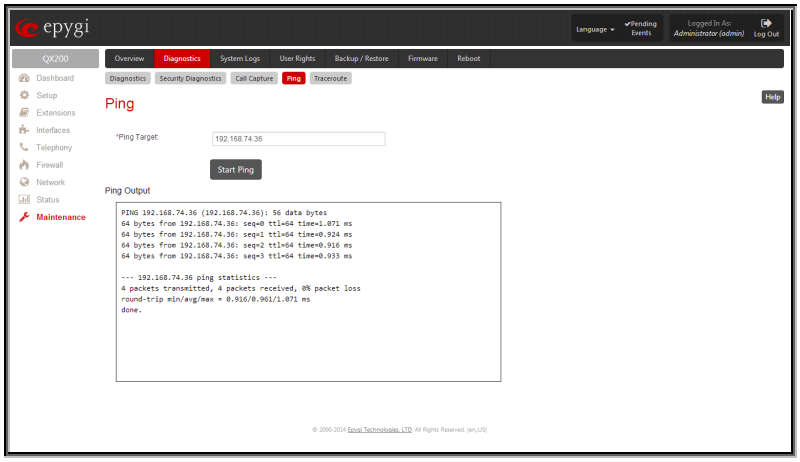


Fig.II- 267: System Diagnostic - Ping page

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.

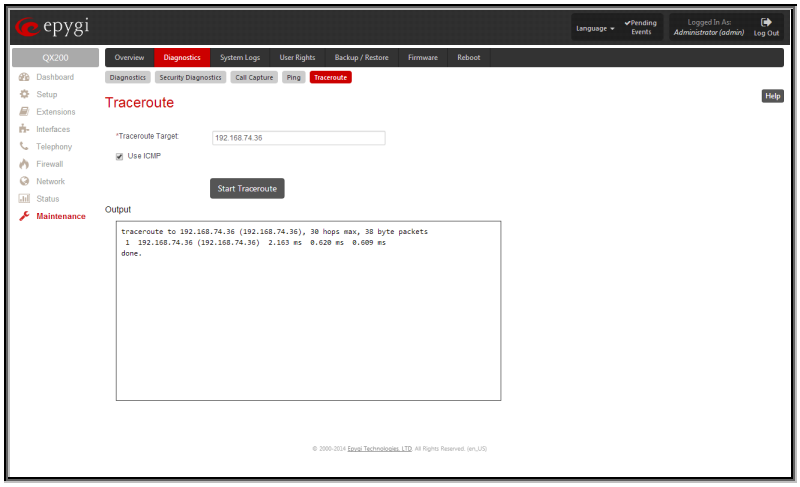


Fig.II- 268: Diagnostics – Traceroute page

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 IP PBX. System logs are useful to determine any king of problems on the QX IP PBX 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 IP PBX) 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.

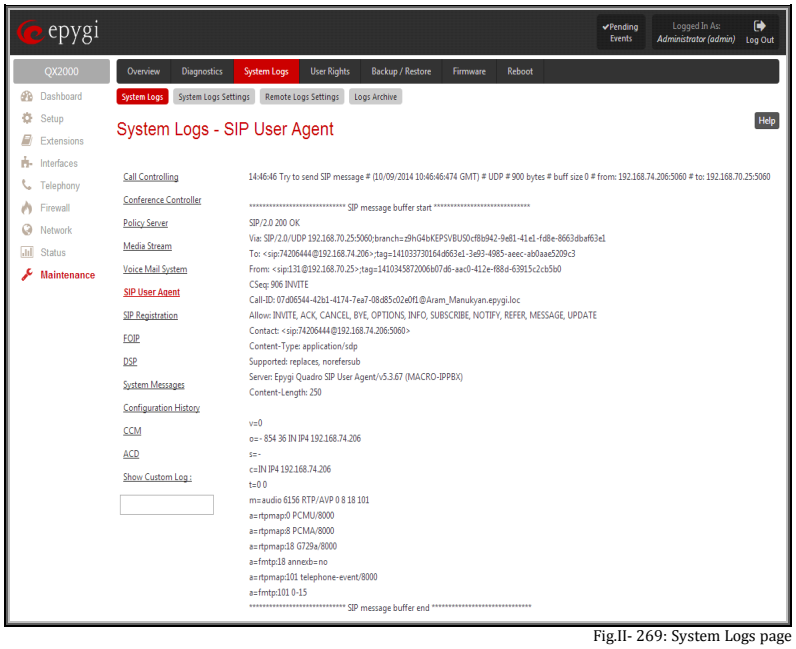


Fig.II- 269: System Logs page

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 IP PBX.

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

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 IP PBX. 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 IP PBX. 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 IP PBX.

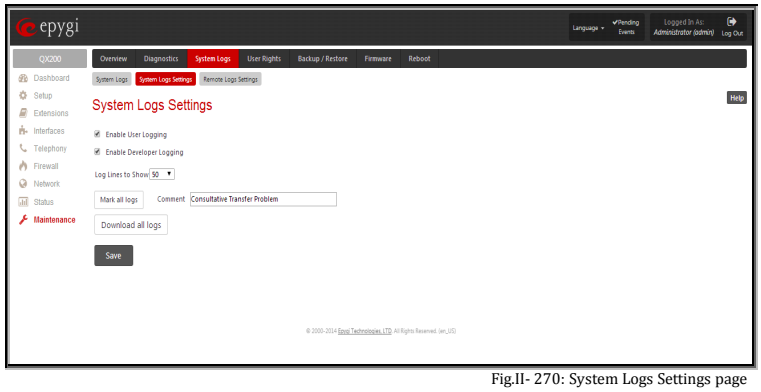


Fig.II- 270: System Logs Settings page

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 IP PBX's logs. When this option is selected, remote administrators may connect QX IP PBX with Telnet protocol (port number 645) and access the logs selected on this page. This is done for remote QX IP PBX's diagnostics and is mainly used by Epygi's Technical Support Office. To make the QX IP PBX'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.

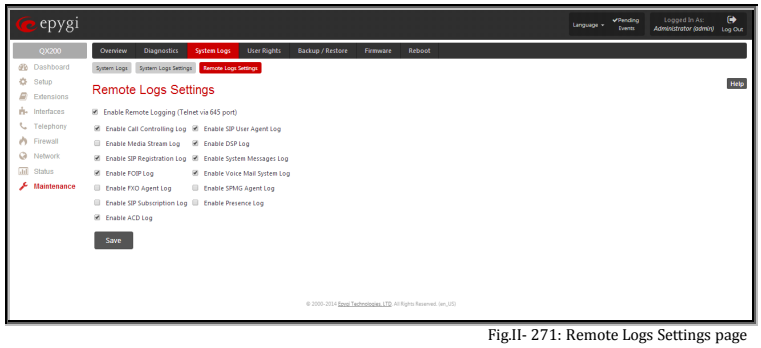


Fig.II- 271: Remote Logs Settings page

Logs Archive

The **System Logs Archive** page (available only for QX2000) shows the archived logs table with time period by **Date**. Clicking on the corresponding date will open the archived system logs table in hourly basis. **Hour** shows the initiation time of the system logs. This could be used to collect the logs at the exact moment when a problem has happened. The **Unpacked size on disk** shows the system logs size on disk for the corresponding **Date** and **Hour**.

The following functional buttons are available on this page:

Download link is used to download the archived system logs file to the PC and opens the file-chooser window where the saving location can be specified.

Delete removes the selected entry from the archived system logs table.

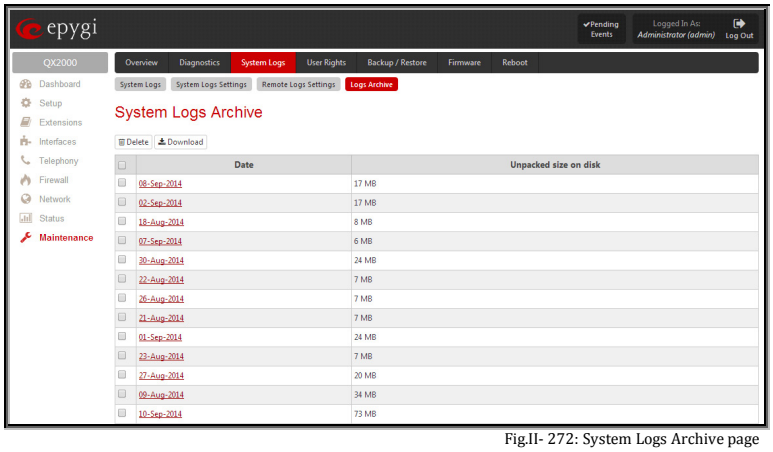


Fig.II- 272: System Logs Archive page

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 IP PBX. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the QX IP PBX's configuration. The **User Rights Management** page consists of two pages. The Users page is used to manage the available users on the QX IP PBX. 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 IP PBX 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 IP PBX. 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.

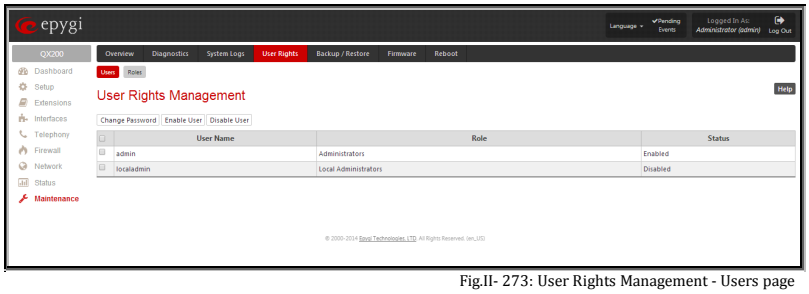


Fig.II- 273: User Rights Management - Users page

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.

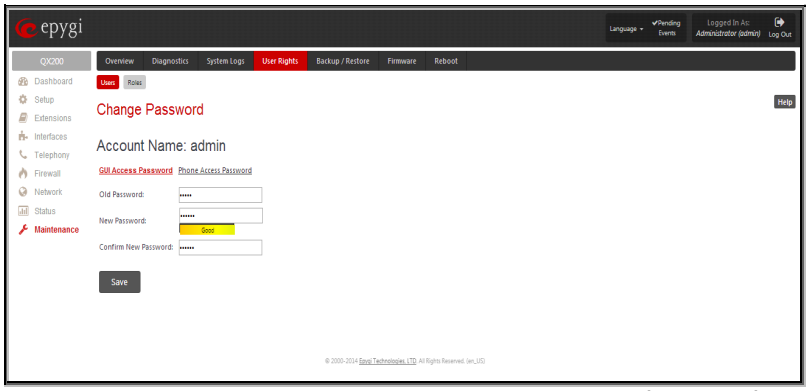


Fig.II- 274: Change Password page

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.

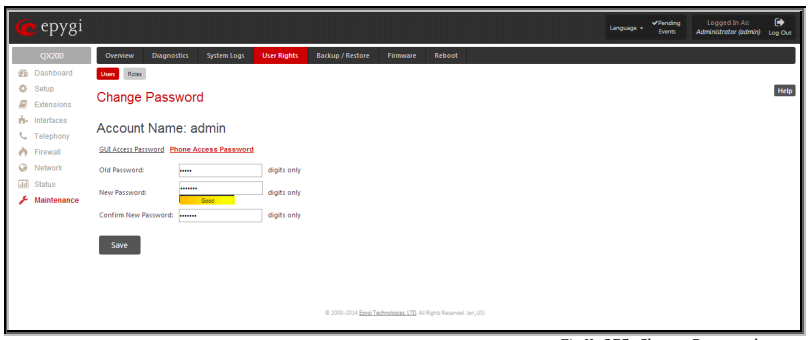


Fig.II- 275: Change Password page

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 IP PBX'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- 276: 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.

