



# Manual-II: Administration Guide for QX IP PBXs

This manual is effective for QX IP PBXs: QX20, QX50, QX200, QX500, QX2000, QX3000, QX5000 and QXISDN4+.

## 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.

## Copyright and Trademarks

Copyright © 2003-2018 Epygi Technologies, LLC. All Rights Reserved. QX and QUADRO are registered trademarks of Epygi Technologies, LLC. Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

## Emergency 911 Calls

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

## Limited Warranty

Epygi Technologies, LLC. ('Epygi') warrants to the original end-user purchaser every QX and Quadro 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, LLC. 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, LLC.

2233 Lee Road Suite 201 Winter Park, Florida 32789

### **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 to 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, LLC.

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 arrester in the AC outlet from which the QX or Quadro is powered.

### **Industry Canada Statement**

This product meets the applicable Industry Canada technical specifications.

### **Safety Information**

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

- To prevent fire or shock hazard, do not expose your QX or Quadro to rain or moisture.
- To avoid electrical shock, do not open the QX or Quadro. 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 non-insulated 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 QX or Quadro during an electrical storm.
- Do not use your QX, Quadro 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 QX or Quadro 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 QX or Quadro. 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 QX and Quadro is a 22 second fragment from Chopin's Nocturne Op.9 #2 performed by Marina Vardanyan and kindly provided to Epygi Technologies, LLC. 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.

## Document Edition History

Revision	Date	Description	Valid for Models	Valid for FW
1.0	24-Mar-17	Initial Release	QX IP PBXs	6.1.45 and higher
1.1	16-Jun-17	Added a new licensable feature - <b>Calling Cost Control</b> . Updated.	QX IP PBXs	6.1.50 and higher
1.2	11-Dec-17	Updated for the new QX3000.	QX20, QX50, QX200, QX500, QX2000 QX3000 and QXISDN4+	6.2.1 and higher
1.3	31-May-18	Updated	QX20, QX50, QX200, QX500, QX2000 QX3000 and QXISDN4+	6.2.11 and higher
1.4	15-Feb-20	Updated	QX20, QX50, QX200, QX500, QX2000 QX3000, QX5000 and QXISDN4+	6.3.1 and higher

## Table of Contents

1	About Administration Guide .....	7
2	Conventions Used in this Guide .....	7
3	QX Graphical Interface .....	9
4	Dashboard .....	10
5	<b>Setup Menu .....</b>	<b>11</b>
5.1	Basic Setup .....	12
5.2	System Security .....	23
5.3	Licensed Features.....	24
5.4	Redundancy .....	26
5.5	Language Pack.....	26
6	<b>Extensions Menu .....</b>	<b>28</b>
6.1	Extensions .....	29
6.2	Dialing Directories .....	66
6.3	Conferences .....	67
6.4	Recordings .....	67
6.5	Receptionist.....	68
6.6	ACD.....	68
6.7	Authorized Phones.....	68
7	<b>Interfaces Menu.....</b>	<b>70</b>
7.1	IP Lines.....	70
7.2	FXS.....	85
7.3	FXO .....	87
7.4	ISDN Trunk .....	89
7.5	E1/T1 Trunk.....	97
7.6	PSTN Gateways .....	98
8	<b>Telephony Menu.....</b>	<b>99</b>
8.1	VoIP Carrier .....	100
8.2	Call Routing .....	103
8.3	Call Recording Settings.....	124
8.4	NAT Traversal .....	125
8.5	RTP .....	128
8.6	SIP.....	130
8.7	Schedules.....	132
8.8	Advanced .....	133
9	<b>Firewall Menu .....</b>	<b>140</b>
9.1	Firewall.....	141
9.2	Filtering Rules .....	143
9.3	Custom Services.....	148
9.4	IP Groups .....	148
9.5	SIP IDS .....	150
10	<b>Network Menu.....</b>	<b>152</b>

10.1	Second LAN Interface.....	153
10.2	IP Routing.....	153
10.3	DHCP.....	155
10.4	DNS.....	158
10.5	PPP/PPTP.....	161
10.6	SNMP.....	163
10.7	VLAN.....	163
10.8	VPN.....	164
10.9	OpenVPN.....	173
<b>11</b>	<b>Status Menu.....</b>	<b>174</b>
11.1	System Status.....	175
11.2	Events.....	180
11.3	Call History.....	182
11.4	Conference History.....	188
11.5	Network Interfaces.....	188
11.6	Statistics.....	189
<b>12</b>	<b>Maintenance Menu.....</b>	<b>190</b>
12.1	Diagnostics.....	191
12.2	System Logs.....	194
12.3	User Rights.....	196
12.4	Backup / Restore.....	198
12.5	Firmware.....	203
12.6	Reboot.....	206
12.7	Registration Form.....	206
<b>13</b>	<b>Appendices.....</b>	<b>207</b>
13.1	Administrator Login.....	207
13.2	Needed Bandwidth for IP Calls.....	208
13.3	System Default Values.....	209
<b>14</b>	<b>References.....</b>	<b>222</b>
<b>15</b>	<b>Software License Agreement.....</b>	<b>223</b>

## 1 About Administration Guide

---

This guide is intended for administrators as an aid to configure and operate QX IP PBXs (herein QX). The functionality and configuration of QX with reference to other guides, manuals and complementary resources are described in this guide.

Many screen illustrations can be found in this guide. Since QX offers a wide variety of features and functionality, the example screenshots shown may not appear exactly the same for a specific QX as they appear in this manual. The example screenshots are for illustrative and explanatory purposes and should not be construed to represent your unique setup and scenarios.

## 2 Conventions Used in this Guide

---

Following conventions are used in this guide:

- **Add** button is used to create and add new entry.
- **Edit** button is used to modify the selected entry(s).
- **Delete** button is used to remove the selected entry(s).
- **Save** button is used to apply the changes.
- **Start** button is used to start a service, connection, etc.
- **Stop** button is used to start a service, connection, etc.
- **Enable/Disable** button is used to enable/disable the selected entry(s).
- **Move Up** and **Move Down** buttons are used to sort the entries in the specific table in the order they need to be accessed.
- **Generate Password** button is used to generate a system defined strong password.
- **Show Hot Desking Settings** and **Hide Hot Desking Settings** links are used to show/hide the **Hot Desking** settings respectively.
- **Hide extensions attached to disabled IP lines** and **Show all extensions** buttons are used to hide extensions which are attached to disabled IP lines or show all created extensions respectively.
- **Call Type** lists the available call types:
  - **PBX** – local calls to QX extensions.
  - **SIP** – calls via SIP.
  - **PSTN** – calls to a legacy telephone network (N/A for QX20, QX500, QX2000, QX3000 and QX5000).
  - **Auto** – calls to a destination resolved by the **Call Routing Table**.
- **Address (Redirect Address, Calling Address or Call to)** field is used to define the destination address the call will be addressed to. The address strictly depends on the call type. Thus, define an extension number for the PBX calls, SIP address for the SIP calls, phone number for the PSTN calls, and, finally, define a routing pattern for the Auto type calls.
- **Description** field is used to enter any optional information about the entry.
- **Wildcard supported** notification is used to mention that wildcards are allowed for the field. Go to the [Allowed Characters and Wildcards](#) section to see the complete list of the supported characters and wildcards.
- The following options are available on QX to select the way custom voice message will be provided:
  - **RTP Channel** is used to stream messages through **RTP Channels**.
  - **Audio Line In** is used to stream messages through **Audio Line In**. This option is not available on QXISDN4+, QX2000, QX3000 and QX5000.
  - **File** is used to upload/record custom messages.
    - ◆ Click **Choose File** to open a file chooser window to upload the file.

- ◆ Click **Record from Extension** to record a message directly on the phone.
- ◆ Once the message has been uploaded/recorded the following links will appear. The **Download ... message** link used to download the uploaded/recorded message. The **Remove ... message** link used to remove the uploaded/recorded message or restore the default one.

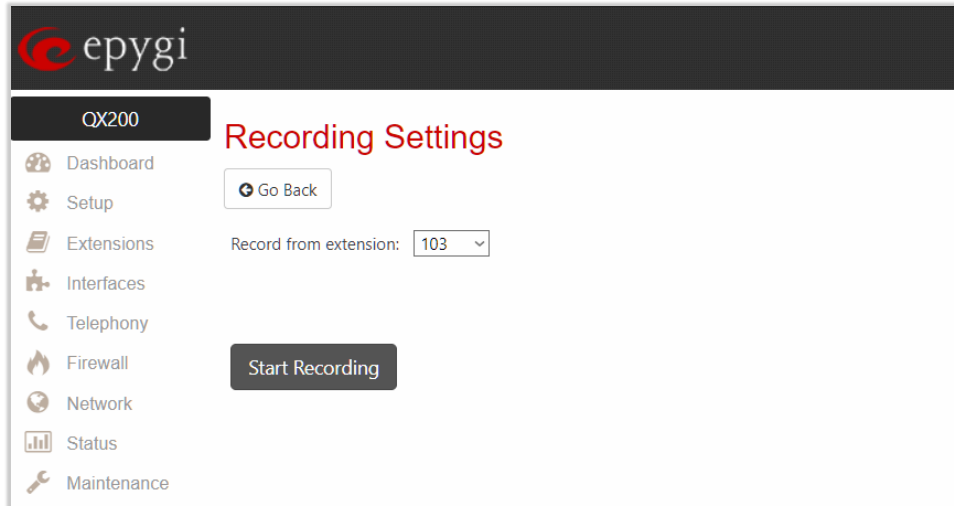


Figure 1: Recording Settings page

The **Recording Settings** page is used to initiate a custom voice message recording for the current extension directly from an IP phone. The **Record from extension** drop-down box lists all phone extensions that are available for recording.

Record a message as follows:

1. Select the extension from the **Record from extension** list.
2. Click **Start Recording**. The phone for the selected extension will start ringing.
3. Answer the call and follow the audio prompts to record a message.
4. Once the message has been recorded the following buttons will appear:
  - **Download Recording** is used to download the recorded message.
  - **Restore Default Recording** is used to remove the recorded message and restore the default one.

**Note:**

- The uploaded file should be either in (\*.wav) or (\*.mp3) format.
- The maximum duration of uploaded file is limited to **5** minutes.
- The maximum size of uploaded file is limited to **7.5** MB.



### 3 QX Graphical Interface

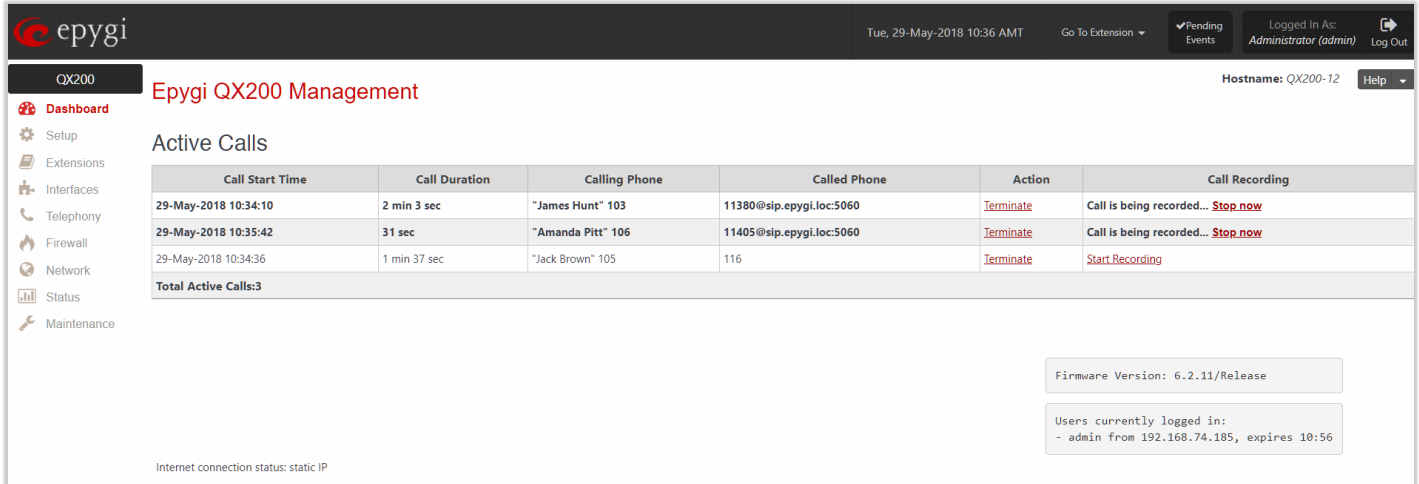
---

The following top menus and links are available when logged in as an administrator:

- [Dashboard](#)
- [Setup](#)
- [Extensions](#)
- [Interfaces](#)
- [Telephony](#)
- [Firewall](#)
- [Network](#)
- [Status](#)
- [Maintenance](#)
- **Go To Extension** allows quick access to **User Settings** for the selected extension.
- **Pending Events** allows quick access to system events and event settings.
- **Language** is available in case a custom **Language Pack** is installed and is used to enable custom language for GUI or revert back to default **English**.
- **Date/Time** displays the current time of device.
- **Hostname** displays the hostname of device.
- **Renew WAN IP Address** is available in case a WAN IP address for QX is assigned dynamically via DHCP.

## 4 Dashboard

If you are logged in as an administrator (**users:** admin or localadmin), you will see the number of calls currently active on the QX. The **Active Calls** table includes information about the calling/called parties, call start time and duration.



The screenshot shows the Epygi QX200 Management interface. The top navigation bar includes the Epygi logo, the date and time (Tue, 29-May-2018 10:36 AMT), a 'Go To Extension' dropdown, a 'Pending Events' indicator, and the user's login information (Administrator (admin) with a Log Out button). The main content area is titled 'Epygi QX200 Management' and features a sidebar menu with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The 'Active Calls' section displays a table with the following data:

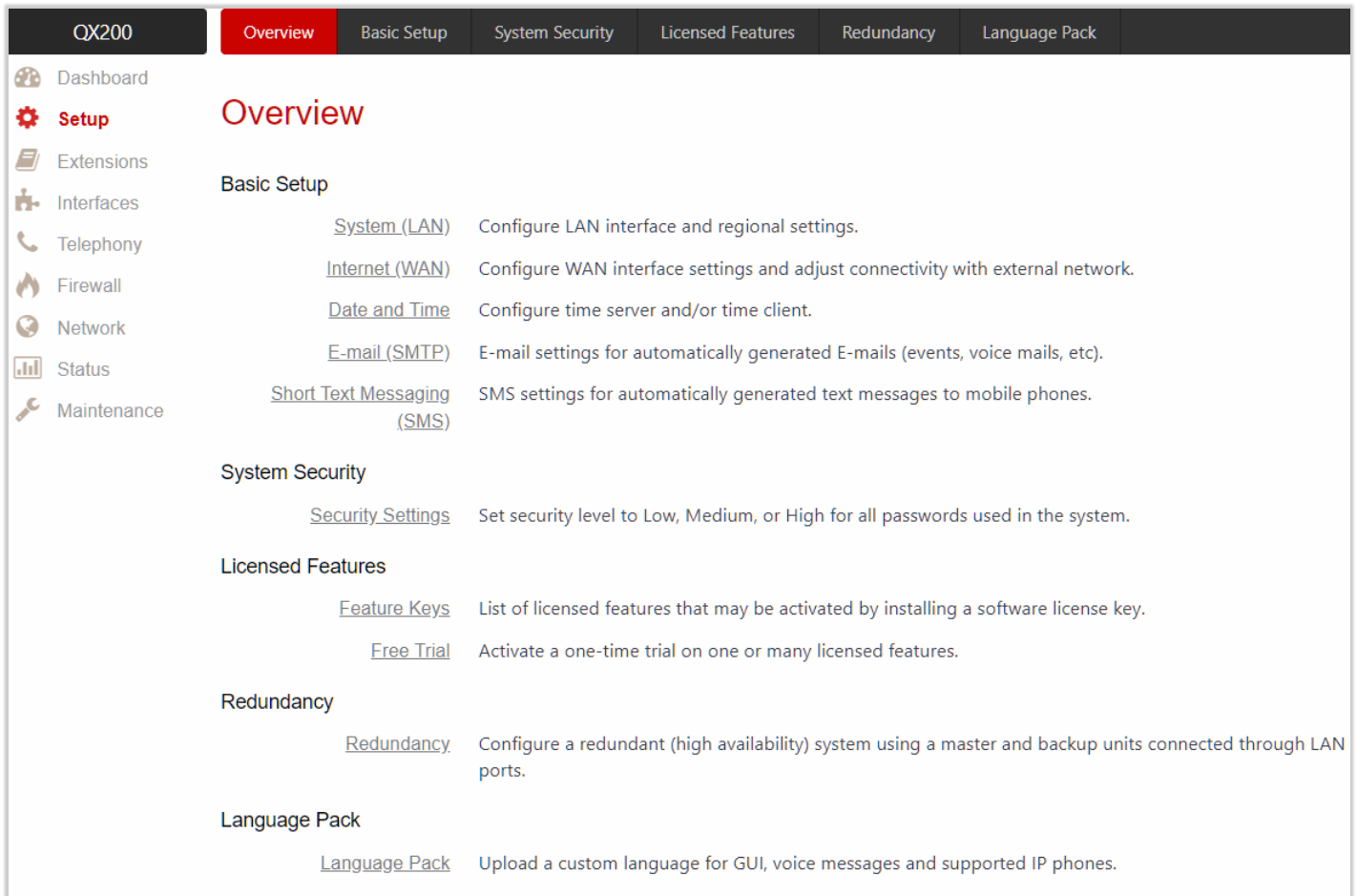
Call Start Time	Call Duration	Calling Phone	Called Phone	Action	Call Recording
29-May-2018 10:34:10	2 min 3 sec	"James Hunt" 103	11380@sip.epygi.loc:5060	<a href="#">Terminate</a>	Call is being recorded... <a href="#">Stop now</a>
29-May-2018 10:35:42	31 sec	"Amanda Pitt" 106	11405@sip.epygi.loc:5060	<a href="#">Terminate</a>	Call is being recorded... <a href="#">Stop now</a>
29-May-2018 10:34:36	1 min 37 sec	"Jack Brown" 105	116	<a href="#">Terminate</a>	<a href="#">Start Recording</a>
<b>Total Active Calls:3</b>					

Additional system information is displayed in the bottom right corner, including the Firmware Version (6.2.11/Release) and a list of users currently logged in (admin from 192.168.74.185, expires 10:56). The bottom left corner shows the Internet connection status as static IP.

Figure 2: Dashboard menu

- **Terminate** link is used to terminate the active call.
- **Start Recording** link is used to manually start the recording of the call. Once the call recording starts, the link changes to **Stop now** and is used to manually stop the recording.
- The list of users currently logged into the system appears in the lower right corner of the page. The IP address of the user, the time until the next automatic logout and the current version of the firmware are displayed as well. The idle session timeout is set to **10** minutes. If no action is performed within **10** minutes, the user will automatically get logged out.

## 5 Setup Menu



QX200	Overview	Basic Setup	System Security	Licensed Features	Redundancy	Language Pack
Dashboard	<b>Overview</b>					
<b>Setup</b>	<b>Basic Setup</b>					
Extensions		<a href="#">System (LAN)</a>	Configure LAN interface and regional settings.			
Interfaces		<a href="#">Internet (WAN)</a>	Configure WAN interface settings and adjust connectivity with external network.			
Telephony		<a href="#">Date and Time</a>	Configure time server and/or time client.			
Firewall		<a href="#">E-mail (SMTP)</a>	E-mail settings for automatically generated E-mails (events, voice mails, etc).			
Network		<a href="#">Short Text Messaging (SMS)</a>	SMS settings for automatically generated text messages to mobile phones.			
Status		<b>System Security</b>				
Maintenance		<a href="#">Security Settings</a>	Set security level to Low, Medium, or High for all passwords used in the system.			
		<b>Licensed Features</b>				
		<a href="#">Feature Keys</a>	List of licensed features that may be activated by installing a software license key.			
		<a href="#">Free Trial</a>	Activate a one-time trial on one or many licensed features.			
		<b>Redundancy</b>				
		<a href="#">Redundancy</a>	Configure a redundant (high availability) system using a master and backup units connected through LAN ports.			
		<b>Language Pack</b>				
		<a href="#">Language Pack</a>	Upload a custom language for GUI, voice messages and supported IP phones.			

Figure 3: Setup Menu overview

## 5.1 Basic Setup

### 5.1.1 System (LAN)

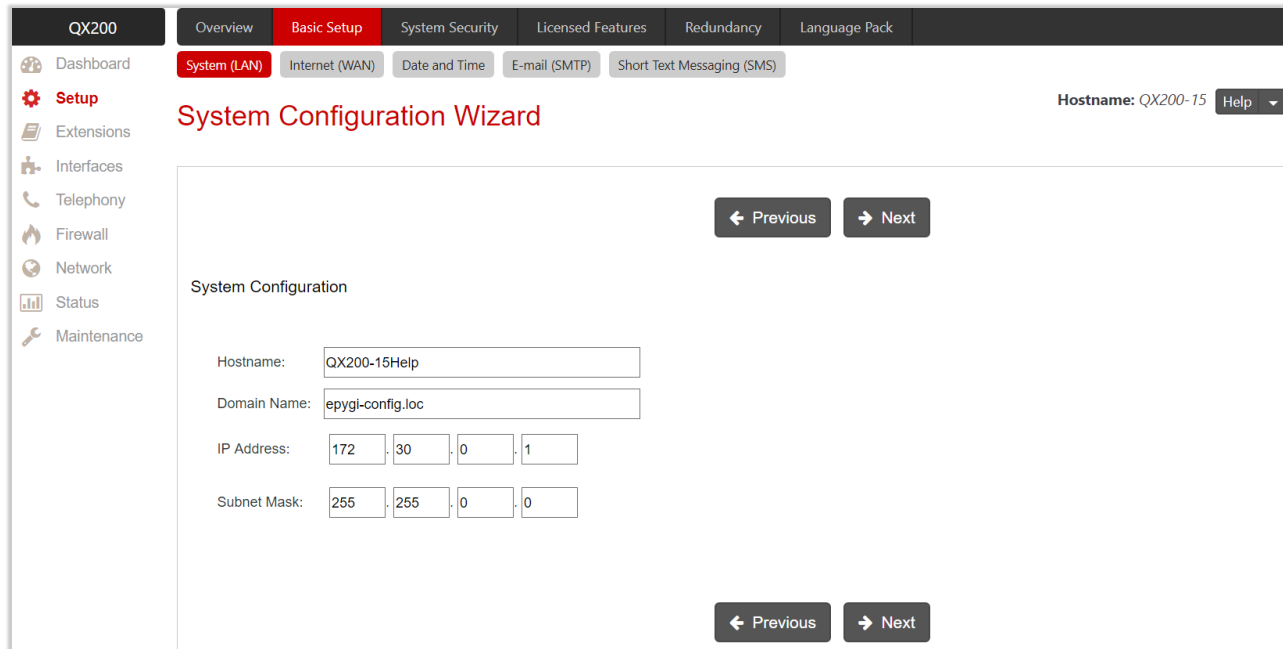
You can login the QX WEB GUI through LAN interface using the default IP address:

- For QX20, QX50, QX200, QX500 and QXISDN4+ – **172.30.0.1**
- For QX2000, QX3000 and QX5000 – **192.168.0.200**

Go to **Setup**→**Basic Setup**→**System (LAN)** to adjust the network parameters for the LAN interface. The **System Configuration Wizard** consists of the following sections:

- [System Configuration](#)
- [DHCP Settings for the LAN Interface](#)
- [Regional Settings and Preferences](#)
- [Emergency Codes and PSTN Access Code Settings](#)
- [Call Alert Settings](#)
- [Summary](#)

### System Configuration



The screenshot shows the 'System Configuration Wizard' interface. At the top, there are tabs for 'Overview', 'Basic Setup' (selected), 'System Security', 'Licensed Features', 'Redundancy', and 'Language Pack'. Below these are sub-tabs for 'System (LAN)', 'Internet (WAN)', 'Date and Time', 'E-mail (SMTP)', and 'Short Text Messaging (SMS)'. The main content area is titled 'System Configuration Wizard' and contains the following fields:

- Hostname:
- Domain Name:
- IP Address:  .  .  .
- Subnet Mask:  .  .  .

Navigation buttons for 'Previous' and 'Next' are located above and below the configuration fields.

Figure 4: System Configuration section

The **System Configuration** section is used to configure the following settings (options):

- Hostname
- Domain Name
- IP Address
- Subnet Mask

## DHCP Settings for the LAN Interface

The screenshot shows the 'System Configuration Wizard' for 'QX200'. The 'Basic Setup' tab is active, and the 'System (LAN)' sub-tab is selected. The main content area is titled 'DHCP Settings for the LAN Interface'. It includes a 'Previous' and 'Next' navigation bar at the top. Below this, there is a checkbox labeled 'Enable DHCP Server' which is checked. Underneath, the 'Dynamic IP Address Range' is set from '172.30.0.100' to '172.30.0.254'. The 'WINS Server' is set to '0.0.0.0'. A 'Static Mappings' section shows '172.30.0.52'. At the bottom, there is another 'Previous' and 'Next' navigation bar.

Figure 5: DHCP Settings for the LAN Interface section

The DHCP Settings for the LAN Interface section is used to configure the following settings (options):

- Enable DHCP Server is used to activate DHCP server on QX.
- Dynamic IP Address Range is used to set the IP address pool.
- WINS Server is used to set the IP address for the WINS server.

## Regional Settings and Preferences

Regional Settings are important for the functionality of QX voice subsystem.

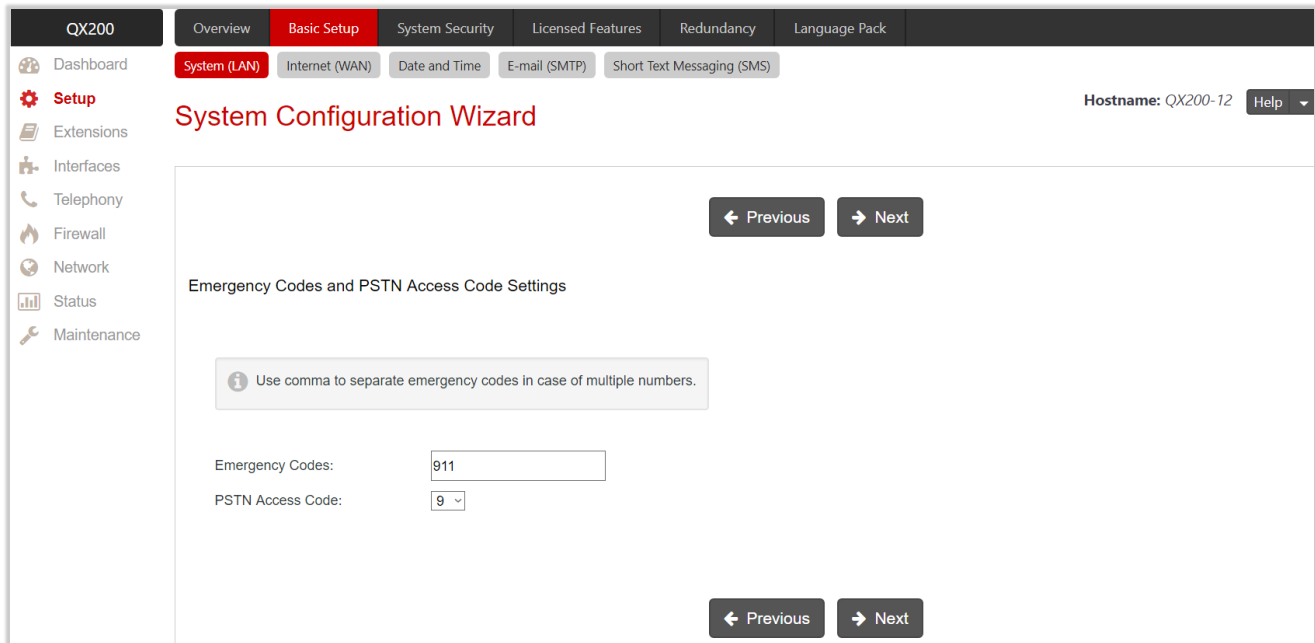
The screenshot shows the 'System Configuration Wizard' for 'QX200'. The 'Basic Setup' tab is active, and the 'System (LAN)' sub-tab is selected. The main content area is titled 'Regional Settings and Preferences'. It includes a 'Previous' and 'Next' navigation bar at the top. Below this, there are two dropdown menus: 'Your locale (location):' set to 'Armenia' and 'Timezone:' set to '(GMT+04:00) Yerevan'. Underneath, there is a section 'Choose System Language' with two radio buttons: 'Italian (Italy)' and 'English (US)', with 'English (US)' selected. At the bottom, there is another 'Previous' and 'Next' navigation bar.

Figure 6: Regional Settings and Preferences section

The **Regional Settings and Preferences** section is used to configure the following settings (options):

- **Your Locale (location)** is used to select the location and time zone of QX.
- **Timezone** is used to select the proper time zone so QX can display the correct time. **TIP:** QX supports **Daylight Savings (DST)** correction if it is available for the selected time zone.
- **Choose System Language** is used to select the language for system voice messages: **custom** or **default English**. **TIP:** This selection is available when a custom **Language Pack** has been uploaded.

## Emergency Codes and PSTN Access Code Settings



The screenshot shows the 'System Configuration Wizard' interface for a QX200 device. The 'Basic Setup' tab is active, and the 'Emergency Codes and PSTN Access Code Settings' section is displayed. The interface includes a navigation bar at the top with tabs for Overview, Basic Setup, System Security, Licensed Features, Redundancy, and Language Pack. Below the navigation bar, there are sub-tabs for System (LAN), Internet (WAN), Date and Time, E-mail (SMTP), and Short Text Messaging (SMS). The main content area features a title 'System Configuration Wizard' and a 'Hostname: QX200-12' label. The 'Emergency Codes and PSTN Access Code Settings' section contains an information box stating 'Use comma to separate emergency codes in case of multiple numbers.' Below this, there are two input fields: 'Emergency Codes' with the value '911' and 'PSTN Access Code' with a dropdown menu showing '9'. Navigation buttons for 'Previous' and 'Next' are located at the top and bottom of the settings area.

Figure 7: Emergency Codes and PSTN Access Code Settings section

The **Emergency Codes and PSTN Access Code Settings** section is used to configure the following settings (options):

- **Emergency Codes** is used to set PSTN number(s) of emergency service(s). For each emergency code, a routing pattern will be generated in the **Call Routing Table**, allowing faster and easier calls to emergency services. **TIP:** Use commas to separate emergency codes in case of multiple numbers.
- **PSTN Access Code** is used to select prefix code for accessing PSTN line through routing table.

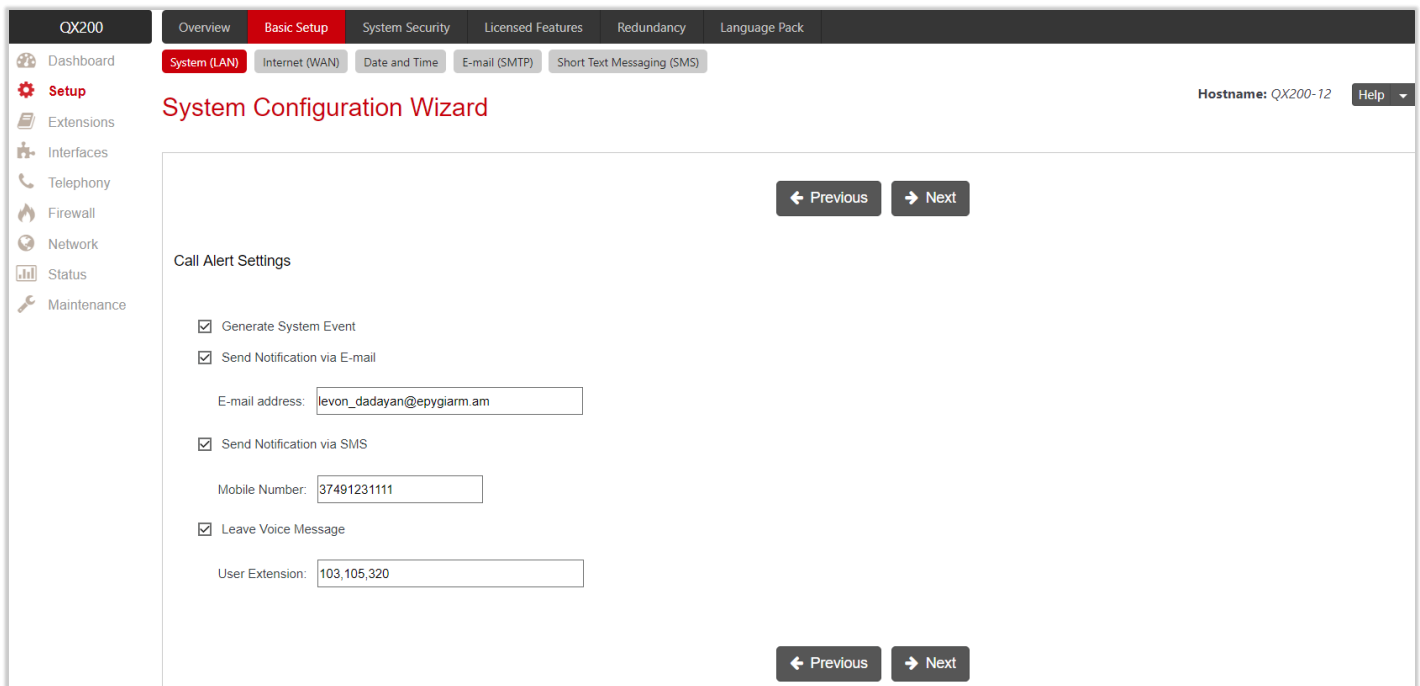
## Call Alert Settings

This section is used to activate the call alert service and configure settings. The **Call Alert** service is used to notify the designated personnel about emergency calls, as well as calls through the certain call routing rules. The following information will be included in the notification: the routing pattern, the user extension who placed the call, the dialed number and the call Date/Time.

The following settings (options) are available:

- **Generate System Event** is used to generate and display event notification in the **System Events**.
- **Send Notification via E-mail** is used to send a notification to a specified address via e-mail.
- **Send Notification via SMS** is used to send a notification to a specified number via SMS.
- **Leave Voice Message** is used to leave a voice mail on defined extension(s) with a voice message.

**Note:** Use commas to separate email addresses, mobile numbers and user extensions in case of multiple entries.



The screenshot shows the 'System Configuration Wizard' interface for a QX200 device. The 'Basic Setup' tab is active, and the 'Call Alert Settings' section is displayed. The settings are as follows:

- Generate System Event
- Send Notification via E-mail
  - E-mail address:
- Send Notification via SMS
  - Mobile Number:
- Leave Voice Message
  - User Extension:

Navigation buttons for 'Previous' and 'Next' are visible at the top and bottom of the form area.

Figure 8: Call Alert Settings section

## Summary

This section displays all configured settings (options) before applying them.

### Note:

- Finish the wizard and click "OK" to apply the changes made in all sections of the wizard. You must confirm the settings within **20** minutes. Otherwise the device will return back to the previous configuration and reboot.
- It is strongly recommended to leave the factory default settings unchanged if their meanings are not fully clear to you.

## 5.1.2 Internet (WAN)

Go to the **Setup**→**Basic Setup**→**Internet (WAN)** to configure or adjust the network parameters for QX WAN interface. **Internet Configuration Wizard** consists of the following sections:

- [Uplink Configuration](#)
- [WAN Interface Configuration](#)
- [DNS Settings](#)
- [Summary](#)

### Uplink Configuration

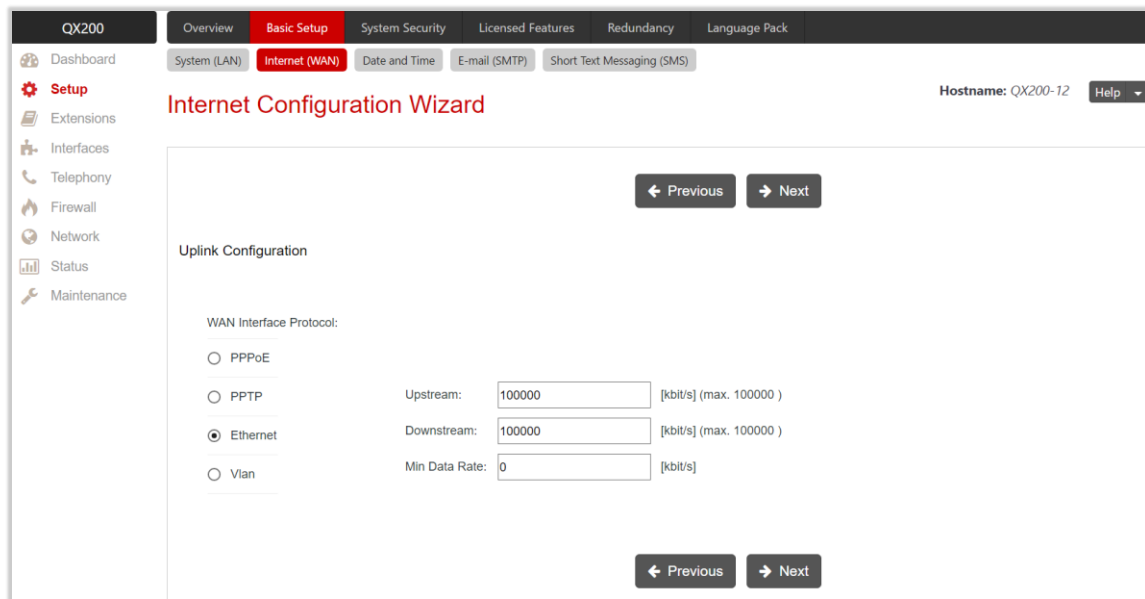


Figure 9: Uplink Configuration section

The **Uplink Configuration** section is used to configure the following settings (options):

- **WAN Interface Protocol** is used to select the protocol for the WAN interface. Based on this selection the wizard configuration sections may differ. The following protocols are available:
  - PPPoE
  - PPTP
  - Ethernet
  - VLAN (**TIP:** This option becomes available only when VLAN is configured on QX.)
- **WAN Interface Bandwidth** is used to specify the upstream and downstream speeds in Kbit/s, helping to assure the quality of IP calls. IP call loses the voice quality if there is no available bandwidth. When the limits of a bandwidth capacity are approaching, another IP call will be rejected.
- **Min Data Rate** is used to set the amount of upstream bandwidth that ought to remain for data traffic even if voice applications use the entire available upstream bandwidth. The value selected here needs to be smaller than the upstream bandwidth.



## PPPoE

- **Keep Connection Alive** is used to keep the connection alive by sending control packets for the link state verification.
- **Authentication Settings** is used to set the authentication parameters (**Username** and **Password**) to register on the ISP server.
- **Dial Behavior** is used to select the **Dial Behavior** type.
  - **Dial manually** – if selected, a button will be displayed on the **Dashboard** to switch the connection on/off.
  - **Always connected** – if selected, the connection will always stay active and connected.
- **IP Address Assignment** is used to select the IP address assignment type:
  - **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.
  - **Use the following IP Address** is used to set the IP address manually.

## PPTP

- **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.
- **Use the following IP Address** is used to set the IP address manually.

Click **Next** to continue the configuration of **PPP/ PPTP** settings:

- **PPTP Server** is used to set the IP address of PPTP server.
- **Encryption** is used to select the encryption for the traffic over PPTP interface.
- **Keep Connection Alive** is used to keep the connection alive by sending control packets for the link state verification.
- **Authentication Settings** is used to set the authentication parameters (Username and Password) to register on the ISP server.
- **Dial Behavior** is used to select the **Dial Behavior** type:
  - **Dial manually** – if selected, a button will be displayed on the **Dashboard** to switch the connection on/off.
  - **Always connected** – if selected, the connection will always stay active and connected.
- **IP Address Assignment** is used to select the IP address assignment type:
  - **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.
  - **Use the following IP Address** is used to set the IP address manually.

## Ethernet

- **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.
- **Use the following IP Address** is used to set the IP address manually.

## VLAN

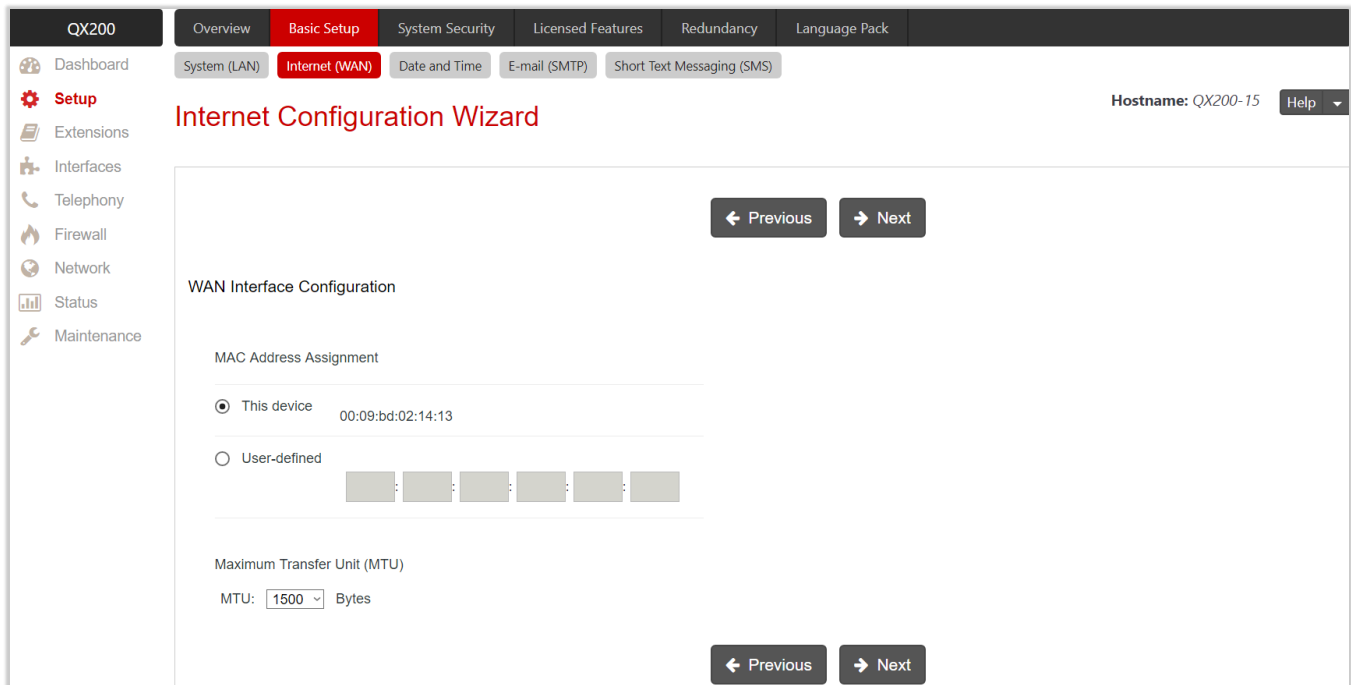
- **VLAN ID** is used to select **VLAN ID** from the configured VLAN list.

Click **Next** to continue the configuration of the **VLAN IP Configuration** settings:

- **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.
- **Use the following IP Address** is used to set the IP address manually.

## WAN Interface Configuration

The **WAN Interface Configuration** section is used to set the MAC address of QX. This might be necessary if the ISP requires a specified MAC address (e.g. for authentication).



The screenshot displays the WAN Interface Configuration section of the QX200 web interface. The navigation bar at the top includes 'Overview', 'Basic Setup', 'System Security', 'Licensed Features', 'Redundancy', and 'Language Pack'. The 'Basic Setup' tab is active, and the 'Internet (WAN)' sub-tab is selected. The main content area is titled 'Internet Configuration Wizard' and shows the 'WAN Interface Configuration' section. Under 'MAC Address Assignment', the 'This device' radio button is selected, showing the MAC address '00:09:bd:02:14:13'. The 'User-defined' option is unselected, with a form for manual entry. Below this, the 'Maximum Transfer Unit (MTU)' is set to '1500' Bytes. Navigation buttons for 'Previous' and 'Next' are located at the top and bottom of the configuration area.

Figure 10: WAN Interface Configuration section

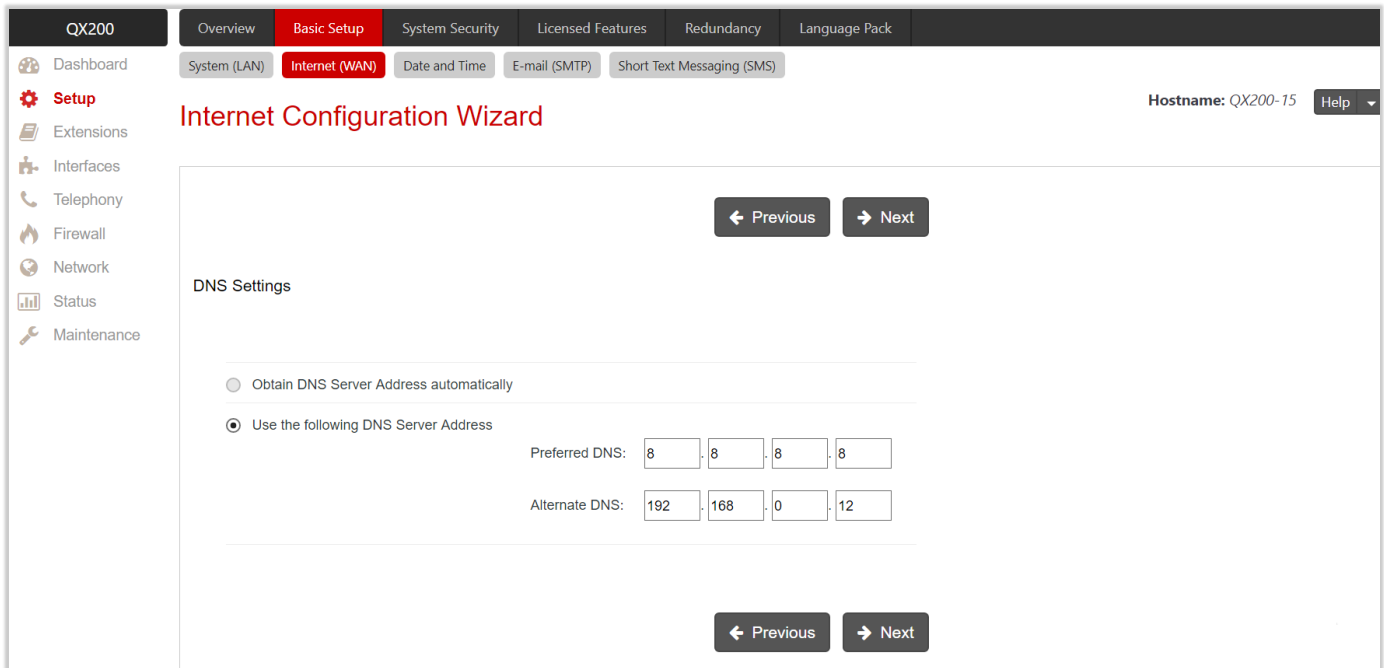
The following settings (options) are available:

- **This device** is used to select the default MAC address of the WAN interface.
- **User-defined** is used to set the MAC Address manually.
- **MTU** is used to select the maximum size of packet that can be sent in a packet or frame-based network such as the Internet. QX supports packet fragmentation. **TIP:** The default MTU size is **1500** bytes for Ethernet protocol and **1400** bytes for PPPoE.

## DNS Settings

The **DNS Settings** section is used to configure the following settings (options):

- **Obtain DNS Server Address automatically** – if selected, QX will get the IP address of DNS server from local network or ISP automatically.
- **Use the following DNS Server Address** is used to manually assign a name server as follows:
  - **Preferred DNS** is used to set the IP address of name server.
  - **Alternate DNS** is used to set the IP address of the secondary name server that will be used if the main name server cannot be accessed.



The screenshot shows the 'Internet Configuration Wizard' for a QX200 device. The 'Basic Setup' tab is active, and the 'Internet (WAN)' sub-tab is selected. The 'DNS Settings' section is visible, with two radio button options: 'Obtain DNS Server Address automatically' (unselected) and 'Use the following DNS Server Address' (selected). Below the selected option, there are two rows of IP address input fields. The 'Preferred DNS' row has four fields containing the values 8, 8, 8, and 8. The 'Alternate DNS' row has four fields containing the values 192, 168, 0, and 12. Navigation buttons for 'Previous' and 'Next' are located above and below the settings area. The top navigation bar includes 'Overview', 'Basic Setup', 'System Security', 'Licensed Features', 'Redundancy', and 'Language Pack'. The left sidebar lists various system components like Dashboard, Setup, Extensions, etc. The top right corner shows the hostname 'QX200-15' and a 'Help' button.

Figure 11: DNS Settings section

## Summary

This section displays all configured settings (options) before applying them.

### **Note:**

- Finish the wizard and click "OK" to apply the changes made in all sections of the wizard. You must confirm the settings within **20** minutes. Otherwise the device will return back to the previous configuration and reboot.
- It is strongly recommended to leave the factory default settings unchanged if their meanings are not fully clear to you.
- **Internet Configuration Wizard** is renamed to **Uplink Configuration Wizard** on QX2000 and QX3000.

### 5.1.3 Date and Time

QX **Date and Time** settings can be updated through international time servers.

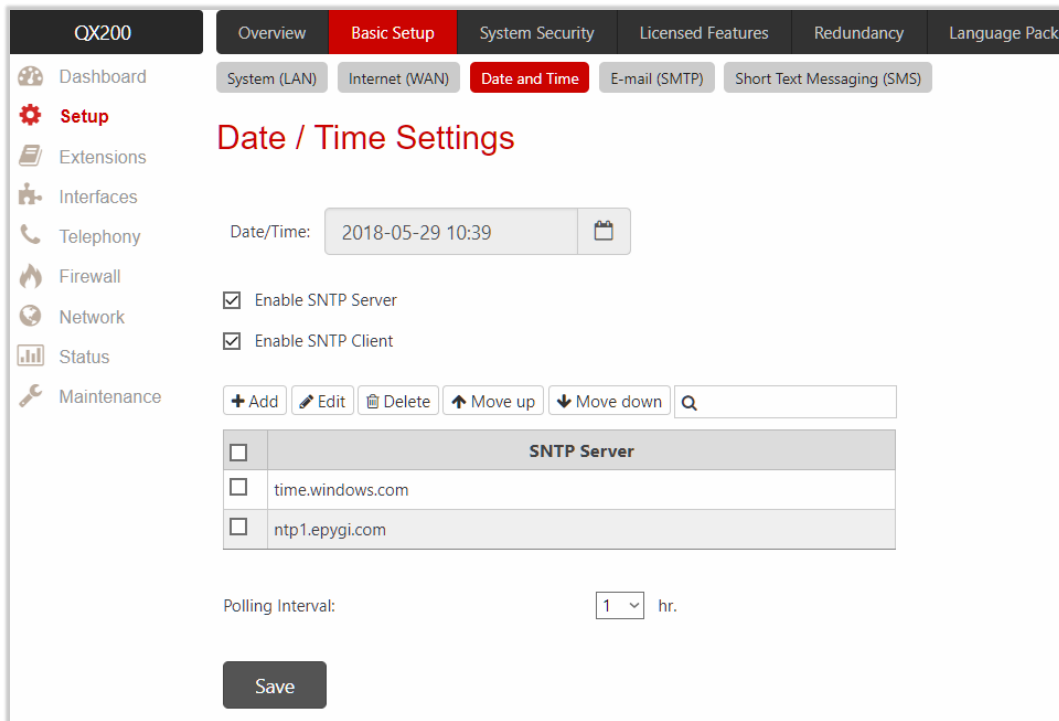


Figure 12: Date / Time Settings page

The following settings (options) are available:

- **Date/Time** shows the current system time.
- **Enable SNTP Server** is used to activate SNTP server on QX.
- **Enable SNTP Client** is used to activate SNTP client on QX. If not selected, the current system time can be configured manually.
- **Polling Interval** is used to select the time interval for periodical synchronization between the timeserver and QX.