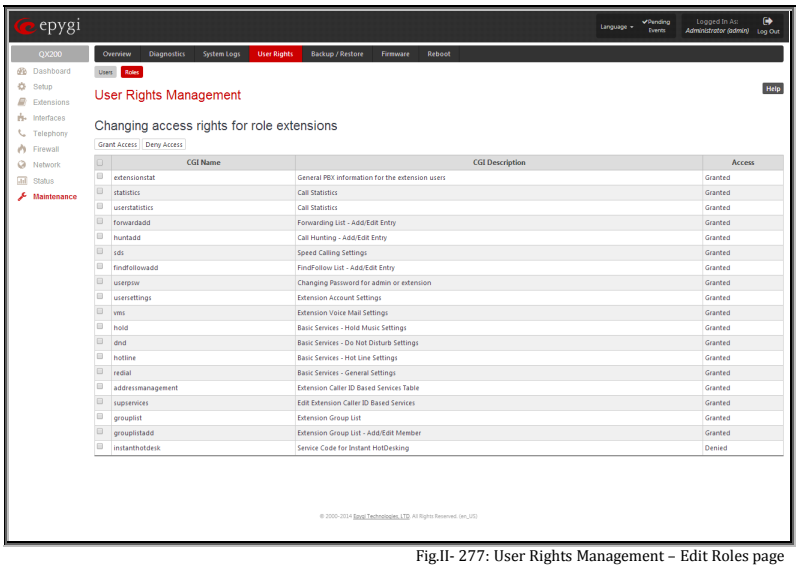


Fig.II- 277: User Rights Management – Edit Roles page

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 IP PBX. 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 IP PBX's configuration. A warning message will ask you to confirm your selection before restoring the default

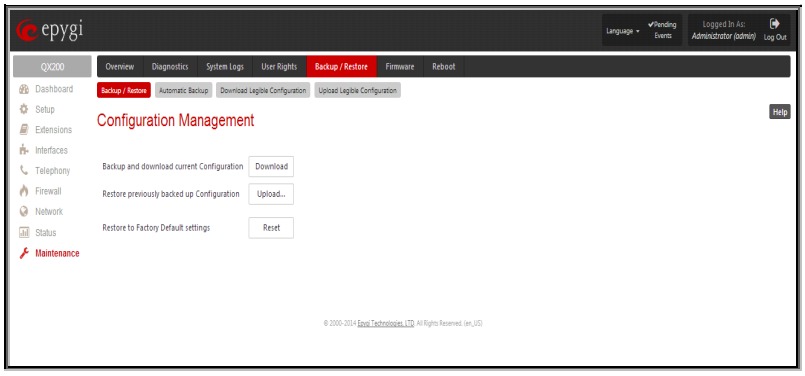


Fig.II- 278: Configuration Management page

configuration.

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

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

Automatic Backup

The **Automatic Backup** page allows you to enable the automatic backup of the system configuration and the voice data on the QX IP PBX. With this service, QX IP PBX will automatically backup the system configuration and the voice data and store it in the specified location.

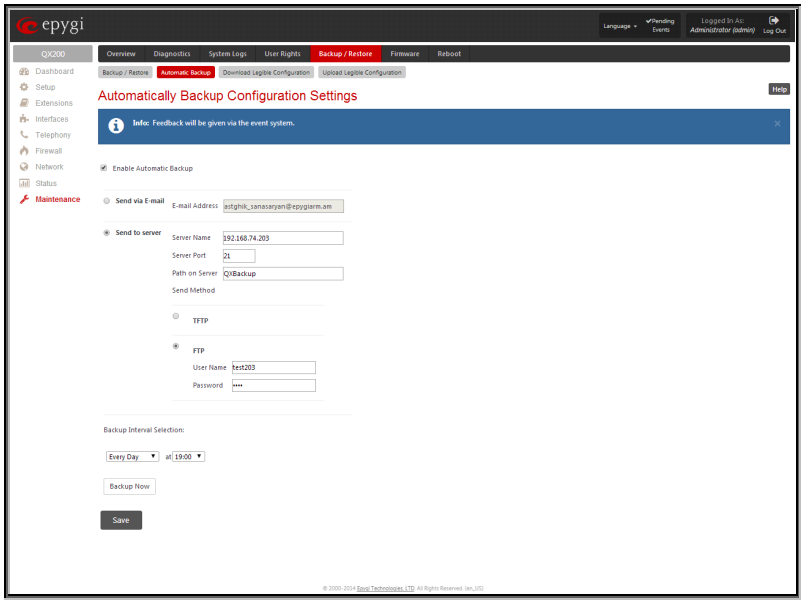


Fig.II- 279: Automatic Backup page

This page contains the following components:

The **Enable Automatic Backup** checkbox enables automatic backup mechanism on the QX IP PBX.

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 IP PBX'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 IP PBX. This will allow you to download a piece of configuration from the QX IP PBX in the way of legible file, to make necessary changes in that file and to upload it back to the same or different QX IP PBX(s). With this service, some pieces of configuration (like extension settings, NAT settings, etc.) of one QX IP PBX can be used on another QX IP PBX. 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 IP PBX) on the same or different QX IP PBXs avoiding manual configuration of each of those instances (i.e. extension) from the web management on each of the QX IP PBXs. The QX IP PBX 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 IP PBX'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 IP PBX 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 IP PBX (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.

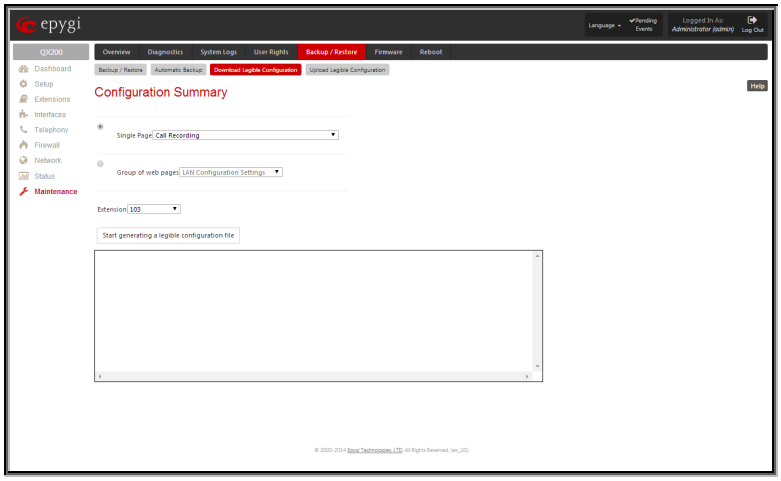


Fig.II- 280: Download Legible Configuration page

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.

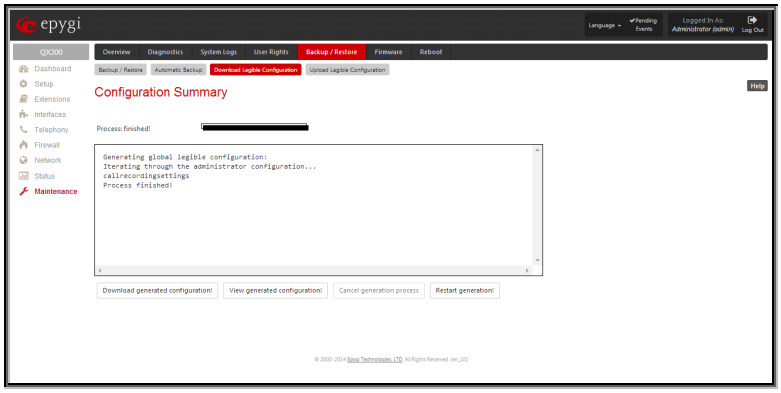


Fig.II- 281: Download Legible Configuration - Configuration Summary Preview page

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 IP PBX's functionality failures may occur.

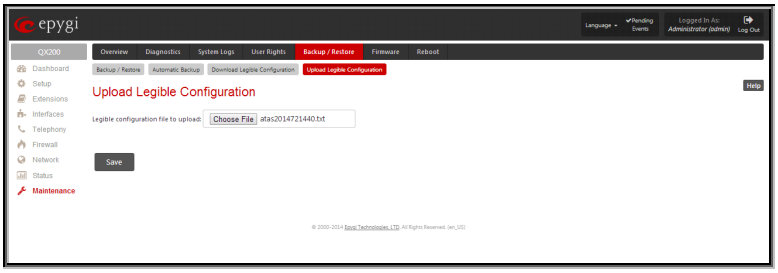


Fig.II- 282: Upload Legible Configuration page

Firmware Update

This window allows updating the software of QX IP PBX 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 IP PBX 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 IP PBX, telephony and Internet access will be disabled.

Attention: When the older firmware is installed on the QX IP PBX, 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.

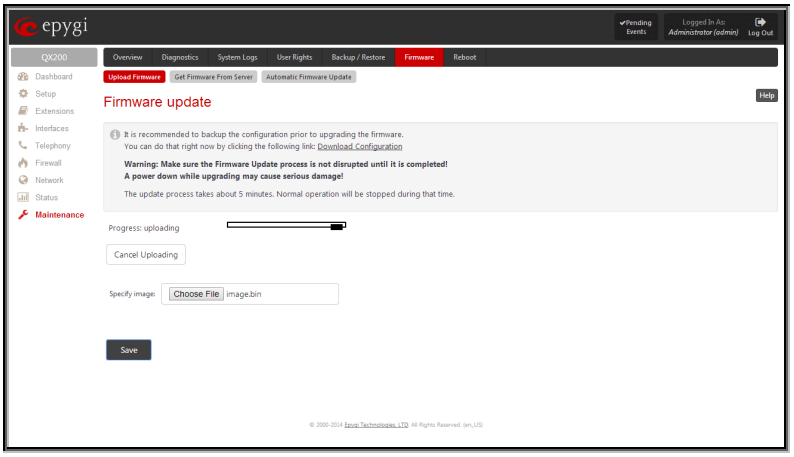


Fig.II- 283: Firmware Update page

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.

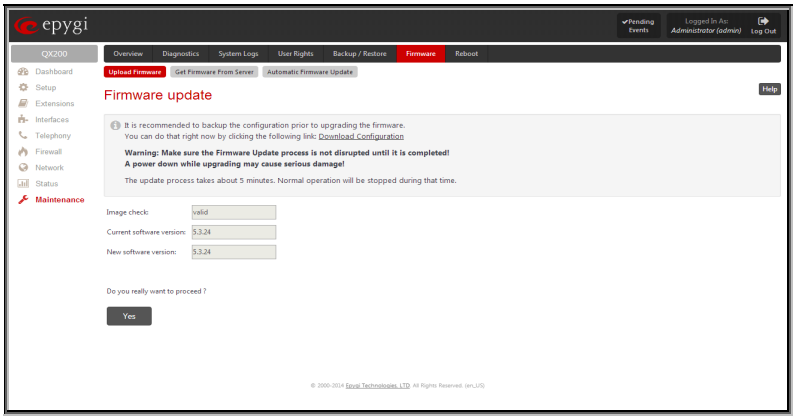


Fig.II- 284: Firmware Check page

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 IP PBX.