The **SNTP Server** table lists all defined SNTP servers. To add a new **SNTP Server**:

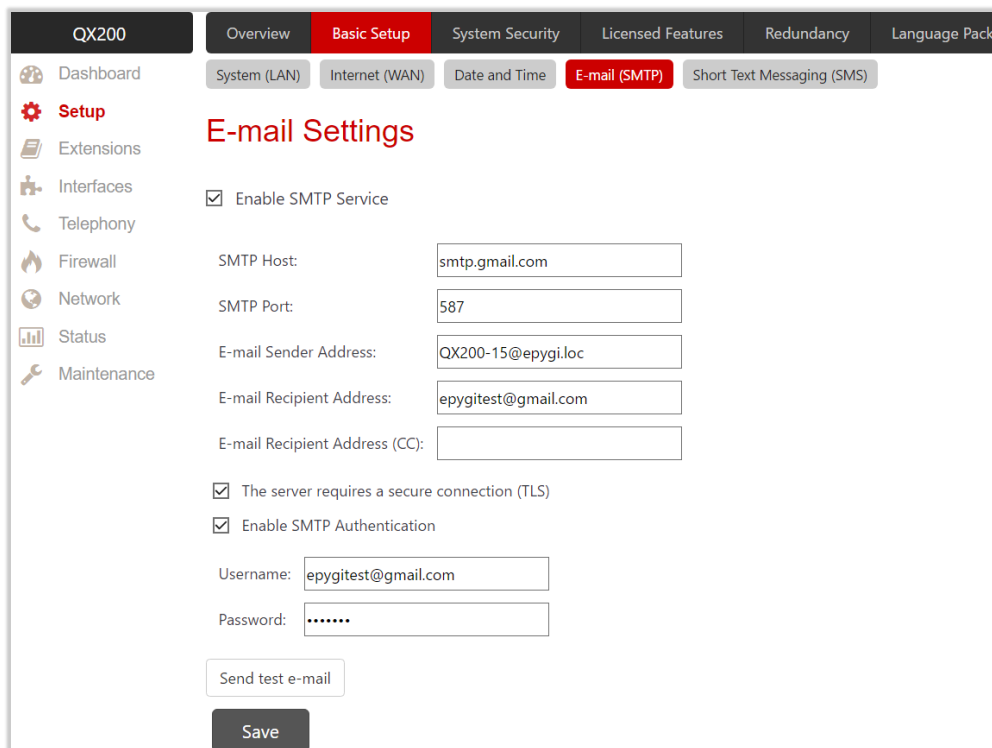
1. Click **Add** to define new server parameters. The following options are available:
  - **Manual** is used to set the **Full Qualified Domain Name (FQDN)** or IP address of the SNTP server.
  - **Predefined** is used to select the FQDN of the SNTP server from the drop-down list.
2. Click **Save** to add the new SNTP server to the **SNTP Servers** table.
3. Click **Move Up** or **Move Down** to sort NTP servers in the order they need to be accessed. **TIP:** If the NTP server in the first position of the **SNTP Server** table does not answer, NTP server in the next position will be attempted to reach.

### 5.1.4 E-mail (SMTP)

The **SMTP** service allows QX to automatically generate and send alert and notification e-mails as specified in the **Event Settings**. The **E-mail Settings** page is used to configure SMTP settings (parameters):

- **Enable SMTP Service** activates the SMTP service.
- **SMTP Host** is used to set the IP address or hostname of the SMTP server.
- **E-mail Sender Address** is used to set the e-mail address that is either registered on the selected SMTP server or has permission to use SMTP server for e-mail transmissions.
- **E-mail Recipient Address** – an active address to send e-mails to.
- **E-mail Recipient Address (CC)** – an active address to deliver e-mails' carbon copy (CC) to.
- **The server requires a secure connection (TLS)** is used to select if the specified SMTP server requires secure connection using TLS. If the specified SMTP server allows to use both secure and unsecure connections, then this selection forces to establish the secure connection.
- **Enable SMTP Authentication** is used to select if the specified SMTP server requires authentication. Then enter the **Username** and **Password** configured on the SMTP server.

Below is the sample of e-mail settings on the QX, (**smtp.gmail.com** is used as a **SMTP** server).



The screenshot displays the 'E-mail Settings' page within the QX200 web interface. The page is organized into a sidebar on the left with navigation options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area is titled 'E-mail Settings' and contains the following configuration fields:

- Enable SMTP Service
- SMTP Host:
- SMTP Port:
- E-mail Sender Address:
- E-mail Recipient Address:
- E-mail Recipient Address (CC):
- The server requires a secure connection (TLS)
- Enable SMTP Authentication
- Username:
- Password:

At the bottom of the form, there are two buttons: 'Send test e-mail' and 'Save'.

Figure 13: E-mail Settings page

Once configured, click **Send test e-mail** to send a test e-mail to the defined e-mail address to verify the settings.

### 5.1.5 Short Text Messaging (SMS)

The **SMS** service allows QX to automatically generate and send alert and notification events via SMS. The **SMS Settings** page is used to configure the SMS parameters:

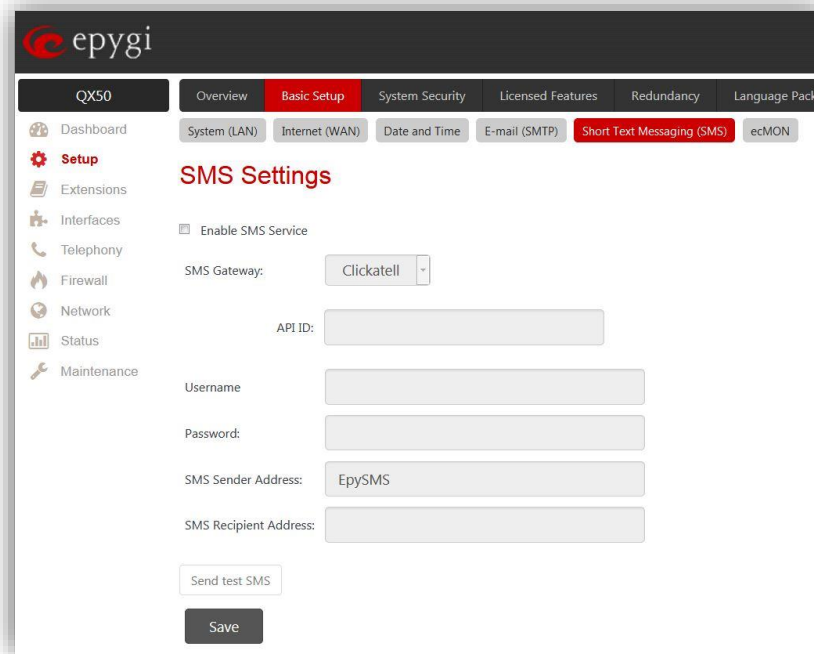


Figure 14: SMS Settings page

- **Enable SMS Service** is used to activate the SMS service on the QX.
- **SMS Gateway** is used to select the SMS gateway type: Clickatell, Twilio or Custom.
- **Username** and **Password** are used to set the authentication parameters configured on the SMS server.
- **SMS Sender Address** is used to set the sender's address.
- **SMS Recipient Address** is used to set the recipient's address. **TIP:** Use a space, semicolon or a comma to separate mobile numbers in case of multiple recipients.

You may either use a predefined SMS gateway (Clickatell/Twilio) or define a custom one.

- **Clickatell** – if selected, then set the **Clickatell** specific parameter provided by the server in the activated **API ID** field. This parameter must be identical on both sides.
- **Twilio** – if selected, then set the **Twilio** specific parameters provided by the server in the activated **SID** and **Auth. Token** fields. These parameters must be identical on both sides.
- **Custom** – if selected, then set the gateway parameters as follows:
  - **Resource** is used to set the HTTP resource name on the SMS gateway.
  - **Parameters** is used to set 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 depends on the SMS gateway requirements. The tokens are the strings that have the following dependencies from the field in this page:
    - ◆ **%username%** indicates the username set in the **Username** field.
    - ◆ **%password%** indicates the password set in the **Password** field.
    - ◆ **%to%** indicates the password set in the **SMS Recipient Address** field.
    - ◆ **%from%** indicates the password set in the **SMS Sender Address** field.
    - ◆ **%text%** indicates the SMS text generated by UC (voice mail notification, event notification, etc.).

**For example:** user=%username%&password=%password%&to=%to%&from=%from%&text=%text%

- **Server** is used to set the IP address or hostname of the SMS gateway.
- **Port** is used to set the port number of the SMS gateway.
- **Use Secure HTTP** to access the SMS server via HTTPS. Then set the port number for HTTPS traffic in the activated **Secure Port** field.
- Select one of the HTTP request methods (**POST** or **GET**) through the **Request Method** options. The UC uses one of these methods to access the SMS gateway.

Once configured, click **Send test SMS** to send a test SMS to the defined mobile number to verify the settings.

## 5.2 System Security

**System Security Management** is used to manage the global security of QX.

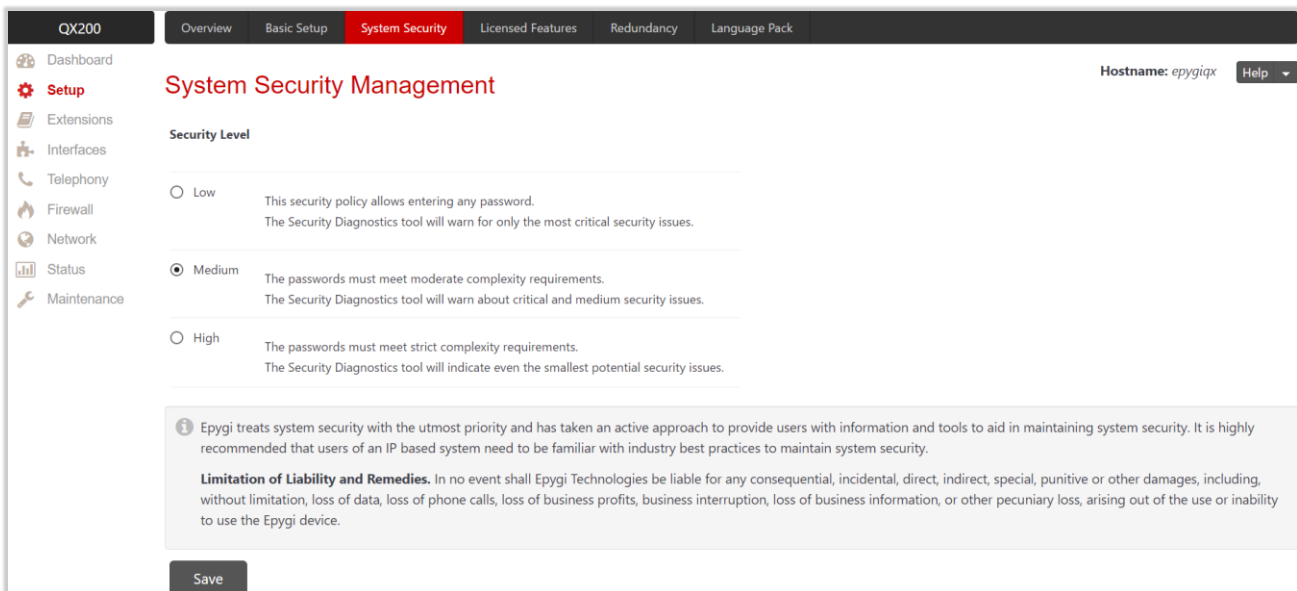


Figure 15: System Security Management page

The security levels are the following:

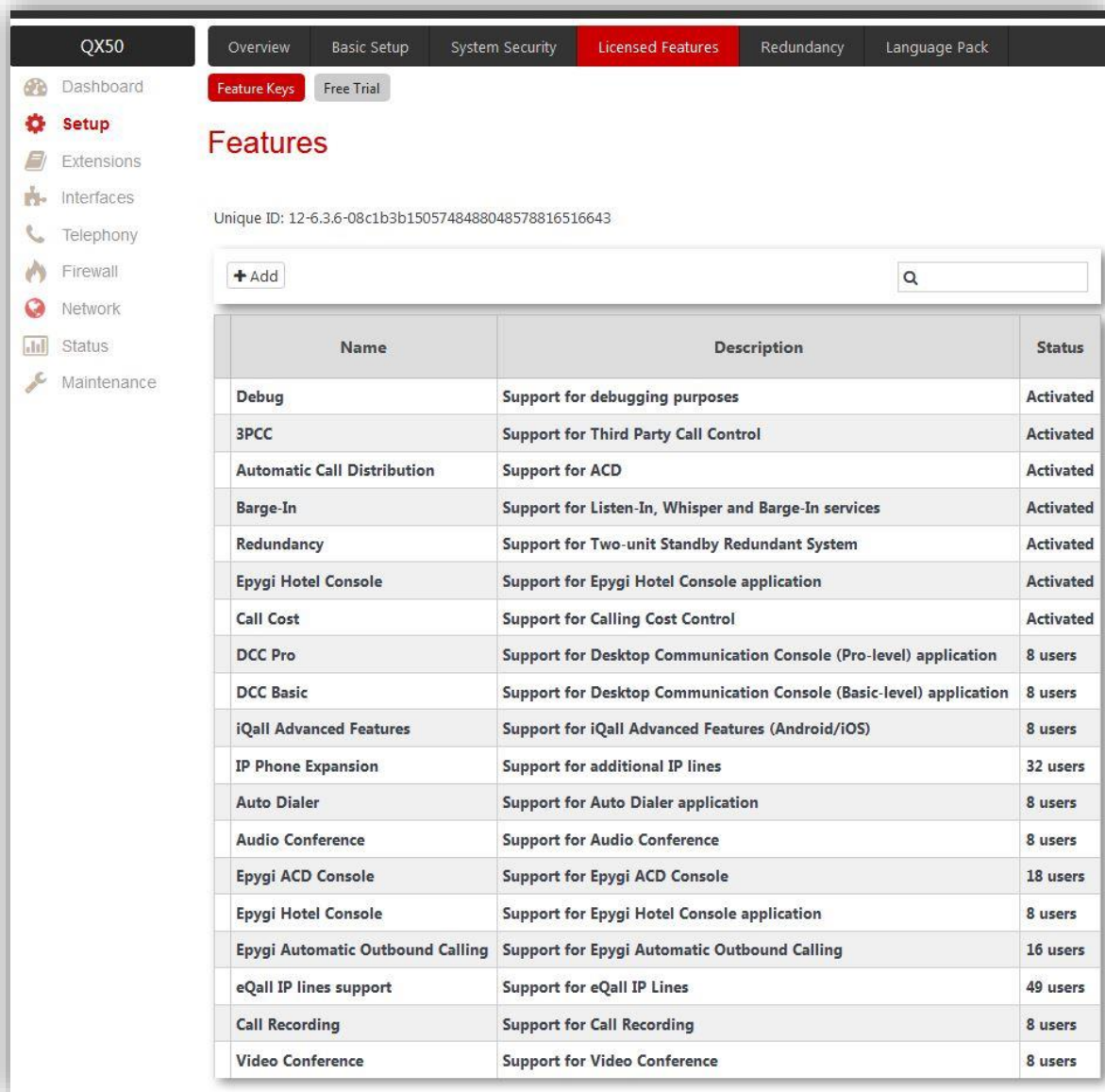
- **Low** – there are no specific restrictions on the strength of the saved password. The **Security Report** will generate warning for critical routing rules (PSTN and IP-PSTN) and if the Firewall and IDS services are disabled.
- **Medium** – the minimum strength of passwords must be "**moderate**". The **Security Report** will generate warnings for all unsecured routing rules, IP line and extension passwords, Firewall level (if it is set below **Medium**), disabled IDS, default administrator passwords.
- **High** – the minimum strength of passwords must be "**strong**". The **Security Report** will generate warnings for the IP line and extension passwords, disabled IDS, all unsecured routing rules, Firewall level (if it is set below **High**), default administrator passwords etc.

## 5.3 Licensed Features

### 5.3.1 Feature Keys

The **Feature Keys** page is used to show available and activated licensable feature keys on QX. Two types of licensable feature keys are available on QX:

- **Permanent keys** is used to activate licensable features on QX permanently, without time limitation. **Permanent keys** is available for all licensable features, except for two: **Epygi ACD Console** and **Epygi Hotel Console**.
- **Time limited keys** is used to activate or extend the operation for already activated licensable feature temporarily, for the specified period. The feature will no longer be functional after the period expiration date. The **Time limited keys** is available for all licensable features.



QX50 Overview Basic Setup System Security **Licensed Features** Redundancy Language Pack

Dashboard Feature Keys Free Trial

## Features

Unique ID: 12-6.3.6-08c1b3b1505748488048578816516643

+ Add

Name	Description	Status
Debug	Support for debugging purposes	Activated
3PCC	Support for Third Party Call Control	Activated
Automatic Call Distribution	Support for ACD	Activated
Barge-In	Support for Listen-In, Whisper and Barge-In services	Activated
Redundancy	Support for Two-unit Standby Redundant System	Activated
Epygi Hotel Console	Support for Epygi Hotel Console application	Activated
Call Cost	Support for Calling Cost Control	Activated
DCC Pro	Support for Desktop Communication Console (Pro-level) application	8 users
DCC Basic	Support for Desktop Communication Console (Basic-level) application	8 users
iQall Advanced Features	Support for iQall Advanced Features (Android/iOS)	8 users
IP Phone Expansion	Support for additional IP lines	32 users
Auto Dialer	Support for Auto Dialer application	8 users
Audio Conference	Support for Audio Conference	8 users
Epygi ACD Console	Support for Epygi ACD Console	18 users
Epygi Hotel Console	Support for Epygi Hotel Console application	8 users
Epygi Automatic Outbound Calling	Support for Epygi Automatic Outbound Calling	16 users
eQall IP lines support	Support for eQall IP Lines	49 users
Call Recording	Support for Call Recording	8 users
Video Conference	Support for Video Conference	8 users

Figure 16: Features page

The following licensable features are available on QX:



- **Debug** enables SSH connection towards the QX for debugging purposes.
- **3PCC** activates **Third Party Call Control** feature on QX. This feature allows the call controlling applications running on PC to remotely initiate and handle calls on QX and to subscribe for certain event notifications from QX.
- **Automatic Call Distribution** activates the **ACD** feature which provides contact center solution for queuing and automatic distribution of the calls between contact center agents.
- **Barge-In** activates the **Barge-In** feature on QX. This feature allows PBX users to participate in the third-party calls while remaining imperceptible.
- **Redundancy** activates the **Redundancy** feature on QX.
- **Epygi Hotel Console** activates **EHC** application support for QX.
- **Call Cost** allows to limit and control the cost of calls through the routing rules on QX.
- **PMSLINK Connection** is used to enable the interface for connecting to **PMSLINK** middleware from **char** and integrate QX with **PMS** used in hotels.
- **DCC Pro** activates **Desktop Communication Console Pro-level** application support for QX.
- **DCC Basic** activates **Desktop Communication Console Basic-level** application support for QX.
- **iQall Mobile Toggling** allows users to alternate between their mobile (iPhone/Android) running **iQall** application and their desk phone without the call being disconnected.
- **IP Phone Expansion** activates additional IP lines (IP phone support) on QX.
- **Auto Dialer** activates **Auto Dialer** application support for QX.
- **Audio Conference** activates the **Conference** feature allowing the system to act as a standalone conference server.
- **Epygi ACD Console** activates **Web monitoring** support for **ACD** processes on QX.
- **Epygi Automatic Outbound Calling** supports automatic outbound calling on QX.
- **eQall IP Lines Support** activates IP line(s) on QX for eQall software phone support.
- **Call Recording** activates the **Call Recording** feature which is used to record PBX, SIP or PSTN calls on QX and save recordings into the local recording box or upload to the remote server.
- **Video Conference** activates the **Video Conference** feature.

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

Enter a **Feature Key** as follows:

1. Click **Add**.
2. Enter the key in the **Feature Key** field.
3. Click **Save**. The status of the selected feature will turn to "Reboot needed".
4. Reboot QX to complete the installation. The status of feature will turn to "Activated".

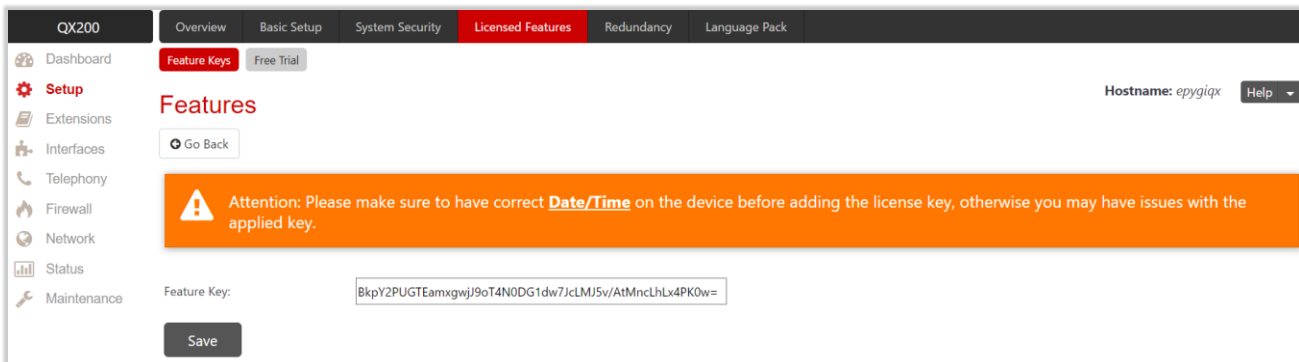


Figure 17: Adding a feature key

**Note:**

- Make sure to have the correct [Date/Time](#) on device before adding the license key, otherwise you may have issues with the applied key.
- When using **Call Recording** and/or **ACD** features on the QX50/QX200 it is advisable to use an SD memory card to expand the system memory. Currently, the recommended SD card's largest capacity is 32 GB.
- When using **Call Recording** and/or **ACD** features on the QX20/QX500 it is advisable to use a micro SD memory card to expand the system memory. Currently, the largest capacity of the recommended micro SD cards is 64 GB.

For more information on **Licensable Features**, refer to the [Licensable Features on QX IP PBXs](#) guide.

### 5.3.2 Free Trial

The **Trial Features Activation** page lists all QX features that can be activated for a trial period.

**Expiration Date/Time** is used to specify the trial period. Upon expiring the specified period, QX will reboot and trial feature(s) will be deactivated. **TIP:** The trial option can be activated on QX only once. You cannot activate the trial for the same or any other feature again after the first activation.

To activate **Trial** feature:

1. Tick the **Activate** checkbox next to the feature.
2. Specify the needed count under the **Count** column (depending on the selected feature).
3. Click **Save**. The QX will reboot and activate the selected trial feature(s).

## 5.4 Redundancy

The **Redundancy** feature is used to increase QX availability by using the second QX 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 purpose of redundancy is to ensure uninterrupted functionality of QX. **Redundancy Settings** must be configured on both units. One of the units is configured as a master, the second one as a backup.

For more information on how to configure and use **Redundancy** feature, refer to the [Redundancy Feature on QX IP PBXs](#) guide.

## 5.5 Language Pack

All Epygi supported **Language Packs** (LPs) will change system voice messages to custom language. Some of LPs will change the QX WEB GUI and also the GUI interface on most of supported IP phones. For more information on **Language Packs**, refer to the [Language Packs Overview for Epygi QX Line](#) guide.

To upload a **Language Pack**:

1. Click **Choose File** to browse and select the LP file.
2. Click **Save** to start uploading the language pack. Clicking **Save** will stop some vital processes on QX, therefore it is required to manually reboot the device even if you have cancelled the LP update procedure.
3. Click **Yes** to proceed the upload. QX will be rebooted automatically.
4. Uploaded LP will appear in the **Current language pack** field. After successful upload, you will be able to:
  - Change the language of WEB GUI session from **Login** page or from **Main Menu**.

- Switch the system voice messages to the custom language and change the GUI interface of some supported IP phones. **TIP:** Choose the language from the [Regional Settings and Preferences](#) section to change the system voice messages and GUI language for the IP phones. The IP phones will be automatically rebooted to change language.

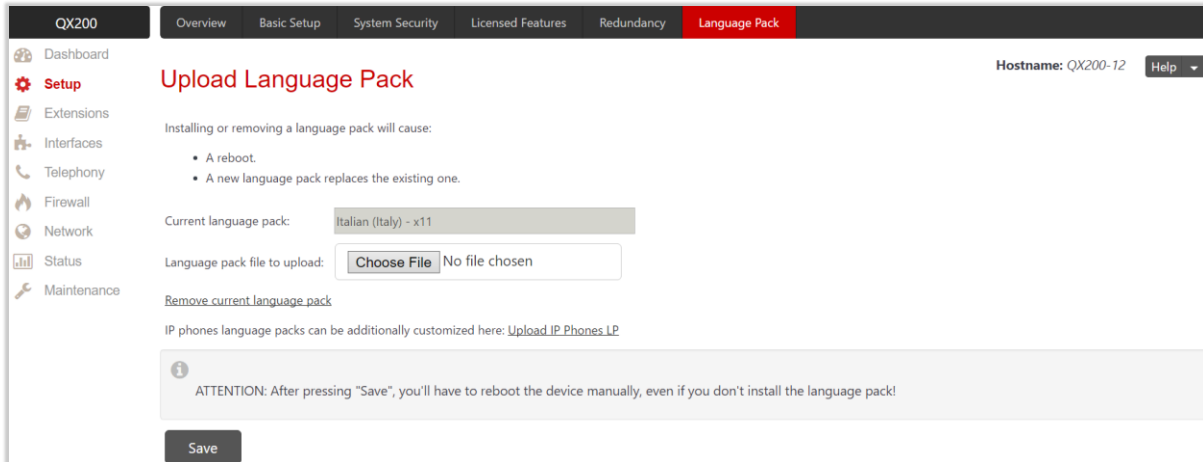


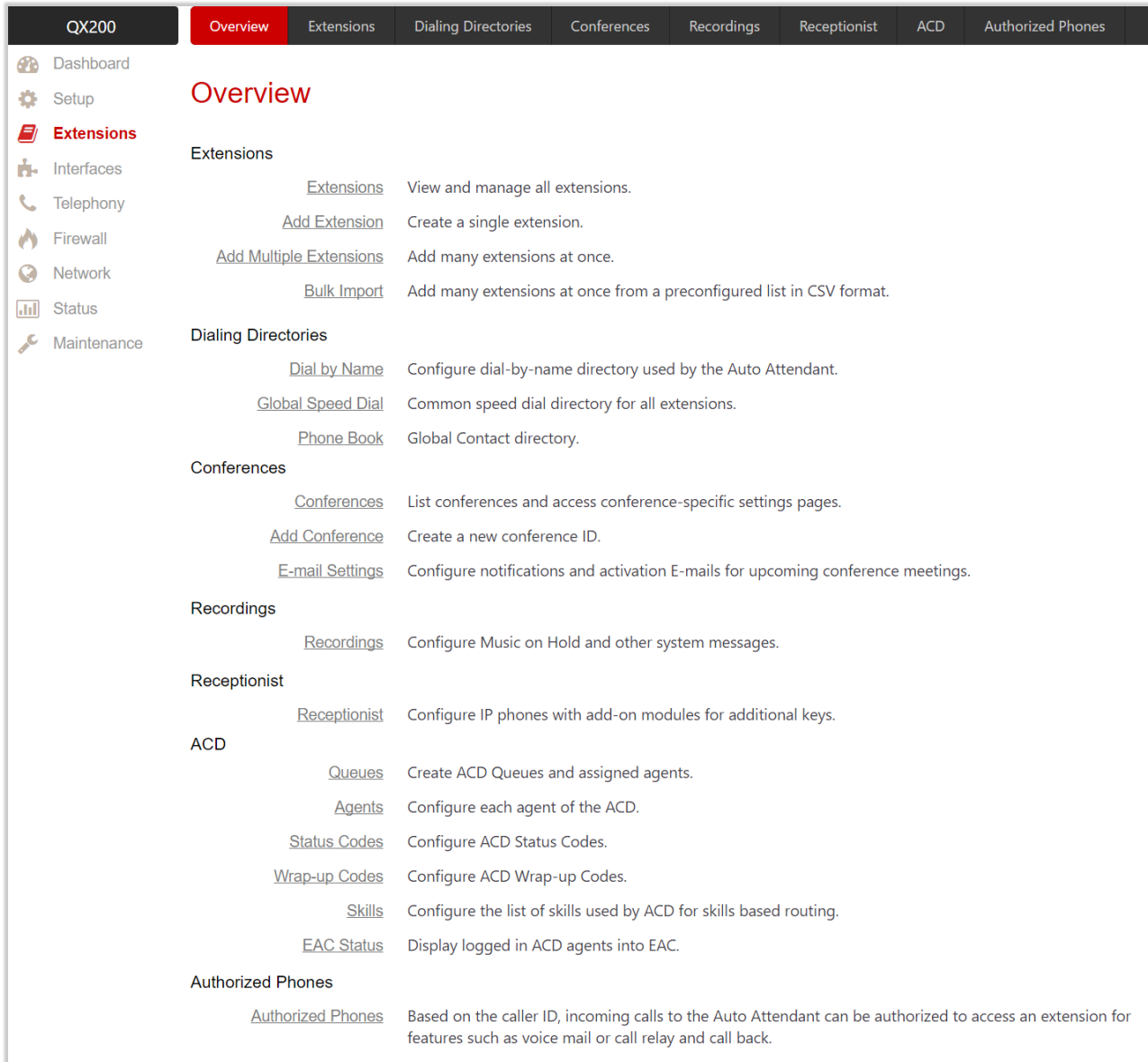
Figure 18: Language Pack page

To upload a custom LP on the IP phone(s):

1. Click the **Upload IP Phones LP** link.
2. Click the hyperlinked IP phone vendor.
3. Click **Choose File** to browse and select the LP file.
4. Click **Yes** to proceed the upload. Then reboot the IP phone to activate the new LP. **TIP:** Clicking **Save** will stop some vital processes on the IP phone, therefore reboot your phone manually even if you have cancelled the LP update procedure.

**Note:** Only one custom LP can be uploaded at a time. Thus, the new LP will remove the existing one and reboot the QX. Once QX is rebooted, the connected IP phones will reboot then.

## 6 Extensions Menu



Category	Option	Description
Extensions	<a href="#">Extensions</a>	View and manage all extensions.
	<a href="#">Add Extension</a>	Create a single extension.
	<a href="#">Add Multiple Extensions</a>	Add many extensions at once.
	<a href="#">Bulk Import</a>	Add many extensions at once from a preconfigured list in CSV format.
Dialing Directories	<a href="#">Dial by Name</a>	Configure dial-by-name directory used by the Auto Attendant.
	<a href="#">Global Speed Dial</a>	Common speed dial directory for all extensions.
	<a href="#">Phone Book</a>	Global Contact directory.
Conferences	<a href="#">Conferences</a>	List conferences and access conference-specific settings pages.
	<a href="#">Add Conference</a>	Create a new conference ID.
	<a href="#">E-mail Settings</a>	Configure notifications and activation E-mails for upcoming conference meetings.
Recordings	<a href="#">Recordings</a>	Configure Music on Hold and other system messages.
Receptionist	<a href="#">Receptionist</a>	Configure IP phones with add-on modules for additional keys.
ACD	<a href="#">Queues</a>	Create ACD Queues and assigned agents.
	<a href="#">Agents</a>	Configure each agent of the ACD.
	<a href="#">Status Codes</a>	Configure ACD Status Codes.
	<a href="#">Wrap-up Codes</a>	Configure ACD Wrap-up Codes.
	<a href="#">Skills</a>	Configure the list of skills used by ACD for skills based routing.
	<a href="#">EAC Status</a>	Display logged in ACD agents into EAC.
Authorized Phones	<a href="#">Authorized Phones</a>	Based on the caller ID, incoming calls to the Auto Attendant can be authorized to access an extension for features such as voice mail or call relay and call back.

Figure 19: Extensions Menu overview

## 6.1 Extensions

### 6.1.1 Extensions

Navigating to the **Extensions Management** page for the first time after the QX initial start or configuration restore you will be prompted to choose the extensions length applicable to all QX default extensions.

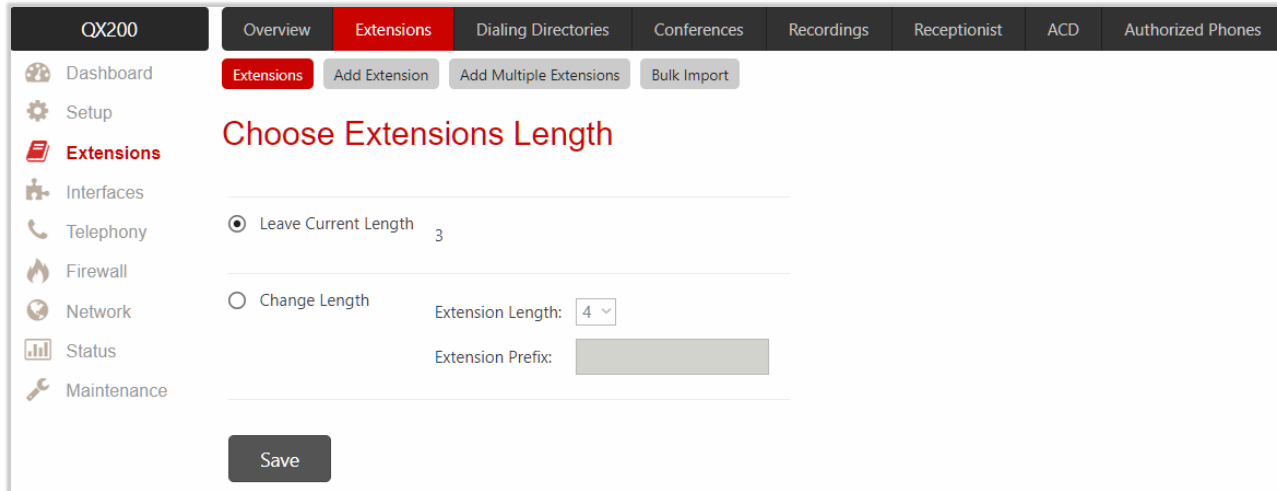


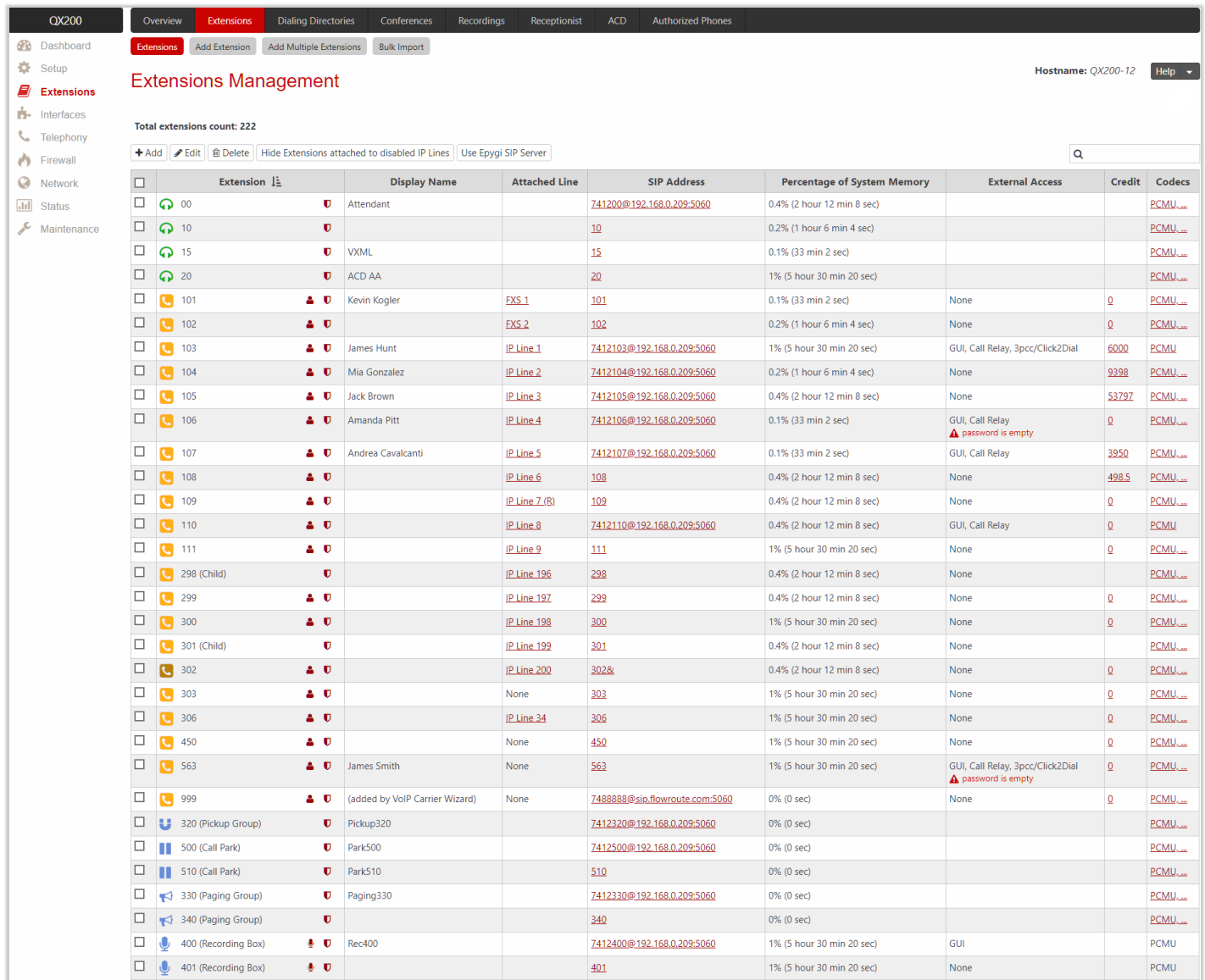
Figure 20: Choose Extensions Length page

The following options are available:

- **Leave Current Length** – by default, extension length is **3** on QX20, QX50, QX200, QX500, QXISDN4+ and is **4** on the QX2000 and QX3000. In front of this selection, the actual length of configured extensions is displayed.
- **Change Length** changes the length of extensions as follows:
  - **Extension Length** is used to select the length of extensions. It will be applied for all existing extensions on QX.
  - **Extension Prefix** is used to set the prefix the existing extensions as well as the newly created extensions should start with. The prefix cannot start with **0** or **9**.

#### Attention:

- In case of saving the settings on the **Choose Extensions Length** page, all existing extensions will lose the custom voice messages and voice mails in the mailbox. The device will be rebooted. The **Choose Extensions Length** page will not appear again unless the default configuration settings are not restored on QX.
- QX20 is limited to **100**, QX50/QXISDN4+ to **200**, QX200 to **400**, QX500 to **800**, QX2000 to **2400** and QX3000 to **3400** extensions in total.



Extension	Display Name	Attached Line	SIP Address	Percentage of System Memory	External Access	Credit	Codecs
00	Attendant		741200@192.168.0.209:5060	0.4% (2 hour 12 min 8 sec)			PCMU ...
10			10	0.2% (1 hour 6 min 4 sec)			PCMU ...
15	VXML		15	0.1% (33 min 2 sec)			PCMU ...
20	ACD AA		20	1% (5 hour 30 min 20 sec)			PCMU ...
101	Kevin Kogler	FXS 1	101	0.1% (33 min 2 sec)	None	0	PCMU ...
102		FXS 2	102	0.2% (1 hour 6 min 4 sec)	None	0	PCMU ...
103	James Hunt	IP Line 1	7412103@192.168.0.209:5060	1% (5 hour 30 min 20 sec)	GUI, Call Relay, 3pcc/Click2Dial	6000	PCMU
104	Mia Gonzalez	IP Line 2	7412104@192.168.0.209:5060	0.2% (1 hour 6 min 4 sec)	None	9398	PCMU ...
105	Jack Brown	IP Line 3	7412105@192.168.0.209:5060	0.4% (2 hour 12 min 8 sec)	None	53797	PCMU ...
106	Amanda Pitt	IP Line 4	7412106@192.168.0.209:5060	0.1% (33 min 2 sec)	GUI, Call Relay ▲ password is empty	0	PCMU ...
107	Andrea Cavalcanti	IP Line 5	7412107@192.168.0.209:5060	0.1% (33 min 2 sec)	GUI, Call Relay	3950	PCMU ...
108		IP Line 6	108	0.4% (2 hour 12 min 8 sec)	None	498.5	PCMU ...
109		IP Line 7 (R)	109	0.4% (2 hour 12 min 8 sec)	None	0	PCMU ...
110		IP Line 8	7412110@192.168.0.209:5060	0.4% (2 hour 12 min 8 sec)	GUI, Call Relay	0	PCMU
111		IP Line 9	111	1% (5 hour 30 min 20 sec)	None	0	PCMU ...
298 (Child)		IP Line 196	298	0.4% (2 hour 12 min 8 sec)	None		PCMU ...
299		IP Line 197	299	0.4% (2 hour 12 min 8 sec)	None	0	PCMU ...
300		IP Line 198	300	1% (5 hour 30 min 20 sec)	None	0	PCMU ...
301 (Child)		IP Line 199	301	0.4% (2 hour 12 min 8 sec)	None		PCMU ...
302		IP Line 200	302	0.4% (2 hour 12 min 8 sec)	None	0	PCMU ...
303		None	303	1% (5 hour 30 min 20 sec)	None	0	PCMU ...
306		IP Line 34	306	1% (5 hour 30 min 20 sec)	None	0	PCMU ...
450		None	450	1% (5 hour 30 min 20 sec)	None	0	PCMU ...
563	James Smith	None	563	1% (5 hour 30 min 20 sec)	GUI, Call Relay, 3pcc/Click2Dial ▲ password is empty	0	PCMU ...
999	(added by VoIP Carrier Wizard)	None	7488888@sip.flowroute.com:5060	0% (0 sec)	None	0	PCMU ...
320 (Pickup Group)	Pickup320		7412320@192.168.0.209:5060	0% (0 sec)			PCMU ...
500 (Call Park)	Park500		7412500@192.168.0.209:5060	0% (0 sec)			PCMU ...
510 (Call Park)	Park510		510	0% (0 sec)			PCMU ...
330 (Paging Group)	Paging330		7412330@192.168.0.209:5060	0% (0 sec)			PCMU ...
340 (Paging Group)			340	0% (0 sec)			PCMU ...
400 (Recording Box)	Rec400		7412400@192.168.0.209:5060	1% (5 hour 30 min 20 sec)	GUI		PCMU
401 (Recording Box)			401	1% (5 hour 30 min 20 sec)	None		PCMU

Figure 21: Extensions Management page

The Extensions Management table consists of the following components:

- **Extension** lists the numbers for extensions on QX. These numbers are used for calling extensions internally.
- **Display Name** is an optional name given to extension mainly to identify the extension owner at the called side.
- **Attached Line** indicates the IP or FXS line the extension is attached to. **TIP:** If the **Remote Extension** service is enabled on the extension, **R** will be shown. **None** is shown when no FXS or IP line is attached to the extension.
- **SIP Address** shows the full SIP address of the extension, (i.e., `username@sipserver:port`) when **Registration on SIP Server** is enabled, otherwise the SIP address will be displayed in the following format: `"username, Proxy: sipserver:port"`. If no **username** is defined, the extension number will be displayed instead.
- **Percentage of System Memory** indicates the part of total memory allocated to extension and shows the duration available for the voice mails and custom messages of the extension. The available time duration depends on the selected [Voice Mail Recording Codec](#).

- **External Access** indicates whether the **Allow Call Relay**, **Allow GUI Login** or **Allow 3pcc/Click2Dial Access** options are enabled on the extension.
- **Credit** indicates the available credit amount of the extension.
- **Codecs** shows activated **Codecs** on the extension. Click the **Codecs** link to access and modify the codecs on the extension.

## 6.1.2 Add Extension

To add a new **Extension**:

1. Click **Add Extension**.
  - Enter the extension number.
  - Select the **extension type**. The following types are available: **Auto Attendant**, **User Extension**, **Pickup Group**, **Call Park**, **Paging Group** and **Recording Box**.
2. Click **Save** to add the new extension to the **Extension Management** table.

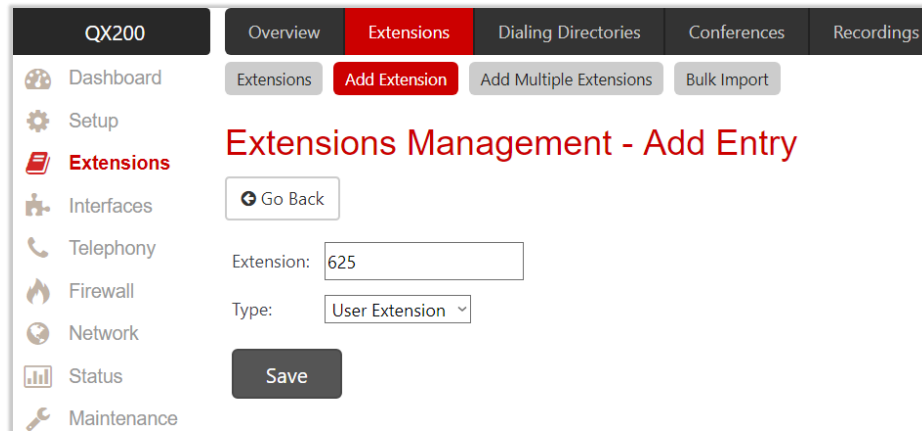


Figure 22: Extensions Management – Add Entry page

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

- **Active extensions** are those that are attached to the line (IP or FXS), can place and receive calls and use available telephony services.
- **Inactive extensions** are those that are not attached to the line (IP or FXS), cannot place and receive calls and use only part of telephony services.

### Note:

- **Manually** adjust the routing rules for calling extensions with custom length since the [call routing rule\(s\)](#) for calling PBX extensions will not be adjusted automatically.
- A maximum extension length is **20** digits.
- The **Recording Box** extension type becomes available if the **Call Recording** feature is activated on QX.

### 6.1.3 Add Multiple Extensions

The **Extensions Management – Add Multiple Extensions** page is used to create multiple extensions at once.

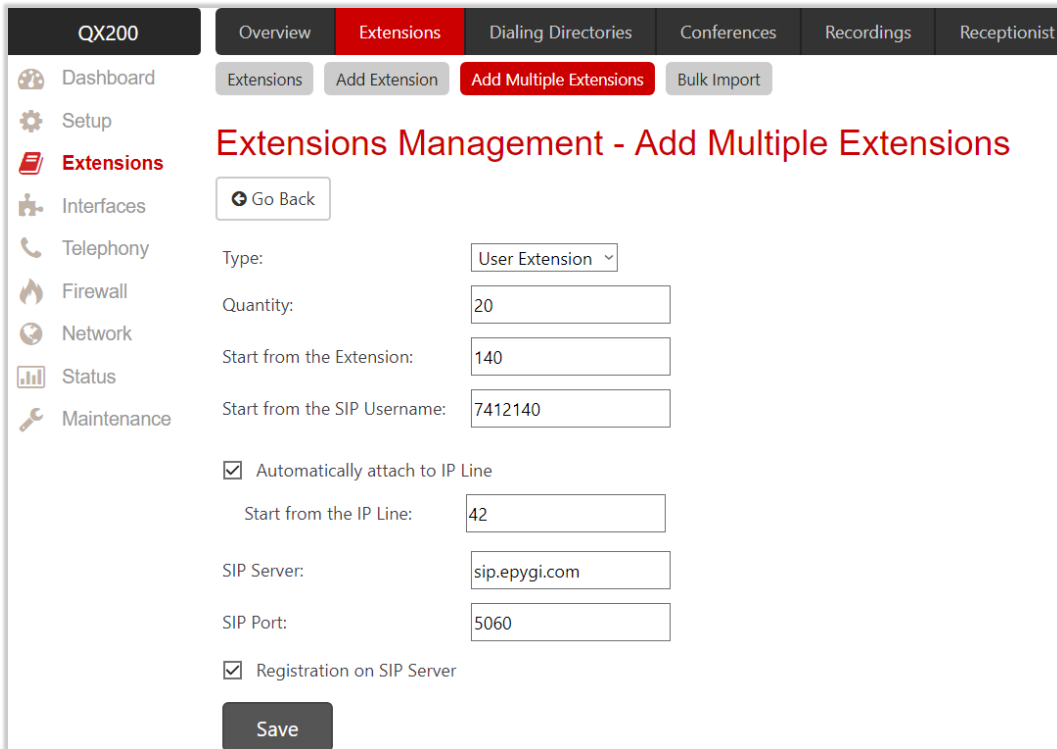


Figure 23: Extensions Management – Add Multiple Extensions page

To add multiple **Extensions**:

1. Select the extension type. The following types are available: **Auto Attendant, User Extension, Pickup Group, Call Park, Paging Group** and **Recording Box**.
2. Enter the amount of extensions.
3. Enter the **number** for the first extension. Based on the **Quantity**, next extensions will have subsequent numbers.
4. Enter the **SIP Username** of the first extension. Based on the **Quantity**, next extensions will have subsequent SIP usernames.
5. Tick the **Automatically attach to IP Line** checkbox to attach user extensions to IP lines.
6. Enter the **number** of the first IP line to be attached.
7. Enter the **SIP Server** and **SIP Port**. If the latter is not specified, QX will access the SIP server via the default **5060** port.
8. Tick the **Registration on SIP Server** checkbox to enable registration of the extensions on the SIP server.
9. Click **Save** to add the new extensions to the **Extension Management** table.

#### Note:

- **Manually** adjust the routing rules for calling extensions with custom length since the [call routing rule\(s\)](#) for PBX extensions will not be adjusted automatically.
- The **Recording Box** extension type becomes available if the **Call Recording** feature is activated on QX.
- A maximum extension length is **20** digits.
- A maximum SIP Username length is **32** characters. The SIP Username can consist of lowercase and uppercase alphabetic characters, digits and symbols.



## 6.1.4 Edit Extension

You can modify both **admin** and **user** settings of the extension.

- To modify extension **admin** settings, click the **Admin Settings** icon or tick the checkbox next to the extension and click **Edit**. Remember to save changes before moving between configuration sections.
- To modify extension **user** settings, click the **User Settings** icon.

You can modify **admin** settings of two or more extensions at once by ticking checkboxes next to extensions and clicking **Edit**. When editing multiple extensions, fields that cannot be edited for multiple records have **Multiple** values. When editing user extension and auto attendant together, only common fields will be shown. Additionally, tick the **Select to modify fields** checkbox to submit changes of the corresponding settings (options), otherwise the changes won't be applied.

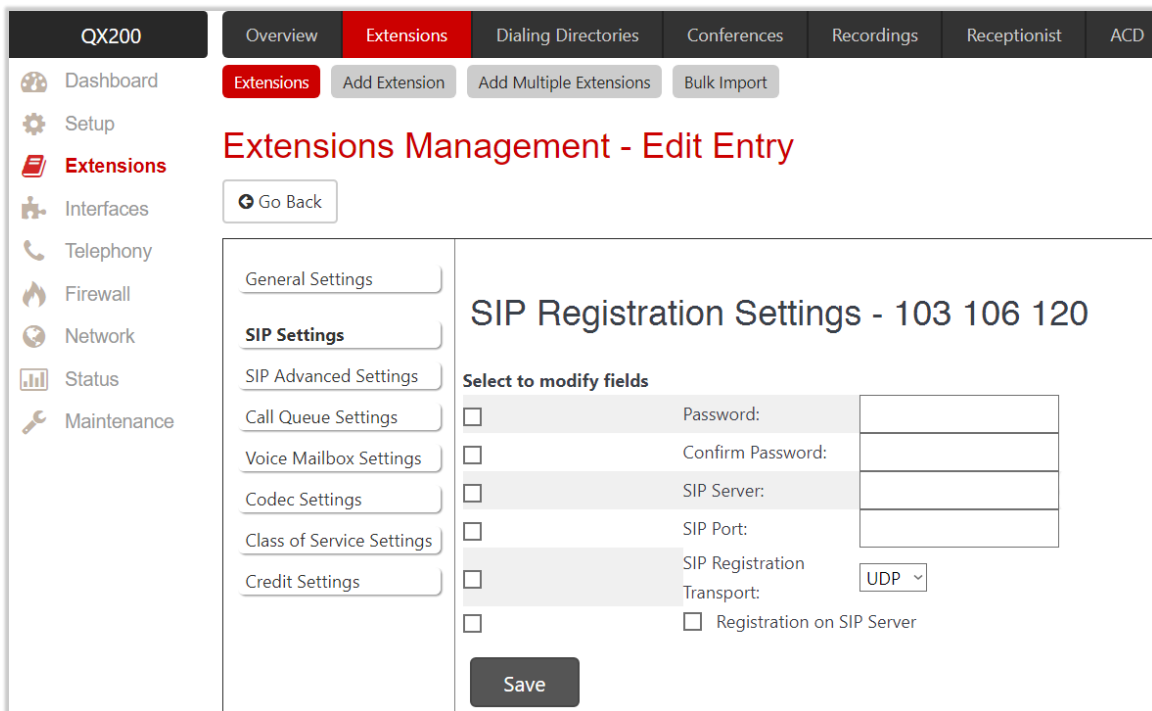


Figure 24: Extensions Management – Edit Entry page (for multiple edit operation)

## 6.1.5 User Extension

The following sections are available for configuration:

- [General Settings](#)
- [SIP Settings](#)
- [SIP Advanced Settings](#)
- [Remote Settings](#)
- [Call Queue Settings](#)
- [Voice Mailbox Settings](#)
- [Class of Service Settings](#)
- [Credit Settings](#)
- [Licensing](#)

## General Settings

This section is used to uniquely identify the extension through parameters described below:

- **Display Name** is the caller ID that will be displayed on the callee's phone.
- **Password** is used to assign a password to the extension. **TIP:** This password will be used for **GUI Login**, for **Call Relay** and **remote access** to voice mailbox.
- **Attached Line** lists all free lines an extension can be attached to. Extension should be attached to a line (either IP or FXS) to be able to make and receive calls. If there is no line attached to an extension, then it is called **Virtual Extension (VE)**. VE can't place/receive calls but is allowed to use a limited number of QX telephony services, such as call forwarding service or voice mail service to store and manage the messages from callers. Any VE can easily become a real extension after attaching a line and vice versa. By default, all extensions on QX have lines attached already. Extensions cannot be detached from the line if the **Remote Extension** service is enabled on. To detach the extension from the line, disable the **Remote Extension** service on the extension first.
- **Use Kickback** enables the **Kickback** service on the extension for the blind transfer scenario. When an extension blindly transfers the call to other extension and if there is no answer from the called extension, 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 extension to be used to access the **Call Relay** service from auto attendant. It is recommended to set a proper and non-blank password when enabling this service in order to protect it from an unauthorized access.
- **Allow GUI Login** activates WEB GUI access (by extension number and password) for the extension.
- **Allow 3pcc/Click2Dial Access** enables the current extension to be used with applications based on the QX interface and QX **Click2Dial** application.
- **Show on Public Directory** – if selected, automatically includes the extension display name and number in the **Phone Book (Directory)** and **Extension Directory**.