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

Attention: After the firmware update, all IP phones attached to the QX IP PBX should be restarted.

Fig.II- 285: 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**.

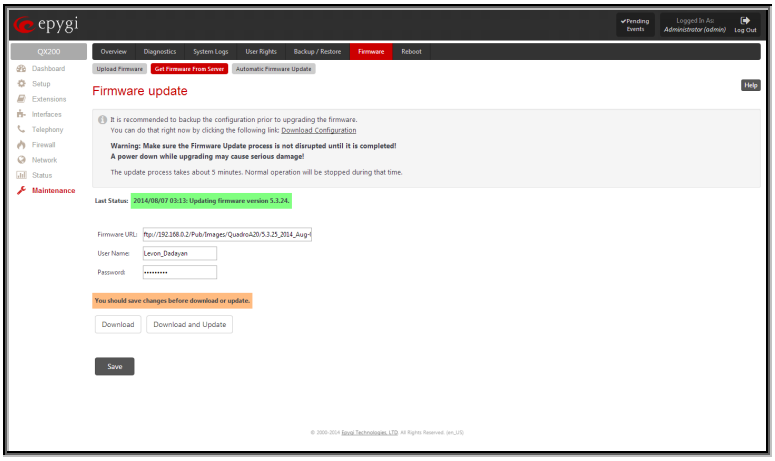


Fig.II- 286: Firmware Update page

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.

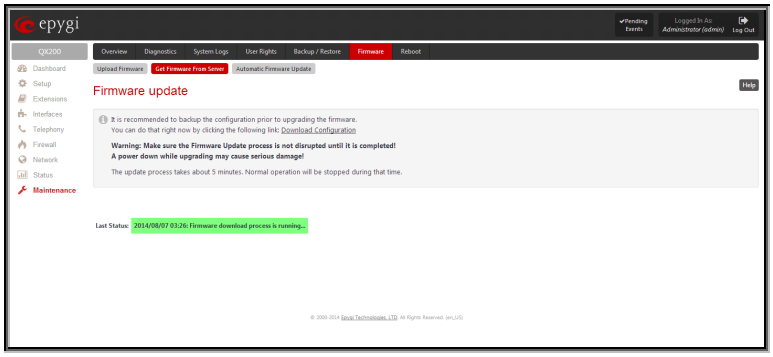


Fig.II- 287: Firmware Update page

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**.

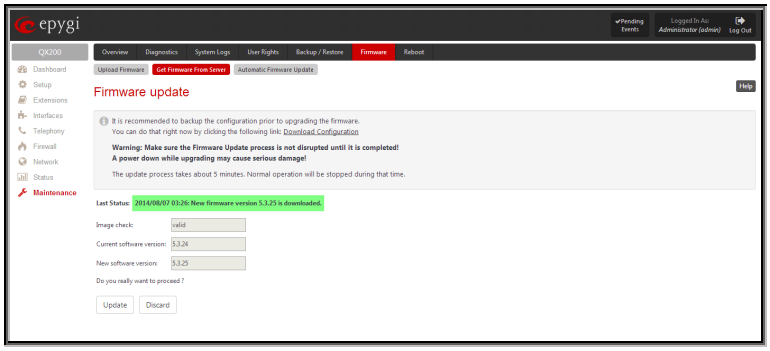


Fig.II- 288: Firmware Update page

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 IP PBX.

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.

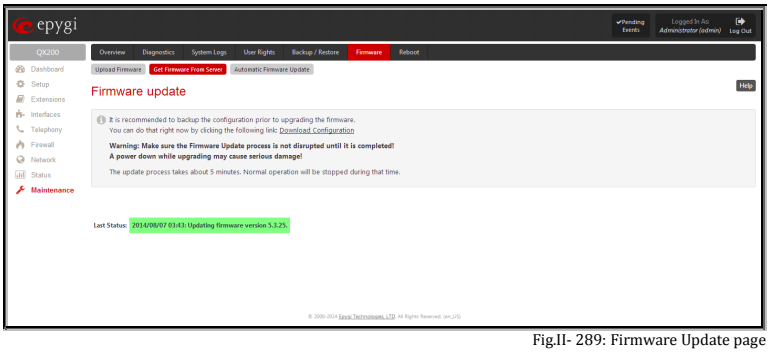


Fig.II- 289: Firmware Update page

Automatic Firmware Update

The **Automatic Firmware Update** page allows you to configure an automatic update of the QX IP PBX's firmware (software image) as it becomes available on the server. When this service is enabled, on the configured day and time QX IP PBX 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 IP PBX 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 IP PBX.

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 IP PBX will check for a new firmware available on the server. The way of notification is configured from the Events page.
- **Check and update** – choose this selection to check and automatically install the new firmware on the QX IP PBX as it becomes available on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the QX IP PBX will check for a new firmware available on the server, will automatically download and install it on the QX IP PBX.

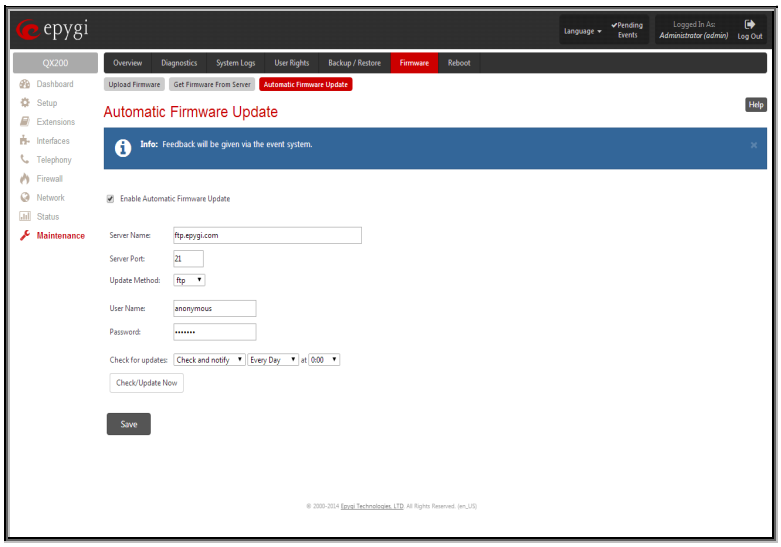


Fig.II- 290: Automatic Firmware Update page

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 IP PBX. Please note that the session with the QX IP PBX will be closed, i.e., the QX IP PBX GUI should be newly opened and a new login will be required afterwards.

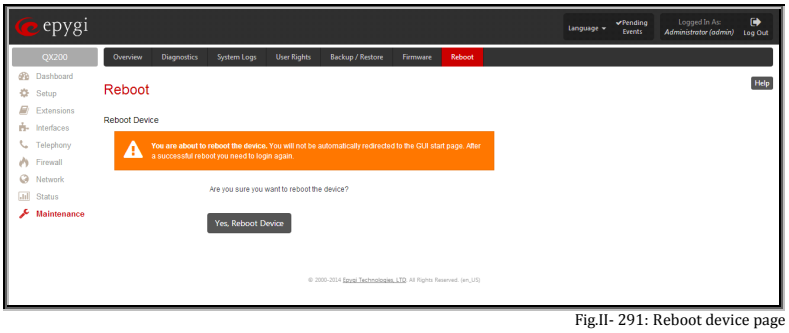


Fig.II- 291: Reboot device page

Registration Form

The **Register Your Device in Technical Support Center** page appears when administrating an unregistered QX IP PBX, 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 IP PBX registration form.

Remind me later hides the registration notification in the QX IP PBX through System Configuration Wizard or Internet Configuration Wizard until the next administrating activities.

Don't remind me again hides the registration notification forever.

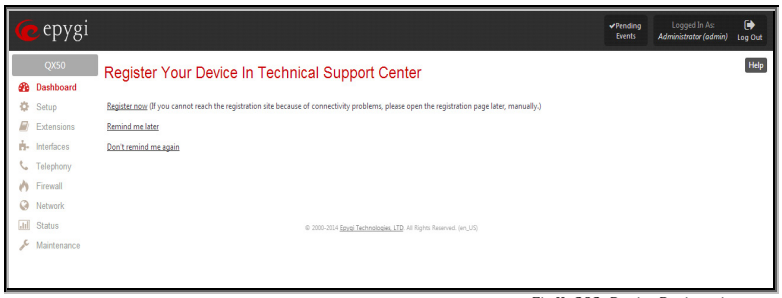


Fig.II- 292: Device Registration page

Appendix: PBX Services for QX IP PBX's Administrator

The following **PBX Services** are accessible at the dial tone, characterized by beginning with the key *:

Administrator Login Allows to modify Auto Attendant greeting and menu messages, as well as to manage universal extension messages.	*75
Enabling/disabling the Call Routing rules Allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry. By dialing *77, you will be required to dial enabler/disabler key 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.	*77

Administrator Login menu has the following sub-menus and the management keys:

***75 Administrator's Login**

1 Auto Attendant Greeting	2 Auto Attendant Menu Message	3 Universal Extension Messages					
		1 Greeting Message	3 Incoming Blocking Message	4 Outgoing Blocking Message	5 Your Name	6 Out of Office Message	7 Find Me/Follow Me Welcome Message
Dial **AA Number** (in case of multiple AAs on the QX IP PBX)	Dial **AA Number** (in case of multiple AAs on the QX IP PBX)						
1 Listen to Current AA Greeting	1 Listen to AA Menu Message	1 Listen to Current Greeting Message	1 Listen to Current Incoming Blocking Message	1 Listen to Current Outgoing Blocking Message	1 Listen to Current Name recorded	1 Listen to Current Out of Office Message	1 Listen to Current Find Me/Follow Me Welcome Message
2 Record a New AA Greeting	2 Record a New AA Menu Message	2 Record a Universal Greeting Message	2 Record a Universal Incoming Blocking Message	2 Record a Universal Outgoing Blocking Message	2 Record a Universal Name	2 Record a Universal Out of Office Message	2 Record a Universal Find Me/Follow Me Welcome Message
3 Restore Default AA Greeting	3 Restore Default AA Menu Message	3 Restore System Default Greeting Message	3 Restore System Default Incoming Blocking Message	3 Restore System Default Outgoing Blocking Message	3 Restore System Default Name	3 Restore System Default Out of Office Message	3 Restore System Default Find Me/Follow Me Welcome Message
# Stop Recording or Playback	# Stop Recording or Playback	# Stop Recording or Playback Greeting Message	# Stop Recording or Playback Incoming Blocking Message	# Stop Recording or Playback Outgoing Blocking Message	# Stop Recording or Playback Name Message	# Stop Recording or Playback Out of Office Message	# Stop Recording or Playback Find Me/Follow Me Welcome Message

*0 Administrator's Logout

Appendix: Conference Services for Moderators and Participants

This chapter describes the feature codes for the Conference Services that enable the moderator and participants to manage call conferences from the phone.

Conference Services accessible during the conference:	Keys
Invite Participant To invite a participant dial *1 + Participant's SIP address (or *1 + Routing Number). Service is available for Moderators only.	*1
Get the number of participants in the conference Plays information about the total number of participants in the conference at the certain moment.	*21
Get the state of recording Plays the state of conference recording (started, stopped or paused).	*22
Lock the conference Locks the conference. When conference is locked, nobody can dial in any more. Service is available for Moderators only.	*31
Unlock the conference Unlocks the conference. Now participants are allowed to dial in to the conference. Service is available for Moderators only.	*32
Dial out to all users with dial out settings enabled Initiates the dial-out to all participants currently inactive in the conference but configured to be dialed out (also those added manually from the handset by moderator). Service is available for Moderators only.	*41
Dial out to all participants to the conference Initiates the dial-out to all participants currently inactive in the conference. Service is available for Moderators only.	*42
Next Phone with Video Capability Shows the next phone with video capability. Also switches from automatic mode to manual one.	*50
Previous Phone with Video Capability Shows the previous phone with video capability. Also switches from automatic mode to manual one.	*51
Automatic Video Switching Mode With this key combination, the loudest speaking participant is displayed on all video-capable phones. If that participant has no video capability, a black screen will be displayed.	*52
Start or Resume Conference Recording Service is available for Moderators only.	*81
Pause Conference Recording Service is available for Moderators only.	*82
Stop Conference Recording Service is available for Moderators only.	*83
Request to Speak With this key combination, a listener requests to speak and a notification hand-up icon is displayed in the Conference Progress table. The moderator can then switch the particular listener either to speaker or lecture mode. With a speaker permission granted, listener can speak to the conference along with other participants. With a lecturer permission granted, listener can speak to the conference having all other participants muted in the conference. This service is available for listener participants only.	*91
Cancel the Request to Speak With this key combination, listener cancels his request to speak and a notification hand-up icon disappears from the Conference Progress table. This service is available for listener participants only.	*92

Mute/Unmute With this key combination, any participants in the conference may mute and unmute themselves during the conference.	#

Please Note: You may accelerate dial out by a pound (#) sign at the end of your dialed number.

Call Codes available in the Auto Attendant:

For external IP calls addressed to the Auto Attendant following key combination is available to access and manipulate within Auto Attendant services:

Incoming Call to Auto Attendant	Key Combination
Conferences Menu - used to access conferences. **Conference ID** should be dialed here.	already in

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name – admin Password – 19
Host Name	epygiqx
Domain Name	epygi-config.loc
LAN IP Address	172.30.0.1 Subnet Mask –255.255.255.0
DHCP Server	Disabled
Regional Settings and Preferences	Locale – US TimeZone – Central Time (US&Canada),
Emergency and PSTN access codes	Emergency Code – 911 PSTN Access Code – 9
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 Settings	Dynamically by provider
Date and Time Settings	Simple Network Time Protocol Server and Client – enabled SNTP Server – ntp1.epygi.com Polling interval – 6
Email(SMTP) Settings	System Mail Settings – disabled TLS – disabled Enable SMTP Authentication – disabled User Name – empty User Password – empty
Short Text Messaging (SMS) Settings	Enable SMS Service – disabled
System Security	Security Level – Medium
Licensed Features	3pcc support – No key found ACD support – No key found Barge In – No key found Redundancy (available only for QX2000) – No key found DCC Pro Support – No key found DCC Basic Support – No key found iQall Toggling Support – No key found IP Phone support – No key found Autodialer Support – No key found Conference Server – No key found Video Conferencing – No key found Call Recording - No key found
Redundancy Settings	Disabled
Language Pack	Default – English Current Language Pack – none
Extensions Management (for QX50/QX200)	Extension Length – 3, once applied extensions 00, 101-150 appear for QX50, 00, 101-302 appear for QX200
Extensions Management (for QX2000)	Extension Length – 4, once applied extensions 00, 1001-1200 appear for QX2000
Extension Settings – General (for QX50/QX200)	Display name – none Password – empty

Parameter	System Default Value
	101 and 102 extensions are attached to the FXS lines 1 and 2 correspondingly 103-118 extensions attached to the IP lines 1-16 (for QX50) 103-126 extensions attached to the IP lines 1-24 (for QX200) Kickback – disabled Call Relay – disabled Login Allowed-disabled 3pcc/Click2Dial Login Allowed-disabled Audio Line-out-disabled Show on Public Directory – disabled Percentage of Total Memory for extensions 101-102 – 5%, Percentage of Total Memory for extensions 103-118 – 0.4% (for QX50) Percentage of Total Memory for extensions 103-126 – 0.4% (for QX200)
Extension Settings – General (for QX2000)	Display name – none Password – empty 1001-1200 extensions attached to the IP lines 1-200 Kickback – disabled Call Relay – disabled Login Allowed-disabled 3pcc/Click2Dial Login Allowed-disabled Audio Line-out-disabled Show on Public Directory – disabled Percentage of Total Memory – 0.04%
Extension Settings – SIP	Registration username – same as extension number Registration password - empty SIP server - empty SIP Server port – 5060 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 – Remote	Remote Extension – disabled
Extension Settings – Call Queue	Call Queue – disabled
Extension Settings – Voice Mailbox	Internal Voice Mail for all extensions Configuration wizard – activated Shared Mailbox – undefined
Extension Settings – Codecs (for QX50/QX200)	For all extensions except 101 and 102: Codecs - G711u (preferred), G711a, G729a – enabled G726/16, G726/24, G726/32, G726/40, iLBC, G.722, G.722.1, TDVC, 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 For extensions 101 and 102: Codecs - G711u (preferred), G711a, G729a, G726/32, G726/16, G726/24, G726/40– enabled iLBC, G.722, G.722.1, H.263,H.263+ and H.264 – disabled Out of Band DTMF Transport – enabled T.38 FAX – enabled

Parameter	System Default Value
	Pass Through FAX – enabled Pass Through Modem – disabled Force Self Codecs Preference for Inbound Calls – disabled SRTP Policy – Make unsecure calls, accept anything
Extension Settings – Codecs (for QX2000)	Codecs - G711u (preferred), G711a, G729a – enabled G726/16, G726/24, G726/32, G726/40, iLBC, G.722, G.722.1, TDVC, 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 QX50/QX200)	Display name – Attendant FAX forwarding – disabled Show on Public Directory – enabled Percentage of System Memory – 5%
Attendant 00 Settings – General (for QX2000)	Display name – Attendant FAX forwarding – disabled Show on Public Directory – enabled Percentage of System Memory – 0.08%
Attendant 00 Settings – Attendant Scenario	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	Registration username – 00 Registration password - empty SIP server - empty SIP Server port – 5060 SIP Server Registration – disabled
Attendant 00 Settings – SIP Advanced	Same as for extensions
Attendant 00 Settings - Codecs	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 – Accept anything
Conference Management and Email Default Settings	Feature is disabled by default
Universal Extension Recordings	For **QX50/QX200**: Percentage of System Memory – 1% For **QX2000**: Percentage of System Memory – 0.08%
Extension Directory	No entries
Receptionist Management	No entries
ACD Management	Undefined
Authorized Phones Database	No entries
IP Lines Settings	IP Lines Configuration: Enable PnP for IP lines – enabled

Parameter	System Default Value
	Enable firmware version control – enabled Configure IP phones from – WAN (for **QX50/QX200**) Phones Default Template – systemdefault IP Phone Templates – no custom templates IP Phone Logo – disabled, no custom logos uploaded FXS Gateway Management – undefined For **QX50**: IP Lines 1-16 – enabled IP Lines 17-48 – disabled 1-16 IP Lines attached to 103-118 extensions. All IP lines are in inactive mode For **QX200**: IP Lines 1-24 – enabled IP Lines 25-200 – disabled 1-24 IP Lines attached to 103-126 extensions. All IP lines are in inactive mode For **QX2000**: IP Lines 1-200 – enabled 1-200 IP Lines attached to 1001-1200 extensions. All IP lines are in inactive mode Disabled IP lines – displayed FXS Lines Loopback Settings – Loopback is disabled for all FXS lines, Loopback timeout is 30
FXS (On-board) settings	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 Off-hook caller ID – disabled for all lines Hot Desking Capability – disabled for all lines
FXO Settings	For **QX50**: 2 FXO lines – all lines enabled, incoming and outgoing calls allowed and routed to 00 Attendant on all lines For **QX200**: 4 FXO lines – all lines enabled, incoming and outgoing calls allowed and routed to 00 Attendant on all lines For **QX2000**: Hardware does not support FXO. Only shared FXO lines are available
E1/T1 Trunk Settings	Hardware does not support E1/T1. Only shared E1/T1 trunks are available
ISDN Trunk Settings	Hardware does not support ISDN. Only shared ISDN trunks are available
External PSTN Gateways	Use PSTN lines of the other device – disabled Authorization Parameters – undefined
VoIP Carrier	VoIP Carrier – Manual Description – Empty
Call Routing Table	Call Routing table - 3 entries defined for a call to the default Auto Attendant 00, for calls to PBX and 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 Tunnels to Slave Devices – no entries Enable Tunnels to Master Devices – disabled Tunnels to Master Devices – no entries
Class of Service	Disabled
Call Recording	**Basic View**: All extensions are disabled **Advanced View**: Call Type – Auto

Parameter	System Default Value
	Address-empty Recording Type – Always start automatically Max Recording Duration – 1 hour Recording To – same as extension number Description – empty
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 except iLBC, G.722, G.722.1, TDVC : Packetization -20ms Silence Suppression – yes iLBC properties: Packetization – 30ms Silence Suppression – yes G.722, G.722.1, TDVC properties-undefined 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 Host Aliases for SIP – undefined
Voice Mail Common Settings	Voice Mail Recording - G729a Email Subject for voice - Voice mail received from $[VM_DISPNAME] $[VM_USERNAME] FAX to E-mail format – TIFF
RTP Streaming Channels	Undefined
Gain Control Settings (for QX50/QX200)	**FXS lines:** Transmit Gain: - 6 Receive Gain: 0 **FXO lines:** Transmit Gain: 0 Receive Gain: 6 **Voice Mail:** Recording Gain: 0 Playback Gain: 0 **Audio Lines:** Transmit Gain(Line out): Off Receive Gain(Line in): Off
Gain Control Settings (for QX2000)	**Voice Mail:** Recording Gain: 0 Playback Gain: 0
3PCC Settings	Secure Connection – disabled Request Timeout – 10 Feature Key – not added WAN Port – not opened.
RADIUS Client Settings	RADIUS client – disabled
Dial Timeout	4 seconds
Call Quality Notification	Disabled
Firewall (for QX50/QX200)	Enable Firewall – disabled Enable IDS – enabled Enable NAT - enabled Ping Stealth – enabled