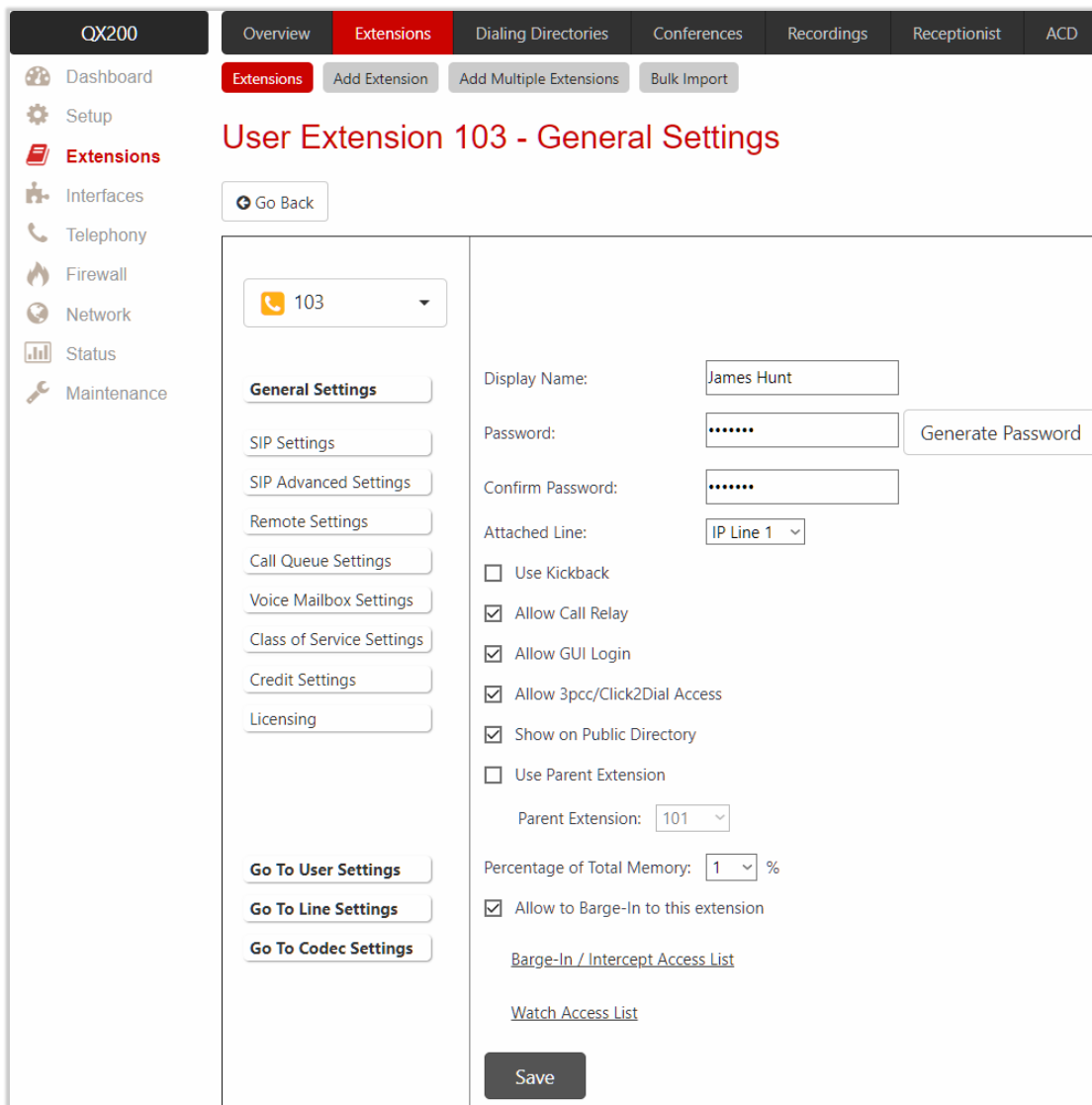


Figure 25: User Extension – General Settings section

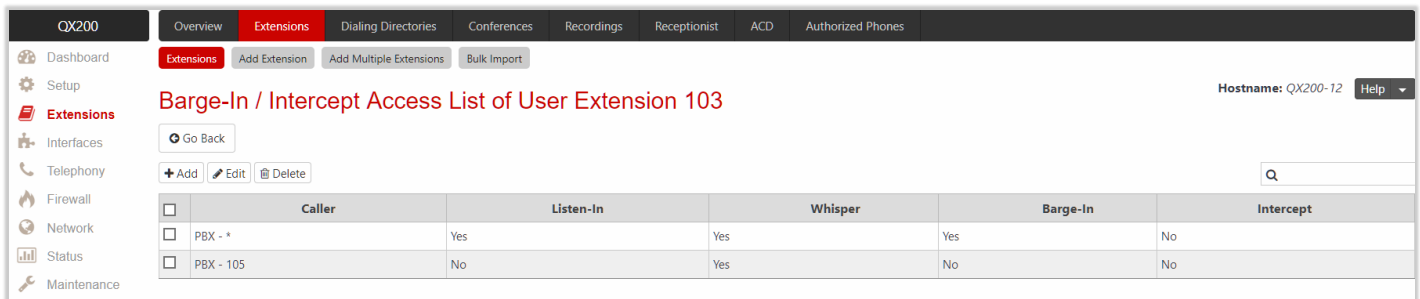
- **Use Parent Extension** allows the current extension to be configured as a **Child** for the **Parent**, selectable from the **Parent Extension** drop-down list. When done, the **Use Parent Extension** checkbox will disappear for the **Parent** and the **Child Extension List** link will appear instead. For more information, refer to the [Parent-Child Configuration](#).
- **Child Extension List** leads to the **Child Extension of Parent Extension** page, where you can see the list of extensions defined as **Child** for the **Parent** extensions. The **General Settings** section of the **Child** extension has the following components:
  - ◆ **Use Parent Extension** – if not selected, interrupts the **Use Parent Extension** service on the **Child** extension.
  - ◆ **Parent Extension** is used to select **Parent** extension for the **Child** extension.
- **Allow Concurrent Calls to Parent-Child Group** allows to choose between the following options available for handling inbound call to **Parent-Child** group:
  - If selected, incoming calls continue ringing on available phones when one of the phones in **Parent-Child** group is busy or rejects the call.
  - If not selected, incoming calls will follow busy state rules (Busy Call Forwarding, Call Queue, VMS, etc.) depending on what is configured, if any of the phones in the **Parent-Child** group is busy. If all extensions in the **Parent-Child** group are free and are ringing, and any of them presses **Reject** button

(or somehow else declines the incoming call), then the **entire group** will be considered as busy. Therefore, incoming call will follow busy state rules depending on what is configured. **Note:** If the **Call Waiting Service** is enabled on the **Parent** extension, then extensions of **Parent-Child** group will receive the second call.

- **Percentage of Total Memory** is used to allocate memory for voice mails and custom messages of the extension.
- **Enable Ringing Simulation** – if selected, extra ring tones will be played to the caller before the voice mail service gets activated (available on **Virtual Extensions** only), otherwise the voice mail service will be activated immediately. The ring tones will be played during the timeout specified in the **Ringing Simulation Timeout**.
- **Intercept Access List** leads to the **Intercept Access List of User Extension** page to define extension(s) allowed to intercept calls.
- **Allow to Barge-In to this extension** enables **Barge-In** on the extension. The **Barge-In / Intercept Access List** leads to the **Call Barge-In / Intercept Access List** page to define extensions allowed to barge-in to the current extension calls or intercept calls.
- **Watch Access List** leads to the **Watch Access List** page to define the extensions allowed to watch calls.

### Barge-In / Intercept Access List of User Extension

This page is used to define a list of extensions that are capable to **Barge-In / Intercept** the extension calls and defines the appropriate permissions.



<input type="checkbox"/>	Caller	Listen-In	Whisper	Barge-In	Intercept
<input type="checkbox"/>	PBX - *	Yes	Yes	Yes	No
<input type="checkbox"/>	PBX - 105	No	Yes	No	No

Figure 26: Call Barge-In/Intercept Access List

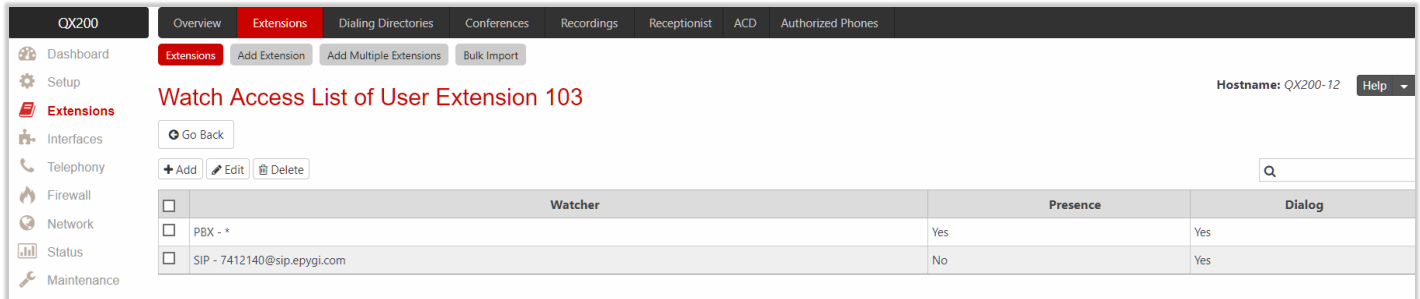
To add a new extension:

1. Click **Add**.
  - Enter the extension number(s) allowed to **Barge-In / Intercept** the current extension calls.
  - Select **Barge-In**, **Intercept** options, to allow the selected action only. The following options are available: **Listen-In**, **Whisper**, **Barge-In** and **Intercept**.
2. Click **Save** to add the new entry to the **Barge-In / Intercept Access List** table.

**Note:** The **Barge-In / Call Intercept** calls neither will be displayed in the **Active Calls** table on the **Dashboard** nor will be registered in the **Call History** table.

## Watch Access List of User Extension

This page is used to define a list of extensions that are able to watch the current extension calls and defines the appropriate permissions.



The screenshot shows the 'Watch Access List of User Extension 103' page. The interface includes a navigation menu on the left with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The top navigation bar has tabs for Overview, Extensions, Dialing Directories, Conferences, Recordings, Receptionist, ACD, and Authorized Phones. The main content area features a search bar, a '+ Add' button, and a table with the following data:

Watcher	Presence	Dialog
<input type="checkbox"/> PBX - *	Yes	Yes
<input type="checkbox"/> SIP - 7412140@sip.epygi.com	No	Yes

Figure 27: Watch Access List

To add a new extension:

1. Click **Add**.
  - Enter the extension number(s).
  - Select the **Allow Presence Subscriptions** and **Allow Dialog Subscriptions** options to allow subscriptions to the current extension.
2. Click **Save** to add the new entry to the **Watch Access List** table.

## SIP Settings

This section describes how to register QX extension on a SIP server to receive external SIP calls.

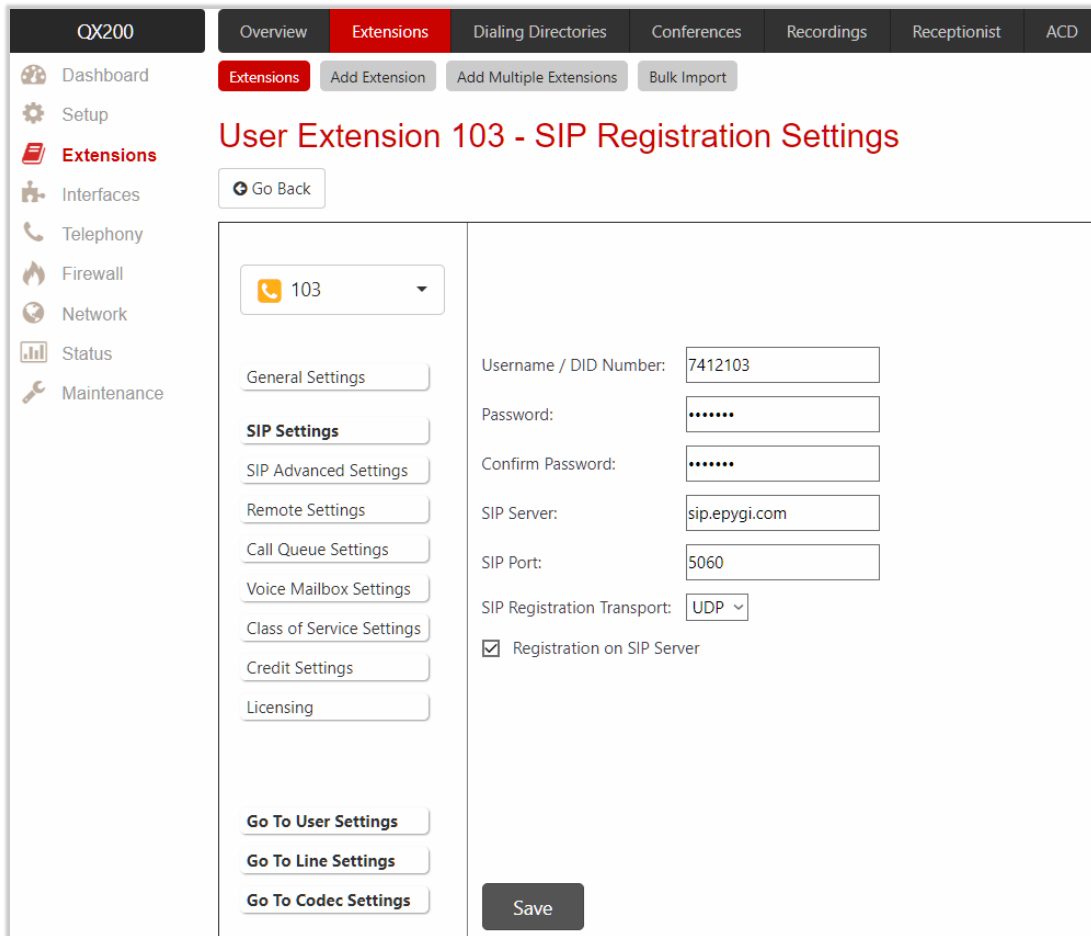


Figure 28: SIP Settings section

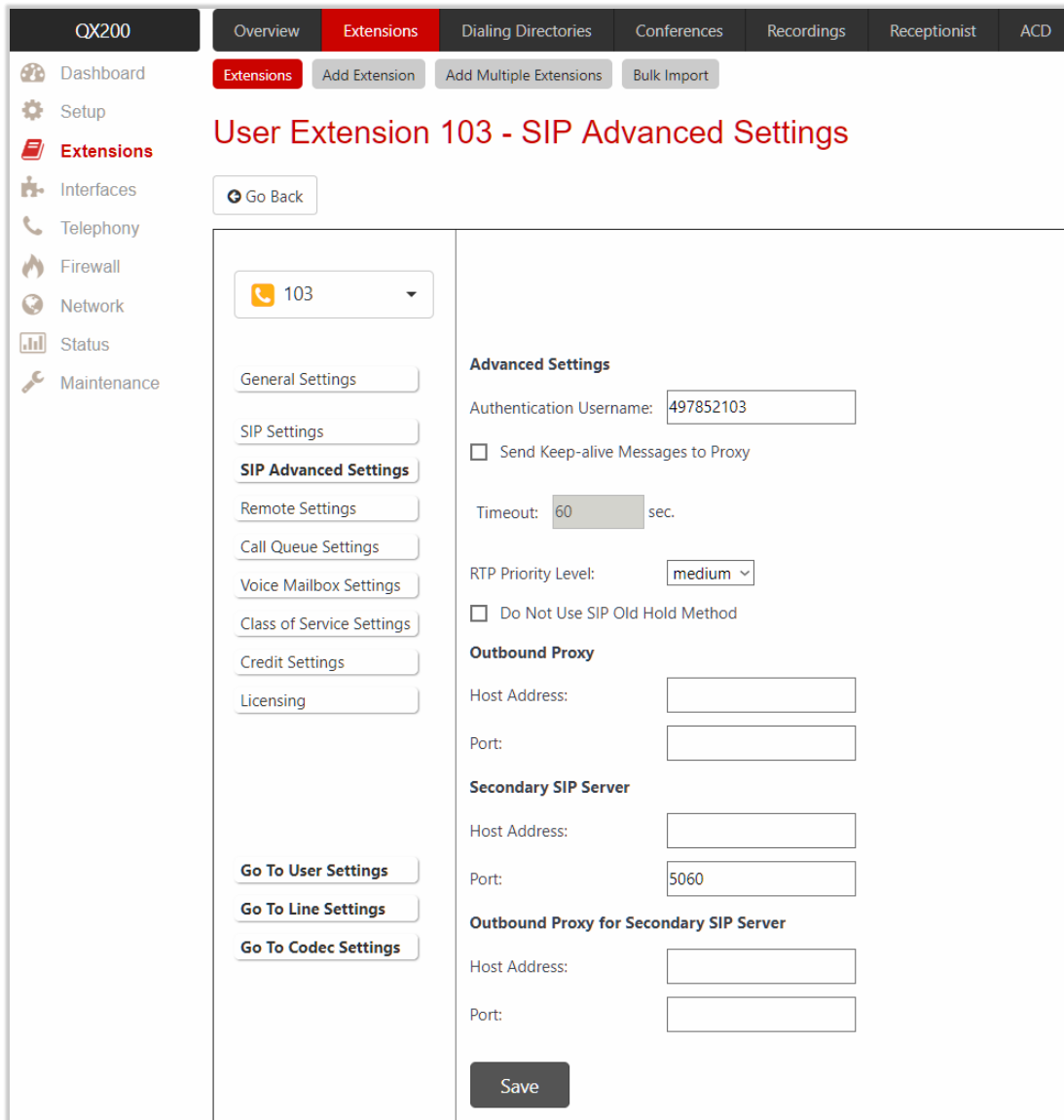
The following settings (options) are available:

- **Username / DID Number** is the registration username or the DID number on the external server.  
**TIP:** The maximum **SIP Username** length is **32** characters. The **SIP Username** can consist of lowercase and uppercase alphabetic characters, digits and symbols.
- **Password** is the registration password on the SIP server.
- **SIP Server** is the address of the SIP server. It can be either an IP address (e.g. 198.51.100.1) or a hostname (e.g. sip.epygi.com). **TIP:** The maximum **SIP server** length is **32** characters. The **SIP server** can consist of lowercase and uppercase alphabetic characters, digits and symbols.
- **SIP Port** is the port number used to connect to the SIP server. **TIP:** If the **SIP port** is not specified, QX will access the **SIP server** through the default **5060**.
- **SIP Registration Transport** is used to select **SIP Transport** (**UDP**, **TCP** and **TLS**) for the registration.  
**TIP:** If the QX is located behind a NAT router, the TCP ports (for TCP and TLS) should be manually configured from [NAT Traversal – SIP Parameters](#) page and opened on the NAT router accordingly.
- **Registration on SIP Server** is used to register extension on the SIP server.

**How it works:** Upon receiving a SIP Invite message from an external server, QX will look to match the called number in the **Username / DID Number** field. If the ITSP does not require each DID to uniquely register on the SIP server, then only enter the DID number in the **Username / DID Number** field and leave other fields blank.

## SIP Advanced Settings

This section describes how to configure advanced and specific SIP settings for QX extension.



The screenshot shows the 'User Extension 103 - SIP Advanced Settings' page. The interface includes a top navigation bar with tabs for Overview, Extensions (active), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. A left sidebar contains menu items: Dashboard, Setup, Extensions (active), Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area features a dropdown menu for extension 103 and a list of settings categories: General Settings, SIP Settings, SIP Advanced Settings (selected), Remote Settings, Call Queue Settings, Voice Mailbox Settings, Class of Service Settings, Credit Settings, and Licensing. Below these are buttons for 'Go To User Settings', 'Go To Line Settings', and 'Go To Codec Settings'. The 'SIP Advanced Settings' section contains the following fields and options:

- Advanced Settings**
  - Authentication Username: 497852103
  - Send Keep-alive Messages to Proxy
  - Timeout: 60 sec.
  - RTP Priority Level: medium
  - Do Not Use SIP Old Hold Method
- Outbound Proxy**
  - Host Address: [text input]
  - Port: [text input]
- Secondary SIP Server**
  - Host Address: [text input]
  - Port: 5060
- Outbound Proxy for Secondary SIP Server**
  - Host Address: [text input]
  - Port: [text input]

A 'Save' button is located at the bottom of the settings area.

Figure 29: SIP Advanced Settings section

The following settings (options) are available:

- **Authentication Username** is used to set an identification parameter. It should be provided by ITSP and can be requested for some SIP servers only. For others, the field should be left blank.
- **Send Keep-alive Messages to Proxy** enables the SIP registration server accessibility to the verification mechanism.
- **Timeout** is used to set 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.
- **RTP Priority Level** is used to select the level of priority (low, medium or high) of the RTP packets sent from the extension. RTP packets with higher priority will be sent first in case of heavy traffic.
- **Do Not Use SIP Old Hold Method** – if selected, a new recommended method of call hold in SIP (the call hold request is indicated with the "a=sendonly" media attribute, rather than with the IP address of

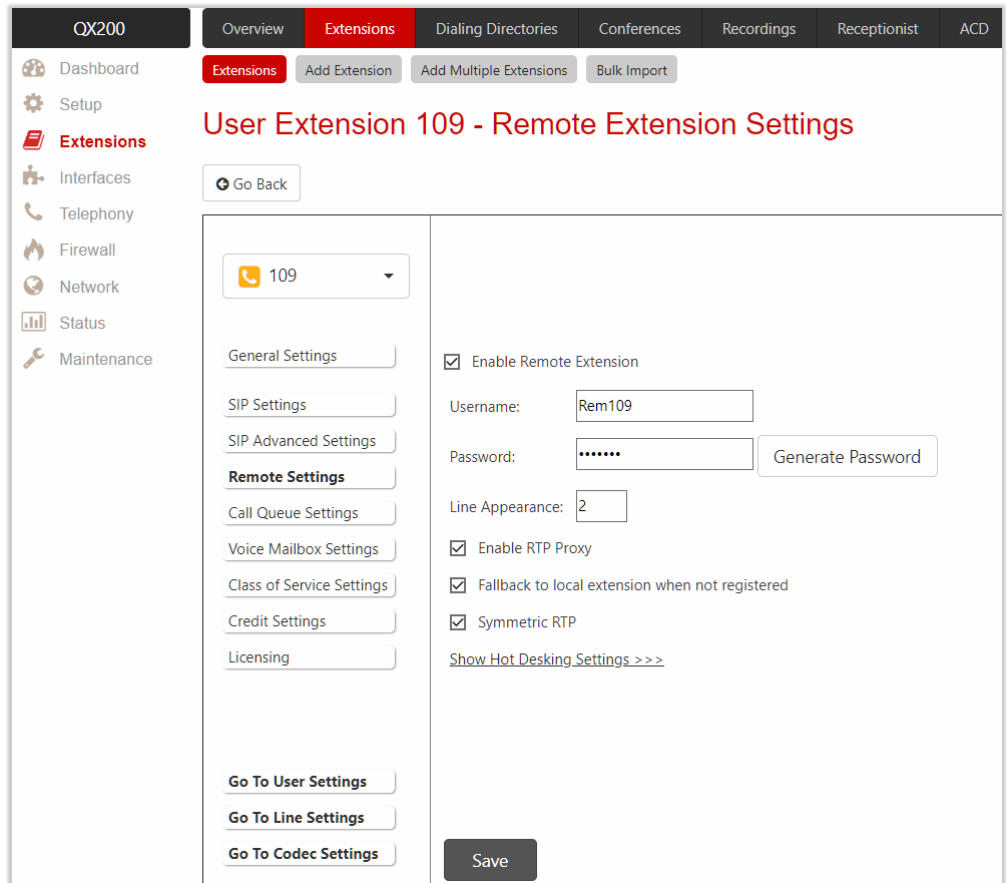
0.0.0.0) will be used. This option should be selected if the remote party does not recognize hold requests initiated from the QX.

- **Outbound Proxy** is the SIP server where all SIP requests and SIP messages are transferred to. Some SIP servers use an outbound proxy to escape NAT restrictions. If an outbound proxy is specified for an extension then all SIP calls originating from that extension will go through that outbound proxy, i.e., all requests will be sent to that outbound proxy.
- **Secondary SIP Server** is used to act as an alternative SIP server when the primary SIP server becomes inaccessible. If the connection with the primary SIP server fails, QX will automatically start sending SIP messages to the secondary SIP server. It will switch back to the primary SIP server as soon as the connection is reestablished.
- **Host Address** and **Port** are used to set the host address and SIP port of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server** respectively. These settings are provided by ITSP and are used by QX to reach the SIP servers.

## Remote Settings

This section describes how to configure **Remote Extension (RE)** service for QX extension. This is an advanced telephony service that allows users to connect phone to QX remotely. The user needs to register an IP phone or softphone on the QX by defining the QX global IP address and an appropriate Username/Password. The registered phone can fully act as a phone connected locally to QX, i.e. you can use all QX telephony services, place and receive calls, access voice mails, etc. **TIP:** The RE service can be enabled only for extensions attached to the line (IP or FXS). The following settings (options) are available:

- **Enable Remote Extension** is used to activate service on QX.
- **Username and Password** are used to set the identification parameters used by the remote phone to register it on QX. **TIP:** The **Username** and **Password** must match on both QX and IP phone for successful registration.
- **Line Appearance** is used to set a number of simultaneous calls supported by the remote phone.
- **Enable RTP Proxy** – if selected, the incoming and outgoing RTP streams to/from the remote IP phone will be routed through QX, otherwise RTP packets will move directly between peers.
- **Fallback to local extension when not registered** – if selected, the incoming calls to the local extension will be forwarded to the remote IP phone only if it is



The screenshot shows the QX200 administration interface. The top navigation bar includes tabs for Overview, Extensions (selected), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. Below the navigation bar, there are buttons for 'Add Extension', 'Add Multiple Extensions', and 'Bulk Import'. The main content area is titled 'User Extension 109 - Remote Extension Settings'. On the left, there is a sidebar menu with options like Dashboard, Setup, Extensions (selected), Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main settings area is divided into sections: General Settings, SIP Settings, SIP Advanced Settings, Remote Settings (expanded), Call Queue Settings, Voice Mailbox Settings, Class of Service Settings, Credit Settings, and Licensing. The 'Remote Settings' section includes a dropdown for extension '109' and several checkboxes: 'Enable Remote Extension' (checked), 'Enable RTP Proxy' (checked), and 'Fallback to local extension when not registered' (checked). There are also input fields for 'Username' (Rem109), 'Password' (masked with dots), and 'Line Appearance' (2). A 'Generate Password' button is next to the password field. At the bottom, there are buttons for 'Go To User Settings', 'Go To Line Settings', 'Go To Codec Settings', and a 'Save' button.

Figure 30: Remote Settings section



registered. Otherwise, when the remote IP phone is unregistered, incoming calls will be routed to the local extension it is attached to.

- **Symmetric RTP** must be selected when RE is located behind the NAT router.
- **Enable Hot Desking** is used to activate [Hot Desking](#) service on RE. **Note:** The **Hot Desking** section is the same as for IP line.

For more information on how to configure and use **Remote Extension** service, refer to the [Remote Extension Configuration on QX IP PBXs](#) guide.

## Call Queue Settings

This section describes how to configure the **Call Queue** service on QX extension allowing multiple incoming calls to wait in the queue and be answered in the order they have been received. This service can be used in the **Receptionist** as well. The following settings (options) are available:

- **Enable Call Queue** is used to activate service on QX.
  - **Call Queue Size** is used to set the length of call queue. This is the maximum number of calls that will be accepted into the queue and kept on hold while the extension is on a call. If the queue is filled up then the next incoming call will be forwarded to the extension **Voice Mail** (if enabled). Otherwise the call will be disconnected.
  - **Max Calls Presented to Extension** is used to set the maximum number of active calls on the line. So, if the maximum call number is set to ① and the extension is in call then an incoming call will go to the call queue. If the maximum call number is set to ② and the extension is in call then the alert for the next incoming will be played in the background (if the **Call Waiting** service is enabled on the extension) and the extension will put the first call on hold to answer the second one or they can be joined for a call conference.
- **Enable No Answer Redirect** – if activated and configured, callers will be redirected to the specified address after some time waiting in the queue. The **Prompt Repetition** is used to set the number of prompts to be played before redirection.
- **ZeroOut Redirection** – if activated and configured, callers dialing ① during queue welcome message or recurring prompt will be redirected to the specified address.
  - **Voice Mail** redirects the call to the extension **Voice Mail**.
  - **Call Type, Calling Address** (identical for both **Call Redirection** and **ZeroOut Redirection**) is used to set the destination address the call will be redirected to. The address strictly depends on the call type.
- **Call Queue Welcome Message** is used to play a message (**default** or **custom**) once when reaching the extension **Call Queue**.
- **Call Queue Prompt** is used to play a queue prompt after **Call Queue Welcome Message**.

**Note:** The **Call Forwarding if Busy** and **Voice Mail** services will function once the call queue will be filled up. Thus, these services will affect those calls that are left out of the queue.

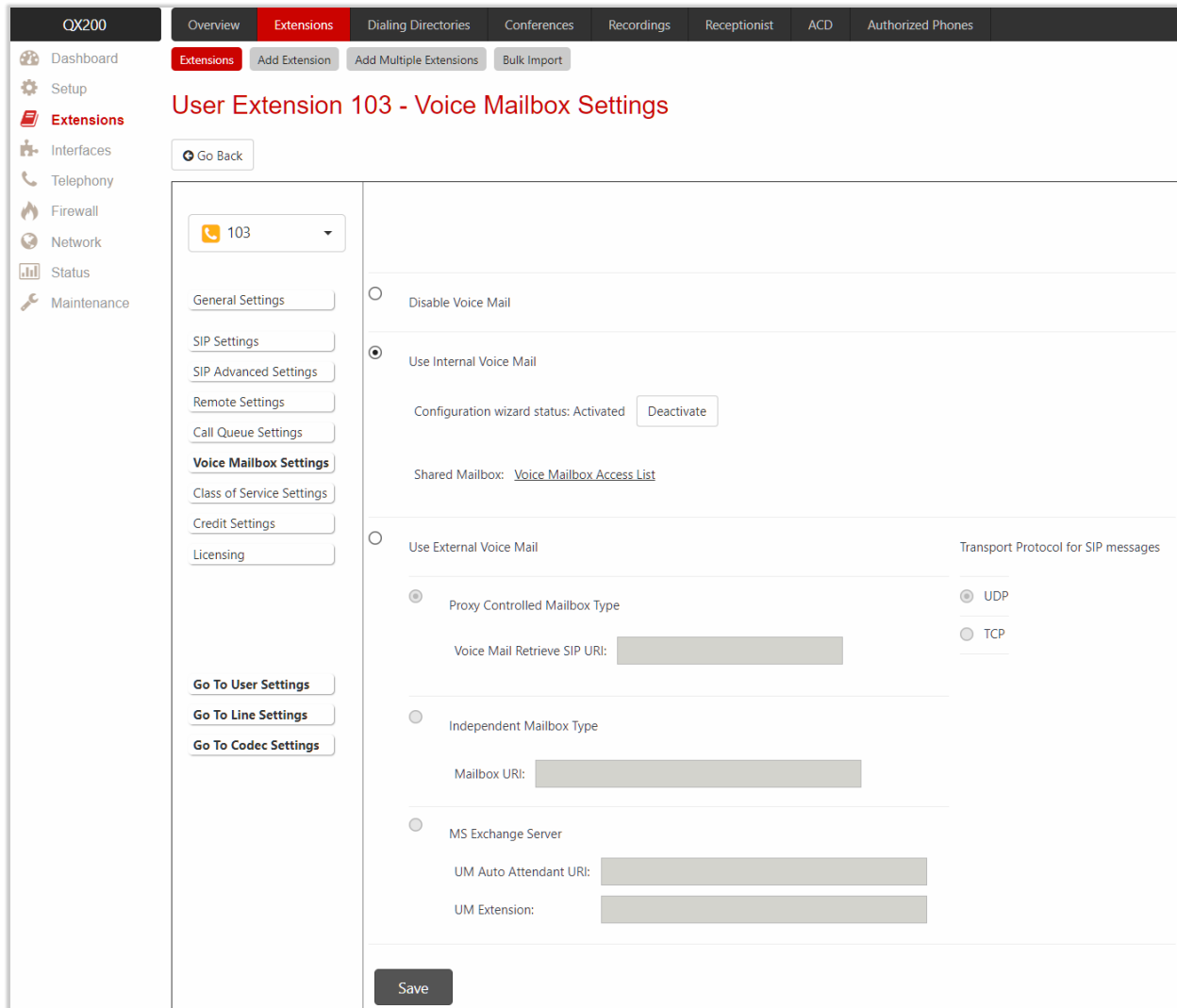
The screenshot displays the 'User Extension 103 - Call Queue Settings' page in the epygi QX200 administration interface. The page is organized into several sections:

- Navigation:** A top bar with tabs for Overview, Extensions (active), Dialing Directories, Conferences, Recordings, and Receptionist. A left sidebar contains menu items like Dashboard, Setup, Extensions (active), Interfaces, Telephony, Firewall, Network, Status, and Maintenance.
- Page Header:** 'User Extension 103 - Call Queue Settings' with a 'Go Back' button.
- Extension Selection:** A dropdown menu showing '103'.
- Settings Menu:** A vertical list of settings categories including General Settings, SIP Settings, SIP Advanced Settings, Remote Settings, **Call Queue Settings** (highlighted), Voice Mailbox Settings, Class of Service Settings, Credit Settings, and Licensing.
- Call Queue Settings:**
  - Enable Call Queue
  - Call Queue Size:
  - Max Calls Presented to Extension:
- Call Redirection:**
  - Enable No Answer Redirect
  - Prompt Repetition:
  - Call Type:
  - Calling Address:
- ZeroOut Redirection:**
  - Voice Mail
  - Call Type:  Calling Address:
- Call Queue Welcome Message:**
  - Upload file:
  - Record file:
- Call Queue Prompt:**
  - Upload file:
  - Record file:
- Save:** A dark 'Save' button at the bottom right.

Figure 31: Call Queue Settings section

## Voice Mailbox Settings

This section describes how to configure **Voice Mailbox Settings** on user extension. By default, the **Voice Mail** service is active for all user extensions and a certain percentage of memory space is assigned.



The screenshot shows the 'User Extension 103 - Voice Mailbox Settings' page. The left sidebar contains a navigation menu with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area has a 'Go Back' button and a dropdown menu for extension '103'. Below this, there are several settings sections: 'General Settings', 'SIP Settings', 'SIP Advanced Settings', 'Remote Settings', 'Call Queue Settings', 'Voice Mailbox Settings' (which is highlighted), 'Class of Service Settings', 'Credit Settings', and 'Licensing'. At the bottom of the settings list are buttons for 'Go To User Settings', 'Go To Line Settings', and 'Go To Codec Settings'. The main settings area is divided into three radio button options: 'Disable Voice Mail', 'Use Internal Voice Mail' (which is selected), and 'Use External Voice Mail'. Under 'Use Internal Voice Mail', there is a 'Configuration wizard status' set to 'Activated' with a 'Deactivate' button, and a 'Shared Mailbox' link to 'Voice Mailbox Access List'. Under 'Use External Voice Mail', there is a 'Transport Protocol for SIP messages' section with radio buttons for 'UDP' (selected) and 'TCP'. Below this are three sub-sections: 'Proxy Controlled Mailbox Type' with a 'Voice Mail Retrieve SIP URI' field, 'Independent Mailbox Type' with a 'Mailbox URI' field, and 'MS Exchange Server' with 'UM Auto Attendant URI' and 'UM Extension' fields. A 'Save' button is located at the bottom right of the settings area.

Figure 32: Voice Mailbox Settings section

The following settings (options) are available:

- **Disable Voice Mail** is used to disable the **Voice Mail** service denying caller to leave a voice message. User will still be able to access his **Voice Mailbox** and manage the existing messages as well as setup the personal settings (password, voice mail greeting and so on) from the handset.
- **Use Internal Voice Mail** is used to enable the **Voice Mail** service and set QX internal storage as a location for voice messages.
  - **Voice Mail Configuration Wizard** – if activated, prompts user to configure personal settings while entering the **Voice Mailbox** first time. Click **Deactivate** to stop the **Voice Mail Configuration Wizard**.
  - **Shared Mailbox** is used to setup **Shared Voice Mailbox** service. The **Voice Mailbox Access List** link leads to the **Voice Mailbox Access List of User Extension** page to define a list of extensions that are capable to access **Voice Mailbox** without password authentication.
- **Use External Voice Mail** is used to enable the **Voice Mail** service and set external storage as a location for the voice messages.

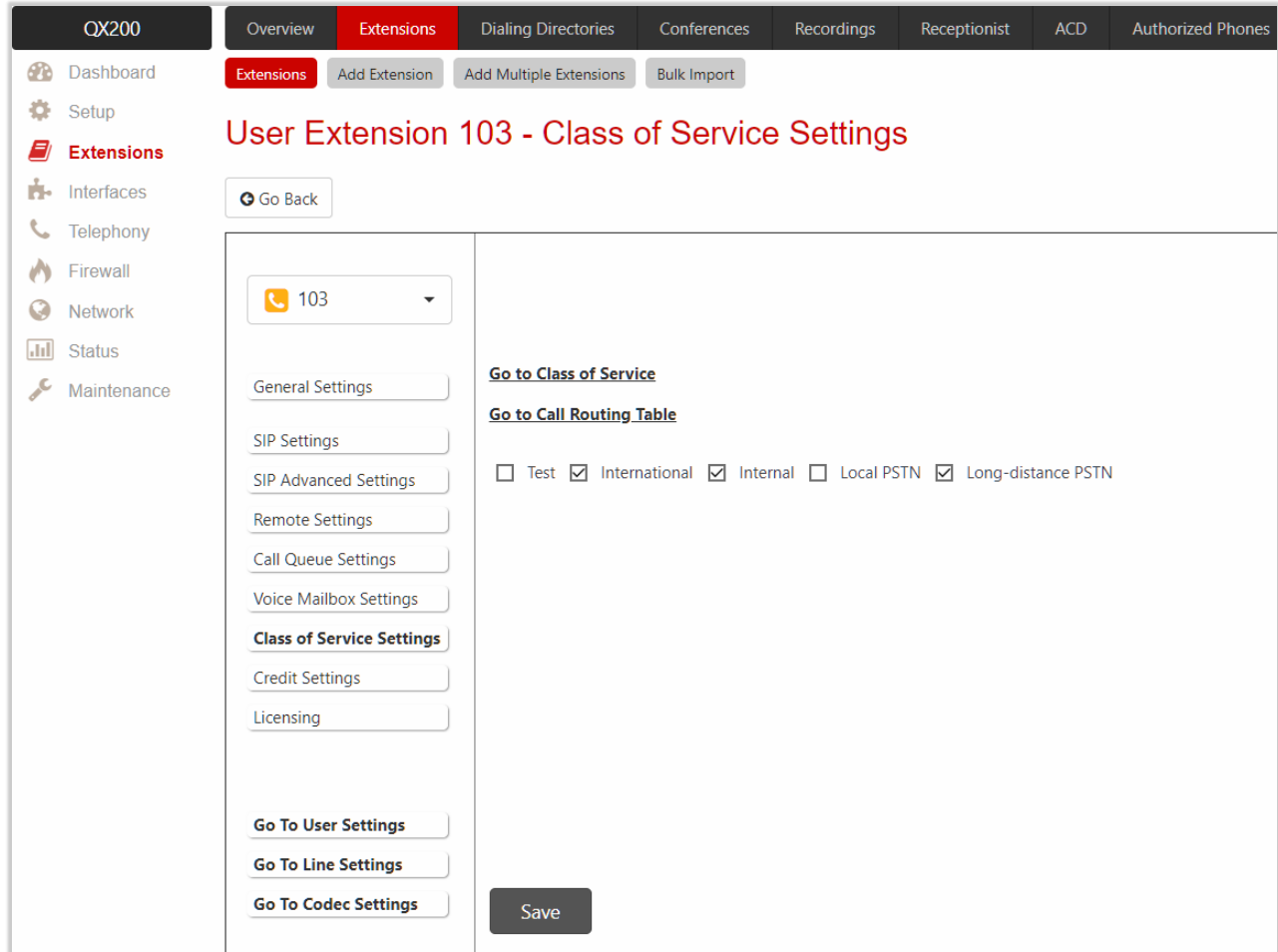
- **Proxy Controlled Mailbox Type** keeps the recorded voice messages on the **SIP Proxy Server**. When user accesses mailbox by dialing \*0, the call will be redirected to the **Voice Mailbox** on the proxy server. It is recommended to select the **Proxy Controlled Mailbox Type** option if the **Voice Mail Server** is combined with the **SIP Proxy Server**.
- **Proxy Controlled Mailbox Type** redirects the recorded voice messages to the preconfigured **Voice Mail Server**. When user accesses the mailbox by dialing \*0, the call will be redirected to the remote **Voice Mail Server**. It is recommended to select the **Independent Mailbox Type** option if the **Voice Mail Server** acts as a standalone location for the voice mails. **TIP:** It is required to set the **SIP URI** of **Voice Mail Server** where voice mails of the current extension will be collected for both options described above.
- **Transport Protocol for SIP messages** is used to select the transport protocol (UDP or TCP) for the transmission of SIP messages.
- **MS Exchange Server** keeps recorded voice messages into one universal inbox.
  - ◆ **UM Auto Attendant URI** is used to set the **SIP URI** of **MS Exchange Server**. When user accesses mailbox by dialing \*0, the call will be redirected to the **Voice Mailbox** on **MS Exchange Server**.
  - ◆ **UM Extension** is used to enter the extension number that **Unified Messaging** will use when voice messages are submitted to user **Voice Mailbox**.

**Note:**

- For more information on how to configure and use **MS Exchange Server**, refer to the [Configuring MS Exchange Server as External VM Server for QX IP PBX](#) guide.
- Some internal **Voice Mail** services will become unavailable while choosing the **Use External Voice Mail** option. Instead, services of external **Voice Mail** service will become available to user. Consult with the external **Voice Mail** service administrator before enabling this option.

## Class of Service Settings

This section describes how to assign the defined classes to extensions. The **Class of Service** specifies **user** or **conference** extensions that can use specific call routing rules to make a call. Extension not assigned to a certain class of service can't use a routing rule with **Class of Service** enabled.



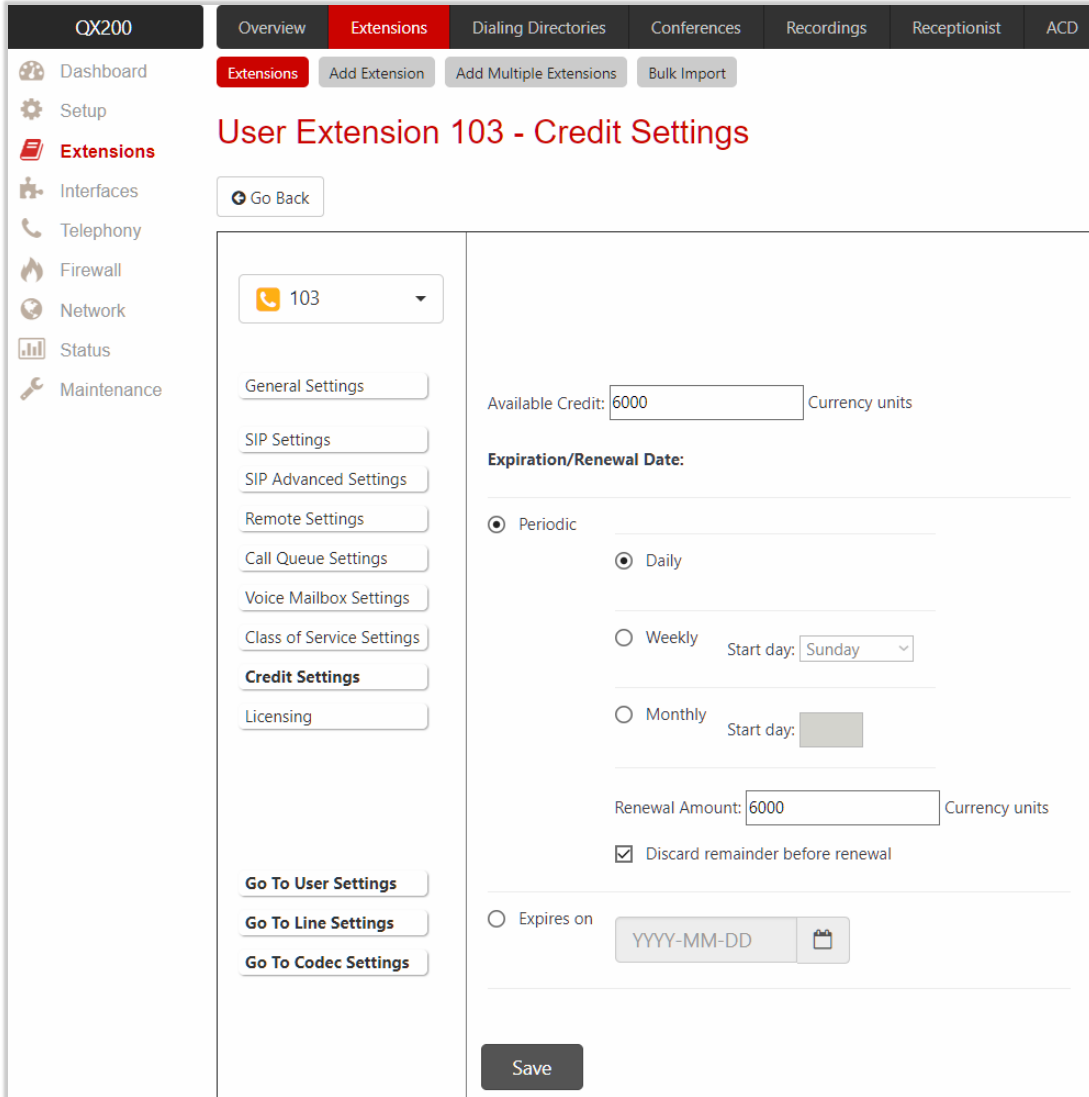
The screenshot shows the QX200 web interface. The top navigation bar includes 'Overview', 'Extensions' (selected), 'Dialing Directories', 'Conferences', 'Recordings', 'Receptionist', 'ACD', and 'Authorized Phones'. The left sidebar contains a navigation menu with items like 'Dashboard', 'Setup', 'Extensions' (highlighted), 'Interfaces', 'Telephony', 'Firewall', 'Network', 'Status', and 'Maintenance'. The main content area is titled 'User Extension 103 - Class of Service Settings'. It features a 'Go Back' button, a dropdown menu for extension '103', and a list of settings tabs: 'General Settings', 'SIP Settings', 'SIP Advanced Settings', 'Remote Settings', 'Call Queue Settings', 'Voice Mailbox Settings', 'Class of Service Settings' (selected), 'Credit Settings', and 'Licensing'. Below these are buttons for 'Go To User Settings', 'Go To Line Settings', and 'Go To Codec Settings'. The right side of the main content area contains links for 'Go to Class of Service' and 'Go to Call Routing Table', followed by a list of checkboxes: 'Test' (unchecked), 'International' (checked), 'Internal' (checked), 'Local PSTN' (unchecked), and 'Long-distance PSTN' (checked). A 'Save' button is located at the bottom right of the main content area.

Figure 33: Class of Service Settings section

**Note:** User and Conference extensions can be attached to several **Class of Services** at the same time.

## Credit Settings

The **Calling Cost Control** service allows to assign and manage credits to each extension for making calls. The assigned credit would be used and controlled when making a call through specific ("payable") call routing rules. Extensions not having credit can't use the routing rules with [Calling Rate Settings](#) enabled. **Credit Settings** is used to set the credit amount for the extension.



The screenshot shows the 'User Extension 103 - Credit Settings' page. The left sidebar contains navigation options: Dashboard, Setup, Extensions (selected), Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The top navigation bar includes Overview, Extensions (selected), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. Below the top bar are buttons for 'Add Extension', 'Add Multiple Extensions', and 'Bulk Import'. The main content area features a 'Go Back' button and a dropdown menu for extension '103'. A list of settings categories is shown: General Settings, SIP Settings, SIP Advanced Settings, Remote Settings, Call Queue Settings, Voice Mailbox Settings, Class of Service Settings, **Credit Settings** (highlighted), and Licensing. Below these are buttons for 'Go To User Settings', 'Go To Line Settings', and 'Go To Codec Settings'. The Credit Settings section includes:
 

- Available Credit: 6000 Currency units
- Expiration/Renewal Date:
  - Periodic
    - Daily
    - Weekly Start day: Sunday
    - Monthly Start day: [calendar icon]
  - Expires on YYYY-MM-DD [calendar icon]
- Renewal Amount: 6000 Currency units
- Discard remainder before renewal

 A 'Save' button is located at the bottom of the form.

Figure 34: Credit Settings section

The following settings (options) are available:

- **Available Credit** is used to set the credit that can be used by extension. Once the **Available Credit** expires, the call will be disconnected without a prior notice. Placing a new call through routing rule(s) with **Call Rate Settings** option enabled is not possible until the **Available Credit** is updated (either manually or automatically by the renewal date and amount).
- **Periodic** is used to select one of the **Renewal Date** options:
  - **Daily** – the defined **Available Credit** will be renewed every day.
  - **Weekly** – the defined **Available Credit** will be renewed every week on a specified weekday.
  - **Monthly** – the defined **Available Credit** will be renewed every month on a specified day.

- **Renewal Amount** is used to set the renewal amount to be added to **Available Credit** when the expiration date of **Available Credit** is reached. Leave the field blank, if you don't need to renew **Available Credit**.
- **Discard remainder before renewal** is used to discard the remainder of **Available Credit** before renewal and set **Renewal Amount** as a new **Available Credit**.
- **Expires on** is used to manually set the expiration date for **Available Credit**. After **Expiration Date**, extension will not be able to make a new call through call routing rule(s) with the **Call Rate Settings** option enabled.

## Licensing

The **Licensing** section becomes available only if the corresponding licenses are activated.

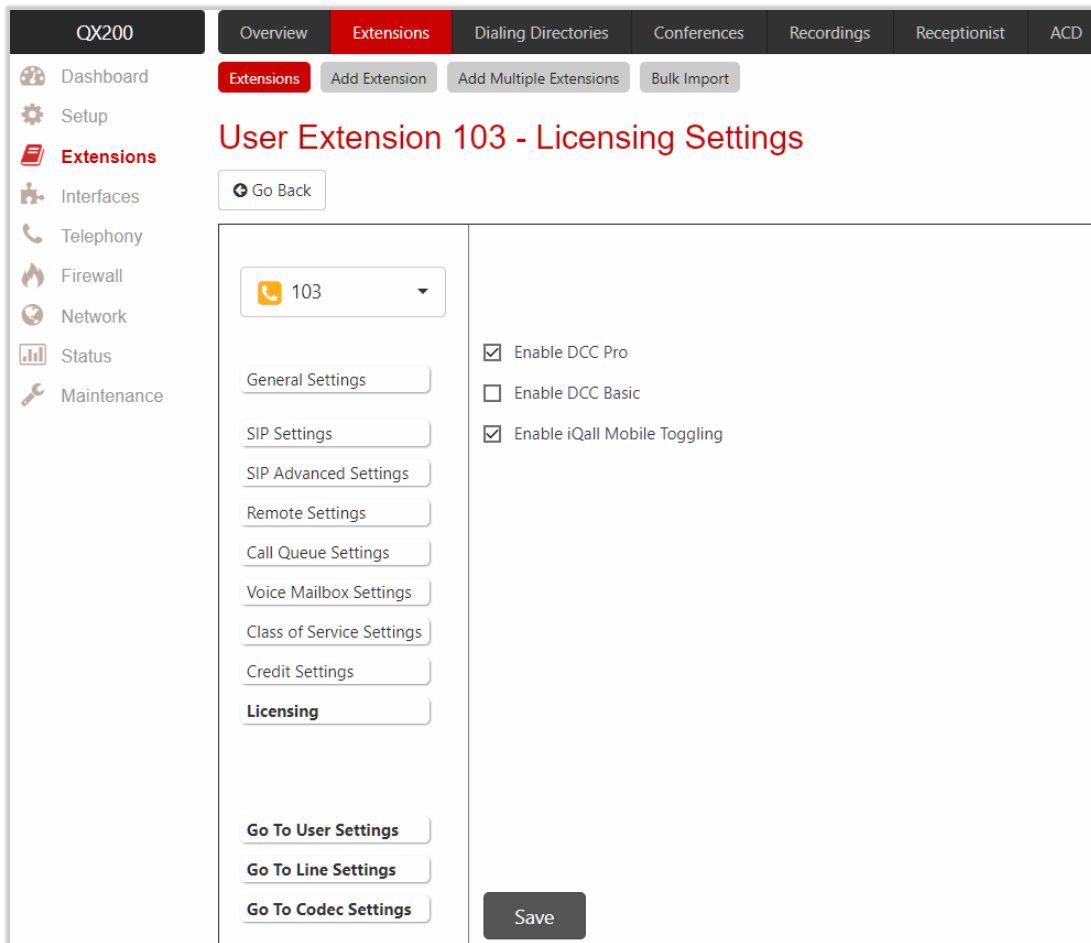


Figure 35: Licensing section

The following settings (options) are available:

- **Enable DCC Pro** allows to set the extension to be used by the **DCC Pro** application. **TIP:** DCC Pro/Basic licenses can't be activated simultaneously for the same extension.
- **Enable DCC Basic** allows to set the extension to be used by the **DCC Basic** application.
- **Enable iQall Mobile Toggling** allows to allocate the **iQall Mobile Toggling** license to the extension.

For more information on how to configure and use these features, refer to the [Licensable Features on QX IP PBXs](#) guide.

## Parent-Child Configuration

The **Parent-Child** configuration allows to assign a number of extensions (phones) to the certain **Parent** extension as a **Child**. Phone(s) configured as a **Child** will make outbound calls on behalf of an extension configured as a **Parent**. **Child** extension(s) will ring simultaneously in case of inbound call to the **Parent**.

The **Parent-Child** configuration can be used in specific cases, to create the appearance that many phones are connected to the same extension. This feature can be used, for example, with **Epygi Hotel Console (EHC)** feature for hotel rooms having many phones or with other applications where many phones are linked to the same extension.

In case of outbound calls, **Child** extensions are not visible for called destinations. When placing an outbound call from the **Child** phone the Caller ID and the name of **Parent** extension would appear at the destination.

In case of inbound calls to the **Parent**, all phones configured as a **Child** will ring simultaneously with the **Parent**. The **Parent** or any of **Child** phones can answer the call.

### Note:

- **Child** extension(s) will lose the SIP registration, the configured **Basic** and **Caller ID Services**.
- **Child** extension(s) will not be able to receive incoming calls directly and will ring only when the **Parent** extension is dialed.

## 6.1.6 Pickup Group

The **Call Pickup** service allows to pick up calls ringing on a certain group of extensions by dialing **Pickup Group** extension number.

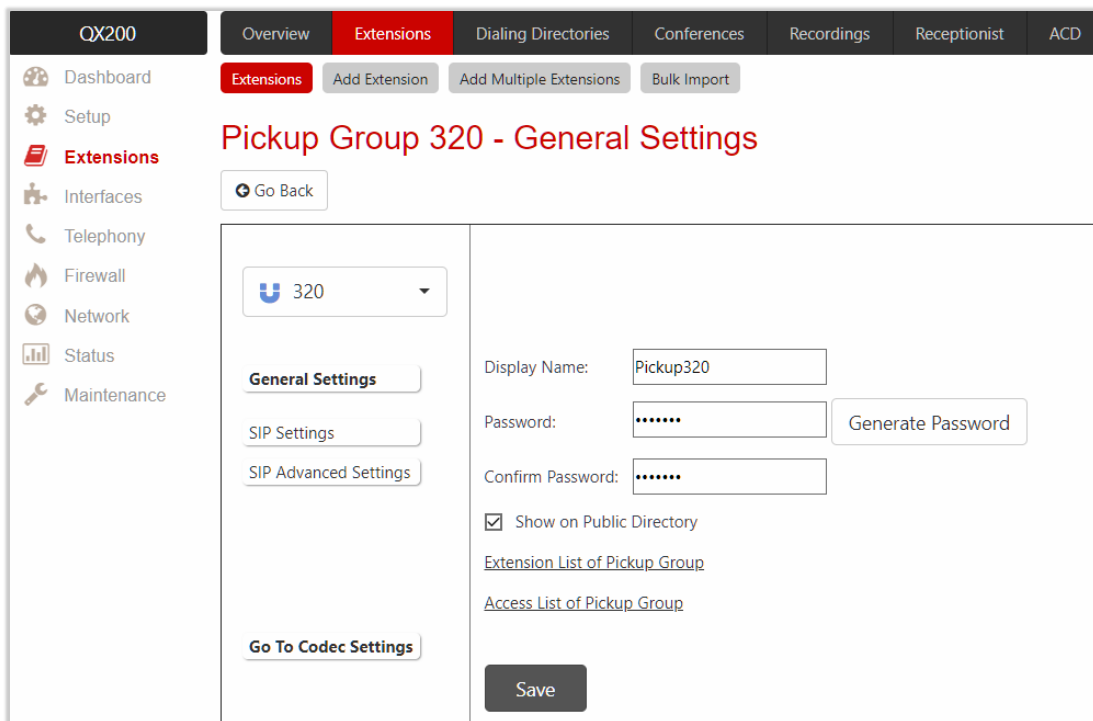


Figure 36: Pickup Group – General Settings section

To configure **Pickup Group** extension:

1. Click the **Extension List of Pickup Group** link.
2. Select the extension(s) and click **Enable**. Calls to these extensions can be picked up.



3. Go **Back** and click the **Access List of Pickup Group** link.
4. Click **Add** and enter the extension(s) allowed or denied permission to pick up the ringing calls.
5. Click **Save** to add the new entry to the **Access List of Pickup Group** table.

**How it works:** When call is ringing on another phone, you can pick up that call on your own phone by dialing the number of the **Pickup Group** extension.

**Note:**

- The [General Settings](#), [SIP Settings](#), [SIP Advanced Settings](#) and [Go To Codec Settings](#) sections are the same as for user extension.
- When a caller not listed in the **Access List** calls the **Pickup Group** extension, password authorization (the password of the **Pickup Group** extension) will be required to allow the call pickup.
- If a user dials the **Pickup Group** extension when several extensions of the **Pickup Group** are ringing, the first (oldest in time) call will be picked up.

### 6.1.7 Call Park

The **Call Park** service allows to park a call, (the call will be automatically placed on hold) then retrieve the parked call from another phone by dialing the **Call Park** extension number.

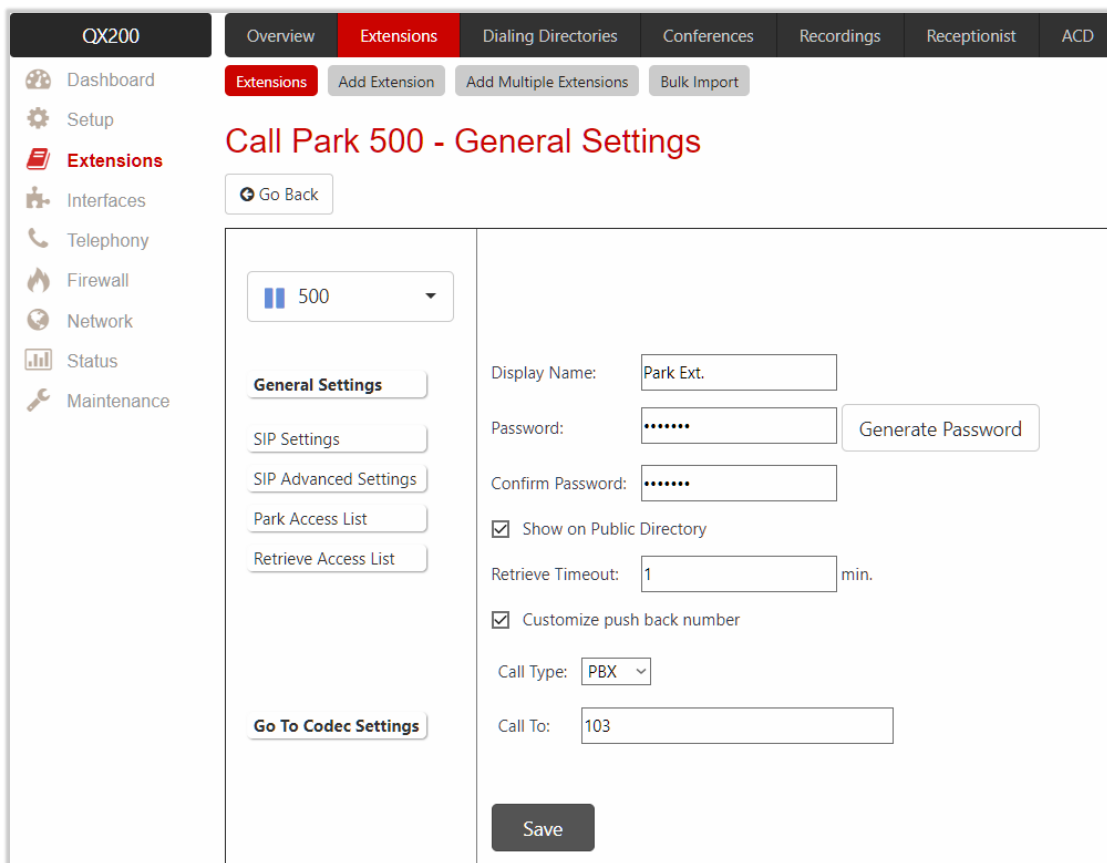


Figure 37: Call Park – General Settings section

The following settings (options) are available:

- **Retrieve Timeout** is used to set the timeout during which the call will stay in Call Park, i.e. the parked user will remain on-hold.

- **Customize push back number** – if selected, after the call park retrieve timeout expires, the hold music will stop playing to the parked party (user) and a new call will be placed towards the push back number configured in the **Customize push back number** field. **TIP:** If the **Customize push back number** option is not selected, then after the call park retrieve timeout expires, the call will be forwarded back to the extension which parked the call.

To configure **Call Park** extension:

1. Click the **Park Access List** link, then click **Add**.
2. Enter the extension number(s). These extensions will be able to park calls on the **Call Park** extension.
3. Click **Save** to add the new entry to the **Park Access List** table.
4. Click the **Retrieve Access List** link, then click **Add**.
5. Enter the extension number(s) allowed to retrieve the parked calls from the current **Call Park** extension.
6. Click **Save** to add the new entry to the **Retrieve Access List** table.

**How it works:** To park a call, put the active call on hold and either dial **\*5** or the **Call Park** extension number. The call will be parked. To retrieve the call, dial the **Call Park** extension number.

**Note:**

- The [General Settings](#), [SIP Settings](#), [SIP Advanced Settings](#) and [Go To Codec Settings](#) sections are the same as for user extension.
- Any extension missing from the **Park Access List** won't be able to park a call to the current call park extension.
- When a caller not listed in the **Retrieve Access List**, calls the **Call Park** extension, password authorization (the password of the **Call Park** extension) will be required to allow retrieving the parked call.
- For more information on how to park/retrieve calls on Epygi supported IP phones, refer to the [QX IP PBX Features on Epygi Supported IP Phones](#) guide.

### 6.1.8 Paging Group

The **Call Paging** service is used to page a group of extensions (phones) by forcing all extensions in the group to go off-hook and opening one-way voice communication. This service allows to page multiple extensions by dialing the **Paging Group** extension.

To configure the **Paging Group** extension:

1. Click the **Extension List of Paging Group** link.
2. Select the extension(s) you want to page and click **Enable**.
3. Go **Back** and click the **Access List of Paging Group**.
4. Click **Add** to add a new user and allow (deny) him access to the **Paging Group**. These users (extensions) will be allowed/denied to dial the **Paging Group** extension.
5. Click **Save** to add the new user to the **Access List of Paging Group**.

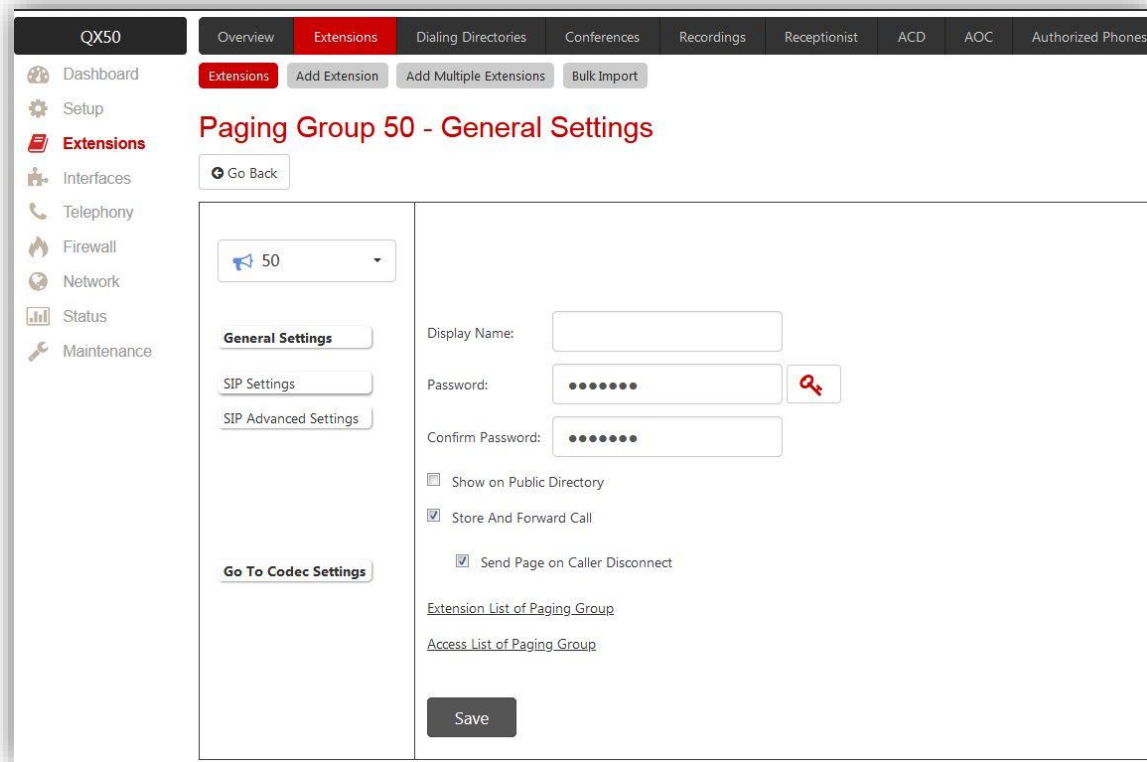


Figure 38: Paging Group – General Settings section

### How it works:

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 and the caller will be able to make 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.

**Store And Forward Call** option can be used in scenarios when the Paging Group service is used intensively, for example, when multiple calls are coming to the same paging group simultaneously. If selected, this option allows recording and storing the announcement messages, putting them in a queue, and delivering the messages to the intended paging group in the order they arrived.

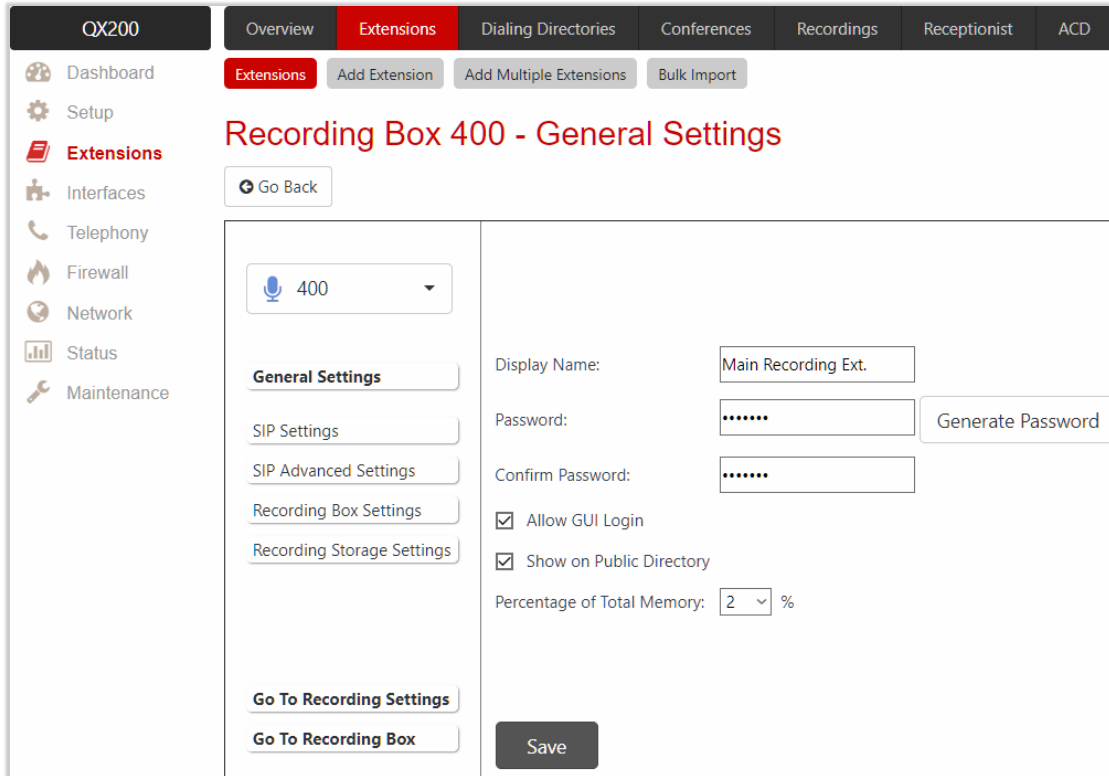
**Send Page on Caller Disconnect** option can be used with the **Store And Forward Call** option. Allows to send the page by simply hanging up the phone, without waiting for #.

### Note:

- The [SIP Settings](#), [SIP Advanced Settings](#) and [Go To Codec Settings](#) sections are the same as for user extension.
- When a caller (not listed in the **Access List of Paging Group** table) calls the **Paging Group** extension, password authorization (the password of the **Paging Group** extension) will be required to start the call paging.
- **Paging** will not work if the called phone is in call.
- Make sure the called phones support automatic off-hook. For more information how to use **Paging** service on Epygi supported IP phones, refer to the [QX IP PBX Features on Epygi Supported IP Phones](#) guide.

## 6.1.9 Recording Box

Recorded calls on QX can either be stored locally in the **Recording Box** or transferred to the remote server. Recording Box is used to store the recorded calls locally. Users can access the Recording Box either from WEB GUI or from handset by calling the corresponding Recording Box extension. In both cases, the user can play and delete the recordings.



The screenshot shows the 'Recording Box 400 - General Settings' page in the QX200 web interface. The page has a dark header with navigation tabs: Overview, Extensions (active), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. Below the header, there are buttons for 'Add Extension', 'Add Multiple Extensions', and 'Bulk Import'. The main content area is titled 'Recording Box 400 - General Settings' and includes a 'Go Back' button. On the left, there is a sidebar with icons for Dashboard, Setup, Extensions (highlighted), Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main settings area includes a dropdown menu for extension '400', a 'General Settings' tab, and several configuration options: 'Display Name' (Main Recording Ext.), 'Password' (with a 'Generate Password' button), 'Confirm Password', 'Allow GUI Login' (checked), 'Show on Public Directory' (checked), and 'Percentage of Total Memory' (2%). At the bottom, there are buttons for 'Go To Recording Settings', 'Go To Recording Box', and a 'Save' button.

Figure 39: General Settings section

### Recording Box Settings

This section describes how to configure specific settings of Recording Box. The following settings (options) are available:

- **Ask Password on Local Access** protects local access to the Recording Box. If selected, the Recording Box password will be required to access the Recording Box locally.
- **Ask Password on Remote Access** protects remote access to the Recording Box. If selected, the Recording Box password will be required to access the Recording Box remotely.
- **Play Welcome Message** enables the welcome message that is played when accessing the Recording Box.
- **Maximum Recordings** refers to the maximum number of recordings allowed to be stored in the **Recording Box**. If this number is reached, some of call recordings should be deleted from the Recording Box, to free up space for new recordings.
- **Single Recording Duration** refers to the maximum recording duration for a single call. When the recording duration expires, recording will be stopped while the call will stay active.
- **Forward/Rewind Duration** is used to select the timeout in seconds to shift the recording playback from the handset.
- **Play announcement when starting recording** is used to play an announcement before starting the recording. The call recording will start without notification if this option is disabled.

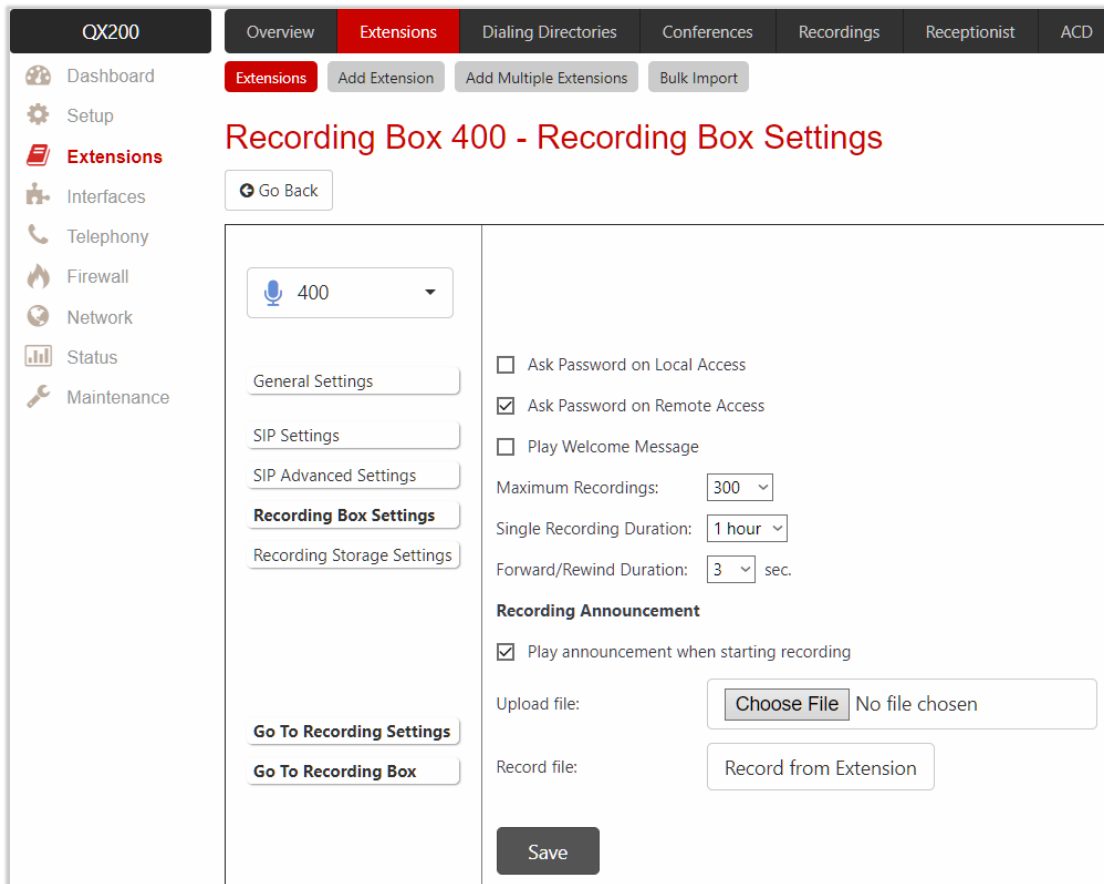


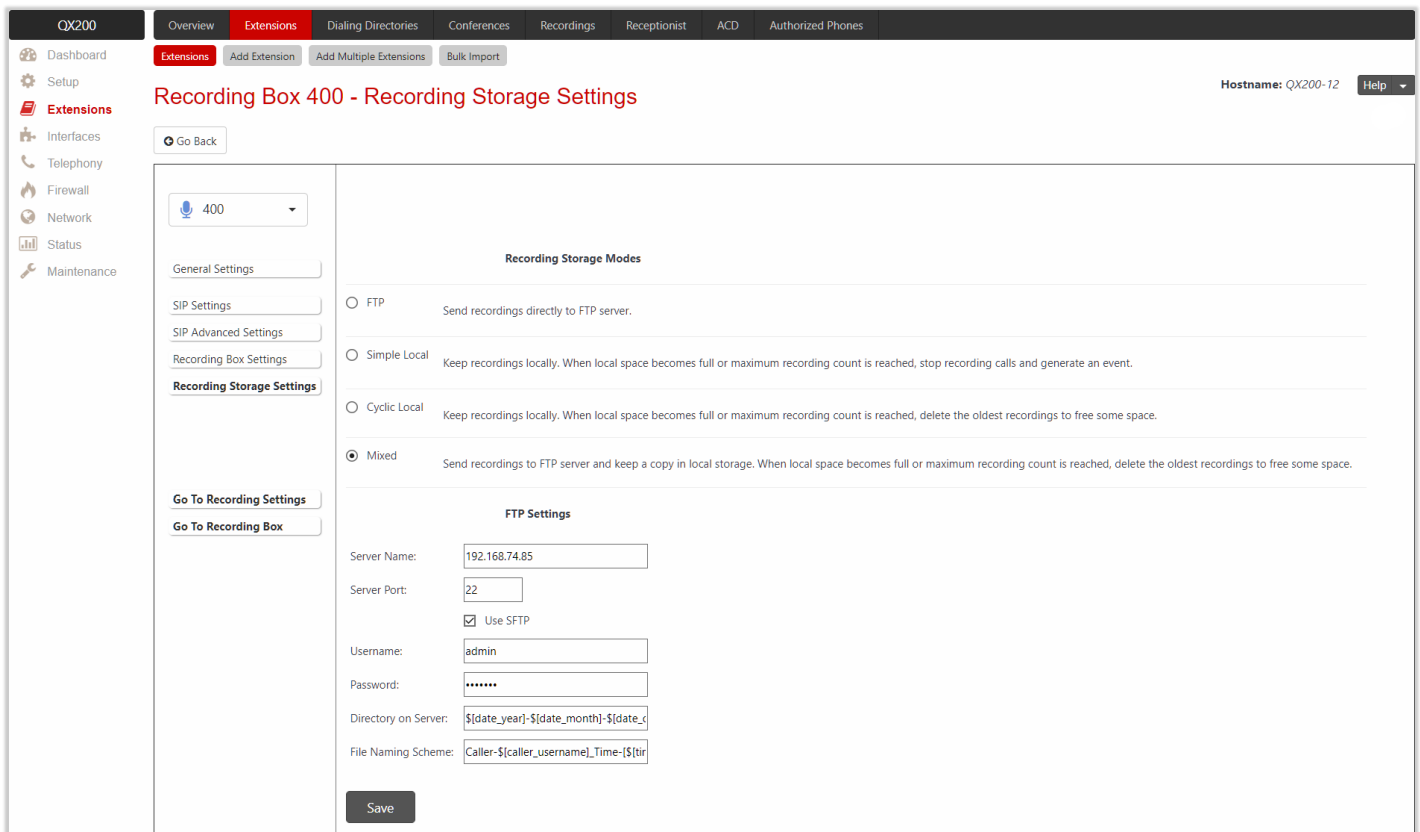
Figure 40: Recording Box Settings section

## Recording Storage Settings

This section describes how to configure the recording storage settings. The following settings (options) are available:

- **Recording Storage Modes** offers the following recording storage options:
  - **FTP** sends recordings directly to FTP server.
  - **Simple Local** keeps recordings locally. When local space is full or maximum recording count is reached, stop recording calls and generate an event.
  - **Cyclic Local** keeps recordings locally. When local space is full or a maximum recording count is reached, delete oldest recordings to free up some space.
  - **Mixed** keeps recordings to FTP server and keeps a copy in local storage. When local space is full or a maximum recording count is reached, delete oldest recordings to free up some space.
- **FTP Settings** is used to set the FTP server parameters:
  - **Server Name** is used to set the IP address or hostname.
  - **Server Port** is used to set the port number.
  - **Use SFTP** enables SSH FTP (SFTP) support, which allows using secure FTP connection.
  - **Username** and **Password** are used to set the authentication parameters.
  - **Directory on Server** is used to set the location on the server where the recordings will be stored.
  - **File Naming Scheme** is used to set 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 field may contain any distinctive text and also offers a list of variables:
    - ◆ **call\_guid** – unique GUID of the call
    - ◆ **recording\_id** – unique recording ID of the call
    - ◆ **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
- ◆ `recording_id` – unique recording ID of the call



The screenshot shows the 'Recording Storage Settings' page for Recording Box 400. The page is part of the QX200 administration interface, with a navigation menu on the left and a top navigation bar. The main content area is titled 'Recording Storage Modes' and contains several radio button options for storage configuration. Below these options is the 'FTP Settings' section, which includes input fields for Server Name, Server Port, Username, Password, Directory on Server, and File Naming Scheme. A 'Save' button is located at the bottom of the form.

**Recording Storage Modes**

- FTP: Send recordings directly to FTP server.
- Simple Local: Keep recordings locally. When local space becomes full or maximum recording count is reached, stop recording calls and generate an event.
- Cyclic Local: Keep recordings locally. When local space becomes full or maximum recording count is reached, delete the oldest recordings to free some space.
- Mixed: Send recordings to FTP server and keep a copy in local storage. When local space becomes full or maximum recording count is reached, delete the oldest recordings to free some space.

**FTP Settings**

Server Name:

Server Port:

Use SFTP

Username:

Password:

Directory on Server:

File Naming Scheme:

Figure 41: Recording Storage Settings section

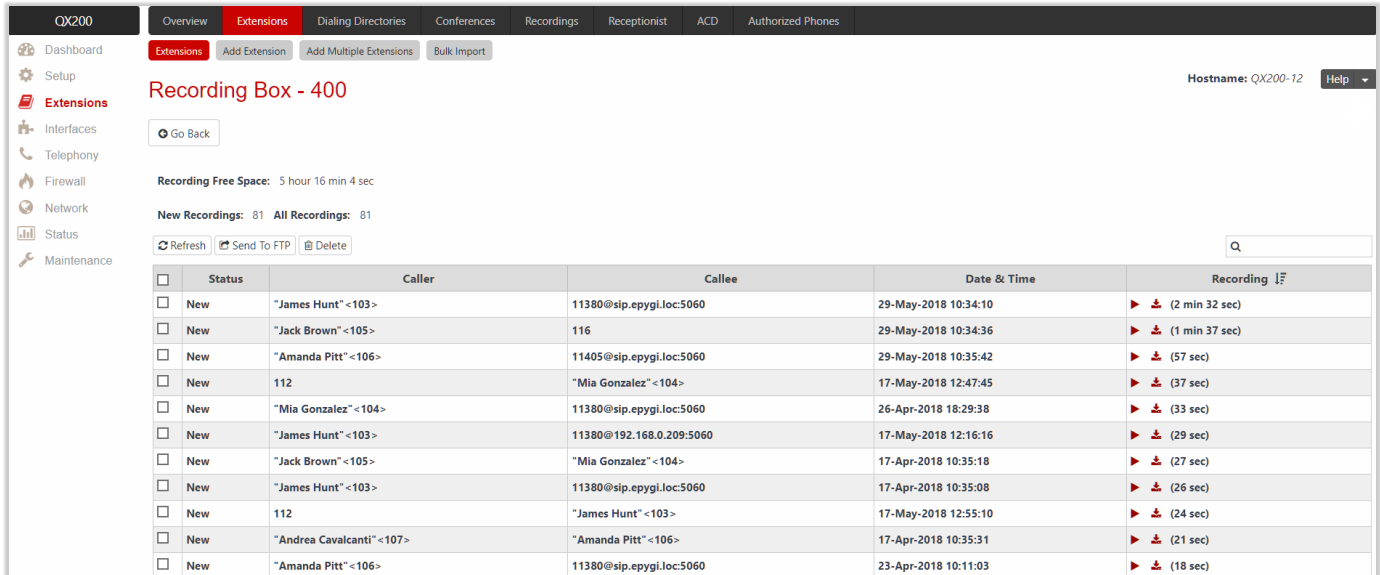
Any combination of listed variables can be used in the **File Naming Scheme** field.

**Example for a file naming scheme:** MyQX-`[$[caller_dispname]-[$[duration]-[$[time_hour]-[$[time_min]` business.

If Andrew is the caller, call recording started at 14:10 and lasted 15 seconds then the files stored on the FTP server for this Recording Box will have the following name: MyQX-Andrew-15 sec-14-10-business.wav

## Recording Box

Users can access the Recording Box either from WEB GUI or from handset by calling the Recording Box extension. In both cases, the user can play and delete the recorded calls in the Recording Box.



The screenshot shows the 'Recording Box - 400' page in the QX200 web GUI. The page includes a navigation menu on the left, a top navigation bar with tabs like Overview, Extensions, and Recordings, and a main content area. The main content area displays the following information:

- Recording Free Space: 5 hour 16 min 4 sec
- New Recordings: 81 All Recordings: 81
- Buttons: Refresh, Send To FTP, Delete
- Search bar
- Table of recordings with columns: Status, Caller, Callee, Date & Time, Recording (with play and delete icons)

Status	Caller	Callee	Date & Time	Recording
New	"James Hunt" <103>	11380@sip.epygi.loc:5060	29-May-2018 10:34:10	(2 min 32 sec)
New	"Jack Brown" <105>	116	29-May-2018 10:34:36	(1 min 37 sec)
New	"Amanda Pitt" <106>	11405@sip.epygi.loc:5060	29-May-2018 10:35:42	(57 sec)
New	112	"Mia Gonzalez" <104>	17-May-2018 12:47:45	(37 sec)
New	"Mia Gonzalez" <104>	11380@sip.epygi.loc:5060	26-Apr-2018 18:29:38	(33 sec)
New	"James Hunt" <103>	11380@192.168.0.209:5060	17-May-2018 12:16:16	(29 sec)
New	"Jack Brown" <105>	"Mia Gonzalez" <104>	17-Apr-2018 10:35:18	(27 sec)
New	"James Hunt" <103>	11380@sip.epygi.loc:5060	17-Apr-2018 10:35:08	(26 sec)
New	112	"James Hunt" <103>	17-May-2018 12:55:10	(24 sec)
New	"Andrea Cavalcanti" <107>	"Amanda Pitt" <106>	17-Apr-2018 10:35:31	(21 sec)
New	"Amanda Pitt" <106>	11380@sip.epygi.loc:5060	23-Apr-2018 10:11:03	(18 sec)

Figure 42: Recording Box page

### Note:

- The [General Settings](#), [SIP Settings](#), [SIP Advanced Settings](#) and [Go To Codec Settings](#) sections are the same as for user extension.
- When using **Call Recording** on the QX50/QX200 it is advisable to use an SD memory card to expand the system memory.
- When using **Call Recording** on the QX20/QX500 it is advisable to use a micro SD memory card to expand the system memory.

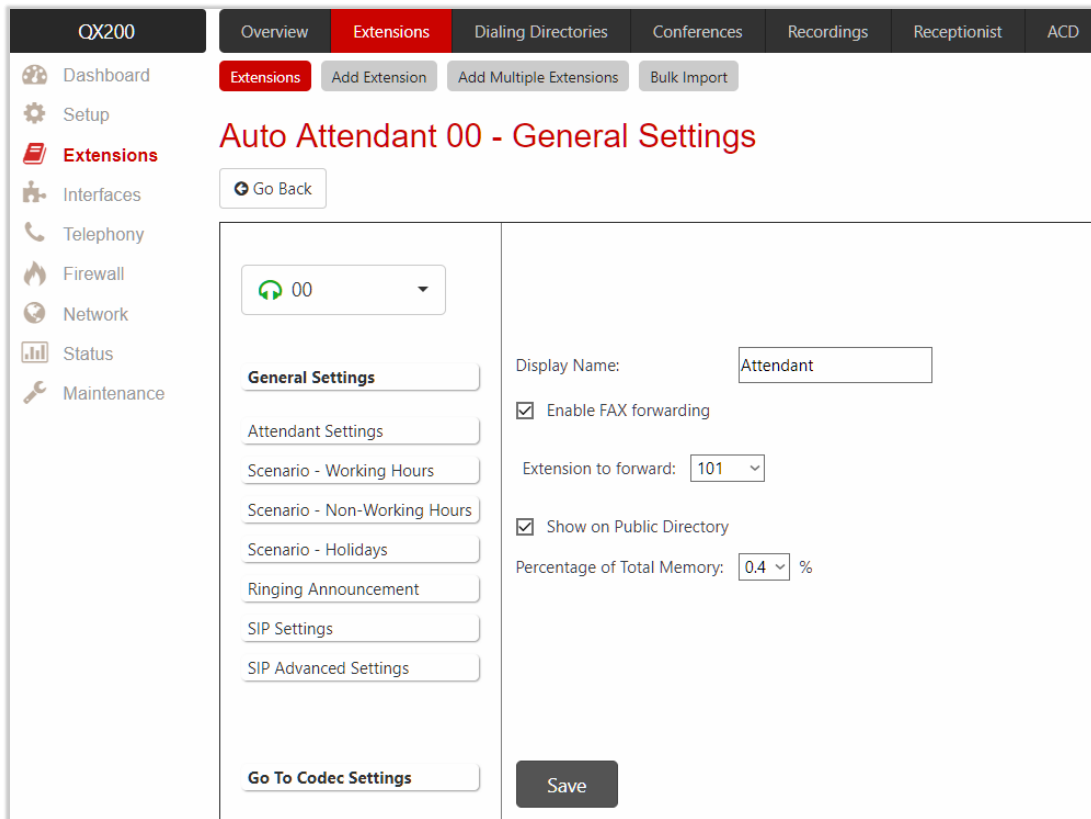
## 6.1.10 Auto Attendant

**Auto Attendant** is an IVR system that replaces a receptionist and allows to distribute calls to QX extensions or services through audio prompts.

**Note:** The [SIP Settings](#), [SIP Advanced Settings](#) and [Go To Codec Settings](#) sections are the same as for user extension.

### General Settings

This section describes how to configure general settings of auto attendant.



The screenshot shows the 'Auto Attendant 00 - General Settings' configuration page. The interface includes a top navigation bar with tabs for Overview, Extensions (selected), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. A left sidebar contains menu items: Dashboard, Setup, Extensions (highlighted), Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area features a 'Go Back' button and a dropdown menu for extension '00'. Below this is a list of settings categories: General Settings (selected), Attendant Settings, Scenario - Working Hours, Scenario - Non-Working Hours, Scenario - Holidays, Ringing Announcement, SIP Settings, and SIP Advanced Settings. At the bottom of this list is a 'Go To Codec Settings' button. The right-hand side of the page contains specific configuration options: 'Display Name' (text input: 'Attendant'), 'Enable FAX forwarding' (checkbox: checked), 'Extension to forward' (dropdown: '101'), 'Show on Public Directory' (checkbox: checked), and 'Percentage of Total Memory' (dropdown: '0.4 %'). A 'Save' button is located at the bottom right of the configuration area.

Figure 43: Auto Attendant – General Settings section

The following settings (options) are available:

- **Display Name** is the caller ID that will be displayed on the phone when making a call to/from auto attendant (e.g. when using **Callback** service).
- **Enable FAX forwarding** – if selected, the system forwards the FAX messages to the selected extension in case incoming calls are routed to the auto attendant and FAX tone is detected.
- **Extension to forward** is used to select the extension where the incoming FAX addressed to the auto attendant will be forwarded. The list contains only those extensions that have FAX support enabled. The FAX support can be enabled from the **Extension Codecs** page. **TIP:** FAX forwarding is applicable only for incoming calls from PSTN and SIP.
- **Show on Public Directory** – if selected, automatically includes the extension display name and number in the **Phone Book (Directory)** and **Extension Directory**.
- **Percentage of Total Memory** is used to allocate memory for custom messages.



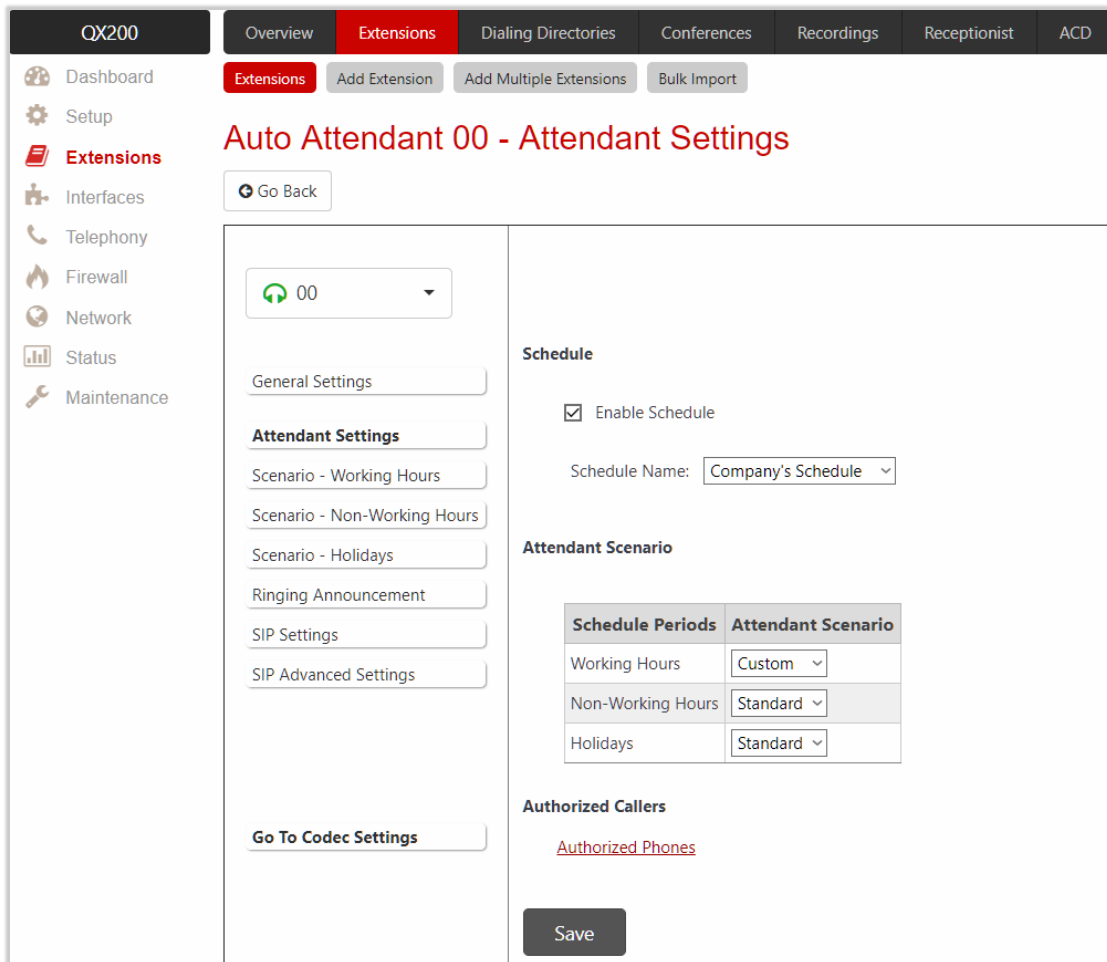
## Attendant Settings

This section describes how to apply schedules and manage the scenario(s) for the scheduled periods. The following settings (options) are available:

- **Enable Schedule** is used to select and apply preconfigured **schedule**. The applied schedule allows to configure different scenarios for scheduled periods (working hours, non-working hours and holidays).
- **Attendant Scenario** is used to select the scenario. The following scenarios are available:
  - [Standard scenario](#) is available and active on the 00 auto attendant and for newly created auto attendants by default.
  - [VXML scenario](#) allows to upload a custom scenario file in VXML format.
  - [Custom scenario](#) allows to configure the custom scenario with the embedded scenario builder.
  - [ACD scenario](#) allows to activate a special scenario for ACD agents.

**Note:** Enable the **Schedule** option and apply a schedule to the auto attendant, to be able to select a scenario for each period.

- **Authorized Phones** leads to the [Authorized Phones](#) page. The trusted user (external SIP or PSTN caller) will be able to use QX services after calling the auto attendant, as if a user extension. If the **Callback** service is activated the trusted user will get a call back from auto attendant.



QX200
Overview **Extensions** Dialing Directories Conferences Recordings Receptionist ACD

Extensions
Add Extension
Add Multiple Extensions
Bulk Import

### Auto Attendant 00 - Attendant Settings

Go Back

00

General Settings

**Attendant Settings**

Scenario - Working Hours

Scenario - Non-Working Hours

Scenario - Holidays

Ringing Announcement

SIP Settings

SIP Advanced Settings

Go To Codec Settings

**Schedule**

Enable Schedule

Schedule Name: Company's Schedule

**Attendant Scenario**

Schedule Periods	Attendant Scenario
Working Hours	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">Custom</span>
Non-Working Hours	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">Standard</span>
Holidays	<span style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;">Standard</span>

**Authorized Callers**

[Authorized Phones](#)

Save

Figure 44: Attendant Settings section

## Attendant Scenario

This section is used to configure the selected scenario.

### Standard scenario

The following settings (options) will be available by selecting the **Standard** scenario:

- **Pass Dialed Digits through Call Routing** – if selected, sends the dialed numbers to the [Call Routing Table](#).
- **Enable No Input Redirect** – if activated and configured, callers will be redirected to the specified address in case if no action by caller on the recurring prompt. The **Prompt Repetition** is used to set the number of prompts to be played before redirection.
- **Enable ZeroOut Redirect** – if activated and configured, callers dialing **0** during welcome message or recurring prompt, will be redirected to the specified address. **Note:** The routing patterns in the **Call Routing Table** starting with digit **0** will not work for incoming calls to auto attendant if both the **ZeroOut** and **Pass Dialed Digits through Call Routing**

options are enabled. The **ZeroOut** option has a higher priority. If enabled, the system will redirect calls to the specified destination. As a result, calls prefixed with **0** will never reach call routing.

- **Welcome Message** allows to enable and customize auto attendant welcome message.
- **Recurring Prompt** allows to customize the auto attendant recurring prompt (played after the welcome message and then periodically repeated while being in the auto attendant).

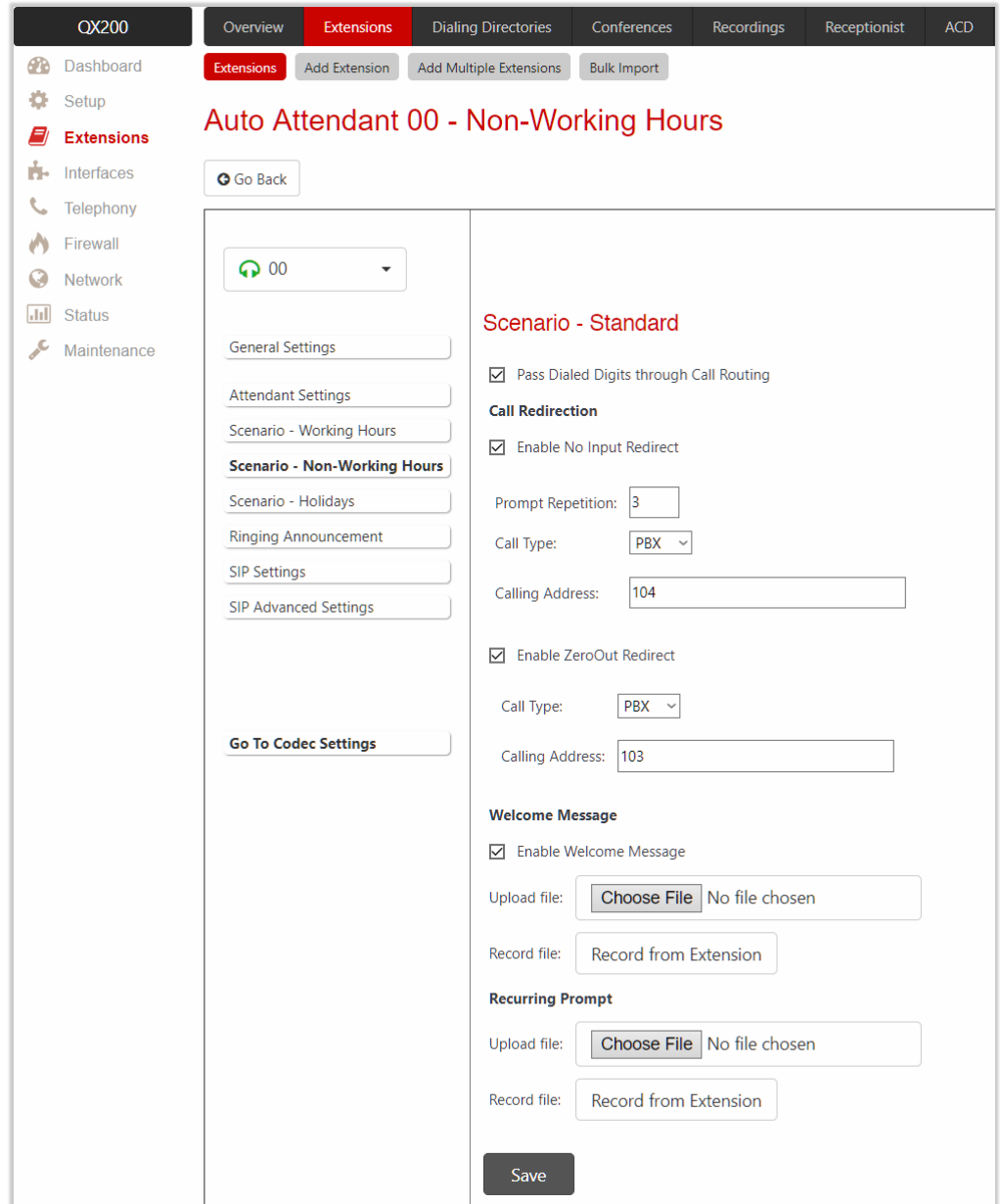


Figure 45: Auto Attendant – Standard scenario

## VXML scenario

The VXML scenario allows to upload a custom scenario file and voice messages.