Parameter	System Default Value
	Fool Portscanner – disabled
Firewall (for QX2000)	Enable Firewall – disabled Ping Stealth – enabled
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all) SIP Access (Allowed for all)
SIP IDS Settings	Enable SIP IDS – enabled 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 – 172.30.0.1 Subnet mask – 255.255.0.0 Domain name servers – 172.30.0.1 NBT name servers – 0.0.0.0 NTP servers – 172.30.0.1 Domain name – epygi-config.loc Overload tftp server name – 172.30.01 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 (available only for QX50/QX200)	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. Additionally, Fan Control critical and major failures have a Flash LED action assigned
Call History	Enable Call Reporting– enabled, 100 entries for all type of calls Percentage of Total Memory used for Archive – 0% Enable Call Detail Records Archive Collection – disabled Call Detail Records Archive Structure – Archive by records count Call Records Count – 50 Time Interval – 10min Send archive files to external server – Send and delete from archive File Format –Tab Delimited Text (.log)
Conference History	Enable Call Reporting– enabled, 100 entries for all type of calls.
System Logs Settings	User Logging – enabled Developer Logging – enabled Log Lines to Show – 25 Comment – undefined
Remote Logs Settings	Disabled
User Rights Management	Users - admin (enabled), localadmin (disabled) Roles - Extension (all accessible pages for extension except for Extension Voice Mail Profiles), 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	Enabled Server Configuration – Assign manually

Parameter	System Default Value
	Server Name – ftp.epygi.com Server Port – 21 Update Method – ftp Username – anonymous Password – empty Check and notify – Every day at 0:00

Extension Settings

Parameter	System Default Value
Voice Mail Settings	Maximal mail message duration - 5 min Ask password before granting local access to mail box – disabled Ask password before granting remote access to mail box – enabled Send welcome message – disabled Play Voice Mail help – enabled Automatically play messages - enabled Send mails count information message – disabled Send date/time information message – enabled Send beep at the end of message – enabled Silent VM recording – disabled Send new voice messages via e-mail – disabled Voice Mail-Send notification with attachment Remove Voice Mail On Send-disabled Fax- Send notification with attachment Remove Fax On Send-disabled Send new voice message notifications via SMS – disabled Send new voice message notifications via phone call – disabled Voice Mail Indication: Lamp indication – enabled for IP lines only Tone indication - enabled for FXS lines only Ringing indication – disabled Zero Out – enabled, Redirect Call Type – PBX, Redirect Address - 00 FAX Redirection – disabled Automatic Fax Receiving Mode – disabled Out of Office – disabled Forward/rewind duration – 3 seconds Greeting message – default
Voice Mail Profiles	Undefined
Group List	No entries
Speed Calling	No entries
Account Settings	Display Name – undefined User Password Protection – disabled both for incoming and outgoing calls User's Name for Extensions Directory – default Custom Voice Messages – default
Basic Services - General	No answer timeout – 20 sec Call Waiting Service – enabled Autoredial Interval - 10 sec Autoredial Period - 15 min
Basic Services - Hold Music	Send Hold Music to remote IP party – enabled Hold Music - Own Music Music file – default
Basic Services - Do Not Disturb	Disabled, Timeout - 30 min Send Message to Caller – enabled
Basic Services – Hotline (available only for QX50/QX200)	Disabled

Parameter	System Default Value
Caller ID Services	No entries in the table For Any Callers – all services are disabled Call Blocking message files – default Intercom – Allow Activation on Request Activation Signal –Ring Only if Requested

Appendix: Moderator's Menus

This Appendix explains all menus that can be accessed and configured by conference moderators. (Applicable if the Conference Server feature is activated on the system.)

Conference Moderator's Main Page

The Moderator's Main Page can be accessed by clicking on the conference ID link on the Conferences Management page or by logging as a moderator on the QX IP PBX login page.

After logging in as a moderator, the page Conference Progress is displayed. Here you may see the active conferences and the participants. From this page you may also access the settings of the conference to operate and perform actions that are available only to the moderator of each conference.

- **Conference Progress**
- **Recorded Conferences**
- **Conference Settings**
  - General
  - Recording
  - Customization
  - Participants
  - Schedule
  - Send Notification Mail

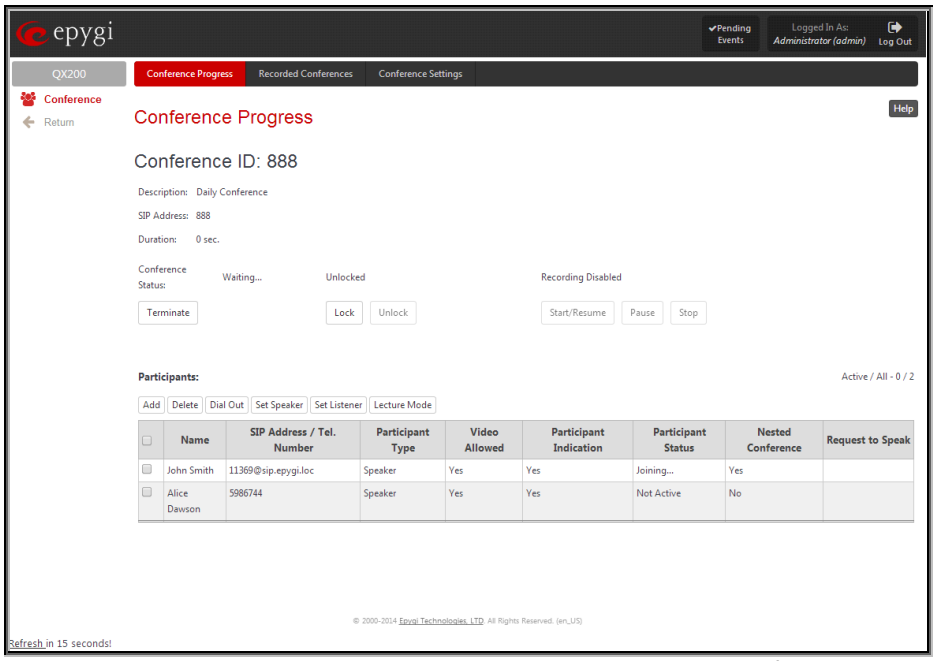


Fig.II- 293: Conference Progress page

Conference Progress

The **Conference Progress** page displays information about the conference, including the list of participants, and allows moderator to manage the conference.

The following read-only data is displayed on this page:

Conference ID – the unique ID on the conference.

Info Text – displays the text uploaded in the Info File from Customization page. In the picture illustration on the right side, the Info Text says "WELCOME to EPYGI's CONFERENCE!!!".

Description – any descriptive information about the conference (optional).

SIP Address - the SIP address of the conference.

Duration – the time the current conference is active.

Conference Status – the conference status (active, not active or waiting). If the conference is active, the information whether the conference is locked or not, and the recording status (recording started, recording paused and recording stopped) is also displayed herein.

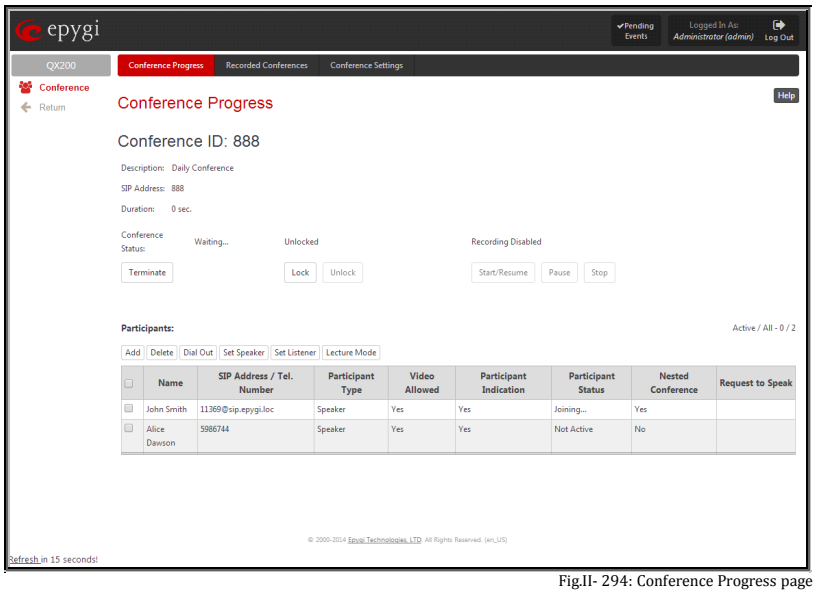


Fig.II- 294: Conference Progress page

The following buttons are available on this page to manage the active conference:

Activate – available for an inactive conference only and used to activate the conference.

Terminate – available for an active conference only and used to terminate the active conference

Lock – available for an active conference only and used to lock the conference. When a conference is locked, no users can connect to it.

Unlock - available for an active conference only and used to unlock the conference.

Start/Resume – available for an active conference only and used to start the recording of the conference or to resume the recording if it was paused.

Pause - available for an active conference only and used to pause the recording of the conference.

Stop - available for an active conference only and used to stop the recording of the conference.

Please Note: **Pausing** and **Resuming** the conference recording can be used to edit the recorded conference audio file. When pause/resume operations are used, conference is recorded in a single file, leaving out the conversation during which conference recording was paused. When using stop/start operations, new files are created each time conference recording is started. All recorded conferences are listed in the Recorded Conferences page only after conference recording termination. In case of **pause/resume**, the recorded file is not terminated. In case of **stop/start** recording starts in new file.

The table of participants on this page lists all preconfigured participants (independent of the conference status), as well as new participants joined the conference (if still connected to the conference) and those participants added from the handset or GUI (unless the conference is terminated).

For the active conference, the table also displays participants added manually from GUI or from the handset and those participants that called in to the conference.

The **Conference Progress** table contains the following information for each participant.

Name – this information is specific to manually added participants only (see below).

SIP Address – indicates the SIP address of the participant.

Participant Type – indicates whether the participant is a speaker or a listener only.

Participant Indication – indicates whether or not a beep indication during the call conference is configured for this participant to be played when he joins or leaves the conference.

Participant Status – this column is only present for active conferences and indicates the state of the participant (active for participants currently in the conference, not active for participants not in the conference, and joining for participants currently joining but not yet connected to the conference).

Nested Conference – indicates if the participant acts as a nested conference or not.

Request to Speak - this column is only present for active conferences and indicates whether a listener participant has requested to speak (by dialing ***9** from the handset, see Feature Codes). When a listener participant requests to speak, a hand-up icon appears in this column. Clicking on the hand icon in this column will grant the speaker permission to the corresponding participant. Participant with the speaker permissions are able to speak to the conference.

The following functional buttons are present on **Conference Progress** page to manipulate with the participants in the conference:

Add functional button opens the **Add Participant** page where a new participant can be manually added to the conference. The **Conference Progress – Add Participant** page consists of the following components:

Participant Name requires optional information (first name, last name, nickname, etc.) about the participant.

SIP Address/Tel. number requires the contact phone number (SIP address or Routing Number) of the participant. This number automatically will be dialed by the system when the participant is configured to be a Dial Out (see below) or when a corresponding Conference Code is used (see Conference Codes).

The participant's SIP address should be a combination of username@hostaddress:port (where hostaddress can be an IP address, for example, 192.168.90.10, or a host name, e.g., sip.epygi.com). The port number is optional for the SIP address. If no port is specified, 5060 will be used. The range of valid ports is between 1024 and 65536.

Please Note: A direct call will be placed toward a participant's SIP address if the corresponding conference is registered on a different SIP server than the participant is registered on, or if the participant is not registered on any SIP server.

The value will be implied as a Routing Number and will be parsed through the Call Routing table if it does not match the SIP URI syntax.

Participant Type list is used to select the type (speaker or listener) of participant in the conference.