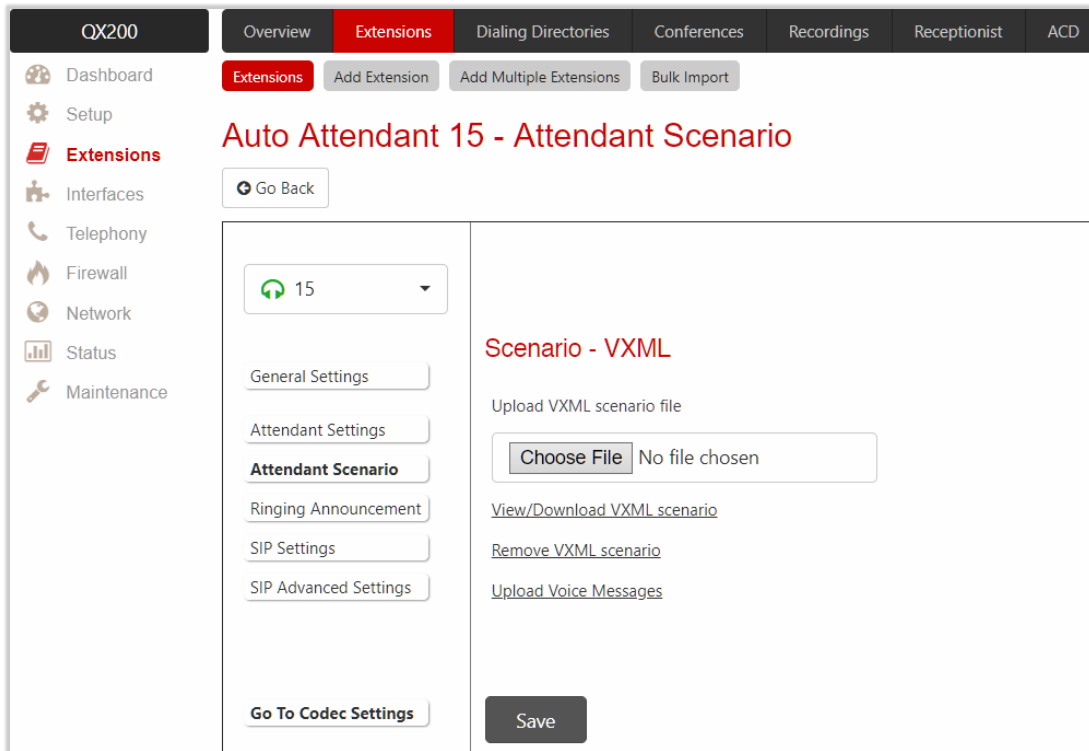


Figure 46: Auto Attendant – VXML scenario

To upload VXML scenario and voice messages:

1. Click **Choose File** to browse and select the VXML scenario file. **TIP:** The uploaded file needs to be in [EpygiXML](#) format and is restricted to 20 KB file size.
2. Click the **Upload Voice Messages** link.
3. Click **Choose File** to browse and upload the voice messages. **TIP:** To upload all voice messages at once, create an archive file of the (\*.tar.gz) type containing all the necessary files and upload it.

## Custom scenario

The Custom scenario allows to use the embedded scenario builder. The following components are available:

- **Create scenario** leads to the **Auto Attendant – Main Menu** page to create a new scenario. **TIP:** The **Create scenario** link will be renamed into the **Edit scenario** after creating a scenario.
- **Import/Export scenario** leads to the **Auto Attendant – Import/Export Scenario** page to import/export the scenario file.
- **Remove scenario** is used to remove the current scenario.
- **View/Download VXML scenario** is used to view and download the scenario script in VXML format.

Click the **Edit scenario** link to modify the custom scenario through scenario builder. Two main sections are available: **Main Menu** and **Submenus**. All incoming calls to auto attendant will be placed to the **Main Menu** first. The **Submenus** are the supplementary menus which can be called from other menus. There are no limitations on the depth and nesting levels of menus.

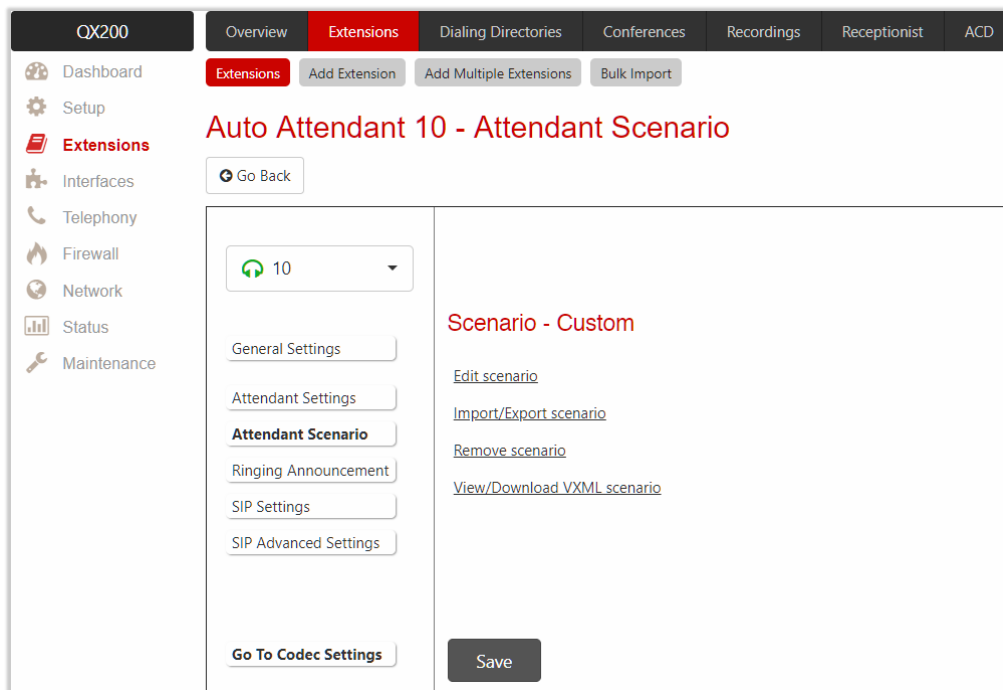


Figure 47: Auto Attendant – Custom scenario

## Main Menu

Main Menu consists of the following sections:

- **Welcome Message** is used to play a welcome message (**default** or **custom**) once when entering the **Main Menu**. **TIP:** If the **Welcome Message** is not specified, then the welcome message for **Standard** scenario will be played.
- **Enable Welcome Message** is used to activate the welcome message (**default** or **custom**).
- **Delay after message** is used to set the break between the welcome message and recurring prompt.

QX200
Overview **Extensions** Dialing Directories Conferences Recordings Receptionist ACD Authorized Phones

- Dashboard
- Setup
- Extensions**
- Interfaces
- Telephony
- Firewall
- Network
- Status
- Maintenance

Extensions
Add Extension
Add Multiple Extensions
Bulk Import

## Auto Attendant 10 - Main Menu

[Go Back](#)

**Main Menu** [Submenus](#)

**Welcome Message**

Enable Welcome Message

Upload file:  No file chosen

Record file:

Delay after Message:  sec.

**Recurring Prompt**

Record file:

Recurring\_Prompt.wav [Download](#) [Remove](#)

Play Count:

Interval:  sec.

**User Input Options**

	User Input	Announcement Message	Action	Description
<input type="checkbox"/>	0	Announcement_for_option_0.wav	Go to the following menu <a href="#">Marketing Department</a>	
<input type="checkbox"/>	1	Announcement_for_option_1.wav	Call to the extension <a href="#">305</a>	Call To AA
<input type="checkbox"/>	2	Announcement_for_option_2.wav	Call to the extension 103 "James Hunt "	Call To James
<input type="checkbox"/>	3	Announcement_for_option_3.wav	Call to the following number 711105	Call To Ashot
<input type="checkbox"/>	*	Announcement_for_option_star_NoAction.wav	No Action	No Action
<input type="checkbox"/>	#	vxml_00_1463120827.wav	Invoke Extension Directory	
<input type="checkbox"/>	Any input other than in the list above	Announcement_for_option_AnyInput.wav	Call to the number dialed	Call To
<input type="checkbox"/>	No input	Announcement_for_option_NoInput.wav	Terminate the Call	Terminate the Call

Dial Timeout:  sec.

**Incorrect number handling**

Figure 48: Create scenario – Main Menu page

- **Recurring Prompt** is used to play a recurring prompt (**default** or **custom**) after the **Welcome Message**. **TIP:** If the **Recurring Prompt** is not specified, then the recurring prompt for **Standard** scenario will be played.
  - **Play Count** is used to set the repetition count of the recurring prompt.
  - **Interval** is used to set the silence duration between consecutively played recurring prompts.
- **User Input Options** table consists of the following components:
  - **Option** is used to select the user input and configure it with some announcement and action to be taken.
  - **Any input other than preconfigured in the list** configures 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** configures the action taken when the caller doesn't enter anything during the certain period. The **No input** timeout is composed of [Welcome Message duration] + Delay after message + [Recurring

Prompt duration] \* Play Count + Play Count \* Interval. If there is no input during that time, the action specified for **No input** will take effect.

- **Dial Timeout** is used set the timeout after user has completed the dialing before the call processing starts. The timer will start after the last digit or symbol is entered. Press the **#** sign to process the call immediately.
- **Incorrect number handling** leads to the **Option Incorrect Number Handling** 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.

**Note:**

- The **Incorrect number handling** will be activated only if either an attempt was made to call to a non-existing extension or to a number not matching with any **Destination Number Pattern** in the **Call Routing Table**.
- The **Incorrect number handling** will be activated only if the call comes to the auto attendant from SIP, PSTN or IP-PSTN side.

Input Option Configuration

- **Add** leads to the **Add Option** page to configure previously unspecified inputs.
- **Edit** leads to the selected **Option** page to modify the actions of **Input** option.

The following components are available:

- **Option** is used to select the user input and configure it with some announcement and action to be taken (applicable only for **User Input**). The following input options are available:
  - Digits (from **0** to **9**)
  - Signs (**\*** and **#**)
- **Announcement** is used to upload/record an announcement message for the selected **User Input** option. As soon as the caller presses the preconfigured digit, the message will be played and only then the action configured for that **User Input** option will be activated.
- **Action** is used to configure the action which will be taken after the **Announcement** message.
  - **No Action** – the system continues playing the **Recurring Prompt**.
  - **Go to the following menu** leads to the selected submenu. The drop-down list allows to select a previously created submenu or create a new one by choosing the **Create New Submenu** option.
  - **Call to the following extension** is used to call to the selected extension.
  - **Call to the following number** is used to call to the specified destination via the **Call Routing Table**.
  - **Call to the number dialed** is used to send the user inputs to the **Call Routing Table** (available only for the **Any input other than in the list above** option).
  - **Invoke Extensions Directory** is used to connect the caller to the **Extension Directory**.
  - **Terminate the call** is used to disconnect the call.

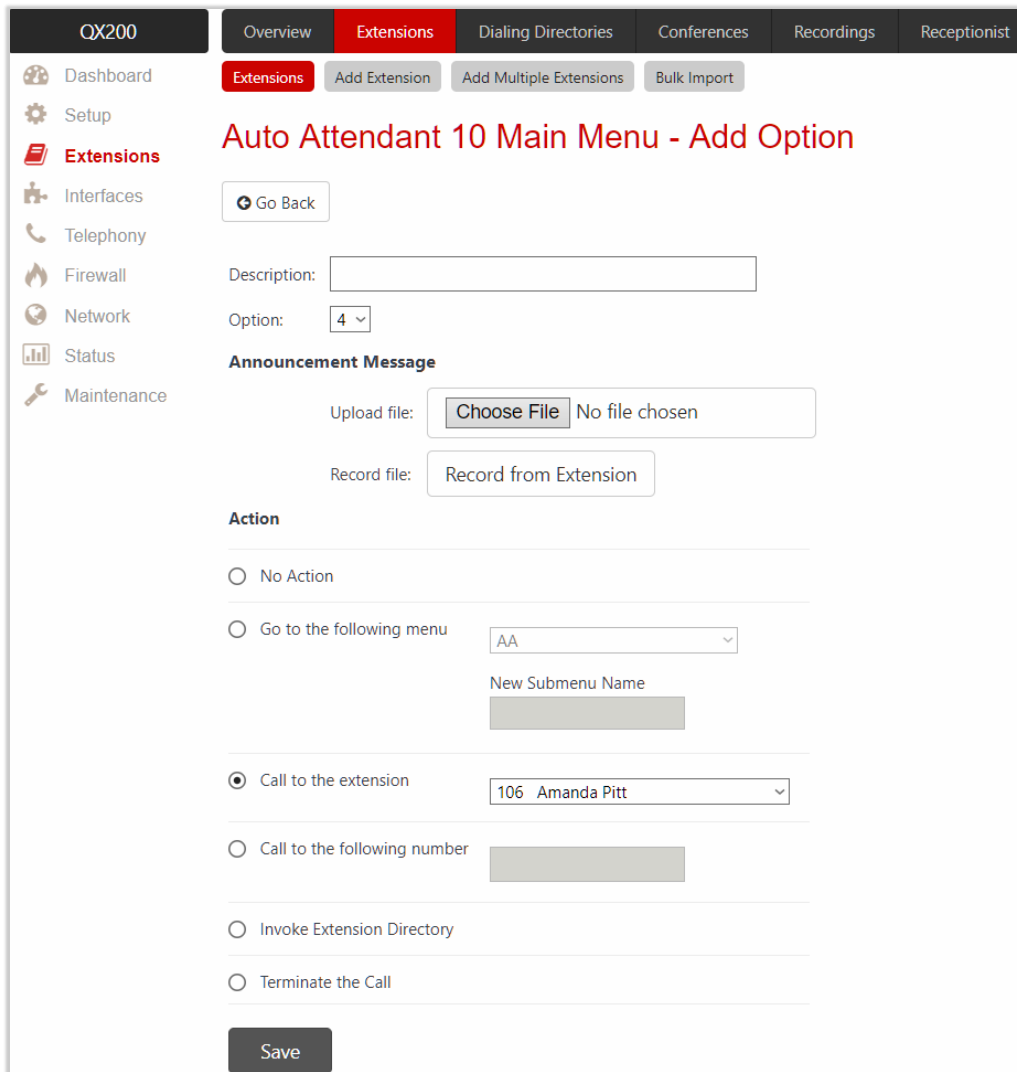


Figure 49: Main Menu – Add Option page

## Submenus

**Submenu** is a supplementary menu accessible from the **Main Menu**. **Submenu** allows to configure multilevel scenarios. **Submenu** consists of the same sections and configuration options as **Main Menu**.

## ACD scenario

**ACD** scenario allows to use a special scenario for **ACD** agents. This scenario allows **ACD** agents to change/update their status by dialing to auto attendant and following voice prompts.

**Note:** This selection is only available if the **ACD** feature is activated.

## Ringling Announcement

The **Ringling Announcement** section is used to play an optional custom message to callers instead of ring-back tones when making calls through the auto attendant. Select the **Enable Ringling Announcement** option to activate service on the auto attendant.

**Note:** Ringing Announcement is played to SIP-to-Extension and PSTN-to-Extension calls only. It can also be played to SIP-Attendant-SIP and PSTN-Attendant-SIP calls if they are made by a call routing rule with the **Use RTP Proxy** option enabled.

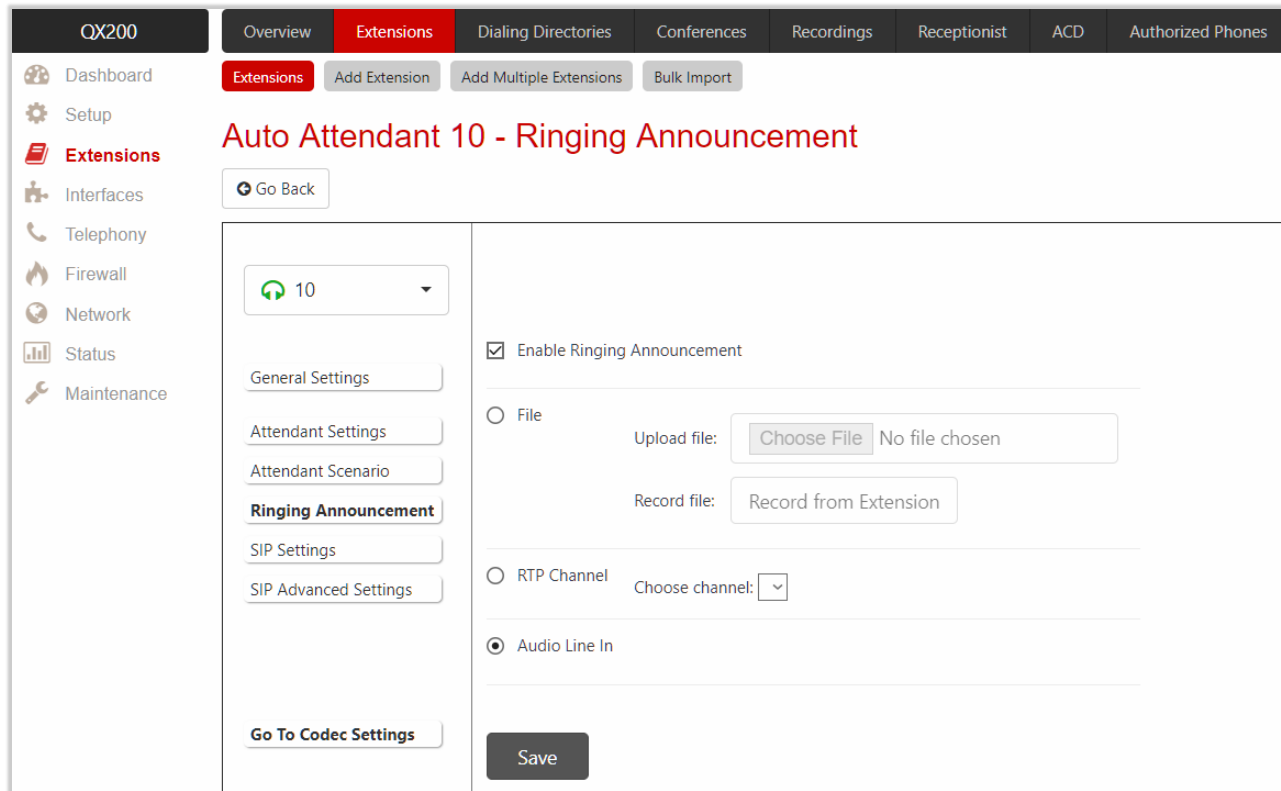


Figure 50: Auto Attendant – Ringing Announcement section

### 6.1.11 Extension Codecs

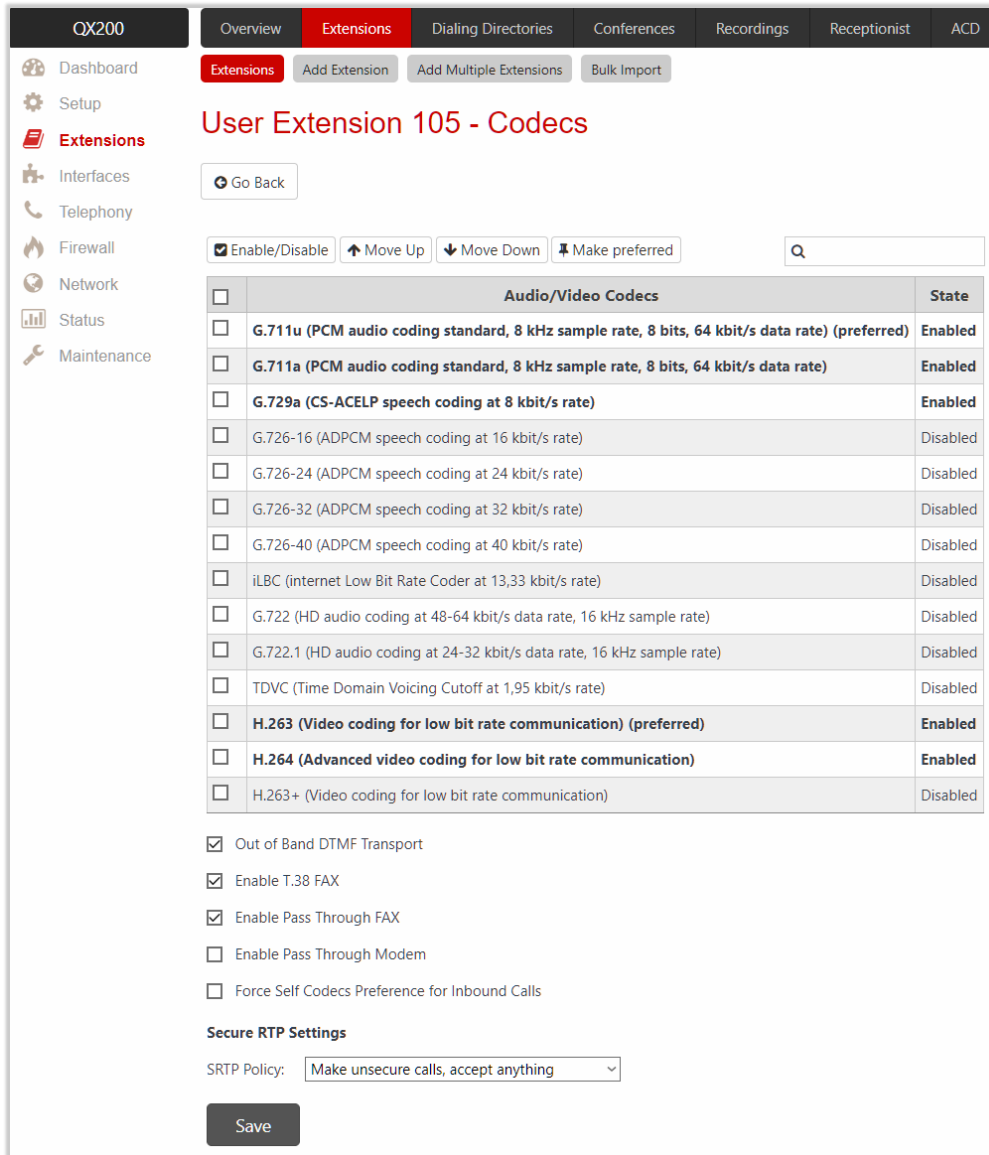
The **Codecs** table lists regular audio and video codecs available for extensions. Checkboxes in the table are used to **enable** or **disable** the selected codec, to **move** it **up** or **down** in the table.

The order of the **enabled codecs** is important. Codec has a higher priority over those located below in the table. **Move Up** moves the selected codec one level up, increasing the codec priority and the **Move Down** moves the selected codec one level down, decreasing its priority.

The codec at the top of the table is used as a **preferred** one. When establishing a call, the system will try this codec first. If the called party does not support the preferred codec, the following codecs will be tried out strictly in the order given in the **Codecs** table. The **Make preferred** button moves the selected codec to the top of the table, setting its priority to the highest. Clicking the **Make preferred** when a disabled codec is selected will first enable that codec, then move it to the top.

**Disabled codec(s)** will never be used for the call setup. At least one codec must be enabled in the table; otherwise communication will be impossible.





The screenshot shows the 'User Extension 105 - Codecs' configuration page. The page has a sidebar on the left with navigation options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The top navigation bar includes Overview, Extensions (active), Dialing Directories, Conferences, Recordings, Receptionist, and ACD. Below the sidebar, there are buttons for 'Add Extension', 'Add Multiple Extensions', and 'Bulk Import'. The main content area is titled 'User Extension 105 - Codecs' and includes a 'Go Back' button, a search bar, and a table of codecs. Below the table are several checkboxes for enabling features like 'Out of Band DTMF Transport', 'Enable T.38 FAX', 'Enable Pass Through FAX', 'Enable Pass Through Modem', and 'Force Self Codecs Preference for Inbound Calls'. There is also a 'Secure RTP Settings' section with a dropdown menu for 'SRTP Policy' set to 'Make insecure calls, accept anything'. A 'Save' button is at the bottom.

<input type="checkbox"/>	Audio/Video Codecs	State
<input type="checkbox"/>	G.711u (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate) (preferred)	Enabled
<input type="checkbox"/>	G.711a (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)	Enabled
<input type="checkbox"/>	G.729a (CS-ACELP speech coding at 8 kbit/s rate)	Enabled
<input type="checkbox"/>	G.726-16 (ADPCM speech coding at 16 kbit/s rate)	Disabled
<input type="checkbox"/>	G.726-24 (ADPCM speech coding at 24 kbit/s rate)	Disabled
<input type="checkbox"/>	G.726-32 (ADPCM speech coding at 32 kbit/s rate)	Disabled
<input type="checkbox"/>	G.726-40 (ADPCM speech coding at 40 kbit/s rate)	Disabled
<input type="checkbox"/>	iLBC (Internet Low Bit Rate Coder at 13,33 kbit/s rate)	Disabled
<input type="checkbox"/>	G.722 (HD audio coding at 48-64 kbit/s data rate, 16 kHz sample rate)	Disabled
<input type="checkbox"/>	G.722.1 (HD audio coding at 24-32 kbit/s data rate, 16 kHz sample rate)	Disabled
<input type="checkbox"/>	TDVC (Time Domain Voicing Cutoff at 1,95 kbit/s rate)	Disabled
<input type="checkbox"/>	H.263 (Video coding for low bit rate communication) (preferred)	Enabled
<input type="checkbox"/>	H.264 (Advanced video coding for low bit rate communication)	Enabled
<input type="checkbox"/>	H.263+ (Video coding for low bit rate communication)	Disabled

Out of Band DTMF Transport  
 Enable T.38 FAX  
 Enable Pass Through FAX  
 Enable Pass Through Modem  
 Force Self Codecs Preference for Inbound Calls

**Secure RTP Settings**  
 SRTP Policy:

Save

Figure 51: Extension Codecs list

The following settings (options) are available:

- Out of Band DTMF Transport** enables the DTMF code transmission in parallel with the voice stream. Destination that received the DTMF code will play it locally if it supports the feature too. This helps to avoid DTMFs loss in case of heavy traffic.
- Enable T.38 FAX** enables the T.38 codec support for the FAX transmission from/to the FAX machine/modem in case if that FAX machine/modem is connected to FXS line attached to target extension. It also enables the T.38 codec support of FAX transmission for incoming unified FAX messages (fax to mailbox) and remote IP devices connected to Epygi device via routing rules which using the target extension user settings.
- Enable Pass Through FAX** enables the G.711 codec support for the FAX transmission from/to the FAX machine/modem in case if that FAX machine/modem is connected to FXS line attached to target extension. It also enables the G.711 codec support for incoming unified FAX messages (fax to mailbox) and IP devices connected to the attached IP line. **TIP:** If both of the above options are enabled, the **T.38 FAX** 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 **Voice Mailbox**. To allow FAX message to be stored in the voice mailbox, the user should not answer the incoming calls, so that they are forwarded to the **Voice Mailbox**. If the **T.38 FAX** and **Pass Through FAX** options are disabled, no FAX transmission to the peer **Voice Mailbox** will be possible.

- **Enable Pass Through Modem** 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, the [Silence Suppression](#) and **Echo Cancellation** are automatically disabled on the line. **TIP:** If the user extension or auto attendant is intended to accept modem connections, disable the **T.38 FAX** option to allow the system to identify the modem tones correctly, otherwise the modem connection may fail.
- **Force Self Codecs Preference for Inbound Calls** enables the usage of your own preferred codecs (if available on both peers).
- **Secure RTP Settings** are used to configure secure VoIP communication on QX. The following options are available:
  - **Make and accept only secure calls** – only secure calls will be generated and accepted.
  - **Make and accept only unsecure calls** – only unsecure calls will be generated and accepted.
  - **Try to establish secure calls, accept anything** – first the system will try to establish a secure call, but will fall back to unsecure call if the party doesn't accept secure calls. Both secure and unsecure incoming calls will be accepted, as requested by the remote party, with the preference given to establishing a secure call.
  - **Make unsecure calls, accept anything** – the system will establish unsecure outgoing calls, but both secure and unsecure incoming calls will be accepted as requested by the remote party.

## 6.1.12 Bulk Import

**Extension Template Management** and **Bulk User Extensions Importer** tools are used to create and update multiple user extensions on QX.

The **Extension Template Management** tool is for configuring common settings for extensions (e.g. SIP Server, SIP Port, etc.), while the **Bulk User Extensions Importer** tool is for configuring specific settings (Display Name, Extension Password, etc).

For more information on how to configure and use **Bulk Import** service, refer to the [Extensions Bulk Import on QX IP PBXs](#) guide.

## 6.2 Dialing Directories

QX provides different services allowing PBX extensions and external callers to dial the desired destinations in a more simplified way. These services are known as **Dialing Directories**:

- **Dial by Name** allows dialing the desired extension by simply spelling the extension's **User name** on the phone keypad.
- **Global Speed Dial** allows dialing the desired destination by using a preconfigured speed dial code (shortcut number).
- **Phone Book** allows to dial the desired contact by using the contact's name from the Local Directory on the phone.

For more information on how to configure and use **Dialing Directories**, refer to the [Dialing Directories on QX IP PBXs](#) guide.

## 6.3 Conferences

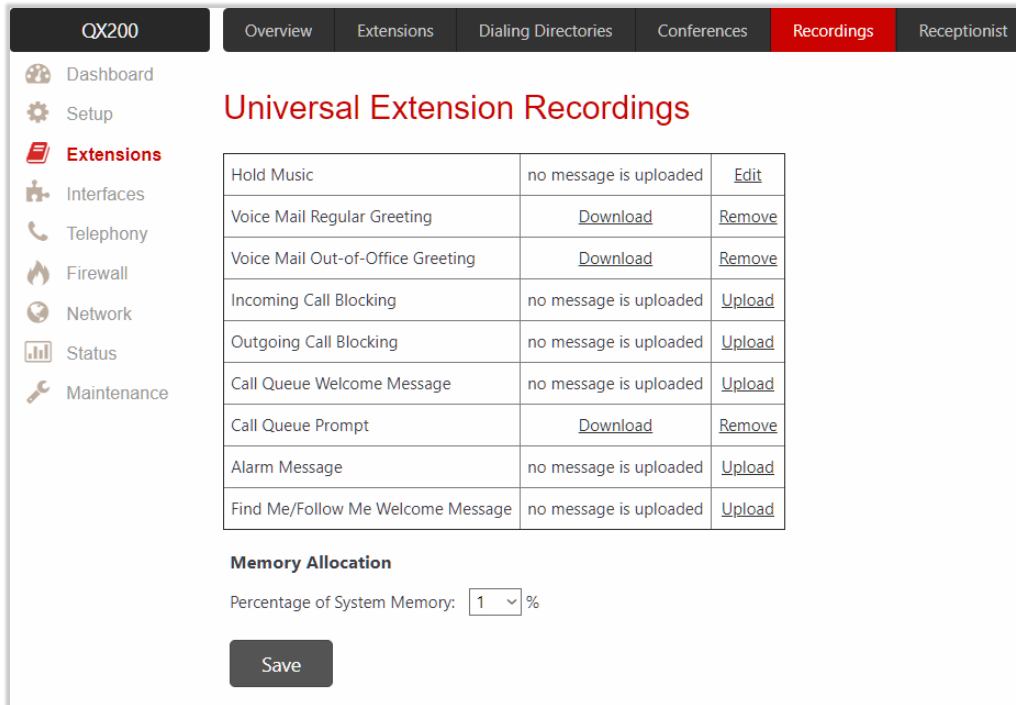
Epygi conferencing is composed of the following two licensable features:

- **Audio conference** feature activated by installing the **Audio Conference** license key.
- **Video conference** feature activated by installing the **Video Conference** license key.

For more information on how to configure and use **Audio-Video conferences**, refer to the [Audio-Video Conferencing on QX IP PBXs](#) guide.

## 6.4 Recordings

**Universal Extension Recordings** is used to define voice messages universal for all user extensions on QX. The defined messages become applicable by default to all extensions, unless no custom messages have been uploaded or recorded.



The screenshot shows the 'Universal Extension Recordings' page in the QX200 administration interface. The page has a navigation menu on the left with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area is titled 'Universal Extension Recordings' and contains a table with the following data:

Hold Music	no message is uploaded	<a href="#">Edit</a>
Voice Mail Regular Greeting	<a href="#">Download</a>	<a href="#">Remove</a>
Voice Mail Out-of-Office Greeting	<a href="#">Download</a>	<a href="#">Remove</a>
Incoming Call Blocking	no message is uploaded	<a href="#">Upload</a>
Outgoing Call Blocking	no message is uploaded	<a href="#">Upload</a>
Call Queue Welcome Message	no message is uploaded	<a href="#">Upload</a>
Call Queue Prompt	<a href="#">Download</a>	<a href="#">Remove</a>
Alarm Message	no message is uploaded	<a href="#">Upload</a>
Find Me/Follow Me Welcome Message	no message is uploaded	<a href="#">Upload</a>

Below the table, there is a 'Memory Allocation' section with a dropdown menu for 'Percentage of System Memory' set to 1% and a 'Save' button.

Figure 52: Universal Extension Recordings page

The following messages are available:

- **Hold Music** – played to the user on hold.
- **Voice Mail Regular Greeting** – played when a caller reaches to the **Voice Mail** of extension.
- **Voice Mail Out-of-Office Greeting** – played when a caller reaches to the **Voice Mail** of extension 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 number.
- **Call Queue Welcome Message** – played when a caller joins the extension call queue.
- **Call Queue Prompt** – played when a caller is being held in the queue.
- **Alarm Message** – played to the user after answering the call.

- **Find Me/Follow Me Welcome Message** – played when a user calls the extension with enabled FM/FM service.

To change the message:

1. Set **Percentage of System Memory** and click **Save** to allocate memory for **Universal Extension Recordings**.
2. Click the **Upload** link next to the message (or **Edit** in case of **Hold Music**).
3. Click **Choose File** to open the file chooser window and browser for the file.
4. Click **Save** to upload the file.

## 6.5 Receptionist

QX **Receptionist** service offers a variety of services to manage multiple calls: answer calls, keep the calls in the queue and forward to users.

For more information on how to configure and use the **Receptionist** service, refer to the [Receptionist Service on QX IP PBXs](#) guide.

## 6.6 ACD

**Automatic Call Distribution** (ACD) feature is a complete solution for today's call centers. ACD is designed to receive and queue high-volume inbound calls, then distribute queued calls to the available agents in a call center.

**Epygi ACD Console** (EAC) is a web application designed to support call center supervisors for monitoring ACD activity and performance on the QX. EAC stores and formats the data and produce real-time information and statistical reports on ACD activity.

**Epygi's Automatic Outbound Calling** (herein **AOC**) is a web application integrated with **ACD**, designed to support **AOC** users for control and monitoring the automatic outbound calling sessions on the QX.

- In order to activate ACD feature the **Automatic Call Distribution** license key should be installed.
- In order to activate EAC feature the **Epygi ACD Console** license key should be installed.
- In order to activate AOC feature the **Epygi Automatic Outbound Calling** license key should be installed.

For more information on how to configure and use **ACD** and **EAC**, refer to the [ACD, EAC and AOC - User Guide](#).

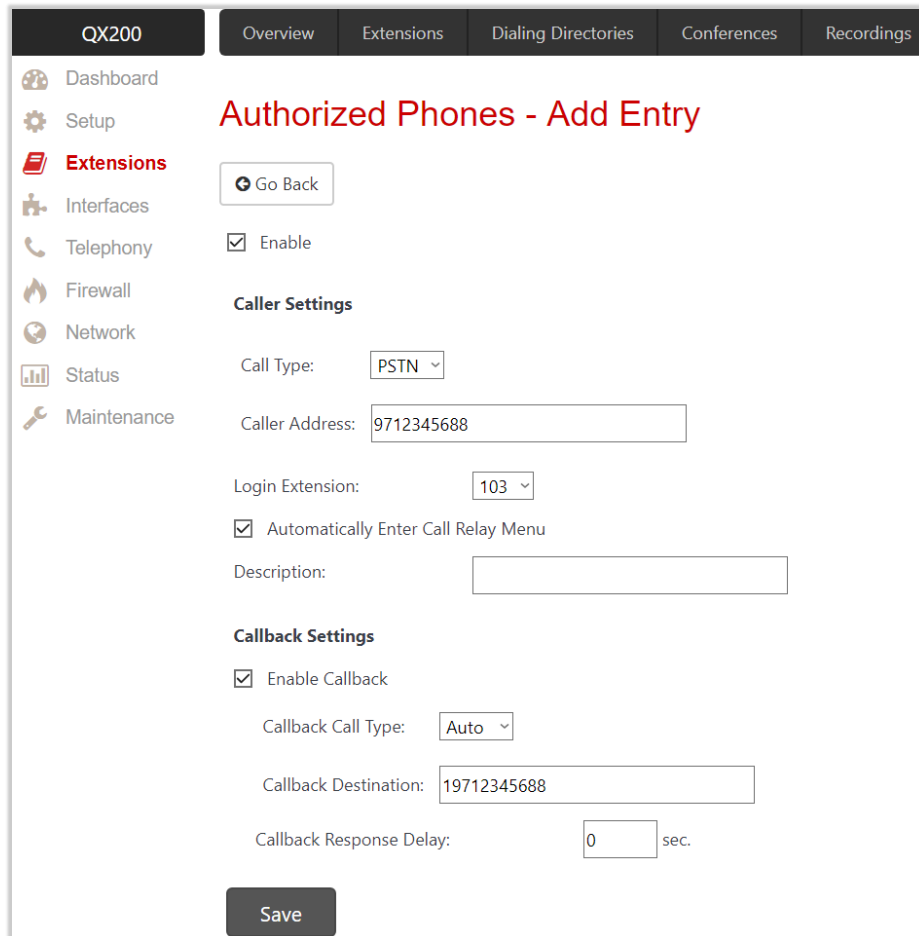
## 6.7 Authorized Phones

**Authorized Phones** is used to create a list of trusted external users allowing them to access QX auto attendant services without authentication.

To add a new entry:

1. Click **Add**. The **Authorized Phones – Add Entry** page will be opened.
2. Tick the **Enable** checkbox to activate service for the created entry.
3. Enter the caller SIP address or PSTN number.

- Select the **Login Extension**. When calling the auto attendant, a trusted user will automatically be logged in as the selected extension (the extension number and password will be automatically submitted by the system and the trusted user will directly access to auto attendant services).



The screenshot shows the 'Authorized Phones - Add Entry' page in the QX200 administration interface. The page has a navigation menu on the left with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area is titled 'Authorized Phones - Add Entry' and includes a 'Go Back' button, an 'Enable' checkbox, and sections for 'Caller Settings' and 'Callback Settings'. The 'Caller Settings' section includes fields for 'Call Type' (set to PSTN), 'Caller Address' (9712345688), and 'Login Extension' (103). There is also a checkbox for 'Automatically Enter Call Relay Menu'. The 'Callback Settings' section includes a checkbox for 'Enable Callback', a 'Callback Call Type' dropdown (set to Auto), a 'Callback Destination' field (19712345688), and a 'Callback Response Delay' field (0 sec). A 'Save' button is located at the bottom of the form.

Figure 53: Authorized Phones – Add Entry page

- Select the **Automatically Enter Call Relay Menu** option. If selected, allows direct access for trusted user to **Call Relay** menu. Otherwise a trusted caller will be only directed to the auto attendant, but still will be able to reach to the **Call Relay** services (by dialing \*2) without authentication.
- Configure **Callback Settings** (optional).
  - Tick **Enable Callback** checkbox to allow a specified caller to use the **Callback** service.
  - Specify the **Callback Destination**. **TIP:** If the **Callback Destination** is left blank, the trusted caller address will be implied as a **Callback** destination.
  - Define **Callback Response Delay** before the **Callback** will be activated.

**How it works:** The trusted user will be able to use QX services after calling the auto attendant, as if a user extension. If the **Callback** service is activated the trusted user will get a call back from auto attendant.

**Note:**

- **Authorized Phones** will only work when the trusted caller connects to the **auto attendant** running the **Standard** scenario.
- For more information on how to configure and use **Callback** service, refer to the [Callback Service on QX IP PBXs](#) guide.

## 7 Interfaces Menu

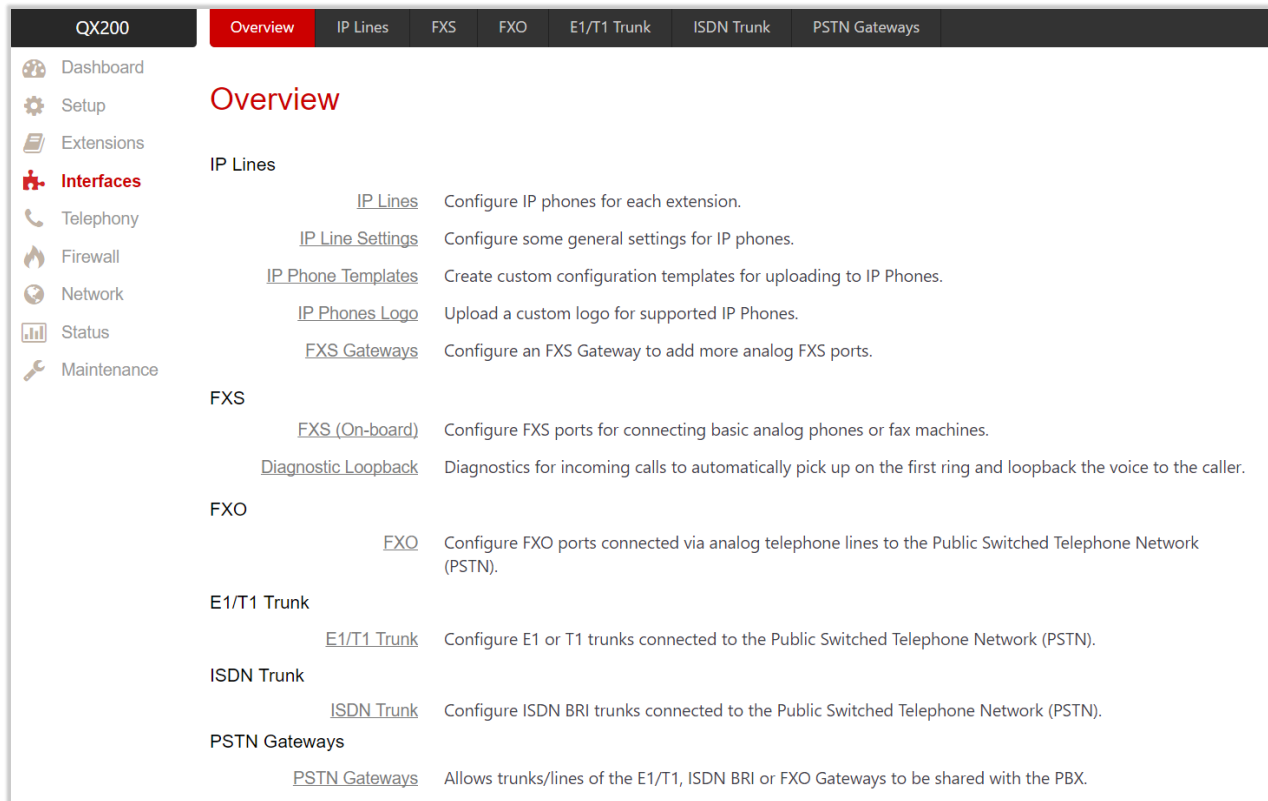


Figure 54: Interfaces Menu overview

### 7.1 IP Lines

The **IP Lines** table lists all IP lines available on QX with specific details for each. The following buttons and parameters are available:

- **Reboot** is used to reboot selected IP phone(s).
- **Deactivate** is used to change the status for selected group(s) of IP lines to **free** (inactive).
- **Show disabled IP lines/Hide disabled IP lines** is used to show or hide the IP lines not activated with a feature key.
- **Enable/Disable OpenVPN** is used to provide configuration file for selected group(s) of IP lines through OpenVPN.

<input type="checkbox"/>	IP Line	Attached Extension	State	Details	Actions
<input type="checkbox"/>	IP Line 1	103	Configured	Username: locext103, Model: Mitel (Aastra) 6739, 00:08:5D:13:BC:15, Template: systemdefault,	MPK Reboot Web
<input type="checkbox"/>	IP Line 2	104	Configured	Username: locext104, Model: Cisco SPA525G2, d0:d0:fd:e9:65:f0, Template: systemdefault,	MPK Reboot Web
<input type="checkbox"/>	IP Line 3	105	Configured	Username: locext105, Model: Panasonic KX-HDV130 (NE/X), bc:c3:42:33:ba:6c, Template: systemdefault,	MPK Reboot Web
<input type="checkbox"/>	IP Line 4	106	Configured	Username: locext106, Model: Polycom VVX 300/310, 00:04:f2:81:3e:ef, Template: systemdefault,	MPK Reboot Web
<input type="checkbox"/>	IP Line 5	107	Configured	Username: locext107, Model: Panasonic KX-UT136 (NE/RU/X), 00:80:F0:C8:d1:42, Template: systemdefault	MPK
<input type="checkbox"/>	IP Line 6	108	Configured	Username: locext108, Model: Panasonic KX-UT123 (NE/RU/X), 00:80:f0:dc:4e:47, Template: systemdefault	
<input type="checkbox"/>	IP Line 7	109	Configured	Username: locext109, Model: Grandstream GXP2200, 00:0b:82:46:f7:bb, Template: systemdefault	MPK
<input type="checkbox"/>	IP Line 8	110	Configured	Username: locext110, Model: Snom 760, 00:04:13:71:00:AE, Template: systemdefault, OpenVPN: Off	MPK
<input type="checkbox"/>	IP Line 9	111	Configured	Username: locext111, Model: Other	
<input type="checkbox"/>	IP Line 10	112	Configured	Username: locext112, Model: Snom D345, 00:04:13:85:14:F7, Template: systemdefault, OpenVPN: Off,	MPK Reboot Web
<input type="checkbox"/>	IP Line 11	113	Configured	Username: locext113, Model: Snom D715/715, 00:04:13:75:6F:4B, Template: systemdefault, OpenVPN: Off	MPK
<input type="checkbox"/>	IP Line 12	114	Configured	Username: locext114, Model: Snom 821, 00:04:13:45:32:AF, Template: systemdefault, OpenVPN: Off	MPK
<input type="checkbox"/>	IP Line 13	115	Configured	Username: locext115, Model: Auvovox SP-R53(P), 45:45:45:45:45:45, Template: systemdefault	MPK
<input type="checkbox"/>	IP Line 14	116	Configured	Username: locext116, Model: Polycom VVX 400/410, 00:04:f2:8d:5b:fe, Template: systemdefault	MPK
<input type="checkbox"/>	IP Line 15	117	Free		
<input type="checkbox"/>	IP Line 16	118	Free		
<input type="checkbox"/>	IP Line 17	119	Free		
<input type="checkbox"/>	IP Line 18	120	Free		

Figure 55: IP Lines page

- **IP Line** shows all IP lines available on QX. Click on **IP Line** to go the [IP Line Settings - IP Line](#) page.
- **Attached Extension** shows the user extension attached to the IP line. **TIP: None** is displayed if there is no extension attached to that line.
  - Click the **Admin Settings** icon to go to the extension **admin** settings.
  - Click the **User Settings** icon to go to the extension **user** settings.
- **State** shows whether the IP line is **Disabled**, **Configured** or **Free**.
- **Details** shows the settings for the IP phone configured on the corresponding line, such as the phone model, MAC address, attached IP phone template and the authorization credentials.
- **Actions** – the following actions are available to manage the IP phone:
  - **MPK** leads to the [Multi-functional Programmable Keys](#) page of the phone.
  - **Reboot** is used to reboot the IP phone.
  - **Restart** is used to restart FXS Gateway (QXFXS24 or QuadroM FXS26) attached to the line.
  - **Web** leads to the WEB GUI of the IP phone. **TIP:** This link only works from the LAN side of the QX, i.e. when the WEB GUI is accessed from a PC located in the LAN of QX. If you wish to access the WEB GUI of the IP phone through WAN, an appropriate [Incoming Traffic/Port Forwarding](#) filtering rule should be added on QX.

## IP Line Settings – IP Line #

The **IP Line Settings – IP Line #** page is used to configure IP phone with QX. The following settings (options) are available:

- **Inactive** – if selected, changes the IP line state from **Configured** to **Free**.
- **IP Phone** – if selected, activates the IP line to configure with the IP phone as follows:

- **Phone Model** is used to select the IP phone model. Select **Other** if the phone model is not listed or the phone should be configured as a [Remote Extension](#).
- **MAC Address** is used to set the MAC Address of the phone.
- **Line Appearance** is used to set the number for intended simultaneous calls (the total number of active and held calls).
- **Username** and **Password** are used to set the authentication parameters to register the IP phone on QX. By default, QX assigns unique username and password to each IP line. You may either keep these values or specify new ones. **TIP:** The **Username** and **Password** should match on both QX and IP phone for the successful registration.
- **Transport** is used to select the transport protocol for SIP messages – **UDP**, **TCP** or **TLS**. For **TLS**, you may activate the [TLS Certificates](#) update mechanism from an IP phone to obtain the latest certificate generated by the QX.
- **Use Template** is used to select a preconfigured custom template for the IP phone. When the **Use default** option is selected, the template selected on the [IP Line Settings](#) page will be used.
- **Use Session Timer** enables the SIP session timer for the IP line. This option allows both user agents and proxies to check and determine if the SIP session is still active.
- **Symmetric RTP** must be selected when the IP phone attached to the IP line is located behind the NAT router.
- **Use OpenVPN Settings** is used to select this option to auto configure phone using the OpenVPN settings. The OpenVPN service for auto configuration is available on majority of **Epygi Supported IP phones**.
- **OpenVPN client configuration** is used to select and download OpenVPN client configuration file for the IP phone attached to the IP line. **TIP:** This option is **NOT** used to apply the OpenVPN configuration on the phone.

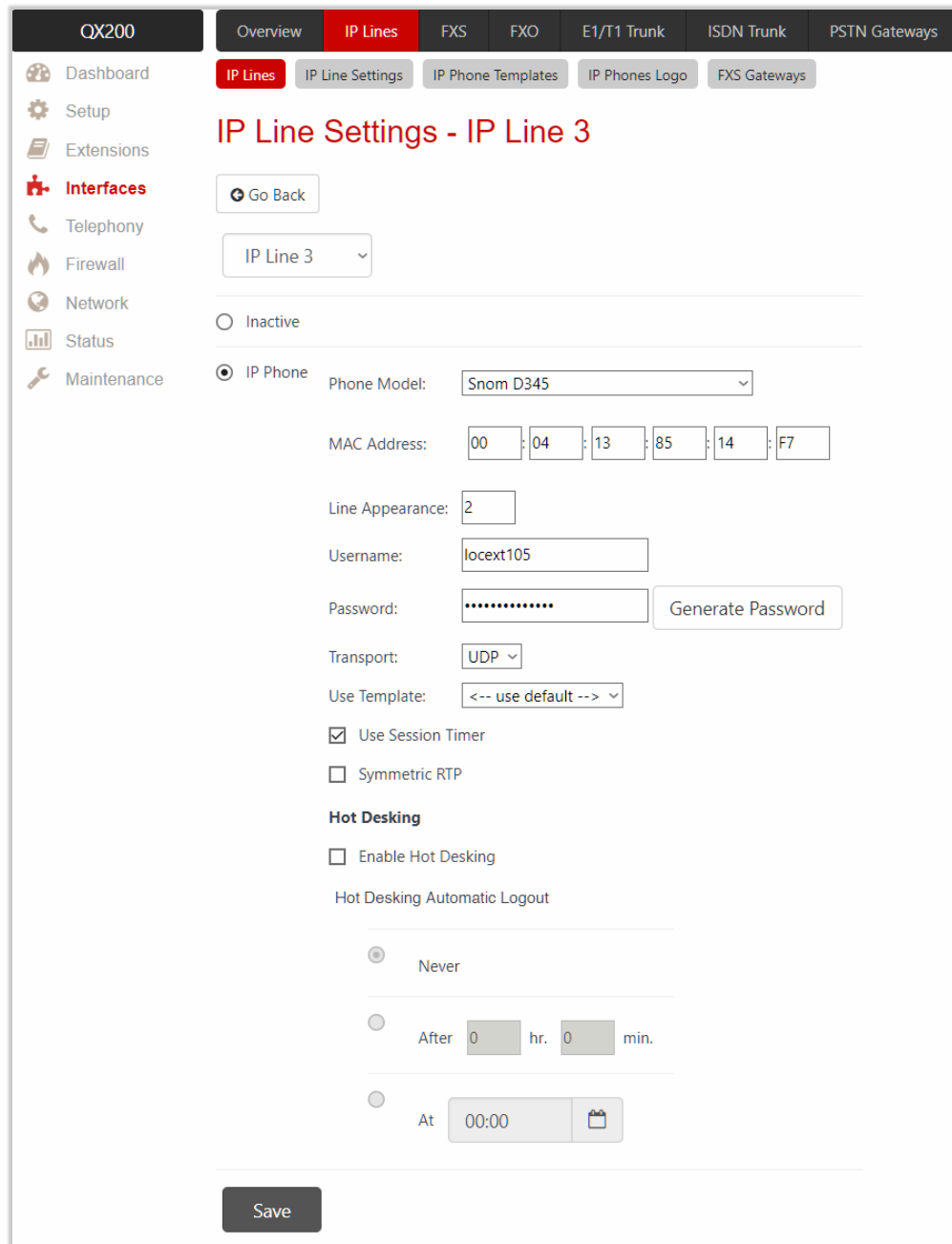
## Hot Desking

If QX has limited number of IP phones connected, but much more users wishing to make and receive calls through QX, some of the connected phones can be announced as "public". "Public" phones have no static owners; they are just connected to the IP lines. Each user that accesses the "public" phone should login using personal credentials (extension number and password).

The **Hot Desking** section is used to enable and configure the **Hot Desking** service on the IP line. The following settings (options) are available:

- **Enable Hot Desking** is used to activate service on the IP line.
- **Hot Desking Automatic Logout** is used to configure the **Hot Desking** service expiration on the current extension. The following options are available:
  - **Never** – the service will never expire and the extension will remain logged into the "public" phone.
  - **After** – the extension will automatically get logged out from the "public" phone after a specified period of time.
  - **At** – the extension will automatically get logged out from the "public" phone at the specified moment (hour and minute).





The screenshot displays the 'IP Line Settings - IP Line 3' configuration page. The interface includes a top navigation bar with tabs for Overview, IP Lines (selected), FXS, FXO, E1/T1 Trunk, ISDN Trunk, and PSTN Gateways. A left sidebar contains navigation options like Dashboard, Setup, Extensions, Interfaces (highlighted), Telephony, Firewall, Network, Status, and Maintenance. The main content area features a 'Go Back' button, a dropdown menu for 'IP Line 3', and radio buttons for 'Inactive' and 'IP Phone' (selected). Under 'IP Phone', settings include: Phone Model (Snom D345), MAC Address (00:04:13:85:14:F7), Line Appearance (2), Username (locext105), Password (masked with dots), Transport (UDP), and Use Template (<-- use default -->). There are checkboxes for 'Use Session Timer' (checked) and 'Symmetric RTP'. The 'Hot Desking' section has an 'Enable Hot Desking' checkbox (unchecked) and a 'Hot Desking Automatic Logout' section with three radio button options: 'Never' (selected), 'After 0 hr. 0 min.', and 'At 00:00'. A 'Save' button is located at the bottom.

Figure 56: IP Line Settings – Edit page

For more information on how to configure and use **Hot Desking** service, refer to the [Hot Desking Service on QX IP PBXs](#) guide.

### Multi-functional Programmable Keys

The **Multi-functional Programmable Keys** page is used to assign functions to the programmable keys of the IP phone. The design of this page depends on the IP phone model. However, regardless of the IP phone model, this page contains a number of programmable keys and a **Function** list assigned to each of them.

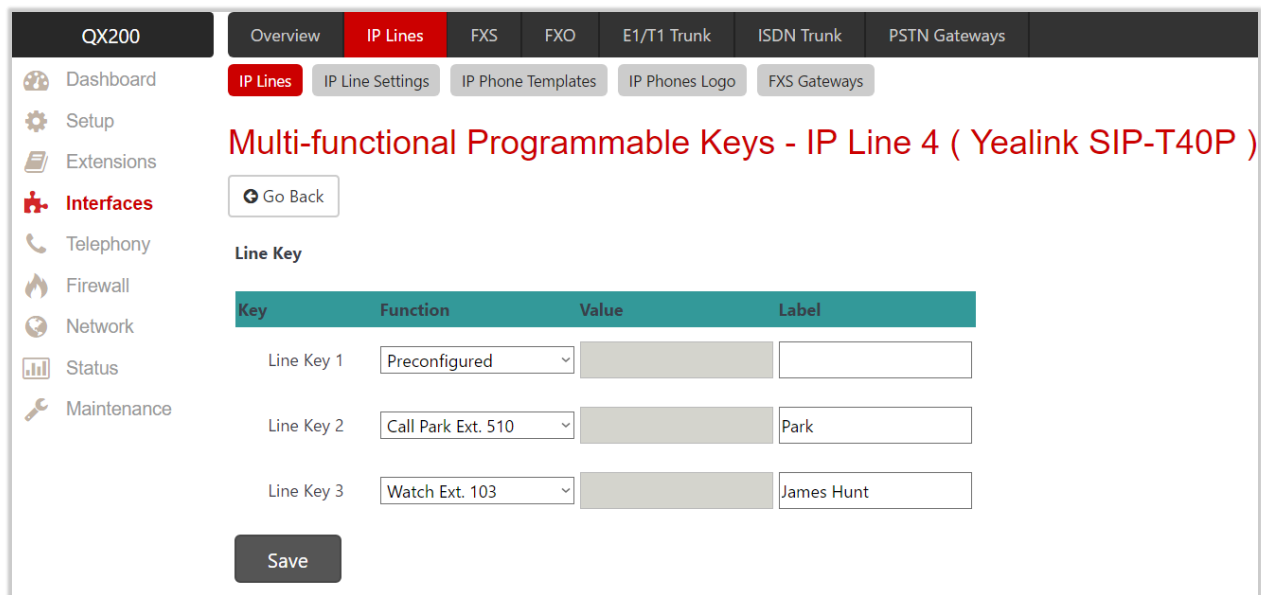


Figure 57: Programmable Keys Configuration page

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

- **Preconfigured** will not change anything for the key functionality. In fact, it will keep the previously configured function for that key.
- **None** eliminates any functionality for the key. In fact, it disables the key.
- **IP Line** allows to assign a key to the corresponding IP line. Press the key to get dial tone. The key will flash when a call is ringing to that line. The key illuminates green when the IP line is busy with another call. **TIP:** Based on the phone model, the status of the BLF key and the status of the IP Line will vary.
- **Watch Ext. #** allows to watch the extension and intercept calls addressed to that extension.
- **Call Park Ext. #** allows to watch the parked calls on the corresponding **Call Park** extension and retrieve the parked calls.
- **Shared Vmail Ext. #** allows to watch and access to the [Shared Voice Mailbox](#).
- **Schedule #** allows to watch and update the state for a specific [schedule](#).
- **Vmail** allows to access to the voice mailbox of the extension.
- **DND** allows to activate/deactivate the **Do Not Disturb** service on the extension.
- **CallFwd** allows to configure/toggle (activate/deactivate) **Unconditional Call Forwarding** on the extension.
- **AutoReDI** automatically redials the last dialed number.
- **CallBack** calls back to the last caller.
- **LineInfo** plays information about the IP line.
- **CallBlk** blocks the last caller.
- **Record** allows to start the call recording (in case if the **Manual** mode for call recording is configured in the [Call Recording Settings](#)).
- **ACD Login/Logout** allows to login/logout the corresponding **ACD agent** to/from all queues he/she is involved in.
- **LDAP** allows to retrieve contacts from 3-rd party LDAP server.
- **URL** is basically HTTP GET Requests (often XML over HTTP) that allow the phone to interact with web server applications. It can be used to retrieve various data from the web server.

**Note:** The system will ask a conformation to remotely reboot the IP phone to save changes. It is recommended to reboot the IP phone after configuration changes on this page to make the new configuration effective on the IP phone.

### Supported IP Phones

Below is the list of IP phones that are officially supported by Epygi and can be configured with QX using **Plug and Play (PnP)** or **Auto Configuration** services.

Vendor	Model	SW/FW Version	PnP		Auto Configuration
			PnP (Multicast)	Assisted PnP (DHCP options 66/67)	
Akuvox	R15(P)	15.0.5.235	Yes	Yes	Yes
Akuvox	SP-R53(P)	53.0.6.115	Yes	Yes	Yes
Alcatel	IP2015 (IP15)	1.0.7A-0	No	No	Yes
Alcatel	Temporis IP100	1.0.6A-0	No	No	Yes
Alcatel	Temporis IP150	1.0.6A-0	No	No	Yes
Alcatel	Temporis IP200	13.60.0.89	Yes	Yes	Yes
Alcatel	Temporis IP300	1.0.7B-0	No	No	Yes
Alcatel	Temporis IP600	14.60.0.89	Yes	Yes	Yes
Alcatel	Temporis IP700G	1.0.7A-0	No	No	Yes
Alcatel	Temporis IP800	15.60.0.89	Yes	Yes	Yes
Alcatel	Lucent - 8058S	1.51.07	Yes	No	Yes
AudioCodes	310HD	1.6.0_build_37	No	No	Yes
AudioCodes	320HD	1.6.0_build_37	No	No	Yes
Cisco	CP-6851	11-1-1	No	No	Yes
Cisco	CP-7861	11-1-1	No	No	Yes
Cisco	CP-8851	11-1-1	No	No	Yes
Cisco	SPA303	7.4.9c	No	Yes	Yes
Cisco	SPA501G	7.4.9c	No	Yes	Yes
Cisco	SPA508G	7.5.2	No	Yes	Yes
Cisco	SPA509G	7.4.9c	No	Yes	Yes
Cisco	SPA525G2	7.4.9c	No	Yes	Yes
Fanvil	C58/C58P	2.3.233.129	No	No	Yes
Fanvil	C62/C62P	2.5.787.97	No	No	Yes
Fanvil	C400	14.0.0.3.r1	No	No	Yes
Fanvil	C600	14.0.0.3.r1	No	No	Yes
Fanvil	F52/F52P	2.3.123.78	Yes	Yes	Yes
Fanvil	H2/H2S	2.8.0.6251	Yes	Yes	Yes
Fanvil	H3	2.8.0.6251	Yes	Yes	Yes
Fanvil	H5	2.8.0.6251	Yes	Yes	Yes
Fanvil	X3/X3P	1.4.0.2016	Yes	Yes	Yes
Fanvil	X3S/X3G	2.8.0.6251	Yes	Yes	Yes
Fanvil	X4/X4G/X4S	2.8.0.6251	Yes	Yes	Yes
Fanvil	X5/X5G	1.4.0.2016	Yes	Yes	Yes
Fanvil	X5S	1.8.0	Yes	Yes	Yes
Fanvil	X6	1.8.0	Yes	Yes	Yes

Vendor	Model	SW/FW Version	PnP		Auto Configuration
			PnP (Multicast)	Assisted PnP (DHCP options 66/67)	
Gigaset	Maxwell 3 PRO	82.2.22.7	Yes	Yes	Yes
Gigaset	N720 DM PRO	70.113.00.000.000	No	No	Yes
Grandstream	GXP1100	1.0.8.6	No	Yes	Yes
Grandstream	GXP1105	1.0.8.6	No	Yes	Yes
Grandstream	GXP1160	1.0.8.6	No	Yes	Yes
Grandstream	GXP1165	1.0.8.6	No	Yes	Yes
Grandstream	GXP1400	1.0.8.6	No	Yes	Yes
Grandstream	GXP1405	1.0.8.6	No	Yes	Yes
Grandstream	GXP1450	1.0.8.6	No	Yes	Yes
Grandstream	GXP1615/1610	1.0.4.55	No	Yes	Yes
Grandstream	GXP1625/1620	1.0.4.55	No	Yes	Yes
Grandstream	GXP1628	1.0.4.55	No	Yes	Yes
Grandstream	GXP1630	1.0.4.55	No	Yes	Yes
Grandstream	GXP1760	1.0.0.48	No	No	Yes
Grandstream	GXP1782/1780	1.0.0.48	No	No	Yes
Grandstream	GXP2100	1.0.8.6	No	Yes	Yes
Grandstream	GXP2110	1.0.8.6	No	Yes	Yes
Grandstream	GXP2120	1.0.8.6	No	Yes	Yes
Grandstream	GXP2124	1.0.8.6	No	Yes	Yes
Grandstream	GXP2130	1.0.7.99	No	Yes	Yes
Grandstream	GXP2135	1.0.7.99	No	Yes	Yes
Grandstream	GXP2140	1.0.7.99	No	Yes	Yes
Grandstream	GXP2160	1.0.7.99	No	Yes	Yes
Grandstream	GXP2170	1.0.7.99	No	Yes	Yes
Grandstream	GXP2200	1.0.3.27	No	Yes	Yes
Grandstream	GXV3140	1.0.7.80	No	Yes	Yes
Grandstream	GXV3175	1.0.3.76	No	Yes	Yes
Grandstream	GXV3240	1.0.3.62	No	Yes	Yes
Grandstream	GXV3275	1.0.3.62	No	Yes	Yes
Htek	UC902	2.0.4.4.41	Yes	Yes	Yes
Htek	UC903	2.0.4.4.41	Yes	Yes	Yes
Htek	UC912E	2.0.4.4.41	Yes	Yes	Yes
Htek	UC912G	2.0.4.4.41	Yes	Yes	Yes
Htek	UC912P	2.0.4.4.41	Yes	Yes	Yes
Htek	UC923	2.0.4.4.41	Yes	Yes	Yes
Htek	UC924	2.0.4.4.41	Yes	Yes	Yes
Htek	UC924E	2.0.4.4.41	Yes	Yes	Yes
Htek	UC926	2.0.4.4.41	Yes	Yes	Yes
Htek	UC926E	2.0.4.4.41	Yes	Yes	Yes
iServ	8660 (8430/8630/8830)	03.55.0025	No	No	Yes
iServ	Escene ES282-PC	V1.1.0.10143324	No	No	Yes
iServ	U3S	V1.1.0.10143813	No	No	Yes
iServ	U6S	V1.1.0.10143813	No	No	Yes

Vendor	Model	SW/FW Version	PnP		Auto Configuration
			PnP (Multicast)	Assisted PnP (DHCP options 66/67)	
Mitel (Aastra)	6730	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	6731	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	6735	3.3.1.8140-SIP	Yes	Yes	Yes
Mitel (Aastra)	6737	3.3.1.8140-SIP	Yes	Yes	Yes
Mitel (Aastra)	6739	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	6753	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	6755	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	6757	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	9143	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel (Aastra)	9480	3.3.1.4305-SIP	Yes	Yes	Yes
Mitel	6863	4.2.0.2023-SIP	Yes	Yes	Yes
Mitel	6865	4.2.0.2023-SIP	Yes	Yes	Yes
Mitel	6867	4.2.0.2023-SIP	Yes	Yes	Yes
Mitel	6869	4.2.0.2023-SIP	Yes	Yes	Yes
Panasonic	KX-HDV130	03.004	Yes	Yes	Yes
Panasonic	KX-HDV130NE, KX-HDV130X	06.101	Yes	Yes	Yes
Panasonic	KX-HDV230	03.004	Yes	Yes	Yes
Panasonic	KX-HDV230NE, KX-HDV230X	06.101	Yes	Yes	Yes
Panasonic	KX-TGP550T04	12.17	No	No	Yes
Panasonic	KX-UT123 (NE/RU/X)	01.302	No	No	Yes
Panasonic	KX-UT136 (NE/RU/X)	01.302	No	No	Yes
Polycom	SoundPoint IP 330	3.3.5.0247	No	Yes	Yes
Polycom	SoundPoint IP 331	4.0.13.1445	No	Yes	Yes
Polycom	SoundPoint IP 335	4.0.13.1445	No	Yes	Yes
Polycom	SoundPoint IP 450	4.0.13.1445	No	Yes	Yes
Polycom	SoundPoint IP 550	4.0.13.1445	No	Yes	Yes
Polycom	SoundPoint IP 650	4.0.13.1445	No	Yes	Yes
Polycom	SoundPoint IP 670	4.0.13.1445	No	Yes	Yes
Polycom	SoundStation IP 5000	4.0.13.1445	No	Yes	Yes
Polycom	SoundStation IP 6000	4.0.13.1445	No	Yes	Yes
Polycom	VX 150	6.1.1.2670	No	No	Yes
Polycom	VX 250	6.1.1.2670	No	No	Yes
Polycom	VX 300/310	5.7.0.14430	No	Yes	Yes
Polycom	VX 301/311	5.7.0.14430	No	No	Yes
Polycom	VX 350	6.1.1.2670	No	No	Yes
Polycom	VX 400/410	5.7.0.14430	No	No	Yes
Polycom	VX 401/411	5.7.0.14430	No	No	Yes
Polycom	VX 450	6.1.1.2670	No	No	Yes
Polycom	VX 500/501	5.7.0.14430	No	No	Yes
Polycom	VX 600/601	5.7.0.14430	No	Yes	Yes
Polycom	VX 1500	5.7.0.14430	No	Yes	Yes

Vendor	Model	SW/FW Version	PnP		Auto Configuration
			PnP (Multicast)	Assisted PnP (DHCP options 66/67)	
QOSIP	Q7104/Q7204	1.0.3.98	No	No	Yes
snom	300	8.4.35	Yes	Yes	Yes
snom	320	8.4.35	Yes	Yes	Yes
snom	360	8.4.35	Yes	Yes	Yes
snom	370	8.7.5.35	Yes	Yes	Yes
snom	720	8.9.3.60	Yes	Yes	Yes
snom	760	8.9.3.60	Yes	Yes	Yes
snom	821	8.7.5.35	Yes	Yes	Yes
snom	870	8.7.5.35	Yes	Yes	Yes
snom	D120	10.1.10.1	Yes	Yes	Yes
snom	D345	8.9.3.60	Yes	Yes	Yes
snom	D375	8.9.3.60	Yes	Yes	Yes
snom	D710/710	8.9.3.60	Yes	Yes	Yes
snom	D712	8.9.3.60	Yes	Yes	Yes
snom	D715/715	8.9.3.60	Yes	Yes	Yes
snom	D717	10.1.33.1	Yes	Yes	Yes
snom	D725	8.9.3.60	Yes	Yes	Yes
snom	D735	10.1.39.11	Yes	Yes	Yes
snom	D745	8.9.3.60	Yes	Yes	Yes
snom	D765	8.9.3.60	Yes	Yes	Yes
snom	D785	10.1.20.0	Yes	Yes	Yes
snom	M700 (M85/M65/M25)	03.24.0007	Yes	Yes	Yes
snom	m9	9.4.7	Yes	Yes	Yes
snom	MeetingPoint	8.7.5.35	Yes	Yes	Yes
Spectralink	KIRK Wireless Server 300	PCS14C_	No	No	Yes
Spectralink	KIRK Wireless Server 6000	PCS14C_	No	No	Yes
VTech	ErisStation VCS754	1.1.4.0-0	No	No	Yes
VTech	ErisTerminal VSP600 (VSP601)	1.1.4.1-0	No	No	Yes
VTech	ErisTerminal VSP715	1.1.4.0-0	No	No	Yes
VTech	ErisTerminal VSP725	1.1.4.0-0	No	No	Yes
VTech	ErisTerminal VSP726	2.0.3.2-0	Yes	Yes	Yes
VTech	ErisTerminal VSP735	1.1.4.0-0	No	No	Yes
VTech	ErisTerminal VSP736	2.0.3.2-0	Yes	Yes	Yes
Yealink	CP860	37.81.0.10	Yes	Yes	Yes
Yealink	CP920	78.84.0.15	Yes	Yes	Yes
Yealink	CP960	73.83.0.30	Yes	Yes	Yes
Yealink	SIP-T19P	31.72.0.1	Yes	Yes	Yes
Yealink	SIP-T19P E2	53.83.0.50	Yes	Yes	Yes
Yealink	SIP-T20P	9.72.0.1	Yes	Yes	Yes
Yealink	SIP-T21P	34.72.0.1	Yes	Yes	Yes
Yealink	SIP-T21P E2	52.83.0.50	Yes	Yes	Yes

Vendor	Model	SW/FW Version	PnP		Auto Configuration
			PnP (Multicast)	Assisted PnP (DHCP options 66/67)	
Yealink	SIP-T22P	7.72.0.1	Yes	Yes	Yes
Yealink	SIP-T23G(P)	44.83.0.50	Yes	Yes	Yes
Yealink	SIP-T26P	6.72.0.1	Yes	Yes	Yes
Yealink	SIP-T27G	69.83.0.50	Yes	Yes	Yes
Yealink	SIP-T27P	45.83.0.50	Yes	Yes	Yes
Yealink	SIP-T28P	2.72.0.1	Yes	Yes	Yes
Yealink	SIP-T29G	46.83.0.50	Yes	Yes	Yes
Yealink	SIP-T32G	32.70.0.130	Yes	Yes	Yes
Yealink	SIP-T38G	38.70.0.125	Yes	Yes	Yes
Yealink	SIP-T40G	76.83.0.50	Yes	Yes	Yes
Yealink	SIP-T40P	54.83.0.50	Yes	Yes	Yes
Yealink	SIP-T41P	36.83.0.50	Yes	Yes	Yes
Yealink	SIP-T41S	66.83.0.50	Yes	Yes	Yes
Yealink	SIP-T42G	29.83.0.50	Yes	Yes	Yes
Yealink	SIP-T42S	66.83.0.50	Yes	Yes	Yes
Yealink	SIP-T46G	28.83.0.50	Yes	Yes	Yes
Yealink	SIP-T46S	66.83.0.50	Yes	Yes	Yes
Yealink	SIP-T48G	35.83.0.50	Yes	Yes	Yes
Yealink	SIP-T48S	66.83.0.50	Yes	Yes	Yes
Yealink	SIP VP-T49G	51.80.0.100	Yes	Yes	Yes
Yealink	SIP-T52S	70.83.0.50	Yes	Yes	Yes
Yealink	SIP-T53/53W	95.84.0.30	Yes	Yes	Yes
Yealink	SIP-T54S	70.83.0.50	Yes	Yes	Yes
Yealink	SIP-T54W	96.84.0.30	Yes	Yes	Yes
Yealink	SIP-T56A	58.83.0.15	Yes	Yes	Yes
Yealink	SIP-T57W	97.84.0.30	Yes	Yes	Yes
Yealink	SIP-T58A/V	58.83.0.15	Yes	Yes	Yes
Yealink	VP-530	23.70.0.40	Yes	Yes	Yes
Yealink	W52P	25.30.0.20	Yes	Yes	Yes
Yealink	W60B	77.83.0.25	Yes	Yes	Yes

Table 1: Supported IP Phones

## 7.1.2 IP Line Settings

IP Line Settings is used to control the basic settings for configuring IP phones.

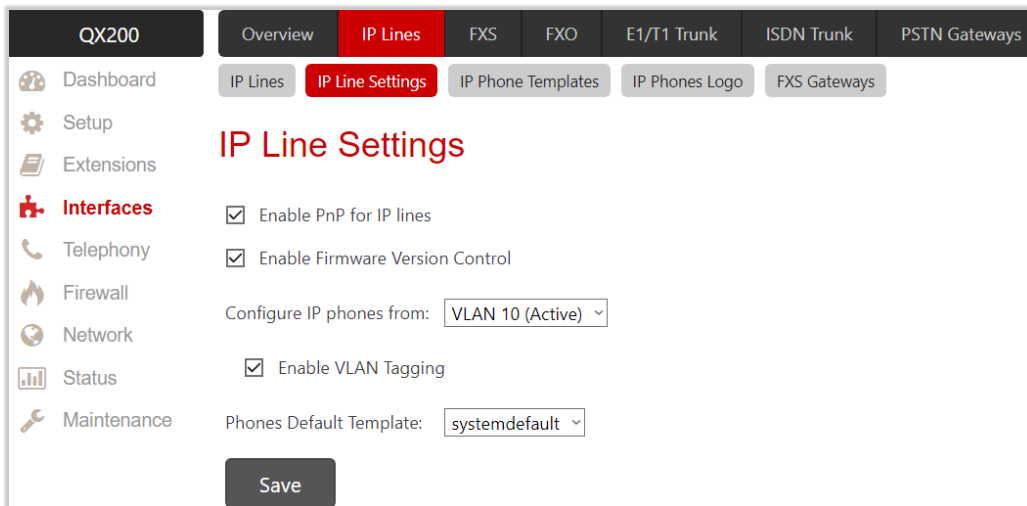


Figure 58: IP Line Settings page

The following settings (options) are available:

- **Enable PnP for IP lines** activates the PnP option on QX. The PnP allows [Epygi supported IP phones](#) to be automatically configured without any manual intervention in the QX and phone settings. If selected, connect the phone to the QX and factory reset the phone. After a clean boot-up of the phone, QX will detect the phone settings, automatically generate the specific configuration file of the phone and upload it. The phone will be then configured on the first **Free** IP line.
- **Enable Firmware Version Control** is used to control and manage the firmware version running on the IP phone. This service will allow to replace the firmware running on the phone (upgrade or downgrade) with the recommended one. **Note:** Currently the **Firmware Version Control** service is applicable for Mitel, Mitel (Aastra), snom and Yealink phones.
- **Configure IP phones from** is used to select the network interface on QX, where the IP phones should be connected to. Besides LAN and WAN (LAN1 for QX2000/QX3000), this list also includes the VLAN interface if available.
  - **Enable VLAN Tagging** is used to set the VLAN ID and priority for IP phones. **TIP:** The provided IP address will always be from VLAN network. This option is enabled by default.
- **Phones Default Template** is used to select the [IP phone template](#) that will be used as default for IP lines.



### 7.1.3 IP Phone Templates

The **Manage IP Phone Templates** page is used to create custom templates for IP phones. The templates contain a set of configuration settings that are applied to the IP phone once it is registered on QX. With the custom templates, the most popular configuration settings may be adjusted accordingly. The saved custom templates can be then configured from the [IP Line Settings – IP Line #](#) page to be used on a particular IP phone.

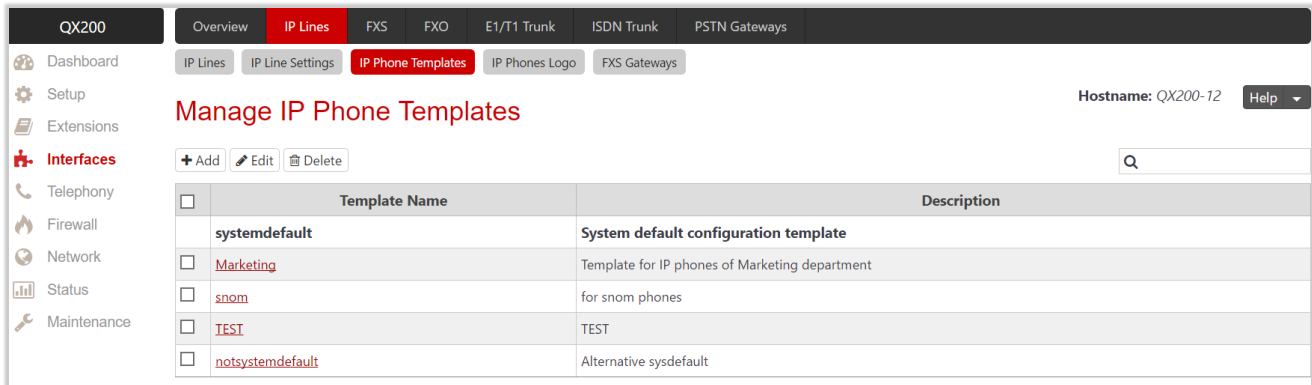


Figure 59: Manage IP Phone Templates page

To create a new IP phone template:

1. Click **Add** to define a template name.
  - **Template Name** is used to set a template name.
  - Enter a **Description**, if needed.
2. Click **Save** to add a new template to the **Manage IP Phone Templates** table.
3. Click on the **Template Name** link to adjust the advanced settings for different IP phone vendors and assigned functions to the [programmable keys](#) for each phone model. You are allowed to manage the settings for a group of IP phones at once.
4. Click **Save** to apply changes.

### 7.1.4 IP Phones Logo

**IP Phones Logo** is used to upload a custom logo for the IP phone. The uploaded custom logo will be visible on the display of the IP phone.

To upload a custom logo:

1. Click the **Choose File** button and browse for a logo file.
2. Tick the **Enable Logo** checkbox.
3. Click **Save** to apply changes.

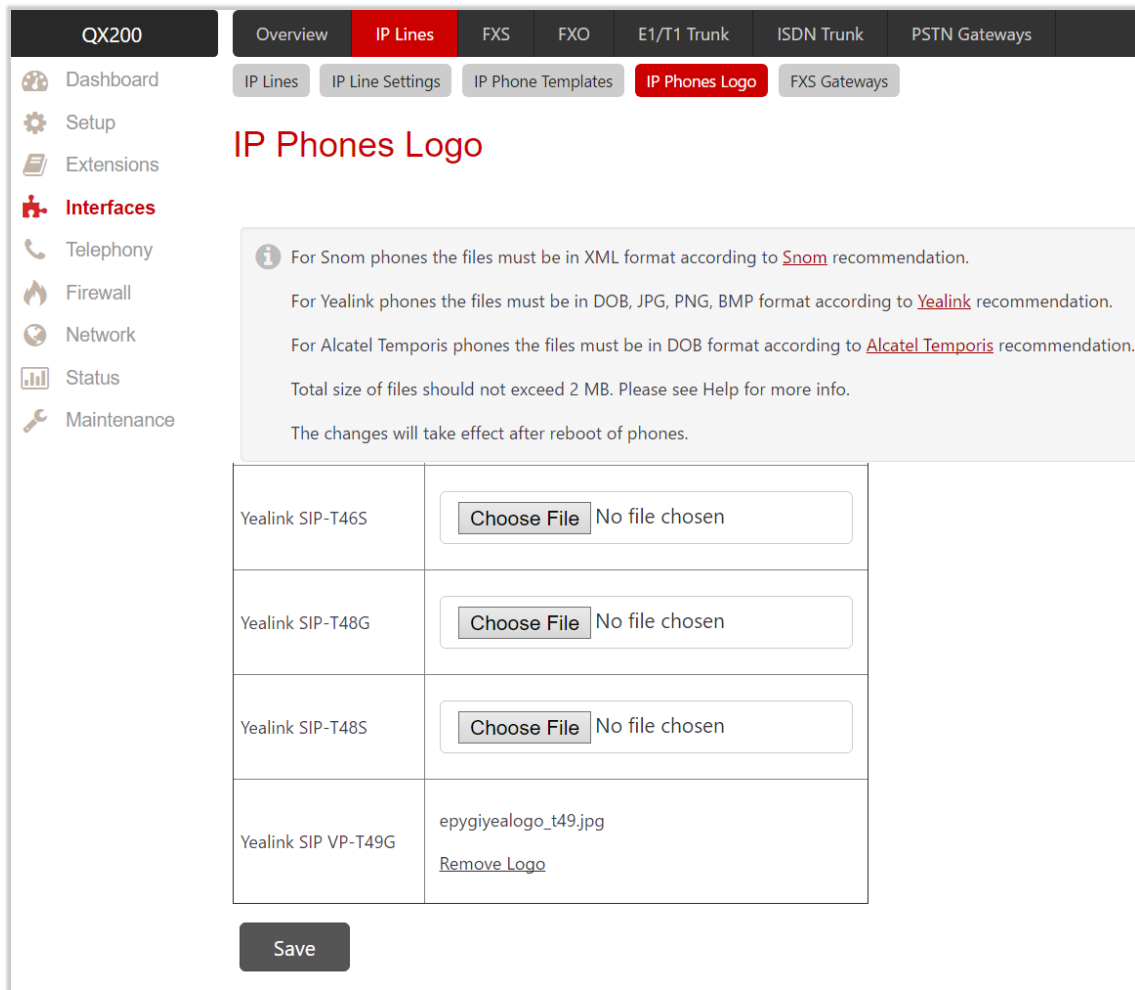


Figure 60: IP Phone Logo page

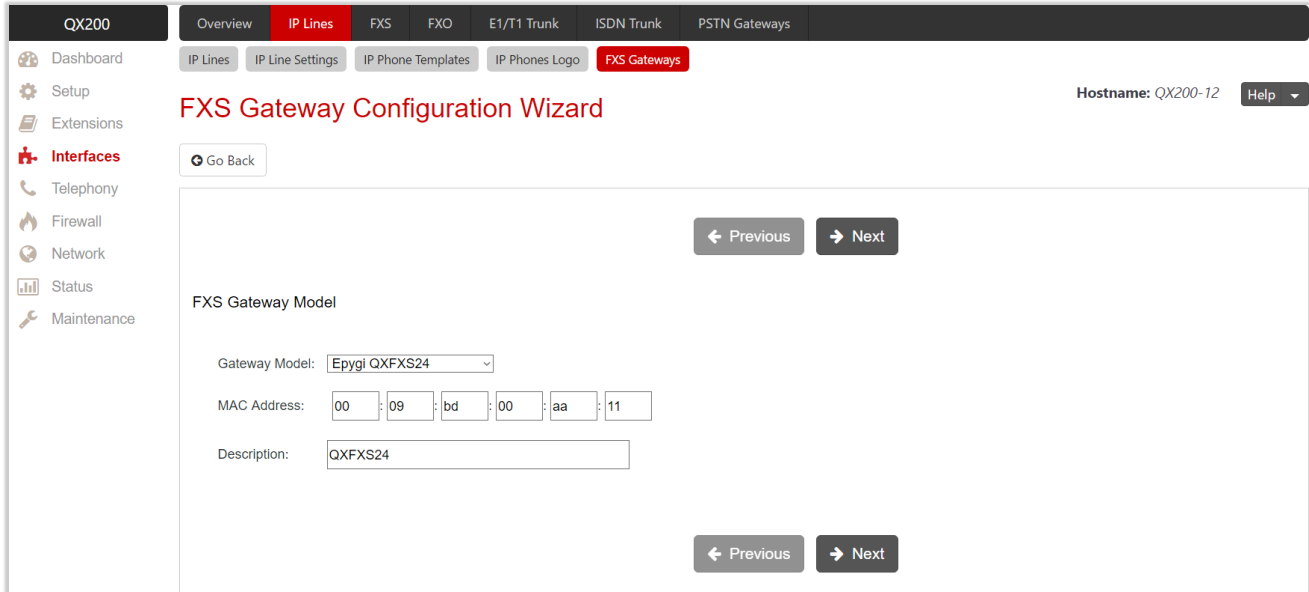
### 7.1.5 FXS Gateways

**FXS Gateway Management** is used to automatically configure QXFXS24 with QX IP PBX. QXFXS24 is an analog VoIP Gateway connects analog phones to a VoIP network. The device can be used with QX IP PBX to emulate FXS ports. The **FXS Gateway Management** table lists all configured FXS gateways.

Click **Add** to run **FXS Gateway Configuration Wizard** and configure FXS gateway with QX. The wizard consists of the following sections:

- [FXS Gateway Model](#)
- [Line Mapping – Add Entry](#)
- [Summary](#)

## FXS Gateway Model



The screenshot shows the 'FXS Gateway Configuration Wizard' interface. At the top, there are navigation tabs for 'Overview', 'IP Lines', 'FXS', 'FXO', 'E1/T1 Trunk', 'ISDN Trunk', and 'PSTN Gateways'. The 'FXS Gateways' tab is active. On the left, there is a sidebar menu with options like 'Dashboard', 'Setup', 'Extensions', 'Interfaces', 'Telephony', 'Firewall', 'Network', 'Status', and 'Maintenance'. The main content area is titled 'FXS Gateway Configuration Wizard' and includes a 'Go Back' button. Below this, there are 'Previous' and 'Next' navigation buttons. The configuration fields are:
 

- Gateway Model:** A dropdown menu currently showing 'Epygi QXFXS24'.
- MAC Address:** A series of six input boxes containing the values '00', '09', 'bd', '00', 'aa', and '11', separated by colons.
- Description:** A text input field containing 'QXFXS24'.

 At the bottom of the configuration area, there are again 'Previous' and 'Next' navigation buttons.

Figure 61: FXS Gateway Model section

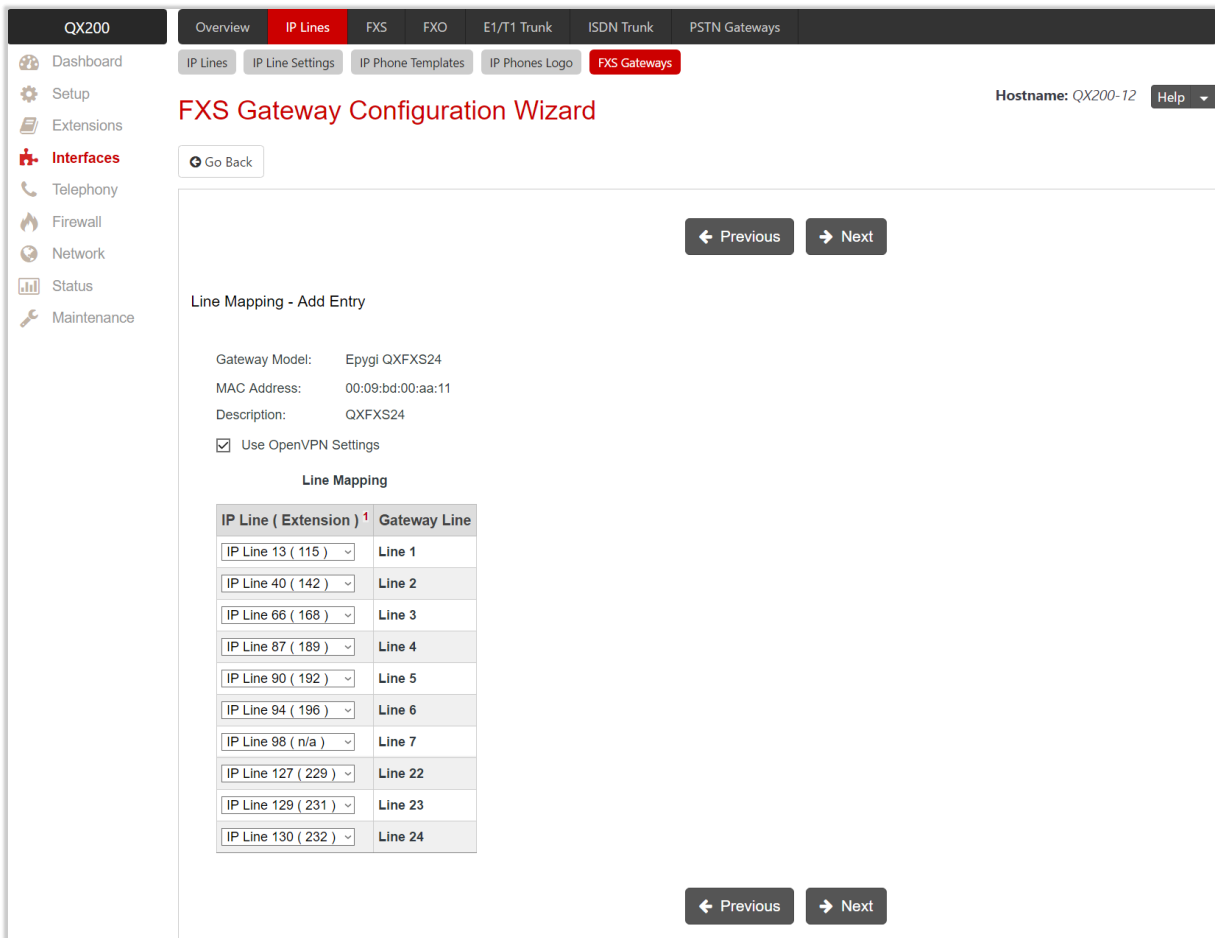
The following settings (options) are available:

- **Gateway Model** is used to select the gateway model from the list.
- **MAC Address** is used to set the MAC Address of the gateway.

### Line Mapping – Add Entry

This section is used to assign each FXS line to an IP line. The system will automatically assign the provided FXS lines to the first available IP lines on QX. **Line Mapping** can be manually adjusted. FXS lines can be assigned only to free (inactive) IP lines on QX. If there aren't any free IP lines, you should first free (deactivate) the IP line.

- **Use OpenVPN Settings** – if selected the configuration file will be provided through OpenVPN.



The screenshot shows the QX200 web interface with the 'FXS Gateway Configuration Wizard' active. The 'Line Mapping - Add Entry' section is visible, showing gateway details and a table for mapping IP lines to gateway lines.

Gateway Model: Epygi QXFXS24  
 MAC Address: 00:09:bd:00:aa:11  
 Description: QXFXS24  
 Use OpenVPN Settings

**Line Mapping**

IP Line ( Extension ) <sup>1</sup>	Gateway Line
IP Line 13 ( 115 )	Line 1
IP Line 40 ( 142 )	Line 2
IP Line 66 ( 168 )	Line 3
IP Line 87 ( 189 )	Line 4
IP Line 90 ( 192 )	Line 5
IP Line 94 ( 196 )	Line 6
IP Line 98 ( n/a )	Line 7
IP Line 127 ( 229 )	Line 22
IP Line 129 ( 231 )	Line 23
IP Line 130 ( 232 )	Line 24

Figure 62: Line Mapping section

## Summary

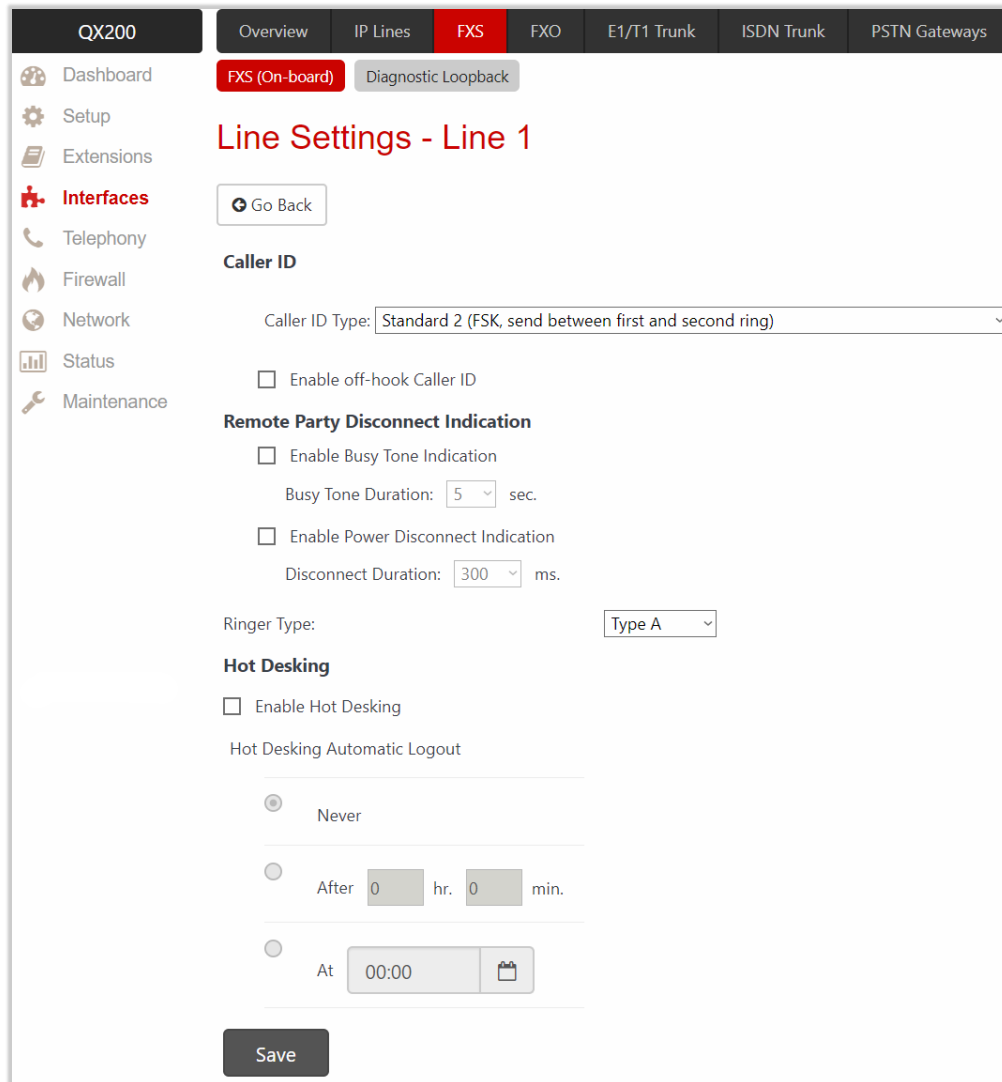
This section displays all configured settings (options) before applying them.

**Note:** FXS gateway (mapped IP lines) will be added in the **IP Lines** table after successful configuration. The corresponding routing rules will be added to the **Call Routing Table** of FXS gateway.

## 7.2 FXS

### 7.2.1 FXS (On-board)

The FXS Line page is used to configure on-board FXS lines, define the **Caller ID Type**, configure **Remote Party Disconnect Indication** and select the **Ringer Type** on each of them.



The screenshot shows the 'Line Settings - Line 1' page in the QX200 web interface. The page is divided into several sections:

- Caller ID:** A dropdown menu is set to 'Standard 2 (FSK, send between first and second ring)'. There is an unchecked checkbox for 'Enable off-hook Caller ID'.
- Remote Party Disconnect Indication:** There are three unchecked checkboxes: 'Enable Busy Tone Indication', 'Enable Power Disconnect Indication', and 'Enable Power Disconnect Indication'. The 'Busy Tone Duration' is set to 5 seconds, and the 'Disconnect Duration' is set to 300 ms.
- Ringer Type:** A dropdown menu is set to 'Type A'.
- Hot Desking:** There is an unchecked checkbox for 'Enable Hot Desking'. Below it, the 'Hot Desking Automatic Logout' is set to 'Never'.

A 'Save' button is located at the bottom of the form.

Figure 63: FXS Line Settings page

Click the hyperlinked **FXS #** to open the **Line Settings** page to configure specific settings for the selected line. The following settings (options) are available:

- **Caller ID Type** 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.

**Note:** The caller ID detection method is different for various types of phones and can be found in the phone manual.

- **Enable off-hook Caller ID** is used to enable 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.
- **Remote Party Disconnect Indication** parameters are used to configure the private PBX attached to the QX FXS port.
  - **Enable Busy Tone Indication** is used to enable a busy tone transmission to the FXS port when the remote party being called is disconnected. **Busy Tone Duration** is used to select the period when a busy tone is transmitted to the FXS port.
  - **Enable Power Disconnect Indication** is used to enable 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. **Disconnect Duration** is used to select the period when the FXS line power will be down.
- **Ringer Type** is used to select the frequency of ringer supported by the phone attached to the line. 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 **Type A** ringer type should be selected, if **N=B**, the **Type B&Z** ringer type should be selected.

The **Hot Desking** section is used to enable and configure the [Hot Desking](#) service on the FXS line. **Note:** The **Hot Desking** section is the same as for IP line.

### Information on the Caller ID system

**Caller ID** service is used to identify the caller (when establishing a call or sending a voice mail) and notify 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 notifications are available on QX: **FSK** and **DTMF**.

#### FSK Standard

The **FSK** standard supports caller ID indication either with the phone handset on-hook or if the called party is already busy with another call. 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.

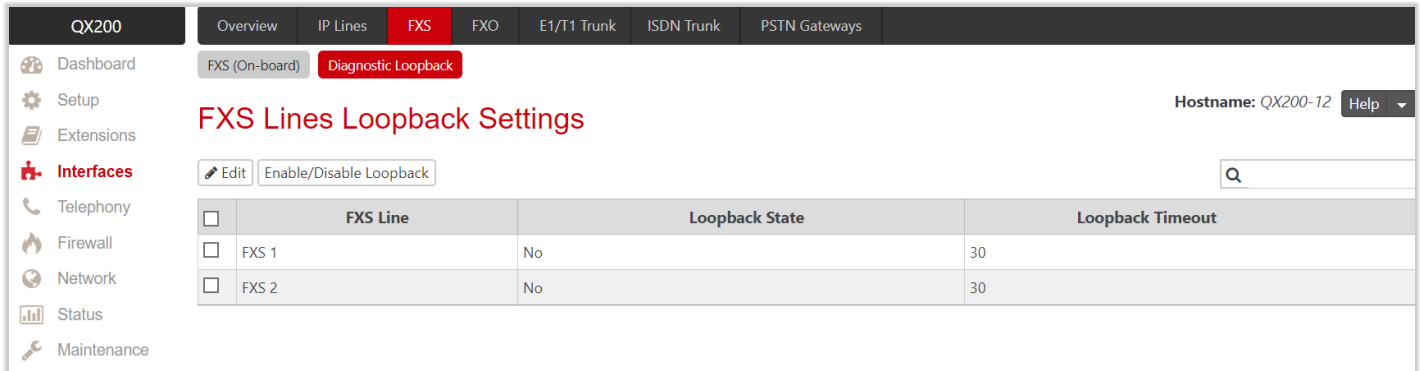
#### DTMF Standard

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.

**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.

## 7.2.2 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, incoming call to the line will be automatically picked up after the first ring and voice towards the line will automatically be sent back to the caller (the caller will hear his voice).



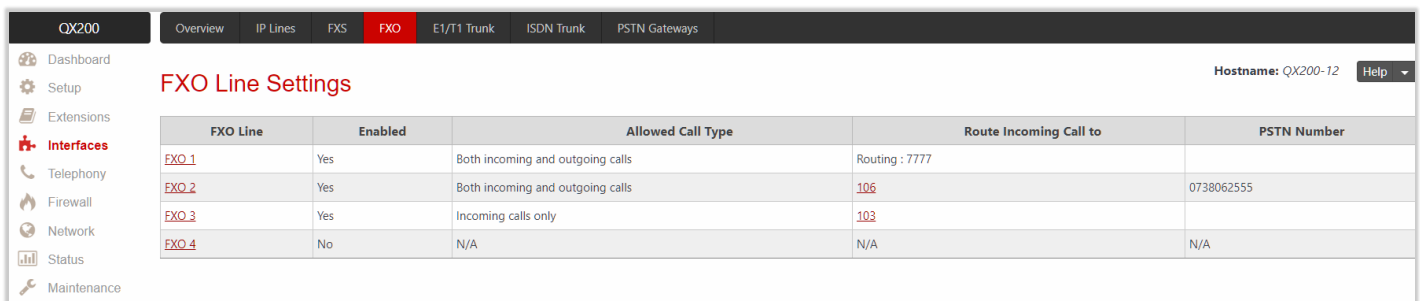
FXS Line	Loopback State	Loopback Timeout
FXS 1	No	30
FXS 2	No	30

Figure 64: FXS Lines Loopback Settings page

- **Edit** leads to **FXS Lines Loopback Settings – Edit Entry** page to configure the **Loopback Timeout** for the selected FXS line(s).
- **Loopback Timeout** is used to put a limit on the voice loopback diagnostics duration, i.e. the caller will be disconnected from the QX when the **Loopback Timeout** expires.
- **Enable/Disable Loopback** is used to enable/disable the service on the selected FXS line(s).

## 7.3 FXO

The **FXO Settings** page is used to configure on-board FXO Lines to make PSTN calls through the on-board FXO ports.



FXO Line	Enabled	Allowed Call Type	Route Incoming Call to	PSTN Number
<a href="#">FXO 1</a>	Yes	Both incoming and outgoing calls	Routing : 7777	
<a href="#">FXO 2</a>	Yes	Both incoming and outgoing calls	<a href="#">106</a>	0738062555
<a href="#">FXO 3</a>	Yes	Incoming calls only	<a href="#">103</a>	
<a href="#">FXO 4</a>	No	N/A	N/A	N/A

Figure 65: FXO Settings page

Click the hyperlinked **FXO #** to open the **FXO Settings – FXO #** page to configure specific settings of the selected line. The following settings (options) are available:

- **Enable Line** is used to activate FXO line.
- **Allowed Call Type** is used to select the allowed call directions for the FXO line. The following options are available:
  - **Both incoming and outgoing calls** will be allowed through the selected FXO line.
  - **Incoming calls only** will be allowed through the selected FXO line.
  - **Outgoing calls only** will be allowed through the selected FXO line.