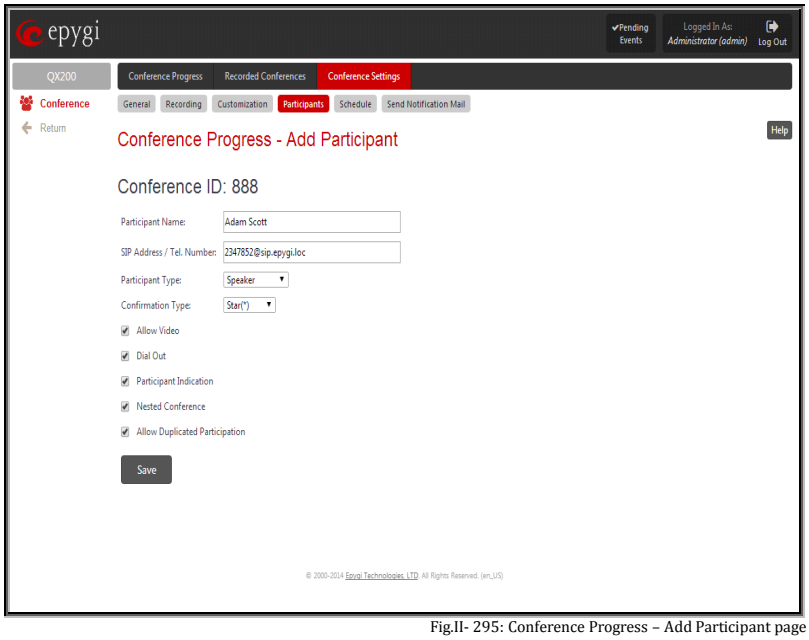


Fig.II- 295: Conference Progress – Add Participant page

Confirmation Type list is used to set the password protection for the participant joining the active conference. **Star (*)** selection allows the participant to accept the conference invitation by pressing the * button. Only participants connected to the conference with the moderator password will be provided with permissions to manipulate the conference.

A group of checkboxes on this page allow configuration of participant specific settings:

- When the **Dial Out** checkbox is selected, the participant will be automatically dialed out when the conference is activated.
- **Participant Indication** enables the beep indication during the conference when this participant joins or leaves the conference.
- **Nested Conference** must be selected if the participant is a Conference itself and enables the correct behavior of conference termination.
- **Allow Duplicated Participation** checkbox allows multiple participants with the selected Caller ID (calling address) to join the corresponding conference. This is applicable when different participants are using the same shared number to place a call.

Dial Out functional button is used call one or more inactive participant(s) inviting them to join the conference.

Delete removes the selected participants from the conference.

Set Speaker functional button is used to grant selected participants a speaker's permissions. A participant with speaker permissions is able to speak to the conference.

Set Listener functional button is used to grant selected participants a listener's permissions. A participant with listener permissions is not able to speak to the conference and is only a listener.

Lecture Mode functional button is used to grant selected participants a lecturer's permissions. Both listener and speaker participants can get lecturer permissions. Enabling lecture mode for a participant will allow him to speak to the conference and will mute all other participants of the conference.

Please Note: Only one participant can act in a lecture mode at the same time.

Recorded Conferences

Conference recording service allows you to record conferences and save them on the system internal or external storage space (depending on the configuration). To use conference recording service, it should be enabled from the Call Recording Settings page.

The maximum duration of the recorded conference can be optionally limited from the Recording Settings page.

Conference recording can be manipulated either from the Conference Progress page or from the handset (see Feature Codes). If the **Recording Indication** is also enabled from the **Recording Settings** page, voice announcements will be played in the conference to inform participants that the conference recording is started, stopped, paused or resumed.

Recorded conferences are stored and are listed in the Recorded Conferences page accessible by the moderator from QX IP PBX Web Management.

The **Recorded Conferences** page displays a table where recorded conferences are listed. The recorded conferences can be played and deleted from this page.

The **Recording free space** field displays the free space allocated for the corresponding conference.

The **New recordings** field displays the number of new recorded conferences in the recording box. All new recordings are marked in bold.

The **All recordings** field displays the number of all recorded conferences in the recording box, including new and played recordings.

The **Check Recordings** functional link refreshes the recording box with any latest recordings (if any).

The **Recorded Conferences** table displays all the recorded conferences with the following parameters:

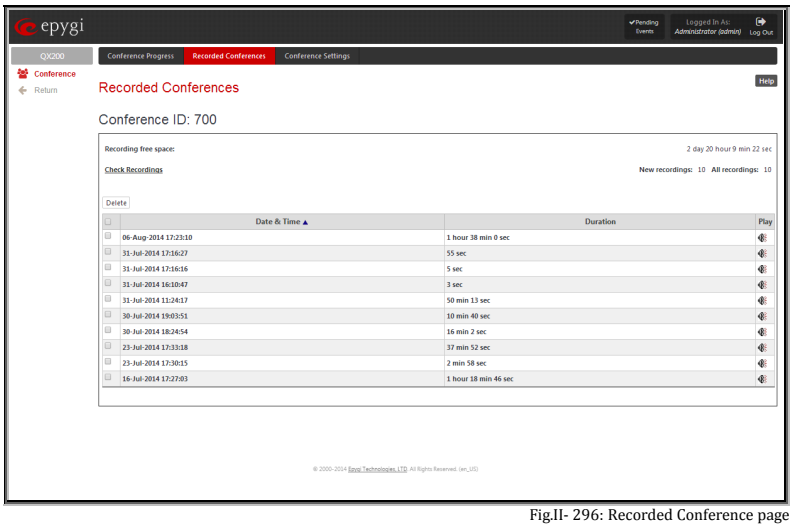


Fig.II- 296: Recorded Conference page

Date & Time shows the initiation date and time of the recorded conference.

Duration shows the duration of the recorded conference (in minutes/seconds).

Play - by clicking on the speaker sign beside every record in the table, the recorded conference will be played (using the available media player supported by your Operatinig System).

The column headings of the **Recorded Conferences** table are organized as links. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will appear next to the column heading. Each row in the table of Recorded Conferences can be selected by the checkbox for deletion.

To Play a Conference

1. Click on the speaker sign of the corresponding recorded conference.
2. Depending on you browser settings, the .wav file will be played directly or an application will ask you to save the .wav file locally to the PC. If you need to save the file, please specify the path then run the media file from the specified location.

To Delete a Recorded Conference

1. Select the checkbox of the corresponding record(s) in the **Recorded Conferences** table that will be deleted.
2. Select the **Delete** button.
3. Confirm the deletion clicking **Yes**. The selected conference then will be deleted. To abort the deletion and keep the conference on the QX IP PBX, select **No**.

Conference Settings

General Settings

The **General Settings** page is used to configure the basic conference settings.

The page contains the following components:

Conference ID indicates the unique ID of the conference.

Description indicates any descriptive information about the conference.

Moderator Password text field requires a password for the moderator access to the conference. The password inserted here should be used by the moderator to join the conference. Moderator is able to use conference codes during the active call conference as well as to access conference specific GUI pages and coordinate the conference (view/change conference properties, activate/deactivate it, start/stop/resume recording, view conference history). **Confirm** text field requires the confirmation of the Moderator Password. Error appears if the password inserted in the **Confirm** text field does not match the one inserted in the **Moderator Password** text field.

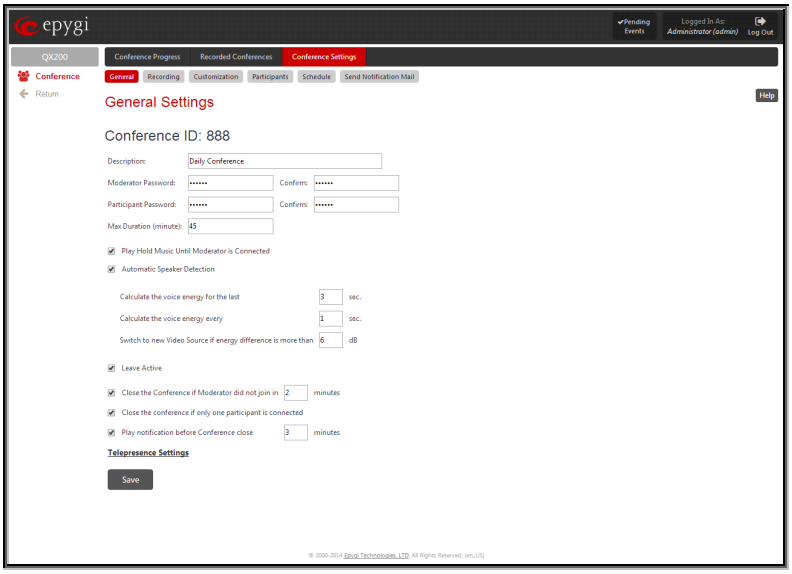


Fig.II- 297: Conference Settings - General Settings Page

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

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

With the **Play Hold Music Until Moderator is Connected** checkbox selected, participants connected to the conference will listen to the hold music unless moderator will join the conference.
Automatic Speaker Detection checkbox enables the automatic detection of the loudest participant in the conference (the current speaker) and switching the video on all of the video conferencing phones in automatic mode to the video from that participant. Initially, when the user joins a conference with **Automatic Speaker Detection** checkbox enabled, his video phone works in automatic mode. Dialing *50 or *51 feature codes will switch the phone to manual mode, displaying the video of the next or previous participant correspondingly. When the phone is in manual mode, it will not switch automatically to display the loudest participant, but it will show the video of the same participant until next time when *50 or *51 is being pressed. Entering the *52 feature code will switch the phone back to automatic mode.
For making the video source switching decision in automatic mode, the video conferencing uses the values of the following parameters:

- **Calculate the voice energy for the last [ ] sec.**
- **Calculate the voice energy every [ ] sec.**
- **Switch to new Video Source if energy difference is more than [ ] dB.**

For example, if the values of the parameters are 3, 1 and 6 (default values) correspondingly, the Conference Server will calculate every one second the average voice energy of each participant during the last three seconds. Then the largest calculated value will be compared to the average voice energy of the participant providing currently the video for all phones in automatic mode. If the difference between energies is more than 6dB then the Conference Server will switch the video to a new source having the largest voice energy.

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

Close the Conference if Moderator did not join in - the idea of including this parameter is as follows:

If the conference is activated by one of the existing ways and the moderator does not join the conference within the first **X** minutes then the conference will be closed by the system. No message will be played to the joined users in this case. The conference will be closed in one of the following cases:

- The conference is activated by a schedule, and the moderator did not join within the first **X** minutes after activation. The only method of distinguishing the moderator from the other participants is the moderator's password. If the user entered the moderator's password during the joining process then he/she is a moderator. There are no other means of distinguishing the moderator from the regular participant.

- The conference is activated by a participant when dialing in, and the **Activate On Dial In** checkbox is enabled for that conference. During the joining process, the participant either did not enter any password or entered a regular participant's password. In this case, the same as above, if the moderator did not join the conference within the first **X** minutes entering moderator's password, the conference will be closed.

- The conference is activated by a moderator from GUI. In this case, even though the moderator activated the conference and did not join within the first **X** minutes, the conference will be closed. In all the above mentioned cases, the conference will be closed regardless of the number of regular participants already joined.

Close the conference if only one participant is connected - if enabled, then the conference will be closed as soon as there is only one participant connected to the conference, after the moderator left the conference. If the moderator did not join yet (during the first **X** minutes as described above), the conference will stay active even if there is only one participant connected yet. If the moderator is the only participant connected to conference then it will stay active.