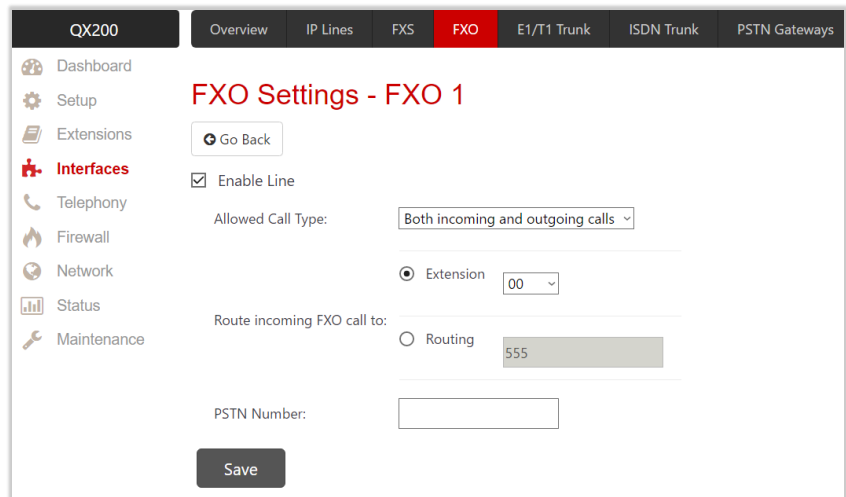


Figure 66: FXO Line Settings page

- **Route incoming FXO Call to** is used to define the destination where the incoming calls will be forwarded to.
  - **Extension** is used to forward the calls to either PBX user extension or auto attendant extension. The calls will be forwarded to **Voice Mailbox** if an inactive extension is chosen.
  - **Routing** is used to forward the calls to the destination defined through the **Call Routing Table**. Enter the routing pattern that will be used for forwarding purposes.
- **PSTN Number** is used to enter any descriptive information, if needed.

For more information on how to configure and use FXO lines, refer to the [Manual-II: Administration Guide for QX Gateways](#).



## 7.4 ISDN Trunk

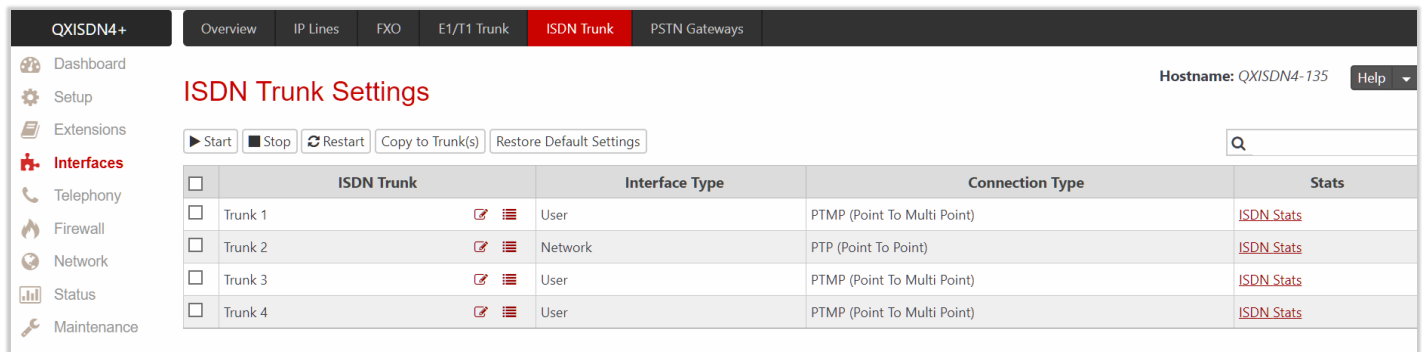
The **Integrated Services Digital Network (ISDN)** involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. The **ISDN Basic Rate Interface (BRI)** service offers two B channels (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.

For more information on how to configure and use **ISDN trunks**, refer to the [Manual-II: Administration Guide for QX Gateways](#).

The **ISDN service** allows QXISDN4+ act in the following modes:

- **network** – if connected to a private PBX
- **user** – if connected to the ISDN trunk from the **Central Office (CO)**. The QXISDN4+ supports the **Multiple Subscriber Number (MSN)** service, i.e., thus it can be subscribed to multiple numbers from the CO allowing to place two simultaneous calls at a time.

The **ISDN Trunk Settings** page is used to configure the ISDN trunks and their signaling parameters.



ISDN Trunk	Interface Type	Connection Type	Stats
Trunk 1	User	PTMP (Point To Multi Point)	<a href="#">ISDN Stats</a>
Trunk 2	Network	PTP (Point To Point)	<a href="#">ISDN Stats</a>
Trunk 3	User	PTMP (Point To Multi Point)	<a href="#">ISDN Stats</a>
Trunk 4	User	PTMP (Point To Multi Point)	<a href="#">ISDN Stats</a>

Figure 67: ISDN Trunk Settings page

The following buttons are available:

- **Start** and **Stop** 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.
- **Restart** is used to bring channel(s) to the initial idle state on both sides, any active traffic on the channel(s) will be terminated.
- **Copy to Trunk(s)** is used to copy the settings of the selected trunk to another trunk(s).
- **Restore Default Settings** is used to restore the default settings of the selected ISDN trunk(s).
- Click the **Incoming Interdigit Service** icon to configure dial plan for incoming ISDN calls from CO/PBX to the QX.
- Click the **Modify ISDN Trunk** icon to run the ISDN wizard to configure the ISDN trunk settings.

## 7.4.1 ISDN Wizard

Click the **Modify ISDN Trunk** icon to run the ISDN wizard to configure the selected trunk settings. In general, the wizard consists of the following sections:

- [ISDN Settings](#)
- [MSN Settings](#)
- [Routing Settings](#)
- [ISDN Low Level Settings](#)
- [L2 & L3 Settings](#)
- [Summary of ISDN Settings](#)

### ISDN Settings

This section is used to select the interface type and the connection type of the selected trunk.

- **Trunk** shows the selected trunk number.
- **Interface Type** allows to select between the **User** and the **Network** options. If the ISDN trunk is connected to the CO, then the **User** option should be selected. If the trunk is connected to legacy PBX, then the **Network** option should be selected.
- **Connection Type** allows to select between the PTP and PTMP connection types.
  - **PTP (Point to Point)** – in case of connection to the CO, **User** interface type is selected. **TIP:** No other ISDN device should be connected to ISDN trunk. In case of connection to the legacy PBX, **Network** interface type is selected. **TIP:** No other ISDN devices should be connected to ISDN trunk. In both cases, with this selection, QX sets the TEI to **manual** mode, assigning the default value (0). **TIP:** If needed, that value can be changed from the **Advanced Settings** section.

The screenshot shows the 'ISDN Wizard' interface. At the top, there is a navigation bar with tabs: Overview, IP Lines, FXO, E1/T1 Trunk, **ISDN Trunk** (highlighted), and PSTN Gateways. On the left, a sidebar menu lists: Dashboard, Setup, Extensions, **Interfaces**, Telephony, Firewall, Network, Status, and Maintenance. The main content area is titled 'ISDN Wizard' and includes a 'Go Back' button. Below this, there are 'Previous' and 'Next' navigation buttons. The 'ISDN Settings' section contains the following fields:

- Trunk : 1
- Interface Type: User (selected in a dropdown menu)
- Connection Type:
  - PTP (Point To Point)
  - PTMP (Point To Multi Point)

At the bottom of the settings area, there are again 'Previous' and 'Next' navigation buttons.

Figure 68: ISDN Settings section

- **PTMP** (Point to Multi Point) – in case of connection to the CO, **User** interface type is selected. In case of connection to the legacy PBX, **Network** interface type is selected. In both cases, with this selection, QX sets the TEI to **automatic** mode.

## MSN Settings

This section is used to turn on the MSN configuration. The section becomes available only in case of **User** interface type. It is recommended to enable the MSN when there are multiple ISDN devices connected to the same ISDN bus.

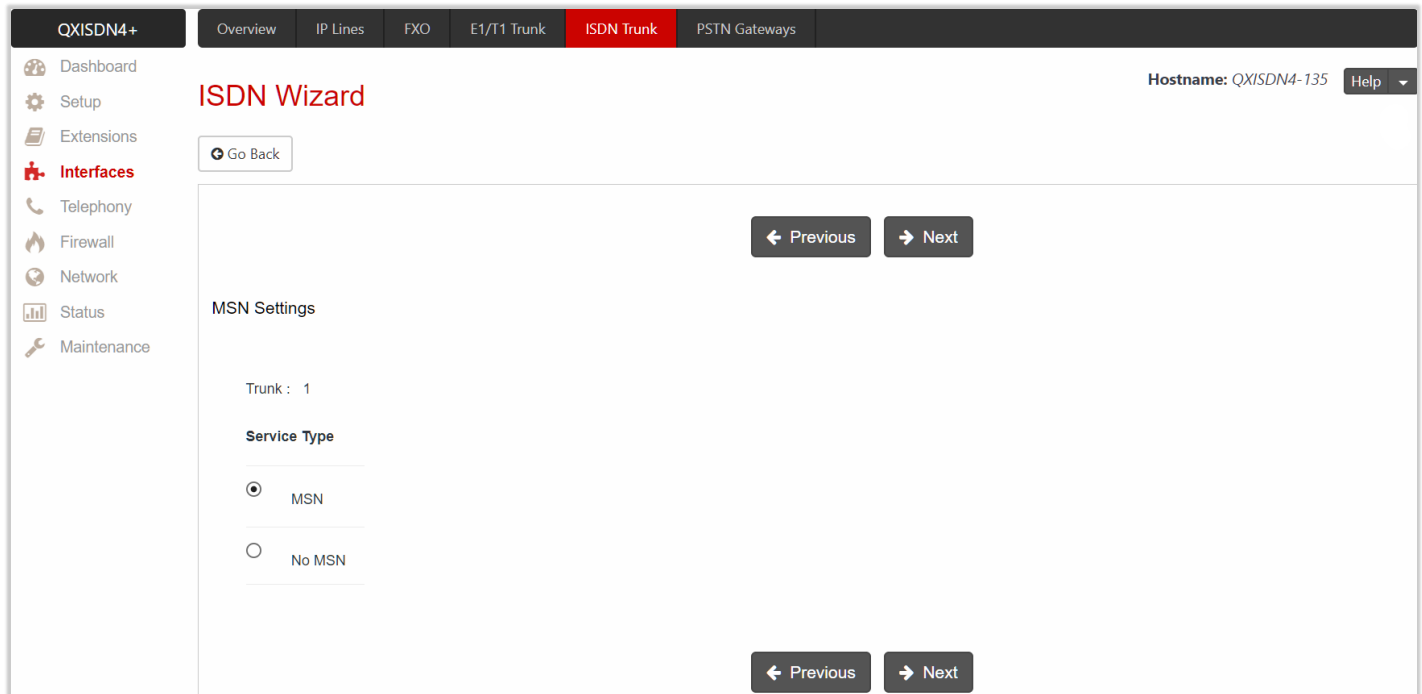


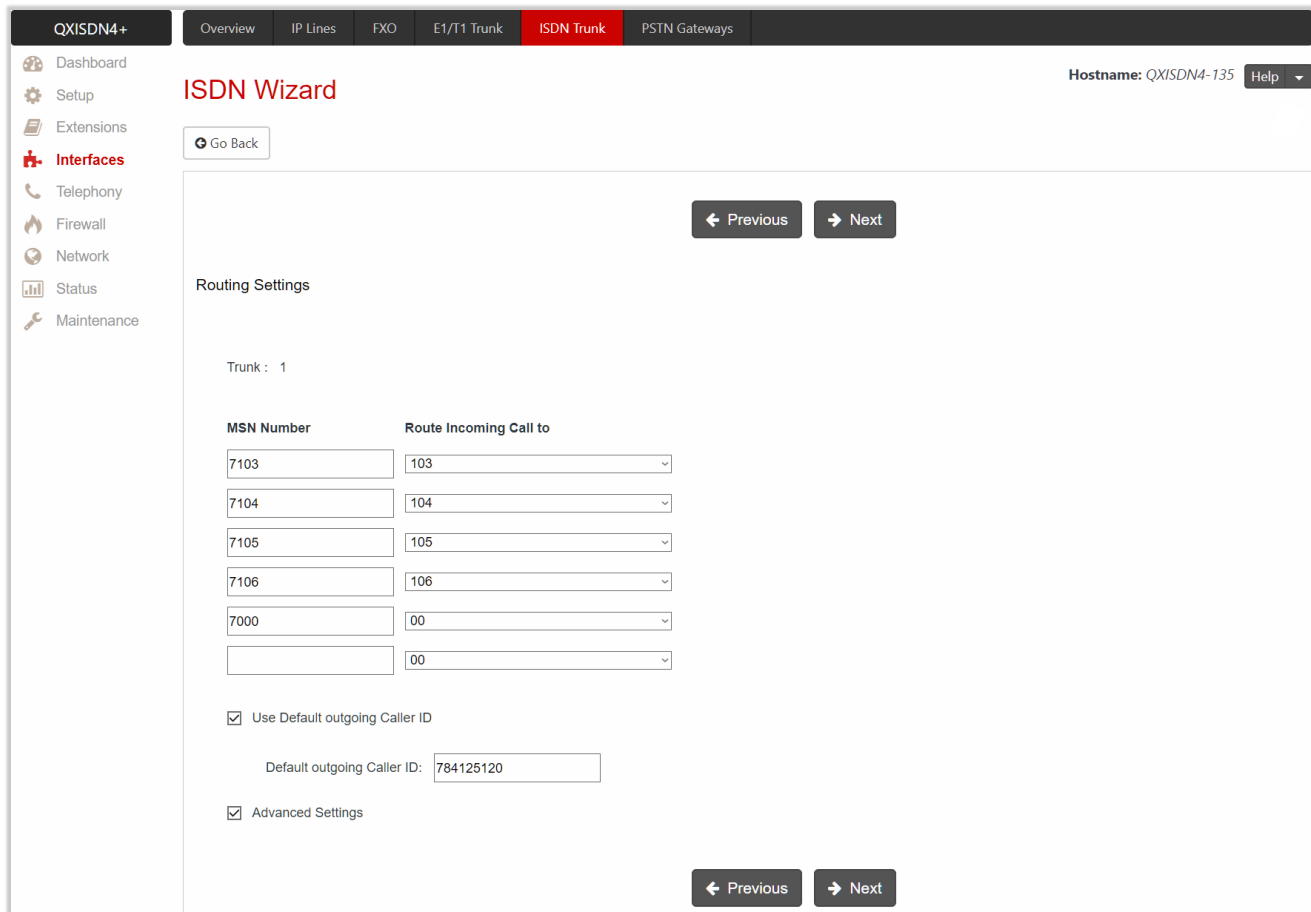
Figure 69: MSN Settings section

## Routing Settings

The content of this section depends on the interface type and service type selected from the previous sections of the wizard.

- **Trunk** displays the selected trunk number.
- **Routing Settings** – if **MSN** service is enabled, this section is used to assign MSN numbers to the certain destinations on QX.
  - The fields in the **MSN Number** column require the MSN numbers allocated to QX. At least one MSN number should be defined.
  - **Route Incoming Call to** is used to define the destination where the incoming calls addressed to the certain MSN number will be forwarded to. The following options are available:
    - ◆ The calls can be forwarded to either **user extension** or **auto attendant**.
    - ◆ **Routing with inbound destination number** is used to forward the calls to the destination defined through **Call Routing Table**.
- **Routing Settings** – if **MSN** service is disabled or the selected interface type is **Network**, this section has only one **Route Incoming Call to** option.
- **Use Default outgoing Caller ID** is used to overwrite the source Caller ID with the one specified in this field.

- **Advanced Settings** – tick this checkbox if you want to adjust **L2** and **L3 Settings** of the trunk manually in the next section.



The screenshot shows the 'ISDN Wizard' interface for 'QXISDN4+'. The 'ISDN Trunk' tab is selected. The 'Routing Settings' section is active, showing 'Trunk : 1'. Below this, there is a table for mapping MSN numbers to route incoming calls. The table has two columns: 'MSN Number' and 'Route Incoming Call to'. The rows are as follows:

MSN Number	Route Incoming Call to
7103	103
7104	104
7105	105
7106	106
7000	00
	00

Below the table, there are two checkboxes: 'Use Default outgoing Caller ID' (checked) and 'Advanced Settings' (checked). The 'Default outgoing Caller ID' field contains the value '784125120'. Navigation buttons for 'Previous' and 'Next' are visible at the top and bottom of the form.

Figure 70: Routing Settings section

## ISDN Low Level Settings

This section is used to enable **Power Source** option. The section becomes available only in case of **Network** interface type.

- **Trunk** displays the selected trunk number.
- **Power Source** – if selected, the QX will supply power for the connected ISDN phones, otherwise ISDN phones should have their own power supplies. **TIP: Power Source** option should be always disabled when a legacy PBX or Telecom is connected to the QX.

## L2 & L3 Settings

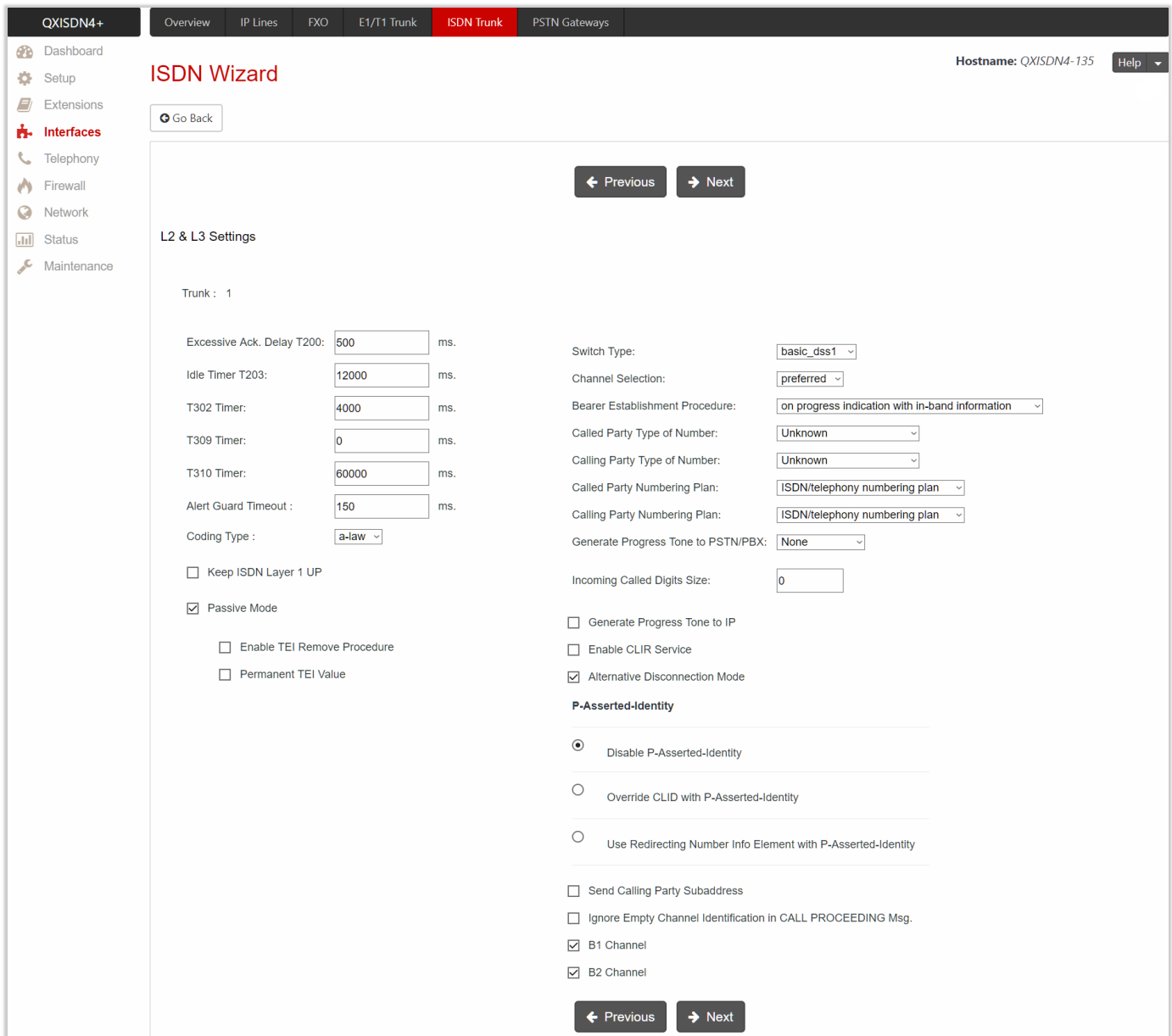
This section is used for the advanced configuration of L2 and L3 settings. The section becomes available only if the **Advanced Settings** checkbox is ticked on the previous section. The following options are available:

- **Trunk** displays the selected trunk number.
- **Excessive Ack. Delay T200** is used to configure the period between the transmitted signaling packet and the acknowledgement received.
- **Idle Timer T203** is used to configure the period for the ISDN client idle timeout.
- **T302 Timer** indicates the time frame, system will wait for digits to be dialed after which the system initiates the call.

- **T309 Timer** is used to configure call steadiness during link disconnection. If the value in this field is 0, the T309 timer will be disabled.
- **T310 Timer** is used to configure the outgoing call steadiness when **CALL PROCEEDING** is already received from the destination but call confirmation (**ALERT**, **CONNECT**, **DISC** or **PROGRESS**) has not arrived yet.
- **Alert Guard Timeout** is used to set the value for the **Alert Guard Timer** between **CALL PROC** and **ALERT** messages. **Alert Guard Timer** is used when QX is connected to an old legacy PBX. Recommended values are:
  - fast connection (0ms)
  - normal (150ms), default
  - slow ISDN-PBX (350ms)
  - very slow ISDN-PBX (500ms)
- **Coding Type** is used to select between **a-law** and **mu-law** coding types.
- **Keep ISDN Layer 1 UP** is used to force ISDN layer 1 connection to always stay active.
- **Passive Mode** is used to leave the ISDN Layer1 connection in the Slave mode. If selected, Layer1 remains idle when calls are not available, otherwise QX keeps its Layer1 always active.
  - **Enable TEI Remove Procedure** – if selected, the trunk will lose the assigned TEI when entering into passive mode on the Layer 2.
  - **Permanent TEI Value** – if 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.

**Note:** These options are available only for **PTMP** connection type. If **PTP** connection type is selected, these two options are replaced with a **TEI Address** option which requires the channel number for connection establishment between the CO and the ISDN client.

- **Switch Type** – this configuration parameter depends on the Service Provider when acting in the **User** mode and the legacy PBX capabilities when acting in the **Network** mode.
- **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.
- **Bearer Establishment Procedure** allows to select the session initiation method on B channels. 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 screenshot shows the 'ISDN Wizard' configuration page for 'Trunk : 1'. The 'L2 & L3 Settings' section includes the following fields and options:

- Excessive Ack. Delay T200: 500 ms.
- Idle Timer T203: 12000 ms.
- T302 Timer: 4000 ms.
- T309 Timer: 0 ms.
- T310 Timer: 60000 ms.
- Alert Guard Timeout: 150 ms.
- Coding Type: a-law
- Switch Type: basic\_dss1
- Channel Selection: preferred
- Bearer Establishment Procedure: on progress indication with in-band information
- Called Party Type of Number: Unknown
- Calling Party Type of Number: Unknown
- Called Party Numbering Plan: ISDN/telephony numbering plan
- Calling Party Numbering Plan: ISDN/telephony numbering plan
- Generate Progress Tone to PSTN/PBX: None
- Incoming Called Digits Size: 0
- Keep ISDN Layer 1 UP
- Passive Mode
  - Enable TEI Remove Procedure
  - Permanent TEI Value
- Generate Progress Tone to IP
- Enable CLIR Service
- Alternative Disconnection Mode
- P-Asserted-Identity**
  - Disable P-Asserted-Identity
  - Override CLID with P-Asserted-Identity
  - Use Redirecting Number Info Element with P-Asserted-Identity
- Send Calling Party Subaddress
- Ignore Empty Channel Identification in CALL PROCEEDING Msg.
- B1 Channel
- B2 Channel

Figure 71: ISDN Low Level Settings section

- **Called Party Type of Number** allows to select the type identifying the sub address of the called party.
- **Calling Party Type of Number** allows to select the type identifying the origin of a call.
- **Called Party Numbering Plan** and **Calling Party Numbering Plan** are used to select numbering plans.
- **Generate Progress Tone to PSTN/PBX** contains the options for sending progress (ring-back) tone to callers from the PSTN/PBX. The following options are available in the list:
  - **None** is used to configure the system to send **ALERT** messages without the **Progress Indicator Information Element**.
  - **Unconditional** is used to configure the system to send **ALERT/PROGRESS** messages with the **Progress Indicator Information Element**. With this option, the system will send its own progress tone.
  - **Conditional** is used to configure the system to send **ALERT/PROGRESS** messages with **Progress Indicator Information Element**. 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** indicates the number of received digits required to establish a call. When this field has 0 value, 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 **#** always cause the call establishment.

- **Generate Progress tone on IP** – if selected, the progress tone to IP (SIP) will be generated.
- **Enable CLIR Service** – if selected, **Calling Line Identification Restriction (CLIR)** service will be activated and this will display 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.
- **Alternative Disconnection Mode** – if not selected, QX will disconnect the call as soon as disconnect message has been received from the peer. Otherwise, the QX user may hear a busy tone when the peer has been disconnected.
- **P-Asserted-Identity** is used to configure **P-Asserted-Identity** for the calls from SIP to ISDN and vice-versa.
  - **Disable P-Asserted-Identity** is used to disable the **P-Asserted-Identity** for both incoming and outgoing calls.
  - **Override CLID with P-Asserted-Identity** enables the SIP P-Asserted-Identity support. For the calls from SIP to ISDN if the Invite SIP message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the Caller ID on ISDN is sent with the original Caller ID. The latter 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 out 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.
  - **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 Caller ID 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.
- **Send Calling Party Subaddress** – if selected, QX will send the extension number as sub address and the value defined in the **Default outgoing Caller ID** field as caller ID on the outgoing call. Otherwise no sub address information will be sent and the caller ID will be defined according to the selection of the **Use Default Outgoing Caller ID** checkbox. Caller ID information, along with the **Subaddress**, can be displayed on the phone display depending on the phone and PBX settings and capabilities.
- **Ignore Empty Channel Identification in CALL PROCEEDING Msg.** – if selected, QX will ignore the empty **ISDN L3 Channel Identification** information element in **CALL PROCEEDING** message and will not response with **STATUS** message, otherwise QX will respond with **STATUS** message on empty Channel Identification information element.
- **B1 Channel** and **B2 Channel** enable/disable timeslots for voice transfer. Disabling the timeslot will prevent both incoming and outgoing calls.

### Summary of ISDN Settings

This section displays all configured settings (options) before applying them.

## 7.4.2 ISDN Stats

The **ISDN Trunk Status** page shows information on the link state, transfer and error statistics. The following sections are available:

### General Information

This section contains the following components:

- **Active Calls** shows the currently active calls.
- **Outgoing Calls** shows the total amount of outgoing calls (historical data).
- **Incoming Calls** shows the total amount of incoming calls (historical data).
- **Last Time Cleared** shows the date and time when the ISDN Stats has been manually cleared last time.  
**TIP:** Click the **Clear Statistics** button, to reset the statistics counters.

### Layer 1 - Trunk Settings and Link Status

This section contains the following components:

- **Link** shows the ISDN link state: up or down.
- **Frame Synchronization** shows the signal synchronization state in the trunk: Yes or No.

### Layer 1 - HDLC Statistics

This section contains the following components:

- **HDLC Receive** shows the number of packets received in HDLC format.
- **HDLC CRC Error** shows the number of packets received with CRC errors.
- **HDLC Packet Abort** shows the number of aborted packets received.
- **HDLC Transmit** shows the number of packets transmitted in HDLC format.
- **HDLC Octet Count** shows the number of error packets received in HDLC format.

### Layer 2 Settings

This section contains the following components:

- **TEI Value** shows the actual TEI assigned value.
- **L2 State** shows the state of BRI L2.

### Layer 2 - Transfer Statistics

This section contains the following components for received and transmitted packets:

- **Information Frame** shows the signaling packets for call initiation and termination.
- **Receive Ready** shows the control packets when the ISDN link is up.
- **Receive Not Ready** shows the control packets when unable to accept calls.
- **SABME** shows the packets when establishing connection.
- **Disconnected Mode** shows the packets when connection is being terminated.
- **Disconnect** shows the packets when connection is terminated.
- **Unnumbered Acknowledgement** shows the packets when accepting connection, call establishment and termination.



- **Framer** shows the packets as a report of an error condition.
- **TEI Request** shows the packets containing TEI to initiate subscription of the device at the network.
- **Unnumbered Information Frame** shows the broadcast signaling packets received for call initiation and termination.
- **Exchange Identification** shows the received packets containing connection management settings.

### Layer 2 - Error Statistics

This section contains the following components:

- **Incorrect Length** shows the packets with incorrect length.
- **Bad Supervisory Frame** shows the packets with incorrect supervisory header.
- **Bad Unnumbered Information Frame** shows the packets with incorrect unnumbered information frame header.
- **Bad Frame Type** shows the packets with bad frame type.
- **Bad Unnumbered Frame** shows the packets with incorrect unnumbered acknowledgement frame header.
- **Foreign TEI Value** shows the packets with bad or foreign TEI value.

## 7.5 E1/T1 Trunk

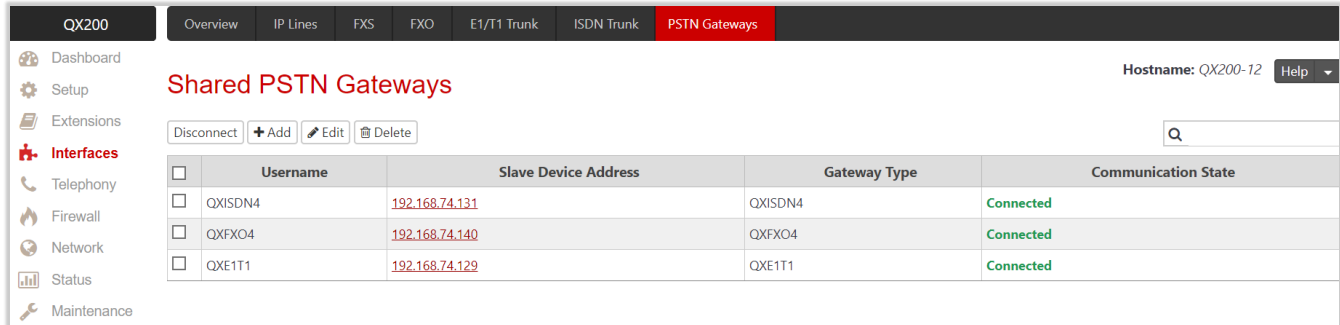
QXs don't have on-board E1/T1 ports. Connect QXE1T1 gateway(s) to use the shared E1/T1 trunks.

For more information on how to configure and use **E1/T1** trunks, refer to the [Manual-II: Administration Guide for QX Gateways](#).

## 7.6 PSTN Gateways

The PSTN lines (FXO, E1/T1 or ISDN) of the QX gateway(s) can be shared with QX IP PBXs.

The **Shared PSTN Gateways** page is used to create accounts for the **slave** QX gateway(s) to connect it to the **master** QX IP PBX for **PSTN line sharing** (FXO lines, E1/T1 and/or ISDN trunks).



	Username	Slave Device Address	Gateway Type	Communication State
<input type="checkbox"/>	QXISDN4	192.168.74.131	QXISDN4	Connected
<input type="checkbox"/>	QXFXO4	192.168.74.140	QXFXO4	Connected
<input type="checkbox"/>	QXE1T1	192.168.74.129	QXE1T1	Connected

Figure 72: Shared PSTN Gateways page

To connect QX gateway to QX IP PBX and share the PSTN lines of the gateway:

1. Click **Add** and enter the following information:
  - **Username** and **Password** are used to set the authentication parameters. **TIP:** The **Username** and **Password** should match on both master and slave for the successful **PSTN line sharing**.
  - Click **Save** to add the new entry to the **Shared PSTN Gateways** table.
2. The QX will start listening connection requests from slave device.
3. Make corresponding configurations on QX gateway to establish **master-slave** connection. Once the **slave-master** connection is successfully established, appropriate routing rules will be created on the **Call Routing Table** for both devices (slave and master) to support **PSTN line sharing**.
4. Click **Disconnect** to disconnect the slave device from the QX. **Note:** The slave device will not be reconnected automatically. You need to manually reconnect the slave device to QX from slave's WEB GUI.

For more information on how to configure and use **QX gateway(s)** with **QX IP PBX** in **Share mode**, refer to the [Configuring QX Gateways with QX IP PBXs in Sharing Mode](#) guide.

## 8 Telephony Menu



Category	Setting	Description
VoIP Carrier	<a href="#">VoIP Carrier</a>	Easily configure the SIP trunking account from the Internet Telephony Service Provider (ITSP).
	<b>Call Routing</b>	
	<a href="#">Call Routing Table</a>	Define the destination for dialed digit patterns and set up options for call routes.
	<a href="#">Call Routing</a>	Send all incoming SIP calls to the Call Routing table.
Call Routing	<a href="#">Local AAA Table</a>	Authentication table used with Call Routing for callers to pass authorization before being allowed to call out.
	<a href="#">SIP Tunnel</a>	Create a SIP Tunnel between two locations (best usage is to register a site with a Dynamic IP address to a site with a static IP address).
	<a href="#">Class of Service</a>	Create Class of Service names that can be assigned to extensions to match rules in the Call Routing table.
	<b>Call Recording</b>	
Call Recording	<a href="#">Call Recording</a>	Configure recording parameters and enable call recording for the extensions.
NAT Traversal	<b>General</b>	
	<a href="#">General</a>	NAT options needed to make external SIP calls on the internet when on a private network.
	<a href="#">SIP Parameters</a>	Configure NAT traversal settings for SIP messages.
	<a href="#">RTP Parameters</a>	Configure NAT traversal settings for RTP packets (voice and video).
	<a href="#">STUN Parameters</a>	Configure STUN server settings used for automatic NAT traversal.
RTP	<a href="#">Exceptions</a>	IP addresses and subnets to exclude from NAT traversal (needed for local or VPN connected subnets).
	<a href="#">RTP</a>	Choose voice and video codecs or modify RTP port range used on this device.
SIP	<a href="#">SIP</a>	Configure SIP ports and other general SIP settings.
	<a href="#">SIP Aliases</a>	DNS Hostnames to recognize when receiving SIP messages by hostname instead of IP.
	<a href="#">TLS Certificates</a>	Generate and install new TLS Certificate or download current one.
Schedules	<a href="#">Schedules</a>	Schedules Settings.
	<a href="#">Holidays</a>	Holidays Settings.
Advanced	<a href="#">Voice Mail</a>	Define the voice mail and fax storage method and E-mail notification settings.
	<a href="#">RTP Streaming Channels</a>	Assign channel names to RTP audio streams emitted by the Epygi Media Streamer application.
	<a href="#">Media Streamer</a>	Configure Media Streamer to stream audio file(s) to the RTP destinations.
	<a href="#">Gain Control</a>	Control transmit/receive levels of audio interface ports and recording/playback level of voice mails.
	<a href="#">3PCC</a>	Adjust Third Party Call Controlling (3PCC) settings. Controlling applications to remotely initiate and handle calls and subscribe to event notifications.
	<a href="#">Radius Client</a>	External RADIUS server connection settings.
	<a href="#">Dial Timeout</a>	Define timeout before sending dialed digits for call processing.
	<a href="#">Call Quality Notification</a>	Notify the user when the call quality falls below the specified threshold.

Figure 73: Telephony Menu overview

## 8.1 VoIP Carrier

QX supports the **SIP trunking** service from VoIP providers. This solution allows QX users to make cost saving calls to the global PSTN. **VoIP Carrier Wizard** simplifies the QX configuration with the **SIP trunking** services from VoIP providers.

Moreover, for many of industry leaders in VoIP business, the pre-configured templates are included in the QX configuration, allowing one-touch setup for SIP trunking services from these providers. For each **SIP trunking** service, the wizard automatically creates a specific IP-PSTN type call routing rule in the **Call Routing Table**. Additionally, a **Virtual Extension** is automatically generated in the [Extensions Management](#) table and registered on the SIP server of VoIP provider. The settings of that extension will be used to make calls towards the configured SIP trunks.

Commonly, just after finishing the wizard, QX users will be able to place calls to the PSTN using the carrier SIP trunk, as well as receive calls. Only in some rare cases some extra configuration should be done.

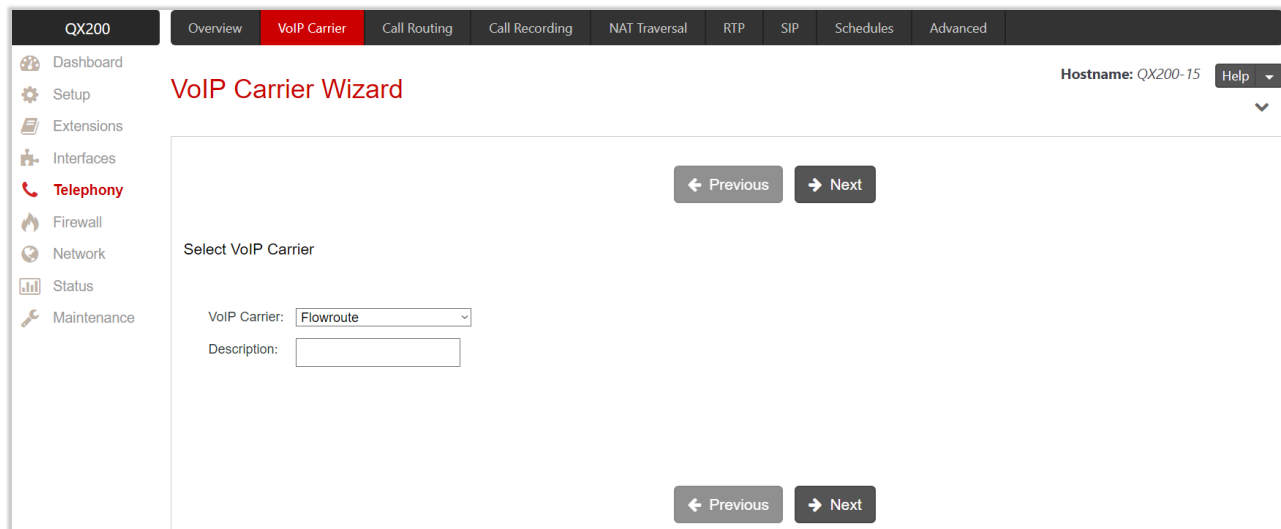


Figure 74: Select VoIP Carrier section

The **VoIP Carrier Wizard** consists of the following sections:

- [Select VoIP Carrier](#)
- [VoIP Carrier Settings](#)
- [VoIP Carrier Access Code](#)
- [Summary](#)

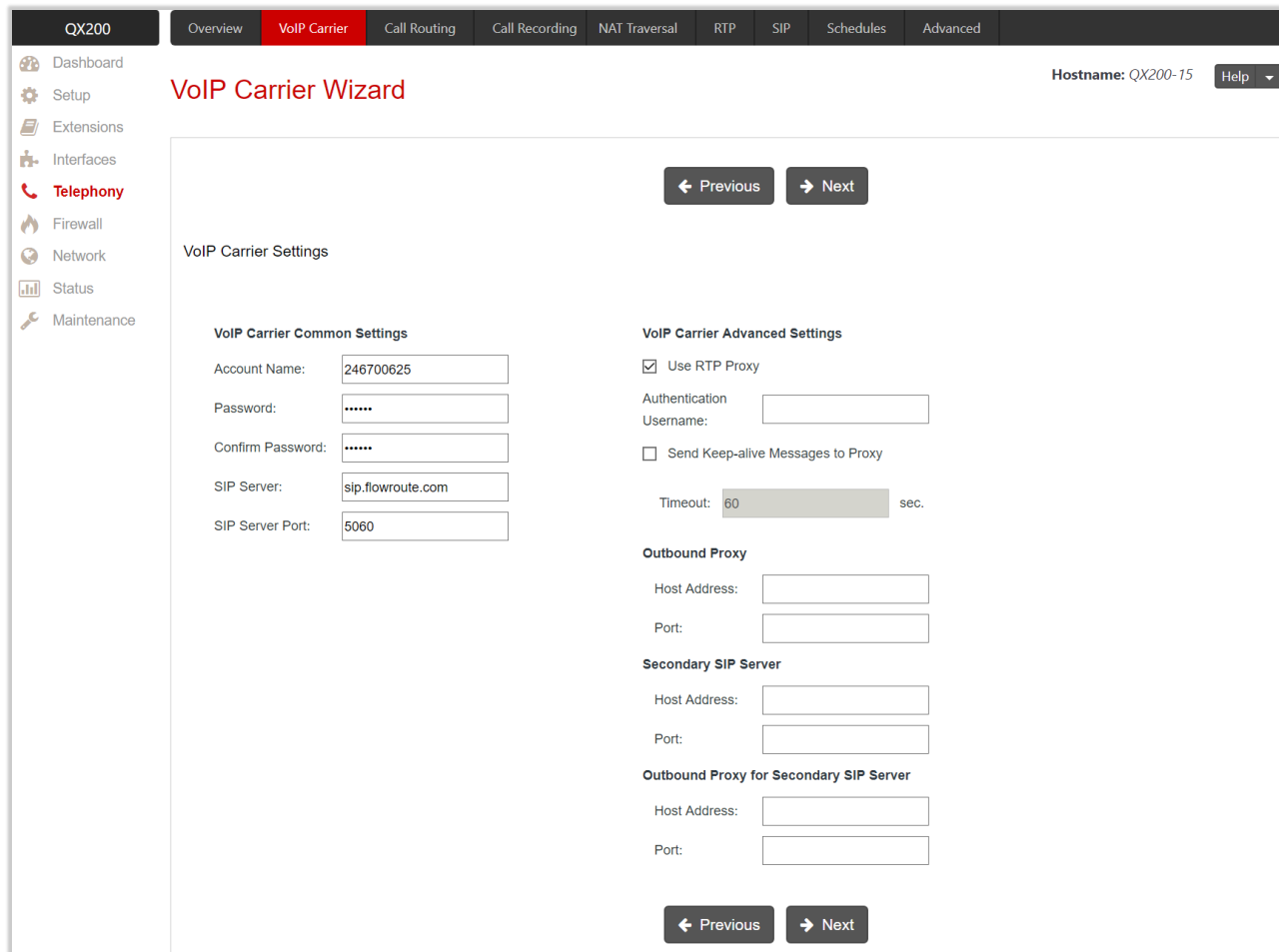
### Select VoIP Carrier

This section is used to select a carrier from the **VoIP Carrier** list. Once the carrier is found and selected, the carrier **SIP Server** and **SIP Port** will automatically appear on the next section of the wizard. The **Manual** option selection allows to configure the **VoIP Carrier Settings** manually from scratch.

## VoIP Carrier Settings

This section is used to define and configure the account from provider. The following settings (options) are available:

- **Authentication by IP Address** – if selected, deactivates the **Account Name** and **Password** fields, thus allowing to skip the account settings. This option is intended for the VoIP carriers requiring IP address authentication instead of account authentication and will be available if Manual option has been selected in the previous section.
- **Account Name** is used to set the username for authentication on the carrier SIP server.
- **Password** is used to set the password for authentication on the carrier SIP server and confirm it in the **Confirm Password** field.
- **SIP Server** is used to set the IP address or hostname.
- **SIP Server Port** is used to set the SIP server port.
- **Use RTP Proxy** – if selected, the RTP (audio) streams between external users will be routed through the QX, otherwise RTP packets will move directly between peers. This option is applicable only when a route is used for calls towards a configured **carrier** from a peer located outside the QX.
- **Authentication Username** is used to set an identification parameter to reach the SIP server. It should be provided by the **SIP trunking** service and may be requested only for certain SIP servers. Commonly, this field should be left blank.



**VoIP Carrier Wizard**

Hostname: QX200-15 Help

← Previous    → Next

**VoIP Carrier Settings**

**VoIP Carrier Common Settings**

Account Name:

Password:

Confirm Password:

SIP Server:

SIP Server Port:

**VoIP Carrier Advanced Settings**

Use RTP Proxy

Authentication Username:

Send Keep-alive Messages to Proxy

Timeout:  sec.

**Outbound Proxy**

Host Address:

Port:

**Secondary SIP Server**

Host Address:

Port:

**Outbound Proxy for Secondary SIP Server**

Host Address:

Port:

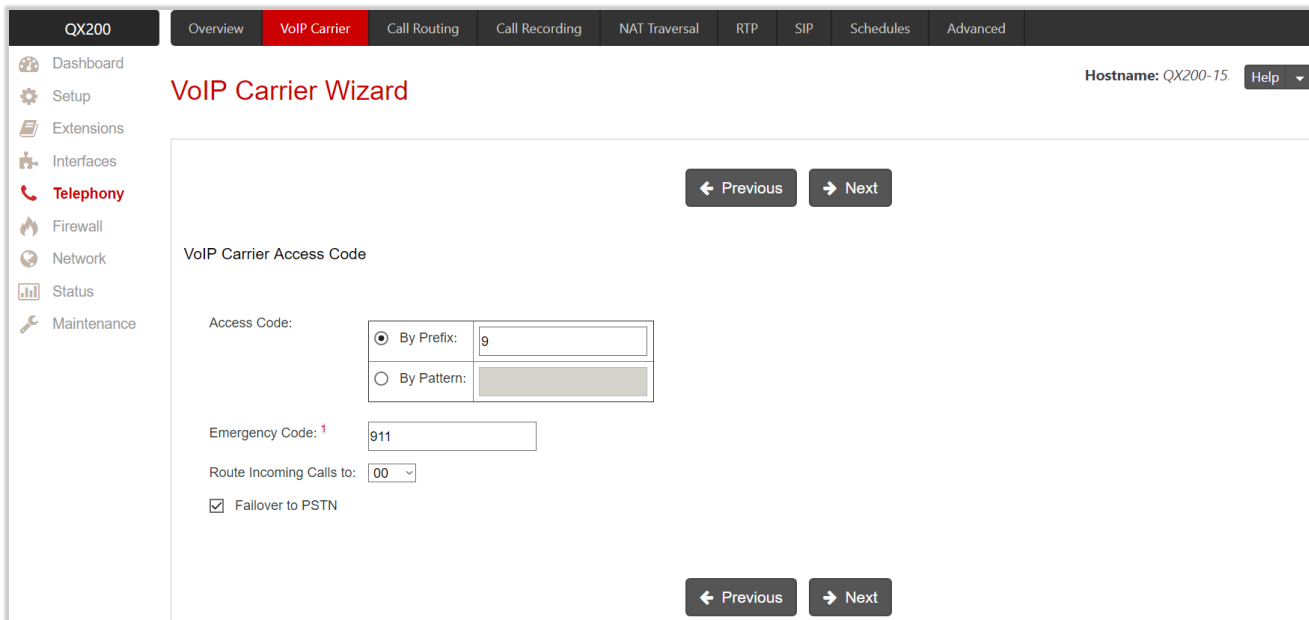
← Previous    → Next

Figure 75: VoIP Carrier Settings section

- **Send Keep-alive Messages to Proxy** enables the SIP registration server accessibility to the verification mechanism. **Timeout** is used to set the timeout between two attempts of SIP registration server accessibility verification. If a response 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.
- Define the **Outbound Proxy**, **Secondary SIP Server** and **Outbound Proxy for Secondary SIP Server** by entering the **Host Address** and **Port** for each of them respectively. These settings are provided by the **SIP Trunking** service and are used by the QX to reach to the selected SIP servers.

## VoIP Carrier Access Code

This section is used to define the routing rules for outbound/inbound calls through the SIP trunks.



The screenshot shows the 'VoIP Carrier Wizard' configuration page. The 'VoIP Carrier Access Code' section is active. It contains the following fields and options:

- Access Code:**
  - By Prefix:** 9
  - By Pattern:** (empty)
- Emergency Code:** 911
- Route Incoming Calls to:** 00
- Failover to PSTN**

Navigation buttons for 'Previous' and 'Next' are located at the top and bottom of the configuration area.

Figure 76: VoIP Carrier Access Code section

The following settings (options) are available:

- **Access Code** is used to define the routing rule for outbound calls.
  - **By Prefix** is used to specify the numeric prefix that should be dialed to route call through the SIP trunks. The system will route all digits matching this prefix to the SIP trunks.
  - **By Pattern** is used to specify the pattern that should be dialed to route call through the SIP trunks. If an outbound call has a destination number that matches the specified pattern, it will be completed according to the current rule.
- **Emergency Code** is used to set the emergency code supported by the specified VoIP provider. By default, this field is filled with the information defined in the [System Configuration Wizard](#). It also allows to set the carrier specific emergency codes. In case your system has both local PSTN emergency codes and IP-PSTN codes configured, when dialing the certain emergency code, QX will first try to reach the local PSTN allocated emergency, and if failed will dial the IP-PSTN emergency.
 

**TIP:** If the defined VoIP service is **911** compliant then you have to bind this account with the geographical address of your device. If the provider is not **911** compliant, then the public safety agency will not be able to determine the address automatically.
- **Route Incoming Calls to** is used to select an extension (user extension or auto attendant) on QX where the incoming calls from the configured carrier should be routed to. The unconditional call forwarding is

configured and activated automatically. This setup will be used to forward incoming calls from the VoIP carrier to the selected extension.

- **Failover to PSTN** – if selected, an additional entry will be added to the **Call Routing Table** to route calls to the PSTN network through the QX on-board PSTN lines in case if the carrier SIP trunks are not available.

## Summary

This section displays all configured settings (options) before applying them.

## 8.2 Call Routing

### 8.2.1 Call Routing Table

All calls from/to QX are being processed according to call routing rules that specify the destinations based on the dialed number. When dialing a number, QX matches that number against the **Destination Number Pattern** among the available call routing records. If the dialed number matches a pattern, then the record with respective pattern will be used to set up the call.

**Call Routing Table** allows to create and manage call routing rules for different type of calls and destinations. **Call Routing Table** lists the settings of all call routing rules (records) either generated manually or added automatically with one of the system wizards of QX: **Call Routing Wizard**, **System Configuration Wizard** or **VoIP Carrier Wizard**.

**Note:** Based on the **Emergency Codes** and **PSTN Access Codes Settings**, the automatically added records in the **Call Routing Table** will be marked in bold and placed in the first position of the table. Additionally, they cannot be modified and deleted from the **Call Routing Table**. To remove these rules, pass through the **System Configuration Wizard** and remove them from the **Emergency Codes and PSTN Access Code Settings** section.

All calls from QX extensions, as well as some calls from external sources, are being routed in QX according to call routing rules that specify the destination based on the dialed number. When user dials a number, QX matches the dialed number against the destination number patterns in the call routing rules.

For more information on how to configure and use **Call Routing Rules**, refer to the [Call Routing on QX IP PBXs](#) guide.

ID	State	Destination Number Pattern	Destination Number Modification	Call Settings	Failover Reason(s)	Local Authentication	Source Number Pattern/ Caller ID Modification	Source Type	DT	Call Rate	UES / URP	Metric	Description
1	Enabled	9?*	NDS: 1	FXO On-board Lines: Any Line	Any	No	*	PBX				10	Make PSTN Call
2	Enabled	45*	NDS: 2	E1/T1 Shared Trunks: E1/T1 Trunk1@192.168.74.129, Timeslots: 1-23	None	No	*	PBX				10	T1 Testing
3	Enabled	8*	NDS: 1	SIP sip.epygi.com:5060, RNSC: No	None	No	*	PBX			URP: Yes	10	Make SIP call
4	Enabled	7*	NDS: 1	SIP 192.168.0.209:5060, RNSC: No	None	No					URP: Yes	10	Make SIP call
5	Enabled	(???,??,???)		PBX	None	No	*				URP: Yes	10	for PBX Calls
6	Enabled	77777	NDS: 5 Prefix: 11	SIP 192.168.0.209:5060, RNSC: No	None	No	*		1000 CCM:Per Second CCF:0		URP: Yes	10	
7	Enabled	5*	NDS: 1	SIP 192.168.0.209:5060, RNSC: No	None	Authorized Users	*				URP: Yes	10	Call Cost Testing
8	Enabled	47*	NDS: 2	FXO On-board Lines: Any Line	None	No	*	PBX		0.1 CCM:Per Minute CCF:0.05		10	

**NDS** - Number of Discarded Symbols      **UES** - Use Extension Settings      **RNSC** - Restrict the Number of Simultaneous Calls      **URP** - Use RTP Proxy  
**AAA** - Authentication, Authorization, Accounting      **CCM** - Cost Calculation Method      **CCF** - Call Completion Fee      **DT** - Date / Time

Figure 77: Call Routing Table (brief view) page

Click **Add** to run **Call Routing Wizard** and configure a new call routing rule. In general, the wizard consists of the following sections:

- [Destination Call Type](#)
- [Call Settings](#)
- [Filter on Source / Modify Caller ID](#)
- [Date / Time Settings](#)
- [Overall Call Duration Limit](#)
- [Calling Rate Settings](#)
- [Tracing / Debug Options](#)
- [Call Alert Settings](#)
- [Summary](#)

## Destination Call Type

This section contains the following components:

- **Enable Record** is used to enable the call routing rule.
- **Destination Number Pattern** is used to specify a template for filtering out the calls that can be routed via respective call routing rule. If destination number of the call matches with a specified pattern, then the call can be completed via respective call routing rule.