Play notification before Conference close. When the **Max Duration (M)** of the conference is reached, the system will close the conference and **M** minutes before closing the conference the system will play the warning message to all participants.

Recording Settings

The settings on this page are addressed to the conference recording configuration, enabling conference recording, defining the recording memory allocation (internal or external storage), etc.

The **Recording Settings** page offers the following components:

The **Enable Recording** checkbox enables an option to be used for active conferences to perform the online recordings. With this checkbox selected, a group of radio buttons is activated to select the storage for the recorded conference audio files.

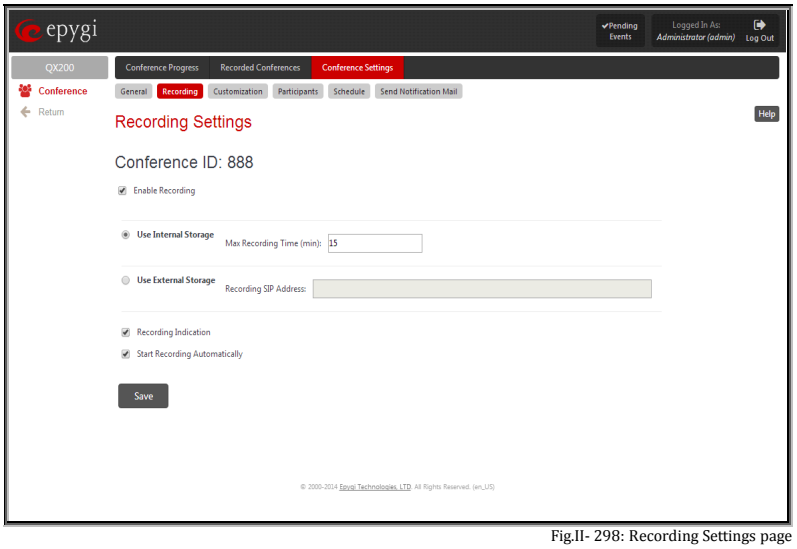


Fig.II- 298: Recording Settings page

- **Use Internal Storage** switches the location used to store the recorded conference audio files to the system internal memory. **Max Recording Time** requires the maximum duration (in minutes) of one recording to be done. If the conference recording has been paused and resumed again, the Max Recording Time value will indicate the actual recorded time. Leave this field empty not to limit the duration of the conference recording.
- **Use External Storage** switches the location used to store the recorded conference audio files to an external destination, which can be any device or application that has audio recording capabilities. The **SIP Address** of the remote destination where the recorded conference will be stored is required to be defined for this selection. Optionally, the SIP address of a user can be inserted here. In this case, the conference will be recorded to the private mailbox of the user or will be directly played to him if he answers the incoming call.

Recording Indication selection enables voice announcements played in the conference to inform participants that the conference recording is started, stopped, paused or resumed.

When the **Start Recording Automatically** checkbox is selected, the conference recording will start automatically as soon as the corresponding conference is activated.

Customization

The **Customization** page is used to manage the voice prompts played during an active conference. The page offers the following options:

When the **Play First in Conference message** checkbox is selected, the system will play a "You are the first participant in the conference" notification message informing you that no more participants are yet connected.

Welcome Message parameters group allows updating the active conference welcome message (played once a user is connected to the conference), downloading it to the PC or removing the custom welcome message. The group offers the following components:

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

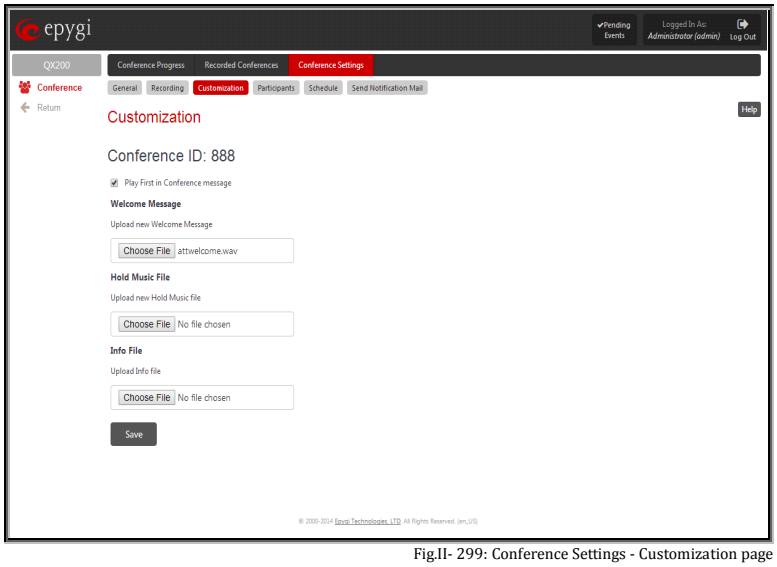


Fig.II- 299: Conference Settings - Customization page

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.

Hold Music File parameters group allows updating the hold music (played when you are alone in the conference), downloading it to the PC or removing the custom welcome message. The group offers the following components:

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

Choose File opens the file chooser window to browse for a new hold music file.

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

Info File parameters group allows you to upload a text file with some conference related announcement, advertisement or any other information to be displayed on the Conference Progress page. The group offers the following components:

Upload Info file indicates the information file name. The system will display the file content exactly in the way it is formatted in the file. It is recommended to use a *.txt formatted plain text file. The uploaded file should not exceed the size of 2000 bytes. The system also prevents uploading if there is not enough memory available for the corresponding conference and the "You do not have enough space" warning message will appear.

Browse opens the file chooser window to browse for an information file.

The **Remove Info File** link appears only when a file has been previously uploaded and is used to remove the uploaded information file.

Participants

This page allows to configure participants of the conference as well as to adjust settings of the participants dialed out during the conference or independently connected to the conference.

The New Participants Configuration moves to the page where the settings of participants independently dialed in to the conference can be configured. Once the new participant connects the conference, he will automatically appear in the Conference Progress table on this page and remain there unless disconnected from the conference.

The Handset Added Participants Configuration moves to the page where the settings of participants dialed out from the handset by the moderator during the active conference can be configured. Once a handset added participant connects the conference, he will automatically be added to the Conference Progress table on this page and remain there unless the conference is terminated.

The table on this page lists all preconfigured participants, allows to add new participants and to modify the settings of the exiting ones.

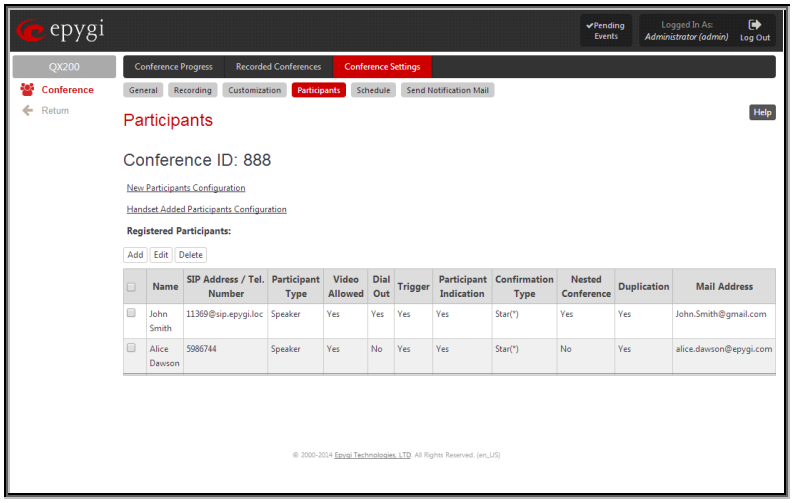


Fig.II- 300: Conference Settings - Participants page

Please Note: By default, no participant is able to make video calls. Administrator should set one of the following checkboxes to enable the video capability of the participant:

- **Allow Video** checkbox from the **Participants - Add Entry** GUI page (see Fig.II-298).
- **New Participant Can Make Video Call** checkbox from the New Participants Configuration GUI page (see Fig.II- 303).
- **Allow Video** checkbox from the Handset Added Participants Configuration GUI page (see Fig.II- 304).

Add opens an **Add Entry** page where new participants can be added to the conference. The following parameters are needed to configure participant settings:

Participant Name requires optional information (first name, last name, nickname, etc.) about the participant.

SIP Address/Tel. number requires the contact phone number (SIP address or Routing Number) of the participant. This number automatically will be dialed by the system when the participant is configured to be a Dial Out (see below) or when a corresponding Conference Code is used (see Conference Codes).

The participant's SIP address should be a combination of username@hostaddress:port (where hostaddress can be an IP address, for example, 192.168.90.10, or a host name, e.g., sip.epygi.com). The port number is optional for the SIP address. If no port is specified, 5060 will be used. The range of valid ports is between 1024 and 65536.

Please Note: A direct call will be placed toward a participant's SIP address if the corresponding conference is registered on a different SIP server than the participant is registered on, or if the participant is not registered on any SIP server.

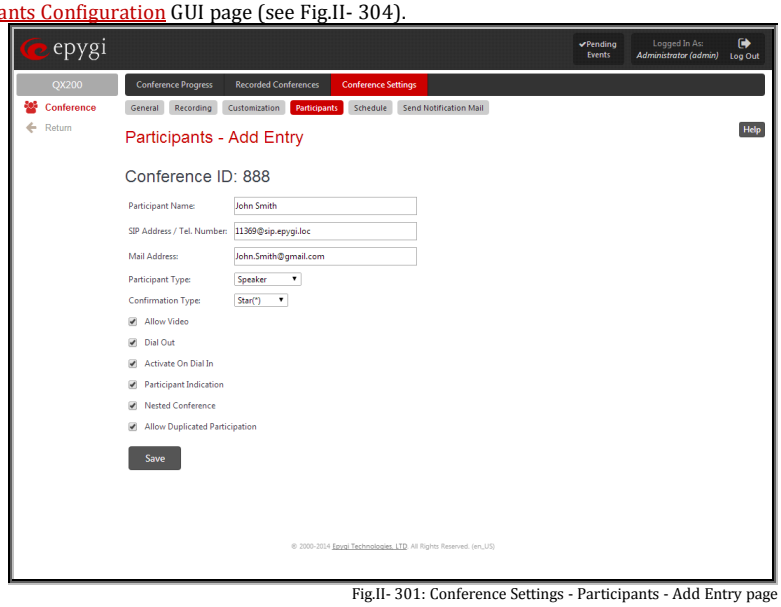


Fig.II- 301: Conference Settings - Participants - Add Entry page

The value will be implied as a Routing Number and will be parsed through the Call Routing table if it does not match the SIP URI syntax.

Email Address requires the email address of the participant. Conference related notifications (configured from the Schedule page or using the Send Notification Mail option) will be sent automatically to this address. This field is not available on this page when it is reached from the Conference Progress page.

Participant Type list is used to select the type (speaker or listener) of the participant in the conference.

Confirmation Type list is used to set the password protection for the participant joining the active conference. **Star (*)** selection allows the participant to accept the conference invitation by pressing the * button. Only participants connected to the conference with the moderator password will be provided with the permissions to manipulate the conference.

Please Note: Confirmation Type should be selected to "none" when the **Participant Type** is listener.

A group of checkboxes on this page allow configuration of participant specific settings:

- **Allow Video** checkbox will allow participant to join the video conference. This checkbox is not available on this page when it is reached from the Conference Progress page.
- When the **Dial Out** checkbox is selected, the participant will be automatically dialed out when the conference is activated.
- **Activate On Dial In** automatically activates the conference when this participant joins the conference call. This checkbox is not available on this page when it is reached from the Conference Progress page.
- **Participant Indication** enables the beep indication during the conference when this participant joins or leaves the conference.
- **Nested Conference** should be selected if the participant is a Conference itself and enables the correct behavior of conference termination.
- **Allow Duplicated Participation** checkbox allows multiple participants with the selected Caller ID (calling address) to join the corresponding conference. This is applicable when different participants are using the same shared number to place a call.

The **Edit** functional button provides a possibility of editing multiple participants at the same time. A **Select to modify fields** checkbox alongside the fields to be modified needs to be selected to submit changes, otherwise the fields will not be updated.

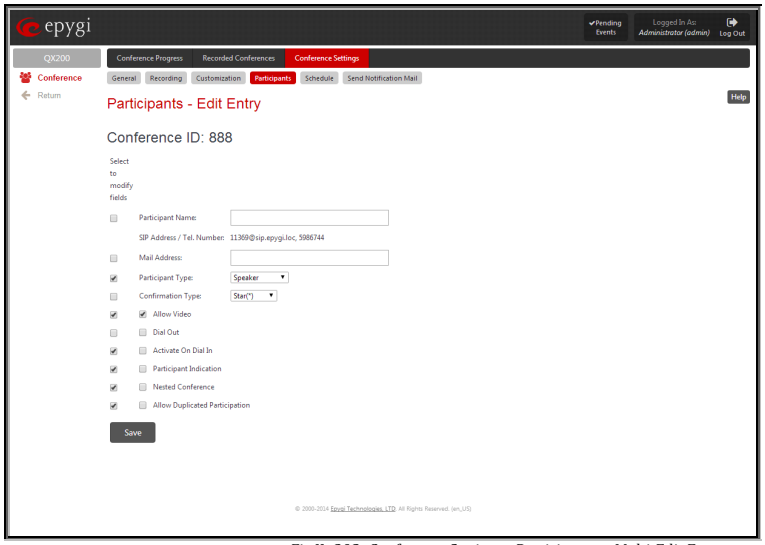


Fig.II- 302: Conference Settings - Participants – Multi-Edit Entry page

New Participants Configuration

This page is used to configure settings of participants independently dialed in to the conference. Once the new participant connects the conference, he will automatically appear in the Conference Progress table and remain there unless disconnected from the conference.

Max New Participant Count text field requires the maximum number of new users allowed to connect to the conference. Leave this field empty to allow unlimited number of new users connecting the conference. In one conference the maximum number of participants allowed to connect to the conference cannot exceed 95.

New Participant Type drop down list is used to select the state (speaker or listener only) of the new participants connected to the conference.

Selecting the **New Participant Can Make Video Call** checkbox will allow participant to join the video conference.

New Participant Confirmation Type drop down list is used to select whether the conference is password protected for the new users or not.

Selecting the **New Participant Can Activate Conference** checkbox will allow new users to activate the conference.

When **Conference Inactive Until Moderator Login** option is enabled, participants will not be able to join the conference until the moderator has logged in. **New Participant Confirmation Type** field should also be set to **Password** to enable this option.

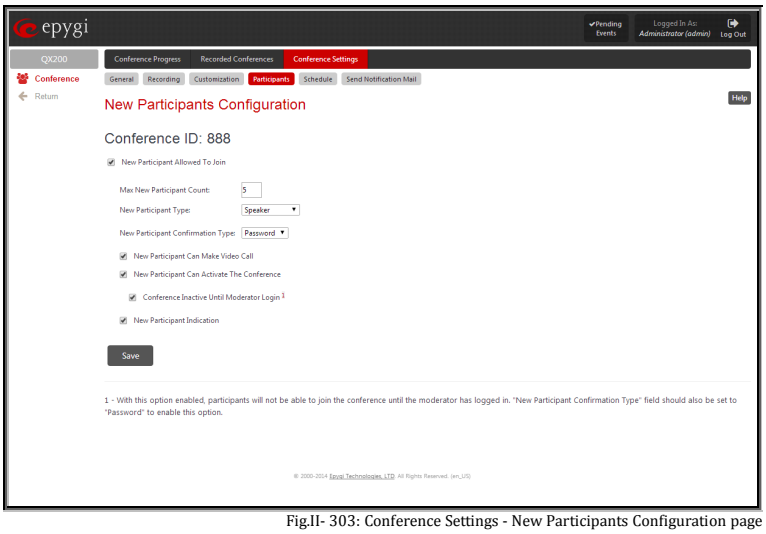


Fig.II- 303: Conference Settings - New Participants Configuration page

Selecting the **New Participant Indication** checkbox will enable a beep indication during the active conference when a new user joins or leaves the conference.

Handset Added Participants Configuration

This page is used to configure the settings of participants dialed out from the handset by the moderator during the active conference. Once the handset added participant connects the conference, he will automatically appear in the Conference Progress table and remain there unless the conference is terminated. This will allow the handset dialed participant to hang up and dial in to the corresponding conference again while it is active.

The page consists of the following components:

Participant Type drop down list is used to select the state (speaker or listener only) of the handset added participants connected to the conference.

Confirmation Type drop down list is used to select whether the conference is password protected for the handset added users or not. When **Star (*)** selection is chosen, the handset added user should accept the conference invitation by pressing the * button.

Selecting the **Allow Video** checkbox will allow participant to join the video conference.
Selecting the **Participant Indication** checkbox will enable a beep indication during the active conference when a handset added user joins or leaves the conference.
The **Allow Duplicated Participation** checkbox selection allows several instances of callers with the same handset added number (caller address) to join the corresponding conference at the same time. This option may be used to allow users from the same network (with the same caller address), like PSTN network, to reach the conference.

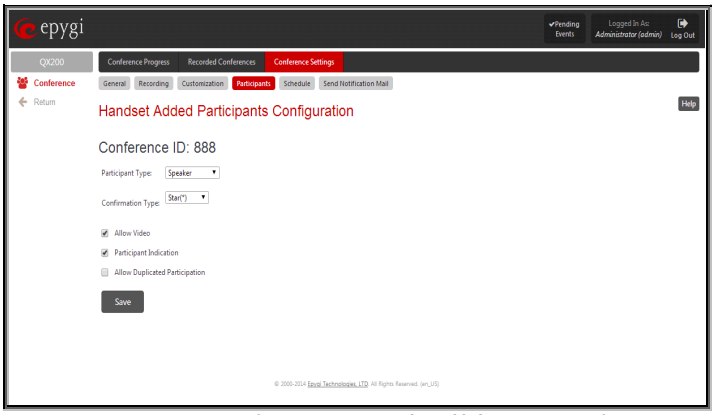


Fig.II- 304: Conference Settings – Handset Added Participants Configuration page

Schedule

The **Schedule** page is used to configure and manage the conference scheduling rules, so that a conference can be automatically activated on the date and time. The Scheduling service may also be configured to send invitation emails to the participants asking them to join the conference or informing about a new conference.

The **Conference Schedule** page offers a table that lists all scheduling rules configured for the corresponding conference. When a scheduled conference is activated, all participants with dial-out option enabled will be dialed.

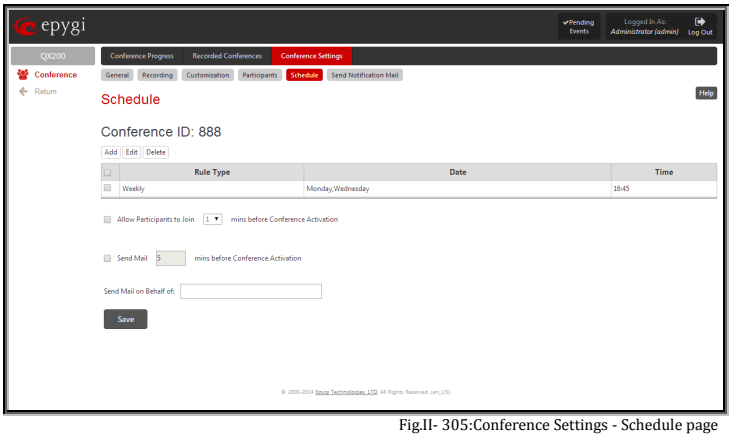


Fig.II- 305:Conference Settings - Schedule page

Clicking the **Add** button takes you to the **Add Entry** page where new scheduling rule can be configured. This page offers the following components:

A group of radio buttons that are used for selecting the frequency of the scheduled conference:

- **Once** – the calendar date (month, day, year) should be specified for this option.
- **Daily**
- **Weekly** – weekdays when scheduling out to be activates should be selected for this option. Use **Select All** and **Select None** to select or deselect all weekdays.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and the month should be selected for this option.

In the **Time** text fields, the time of the scheduled conference activation should be defined. The time selected in these fields will be considered according to the Date and Time Settings.

The **Allow Participants to join conference before Conference Activation** checkbox selection allows participants to dial in to the conference before conference activation.

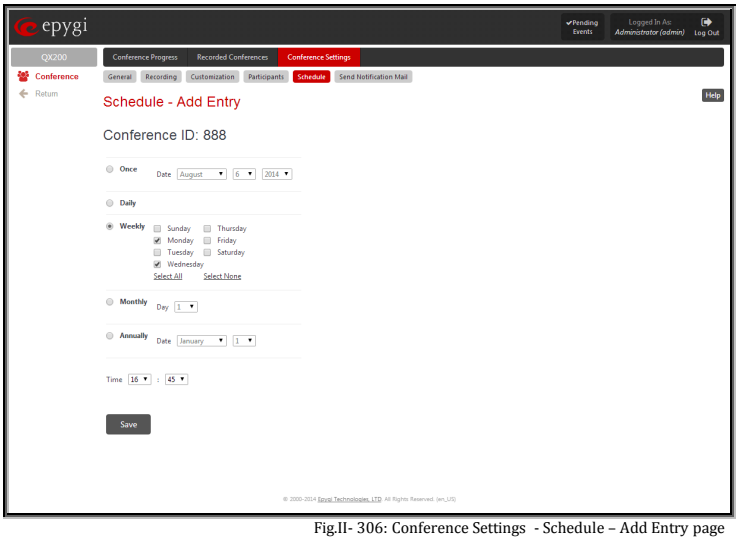


Fig.II- 306: Conference Settings - Schedule – Add Entry page

During this period, participants will be able to communicate with each other. However, this does not mean that the conference is activated; the participants will be dialed out (if any) and the recording will start (if configured) only after the configured scheduled time comes.

The **Send Mail before Conference Activation** checkbox enables email notification delivery to the participants before the conference activation. The text field requires the timeout (in minutes) before the conference activation when the email notifications to the conference participants with **Email Address** configured from the Add Participant page should be delivered. This option is only valid if the Email Address is configured for the participant.

The **Send Mail on behalf of** text field requires an email address or a conditional name related to the conference to be transmitted in the **From** field of the email notifications.

Send Notification Mail

This link is used to send an email to the participants notifying them about the start of a conference and inviting them to join. The text of the notification email is being configured by the administrator.

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.