- **Number of Discarded Symbols** is used to specify the number of digits/characters/symbols that should be removed from the beginning of the destination number after matching it against **Destination Number Pattern**. Leave the field blank, if nothing needs to be discarded.
- **Prefix** is used to specify the digits/characters/symbols that will be added in front of the destination number after discarding the digits/characters/symbols as described above. Except for single characters or character strings, the following tags can be used for this field:
  - **<callerid:range>** allows to use the caller ID or its part 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 3<sup>rd</sup> digit and up to the end will be assigned to prefix.
  - **<dialnum:range>** allows to use the dialed number or its part as a prefix. **For example:** **<dialnum:1-3>** indicates that the first 3 digits of the dialed number will be as assigned to the prefix, **<dialnum:1-end>** indicates that the dialed number from its 3<sup>rd</sup> digit and up to the end will be assigned to prefix.
  - **aaa,,bbb** allows 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. **For example:** 11,,11018 will call to 11, wait until the call is established, wait for three seconds and then dial/inject 11018. The two-stage dialing is available for FXO, ISDN, and E1/T1 call types.
- **Suffix** is used to specify the digits/characters/symbols that will be added to destination number from the end after discarding the digits/characters/symbols and adding the prefix as described above.
- **Call Type** is used to select the call destination type. The following call types are available:
  - **PBX** – local call to QX extension.
  - **PBX-Voicemail** – call directly to the user extension **Voice Mailbox**.
  - **PBX-Intercom** – call to user extension with request to activate the **Intercom** service.
  - **SIP** – calls through a SIP server.
  - **SIP Tunnel** – calls through an established SIP Tunnel.
  - **IP-PSTN** – calls through the IP-PSTN provider to the global PSTN network.
  - **RTSP** – connection to **RTSP** server. The **Number of Discarded Symbols**, **Prefix** and **Suffix** fields are not available for the **RTSP** call type.
  - **FXO** – calls to the PSTN network either through on-board FXO lines or available shared FXO lines.
  - **ISDN** – calls to the PSTN network either through on-board ISDN trunks or available shared ISDN trunks.
  - **E1/T1** – calls to the PSTN network through available shared E1/T1trunk(s).
- **Metric** is used to set a rating for the routing pattern in a range from **0** to **20**. If no value is set, **10** will be used as the default. If two route entries match the dialed string, the routing pattern with the lower metric will be chosen.
- **Description** is used to enter description, if needed.
- **Enabler Key** and **Disabler Key** are digital codes which should be dialed from handset or auto attendant to enable or disable the routing rule. You can set the same **Enabler/Disabler** key for multiple routing rules (the same key may be used as enabler for one call routing rule, and as a disabler for another one). This will allow to manage several call routing rules with a single key.
  - **Require Authorization for Enabling/Disabling** – if selected, enter **Phone Access Password** after the **Enabler/Disabler** key to pass authorization. **TIP:** If the password has been entered incorrectly for **3** times, no status changes will be applied to any of the call routing rule(s), even to those which have no authorization enabled.

The following options give additional configuration possibilities:

- **Filter on Source / Modify Caller ID** puts a limit on the routing pattern availability for selected caller(s) or allows to modify the caller ID. This option is checked off by default.
- **Date / Time Settings** allows to set a validity period for the routing pattern by setting date/time rules manually or simply assigning a working [schedule](#).

- **Overall Call Duration Limit** allows to control and limit the total calls duration for the routing pattern.
- **Calling Rate Settings** is used to configure calling rate settings.
- **Tracing / Debug Options** allows to enable generating event notifications on the result of using the call routing rule.
- **Call Alert Settings** allows to notify the designated personnel about the emergency calls, as well as calls through the certain call routing rules.

## Call Settings

The content of this section strictly depends on the [Call Type](#) selected on the previous section.

### Call Type – PBX

- **Use RTP Proxy** – if selected, RTP (audio) streams between the peers will be routed through QX. This is applicable when peers are located in different subnets. If not selected, the RTP streams will move directly between peers.
- **Local Authentication** – if selected, the caller(s) will need to pass authentication to make PBX calls.
- **Client Code Identification** – if selected, the **Code Identification** service will be activated. After dialing the destination phone number, the caller may optionally enter \* and then the **Identity Code**. The **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 **Call Detail Reports** (CDRs) and might be used by a billing program for grouping the calls having the same code.
- **Check with 3PCC** is used to request a **3-rd party call control** (3PCC) approval before placing a call through the routing rule. If the checkbox is selected and the routing rule is used to place a call, QX sends a request to the 3PCC application to accept or reject the specific call. The call will be placed if the request is accepted, otherwise it 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 3PCC application.
- **Failover Reason(s)** – the system will use next matching routing pattern(s) to establish the call if the call setup fails due to the failover reasons presented below:
  - **None** – the system will not use next matching routing pattern(s) regardless of the failover.
  - **Busy** – the system will use next matching routing pattern(s) if the dialed destination is busy.
  - **Wrong Number** – the system will use next matching routing pattern(s) if the dialed number is wrong.
  - **Any** – the system will use next matching routing pattern(s) regardless of the failover reason.

**Note:** The above-mentioned configuration settings (options) are available and applicable for other call types.

### Call Type – PBX-Voicemail

**Voice Mail Profile** is used to define the custom **Voice Mail Profile** name to activate custom **Voice Mail Settings** on the extension. If the extension does not have a profile specified here or the specified profile name is incorrect, the default profile will be used.

**Note:** Other settings (options) are the same as for [Call Type – PBX](#).

### Call Type – PBX Intercom

**Play audible signal before Intercom activation** – if selected, the audible signal will be played once **Intercom** service is activated.

**Note:** Other settings (options) are the same as for [Call Type – PBX](#).

## Call Type – SIP

- **Use Extension Settings** is used to select the extension (user extension or auto attendant) the call will be placed from. **SIP settings** of the selected extension will be used as caller information. If nothing is selected from the list, the original caller information will be kept.
- **Keep Original Caller ID** – if selected, the called destination will receive the original caller information.
- **Add Remote Party ID** – if selected, the **Remote Party ID** parameter will be added in the outgoing **Invite** message.
- **Destination Host** is the IP address or hostname of the destination (for a direct call) or SIP server (for calls through the SIP server). **TIP:** This field is renamed to **Modified Destination Host** if the configured **Destination Number Pattern** contains "@" symbol.
- **Destination Port** is the port number of the destination or the SIP server. **TIP:** This field is renamed to **Modified Destination Port** if the configured **Destination Number Pattern** contains "@" symbol.
- **Username** and **Password** are used to set the authentication parameters for the SIP server if needed.
- **Restrict the Number of Simultaneous Calls** is used to restrict the number of simultaneous calls to the SIP server with the same username. **Allowed Call Count** is used to set the number of simultaneous calls.
- **Use RTP Proxy** – if selected, RTP (audio) streams between the peers will be routed through QX. This is applicable when peers are located in different subnets. If not selected, the RTP streams will move directly between peers.
- **Single Call Duration Limit** is used to limit the duration of the call placed through the routing rule. **Maximum Duration** is used to set the maximum duration of the call. The call will be disconnected without prior notice if the maximum duration is reached.
- **Local Authentication** – if selected, the caller(s) will need to pass authentication to make SIP calls.
- **Client Code Identification** – if selected, the **Code Identification** service will be activated. After dialing the destination phone number, the caller may optionally enter \* and then the **Identity Code**. The **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 CDRs and might be used by a billing program for grouping the calls having the same code.
- **Check with 3PCC** is used to request a 3PCC approval before placing a call through the routing rule. If the checkbox is selected and the routing rule is used to place a call, QX sends a request to the 3PCC application to accept or reject a specific call. The call will be placed if the request is accepted, otherwise it 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 3PCC application.
- **Failover Reason(s)** – the system will use next matching routing pattern(s) to establish a call if the call setup fails due to the failover reasons presented below:
  - **None** – the system will not use next matching routing pattern(s) regardless of the failover.
  - **Busy** – the system will use next matching routing pattern(s) if the dialed destination is busy.
  - **Wrong Number** – the system will use next matching routing pattern(s) if the dialed number is wrong.
  - **Network Failure** – the system will use next matching routing pattern(s) in case of system overload, network failure or timeout expiration.
  - **Other** – the system will use next matching routing pattern(s) in case of **Server Failure Responses** (5xx messages) and **Global Failure Responses** (6xx messages).
  - **Any** – stands for all failure reasons mentioned in the **Failover Reason(s)** group.
- **Enable Failover Timeout** is used to set the period after which the call can be considered as failed (SIP response message isn't received). The **Failover Timeout** is used to set the timeout duration (in the range from 1 to 180 seconds). The call will be established through next matching routing pattern(s) after the timeout expires if the failover reason is enabled for the call routing rule.

- **SIP Privacy** is used to select the security level 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** – if selected, no QX specific SIP privacy will be applied, and all privacy will be relied on the configuration of the SIP server.
  - **Disable Privacy** – if selected, SIP call security will be disabled, all headers of the SIP message will be transparently visible to the destination.
  - **Enable Privacy** – if selected, QX specific SIP privacy will be applied. Selection enables a group of checkboxes to choose the key headers to be fully or partly hidden or replaced. The **Require Privacy** option is used to restrict the delivery of the SIP message if either of the selected headers cannot be hidden (or replaced, depending on the configuration of the SIP server) before being sent to destination.
- **Transport Protocol for SIP messages** is used to select the transport protocol (UDP, TCP or TLS) for transmitting the SIP messages.

### Call Type – SIP Tunnel

**SIP Tunnel** is used to select the SIP tunnel to route the calls through tunnel to the remote QX device (QX IP PBXs and QX Gateways).

**Note:** Other settings (options) are the same as for [Call Type – SIP](#).

### Call Type – IP-PSTN

**Note:** Settings (options) are the same as for [Call Type – SIP](#).

### Call Type – RTSP

- **RTSP URI** is used to define the RTSP server URI for receiving stream(s). Audio and video streams are available depending on RTSP server configuration.
- **Username** and **Password** are used to set the authentication parameters for RTSP server if needed.

**Note:** Other settings (options) are the same as for [Call Type – SIP](#).

### Call Type – FXO

- **FXO Lines to Use** – a group of radio buttons allowing to select whether a specific or any available FXO line will be used to route the call. The following options are available:
  - **None** – selection means no **on-board** (local) FXO lines will be used to route the call.
  - **Any Line** – the call will be established through the first available **on-board** FXO line.
  - **Specific Line** – the call will be established only through the selected **on-board** FXO line.

If QXFXO4 gateway is connected to QX in **share** mode, the following options will be available:

- **Any Available Line** – the call will be established through the first available **on-board** FXO line, then through **shared** FXO lines.
- **Any Line@** – the call will be established through the first available **shared** FXO line.
- **Specific Line@** – the call will be established only through a selected **shared** FXO line.
- **FXO Lines Load Balancing** is used to enable load balancing mechanism on FXO lines.
  - **None** – the system will not apply load balancing mechanism and the call will be routed through the first available FXO line (among the selected ones).
  - **Round Robin** – the system will apply load balancing mechanism according to internally gained statistics of most used FXO lines, the call will be routed to the less used and currently available FXO line (among the selected ones).

- **Single Call Duration Limit** is used to limit the duration of the call placed through the routing rule. **Maximum Duration** is used to set the maximum duration of the call. The call will be disconnected without prior notice if the maximum duration is reached.
- **Local Authentication** – if selected, caller(s) will need to pass authentication to make FXO calls.
- **Client Code Identification** – if selected, the **Code Identification** service will be activated. After dialing the destination phone number, the caller may optionally enter \* and then the **Identity Code**. The **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 CDRs and might be used by a billing program for grouping the calls having the same code.
- **Check with 3PCC** is used to request a 3PCC approval before placing a call through the routing rule. If the checkbox is selected and the routing rule is used to place a call, QX sends a request to the 3PCC application to accept or reject a specific call. The call will be placed if the request is accepted, otherwise it 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 3PCC application.
- **Failover Reason(s)** – the system will use next matching routing pattern(s) to establish a call if the call setup fails due to the failover reasons presented below:
  - **None** – the system will not use next matching routing pattern(s) regardless of the failover.
  - **Cannot Establish Connection** – the system will use next matching routing pattern(s) if the connection cannot be established.
  - **Any** – the system will use next matching routing pattern(s) regardless the failover reason.

### Call Type – ISDN

- **Keep Original Caller ID** – if selected, the called party will receive the original caller information (mobile number, PSTN/SIP number, etc.) instead of extension information when call(s) are forwarded.
- **ISDN Trunks to Use** is used to select a specific or any available trunk to route the call(s). The following options are available only for QXISDN4+:
- **Any Trunk(User)** – calls will be established through any ISDN trunk running in **User** mode.
- **Any Trunk(Network)** – calls will be established through any ISDN trunk running in **Network** mode.
- **ISDN Trunk#** – calls will be established through the selected ISDN trunk.

If QXISDN4 gateway is connected to the QX in **share** mode, the following options will be available:

- **Any Trunk(User)@Any** – calls will be established through the first available **on-board** ISDN trunk running in **User** mode, then through shared ISDN trunks (running in **User** mode).
- **Any Trunk(Network)@Any** – calls will be established through the first available **on-board** ISDN trunk running in **Network** mode, then through shared ISDN trunks (running in **Network** mode).
- **ISDN Trunk@** – calls will be established through the selected **shared** ISDN trunk.
- **Any Trunk(User)@** – calls will be established through the first available **shared** ISDN trunk running in **User** mode.
- **Any Trunk(Network)@** – calls will be established through the first available **shared** ISDN trunk running in **Network** mode.
- **Collect Call** is used when the calling party wants to place a call at the called party's expense. This service is applicable only if the **Collect Call** service is enabled on both calling and called party.
- **Single Call Duration Limit** is used to limit the duration of the call placed through the routing rule. **Maximum Duration** is used to set the maximum duration of the call. The call will be disconnected without prior notice if the maximum duration is reached.
- **Local Authentication** – if selected, the caller(s) will need to pass authentication to make ISDN calls.
- **Client Code Identification** – if selected, the **Code Identification** service will be activated. After dialing the destination phone number, the caller may optionally enter \* and then the **Identity Code**. The **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 CDRs and might be used by a billing program for grouping the calls having the same code.

- **Check with 3PCC** is used to request a 3PCC approval before placing a call through the routing rule. If the checkbox is selected and the routing rule is used to place a call, QX sends a request to the 3PCC application to accept or reject a specific call. The call will be placed if the request is accepted, otherwise it 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 3PCC application.
- **Failover Reason(s)** – the system will use next matching routing pattern(s) to establish a call if the call setup fails due to the failover reasons presented below:
  - **None** – the system will not use next matching routing pattern(s) regardless of the failover.
  - **Cannot Establish Connection** – the system will use next matching routing pattern(s) if the connection cannot be established.
  - **Any** – the system will use next matching routing pattern(s) regardless the failover reason.

**Note:** Additional wizard section will be available for ISDN call type to configure trunk timeslots.

- **Select Timeslots** is used to select timeslot(s) which will be used for placing ISDN calls.

### Call Type – E1/T1

QX IP PBXs don't have on-board E1/T1 trunks. The E1T1 call type becomes available when QXE1T1 gateway is connected to QX in share mode.

- **Keep Original Caller ID** – if selected, the called party will receive the original caller information (mobile number, PSTN/SIP number, etc.) instead of extension information when the call(s) are forwarded.
- **E1/T1 Trunks to Use** is used to select a specific E1/T1 trunk to route the call(s). The following option is available:
  - **E1/T1 Trunk1@** – the calls will be established through the selected E1/T1 trunk.
- **Collect Call** is used when the calling party wants to place a call at the called party's expense. This service is applicable only if the **Collect Call** service is enabled on both calling and called party.
- **Single Call Duration Limit** is used to limit the duration of the call placed through the routing rule. **Maximum Duration** is used to set the maximum duration of the call. The call will be disconnected without prior notice if the maximum duration is reached.
- **Local Authentication** – if selected, the caller(s) will need to pass authentication to make E1/T1 call.
- **Client Code Identification** – if selected, the **Code Identification** service will be activated. After dialing the destination phone number, the caller may optionally enter \* and then the **Identity Code**. The **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 CDRs and might be used by a billing program for grouping the calls having the same code.
- **Check with 3PCC** is used to request a 3PCC approval before placing a call through the routing rule. If the checkbox is selected and the routing rule is used to place a call, QX sends a request to the 3PCC application to accept or reject a specific call. The call will be placed if the request is accepted, otherwise it 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 3PCC application.
- **Failover Reason(s)** – the system will use next matching routing pattern(s) to establish a call if the call setup fails due to the failover reasons presented below:
  - **None** – the system will not use next matching routing pattern(s) regardless of the failover.
  - **Cannot Establish Connection** – the system will use next matching pattern(s) if the connection cannot be established.
  - **Any** – the system will use next matching routing pattern(s) regardless of the failover reason.

**Note:** Additional wizard section will be available for E1/T1 call type to configure trunk timeslots.

- **Select Timeslots** is used to select timeslot(s) which will be used for placing E1/T1 calls.
  - Up to **30** timeslots will be available for placing **E1** calls regardless of the signaling type of trunk.
  - Up to **23** timeslots will be available for placing **T1** calls if the trunk signaling type is **CCS**.
  - Up to **24** timeslots will be available for placing **T1** calls if the trunk signaling type is **CAS**.

### Radius Authentication and Authorization

The **RADIUS Authentication** and **Authorization** options are available for the routing pattern regardless of **Destination Call Type**, if the **RADIUS Client** is enabled.

- **RADIUS Authentication and Authorization** is used to make the caller pass authentication through the **RADIUS server** to make calls.
- **RADIUS Accounting** is used to send the **CDRs** of the calls made through the call routing rule to the **RADIUS server**.

### Filter on Source / Modify Caller ID

The following settings (options) are available:

- **Source Filter** is used to limit the routing pattern availability for selected caller(s).
  - **Source Number Pattern** is used to enter the caller address the routing pattern will be available for.
  - **Source Type** is used to select the caller source type. The following options are available:
    - ◆ **Any** – any caller will be able to make calls regardless of caller source type.
    - ◆ **PBX** – only PBX extensions will be able to make calls. **TIP:** The **Class of Service** section will become available to select **Class of Service(s)**.
    - ◆ **SIP** – only inbound SIP callers will be able to make calls. **TIP:** The **Source Filter** section will become available to configure **Source Host** address (IP address or hostname).
    - ◆ **SIP\_Tunnel** – only inbound callers from the selected SIP\_Tunnel will be able to make calls. **TIP:** **Source Filter** section will become available to select **Inbound SIP Tunnel**.
    - ◆ **FXO** – only inbound FXO callers will be able to make calls. **TIP:** The **Source Filter** section will become available to select **Port ID** for FXO call type.
    - ◆ **ISDN** – only inbound ISDN caller(s) will be able to make calls. **TIP:** The **Source Filter** section will become available to select **Port ID** for ISDN call type.
    - ◆ **E1/T1** – only inbound E1/T1 caller(s) will be able to make calls. **TIP:** The **Source Filter** section will become available to select **Port ID** for E1/T1 call type.

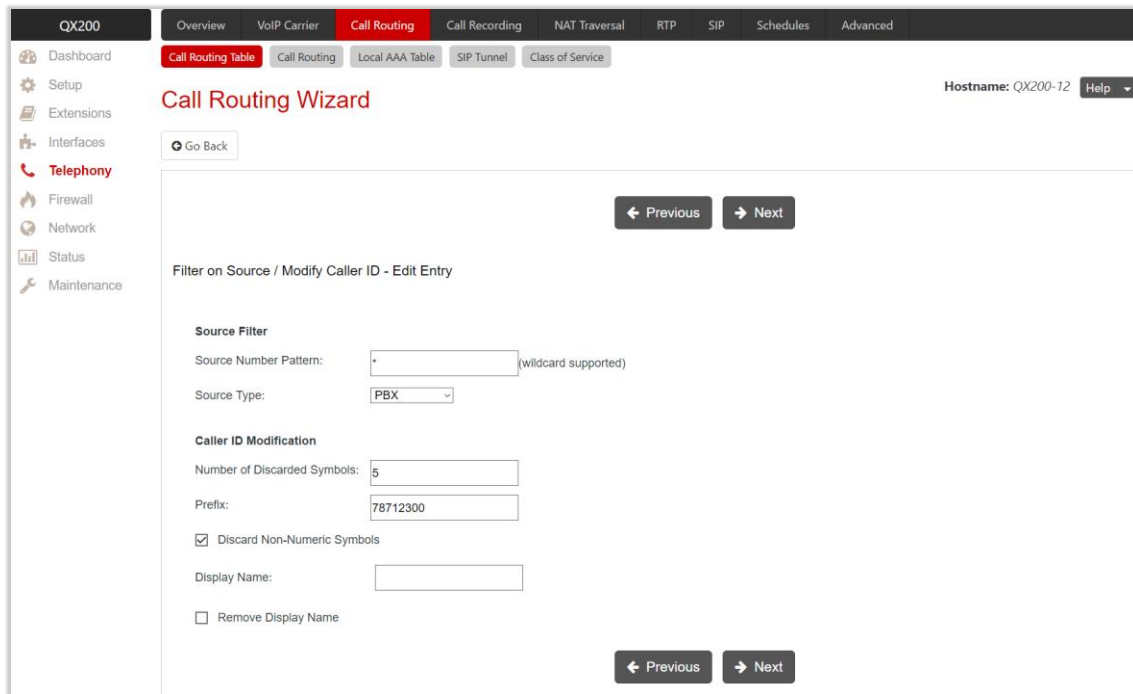


Figure 78: Filter on Source / Modify Caller ID section

- **Caller ID Modification** is used to modify the **Caller ID** before sending them to remote party.
  - **Number of Discarded Symbols** is used to specify the number of digits/characters/symbols that should be discarded from the beginning of the **Source Number Pattern**. Leave the field blank if there is no need to discard the digits.
  - **Prefix** is used to specify the digits/characters/symbols that will be placed in front of the **Source Number Pattern**.
  - **Discard Non-Numeric Symbols** is used to discard any non-numeric symbols/characters from the **Source Number Pattern**.
  - **Display Name** is used to replace an original **Caller ID** with the custom display name.
  - **Remove Display Name** is used to remove **Caller ID**.

### Date / Time Settings

This section is used to set a validity period(s) for the routing pattern.



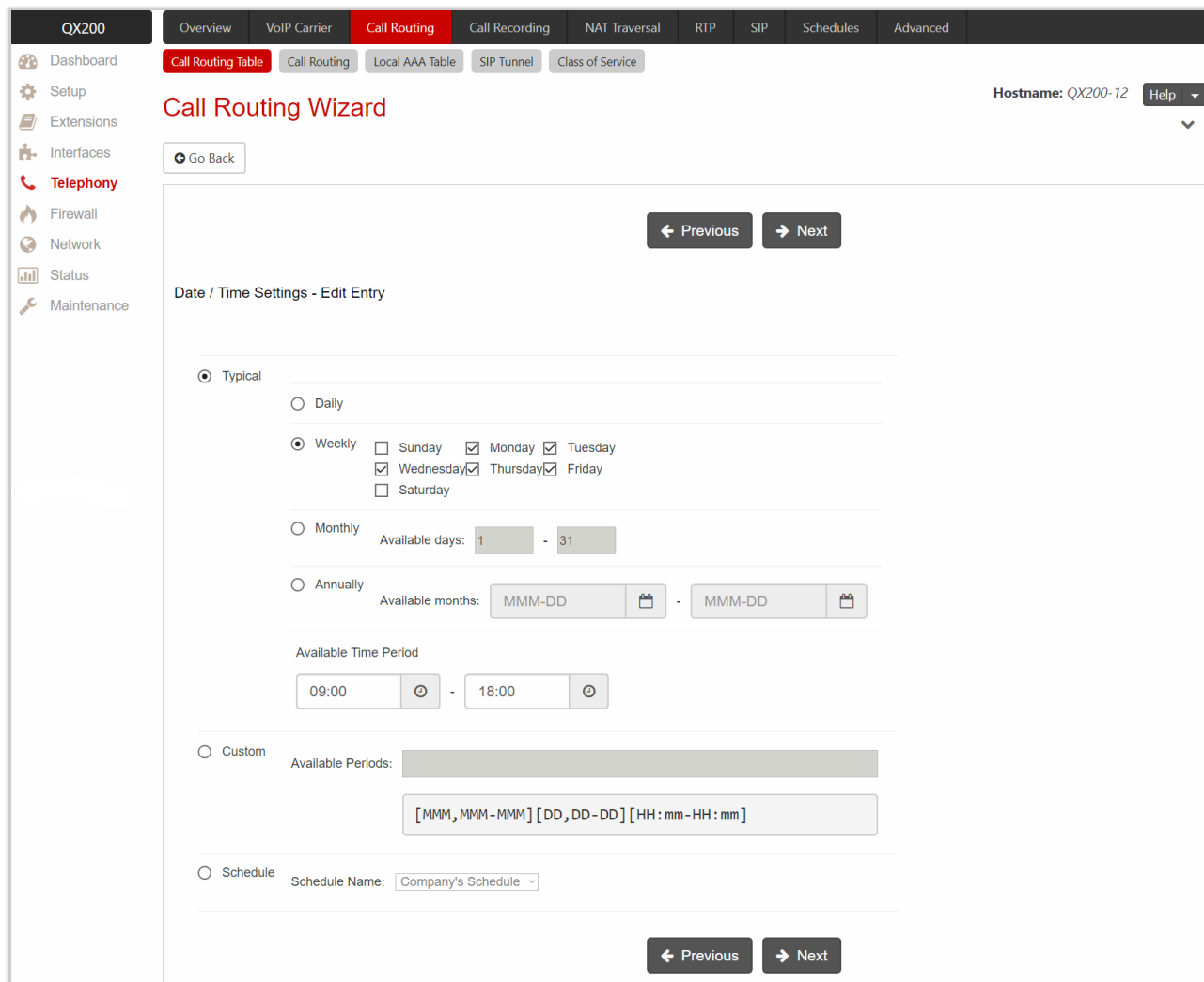


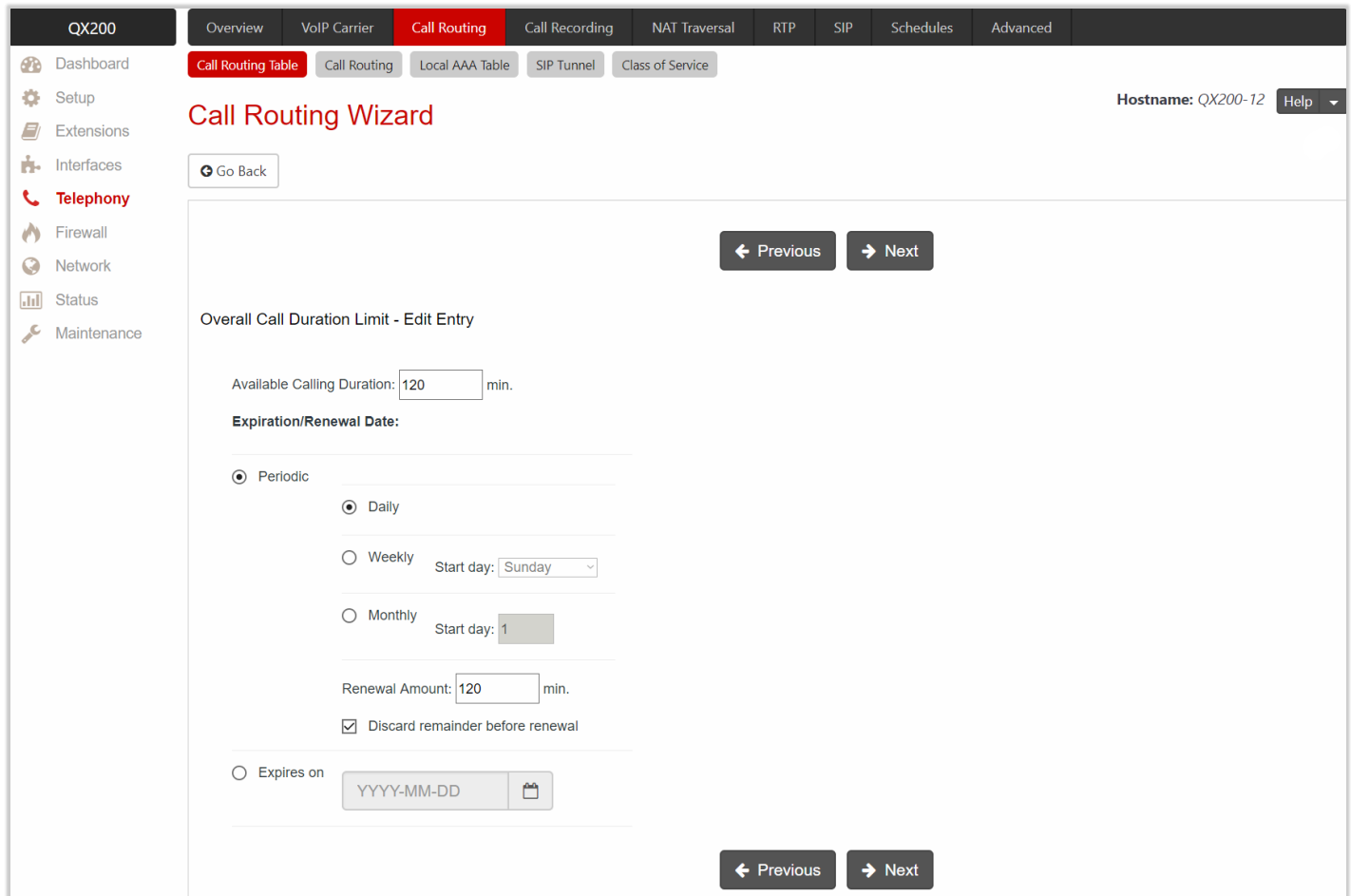
Figure 79: Date / Time Settings section

The following settings (options) are available:

- **Typical** is used to select one of the **validity** periods:
  - **Daily** – the routing pattern will be available for each day.
  - **Weekly** – the routing pattern will be available for the selected weekday(s).
  - **Monthly** – the routing pattern will be available for the selected day(s) in each month.
  - **Annually** – the routing pattern will be available for the selected day(s) and month(s) for each year.
  - **Available Time Period** is used to set the validation time range for the routing pattern.
- **Custom** is used to manually set the validity period(s). **TIP:** The entered values need to be in the following format: [MMM,MMM-MMM][DD,DD-DD][HH:mm-HH:mm]
- **Schedule** is used to apply one of the configured [schedules](#) to the routing pattern. Select the desired schedule from the **Schedule Name** drop-down list.

## Overall Call Duration Limit

This section is used to limit and control the total duration of calls through the routing pattern.



The screenshot shows the 'Overall Call Duration Limit - Edit Entry' configuration page in the QX200 web interface. The page is part of the 'Call Routing Wizard' and includes the following elements:

- Navigation:** A top navigation bar with tabs for 'Overview', 'VoIP Carrier', 'Call Routing' (selected), 'Call Recording', 'NAT Traversal', 'RTP', 'SIP', 'Schedules', and 'Advanced'. Below this, there are sub-tabs for 'Call Routing Table', 'Call Routing', 'Local AAA Table', 'SIP Tunnel', and 'Class of Service'. A 'Go Back' button is located at the top left of the main content area.
- Page Information:** The hostname 'QX200-12' and a 'Help' dropdown menu are displayed in the top right corner.
- Form Fields:**
  - Available Calling Duration:** A text input field containing '120' followed by 'min.'.
  - Expiration/Renewal Date:** A section with a radio button selected for 'Periodic'. Under this, there are three options:
    - Daily:** A radio button selected.
    - Weekly:** A radio button with a 'Start day' dropdown menu set to 'Sunday'.
    - Monthly:** A radio button with a 'Start day' input field containing '1'.
  - Renewal Amount:** A text input field containing '120' followed by 'min.'.
  - Discard remainder before renewal:** A checked checkbox.
  - Expires on:** A radio button with a date input field showing 'YYYY-MM-DD' and a calendar icon.
- Navigation Buttons:** 'Previous' and 'Next' buttons are located at the top and bottom right of the main content area.

Figure 80: Overall Call Duration Limit section

The following settings (options) are available:

- **Available Calling Duration** is used to set the total duration for the calls through the selected call routing rule. Once **Available Calling Duration** expires, the current call will be disconnected without prior notice. Placing new calls through this rule is not possible until **Available Calling Duration** is not updated either manually or automatically by **Renewal Date** and **Amount**.
- **Periodic** is used to select one of the **Renewal Date** options:
  - **Daily** – the defined **Available Calling Duration** will be renewed every day.
  - **Weekly** – the defined **Available Calling Duration** will be renewed every week on a specified weekday.
  - **Monthly** – the defined **Available Calling Duration** will be renewed every month on a specified day.
  - **Renewal Amount** is used to set the renewal amount to be added to the available calling duration when the expiration date of **Available Calling Duration** is reached. Leave the field blank, if you don't need to renew **Available Calling Duration**.
  - **Discard remainder before renewal** is used to discard the remainder of **Available Calling Duration** before renewal and set **Renewal Amount** as new **Available Calling Duration**.
- **Expires on** is used to set the expiration date for **Available Calling Duration**. After **Expiration Date**, the call routing rule becomes unavailable and it is impossible to place a new call until this field is updated.

## Calling Rate Settings

This section is used to configure calling rate settings. The following settings (options) are available:

- **Call Completion Fee** is used to set the cost of a single call, regardless of the call duration. The actual cost of the call depends on the cost calculation method.
- **Rate per Minute** is used to set the cost of one minute of call. The actual cost of the call depends on the cost calculation method.
- **Cost Calculation Method** is used to select one of the options:
  - **Per Second** – if this method is selected, the call cost is calculated as:

$$\text{Call Cost} = \text{Call Completion Fee} + \frac{\text{CDIS}}{60} \times \text{CRPM}$$

- **Per Minute** – if this method is selected, the call cost is calculated as:

$$\text{Call Cost} = \text{Call Completion Fee} + \text{Roundup}(\frac{\text{CDIS}}{60}) \times \text{CRPM}.$$

**TIP:** If CRPM is equal to 0, flat fee is charged for the call.

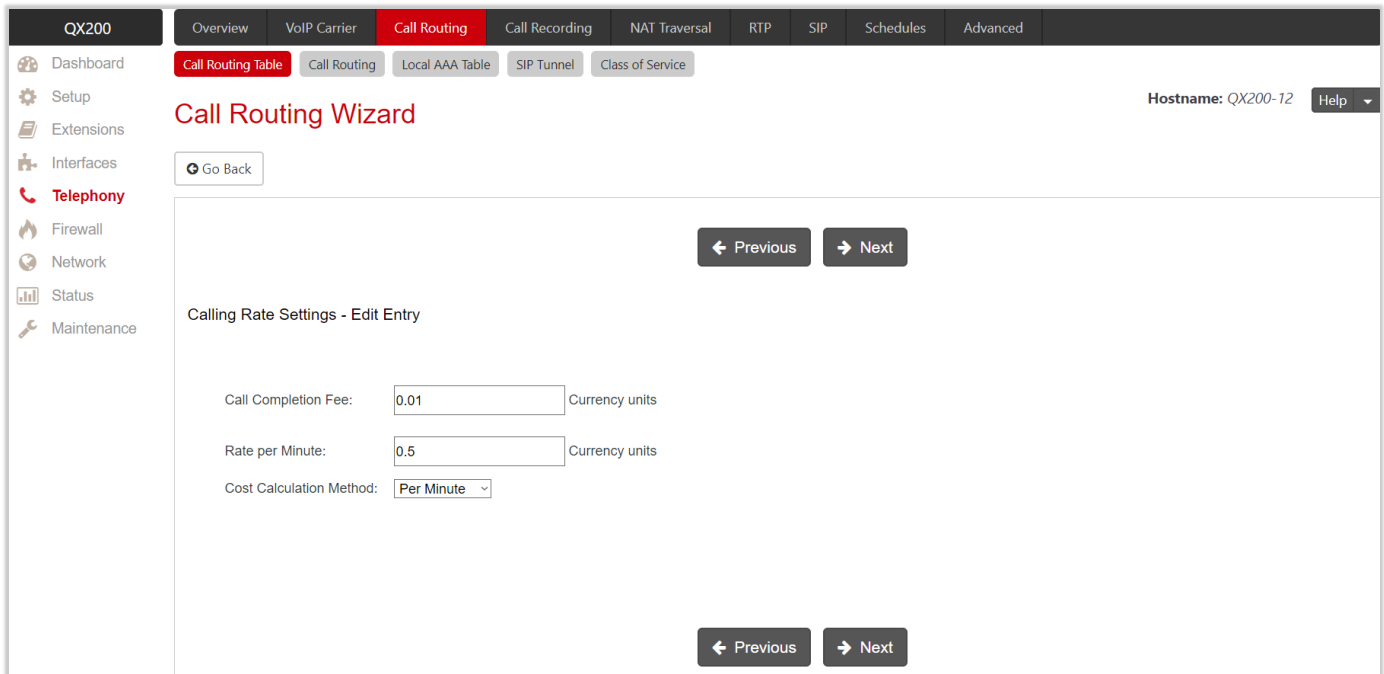


Figure 81: Calling Rate Settings section

The calling credit assigned to extension will be charged in the following scenarios:

- Extension places a call to the destination through a payable routing rule directly.
- Extension transfers incoming call (blind or consultative) to destination through a payable routing rule.
- Extension forwards the call to destination through a payable routing rule automatically.
- Trusted caller uses the **Call Relay** service on auto attendant to make call to destination passing authentication by the extension credentials (number and the password).

### Note:

- The **Calling Rate Settings** section becomes available once **Call Cost** feature is activated.
- The **Calling Rate Settings** is not applicable for PBX, PBX-Voicemail and PBX-Intercom call types.
- The **Single Call Duration Limit** option cannot be used with **Calling Rate Settings**.

## Tracing / Debug Options

These options are used to generate event notifications on a certain execution result for the call routing rule.

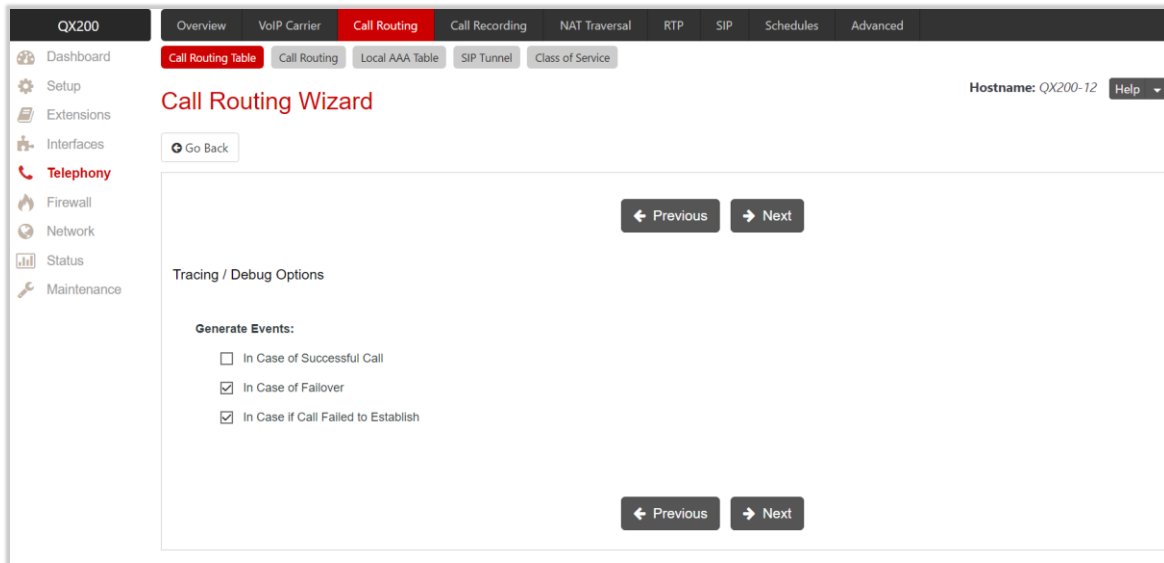


Figure 82: Tracing / Debug Options section

The events will be generated and displayed in the **System Events** for the following cases:

- In Case of Successful Call
- In Case of Fallback
- In Case if Call Failed to Establish

## Call Alert Settings

This section is used to activate the call alert service and configure settings. The **Call Alert** service is used to notify the designated personnel about the emergency calls, as well as calls through certain call routing rules. The following information will be included in the notification: the routing pattern, the extension who placed the call, the dialed number and the call Date/Time.

The following settings (options) are available:

- **Generate System Event** – this option is used to generate and display event notification in the **System Events**.
- **Send Notification via E-mail** – this option is used to send notification to a specified address via e-mail.
- **Send Notification via SMS** – this option is used to send notification to a specified number via SMS.
- **Leave Voice Message** – this option is used to leave voice mail on the defined extension(s) with a voice message.

**Note:** Use commas to separate email addresses, mobile numbers and user extensions in case of multiple entries.

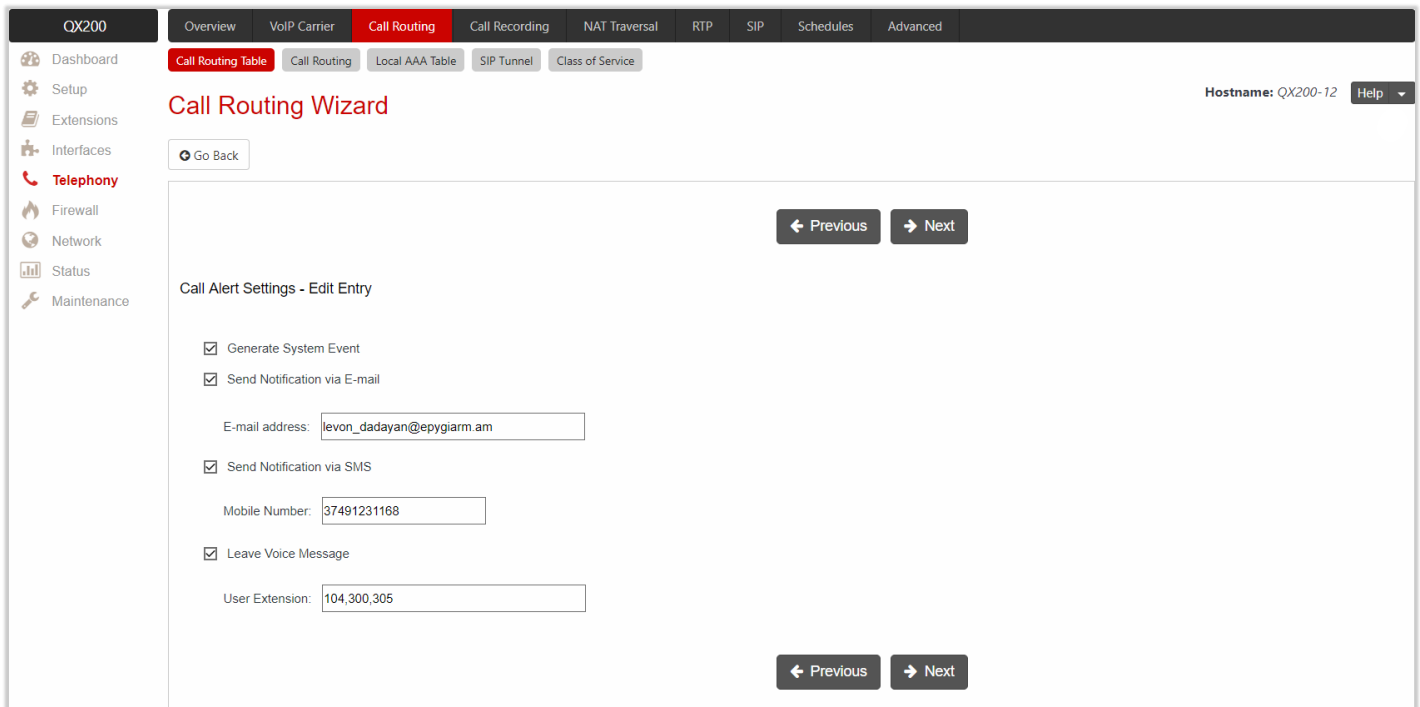


Figure 83: Call Alert Settings section

## Summary

This section displays all configured settings (options) before applying them.

## 8.2.2 Call Routing

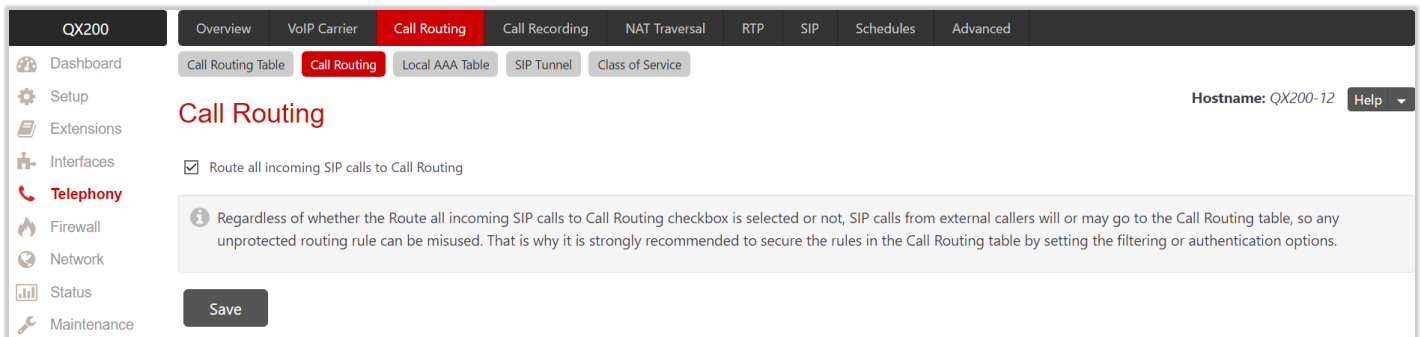


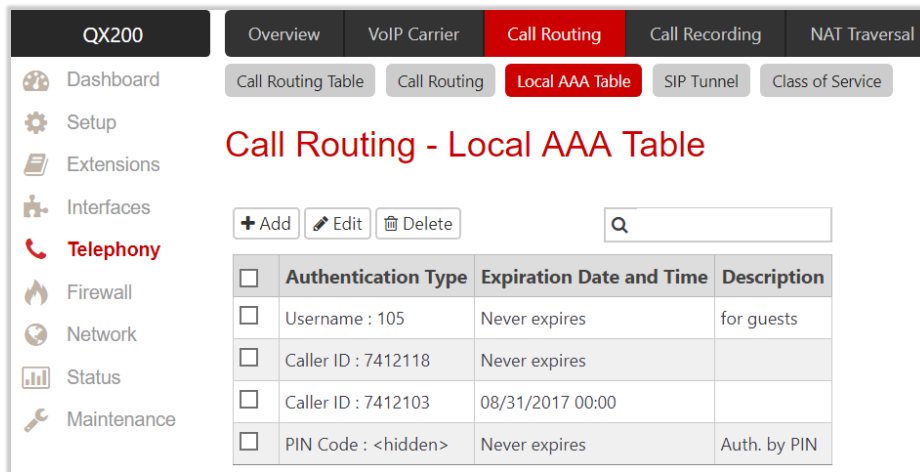
Figure 84: Call Routing page

**Route all incoming SIP calls to Call Routing** – if selected the system will directly look for a matching call routing rule in the **Call Routing Table** and ignore the possible matches with the SIP address of extension (Username or DID Number). Otherwise the system will first try to match the SIP address of extension. If it matches, the incoming call will ring on the extension, otherwise the system will look for a matching call routing rule in the **Call Routing Table**.

**Note:** Regardless of whether **Route all incoming SIP calls to Call Routing** is selected or not, SIP calls from external callers will or may go to the **Call Routing Table**, so any unprotected 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.

## 8.2.3 Local AAA Table

The **Call Routing – Local AAA Table** page is used to configure and manage the local authentication database.



The screenshot shows the 'Call Routing - Local AAA Table' page in the QX200 administration interface. The page title is 'Call Routing - Local AAA Table'. Below the title, there are buttons for '+ Add', 'Edit', and 'Delete', along with a search box. A table with the following data is displayed:

<input type="checkbox"/>	Authentication Type	Expiration Date and Time	Description
<input type="checkbox"/>	Username : 105	Never expires	for guests
<input type="checkbox"/>	Caller ID : 7412118	Never expires	
<input type="checkbox"/>	Caller ID : 7412103	08/31/2017 00:00	
<input type="checkbox"/>	PIN Code : <hidden>	Never expires	Auth. by PIN

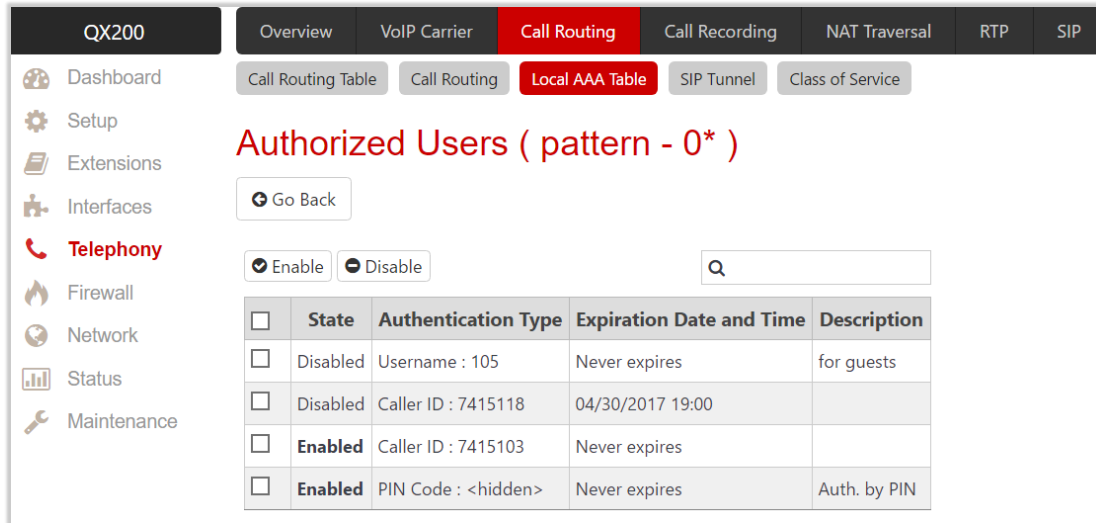
Figure 85: Call Routing - Local AAA Table page

To add a new **AAA** entry:

1. Click **Add** and configure the following information:
2. Select one of the **Authentication** methods.
  - **Authentication by Caller ID** is used to set the authentication based on the caller phone number or SIP address (Username or DID Number). The system will automatically pass the authentication.
  - **Authentication by Login** is used to set the authentication based on the **Username** and **Password** provided by the user upon login.
  - **Authentication by PIN** is used to set the authentication based on the **PIN Code** provided by the user upon login.
3. Configure the **Expiration Date and Time**, if needed.
  - **Expires on** is used to set the expiration date for the configured **AAA** entry.
4. Enter any **Description**, if needed.
5. Click **Save** to add the new **AAA** entry to the **Call Routing – Local AAA** table.

## Authorized Users

If the **Local Authentication** option is enabled on the call routing rule, then the caller should use configured **AAA** entries to pass authentication in order to make calls. The caller will automatically pass authentication if the caller's phone number or SIP address (Username or DID Number) is enabled in the **Authorized Users** table. Otherwise the caller will be asked to login (enter username and password) or enter the **PIN Code**.



<input type="checkbox"/>	State	Authentication Type	Expiration Date and Time	Description
<input type="checkbox"/>	Disabled	Username : 105	Never expires	for guests
<input type="checkbox"/>	Disabled	Caller ID : 7415118	04/30/2017 19:00	
<input type="checkbox"/>	Enabled	Caller ID : 7415103	Never expires	
<input type="checkbox"/>	Enabled	PIN Code : <hidden>	Never expires	Auth. by PIN

Figure 86: Authorized Users

**Note:** Authentication by Login cannot be combined with Authentication by PIN on the same call routing rule.

### 8.2.4 SIP Tunnel

The **SIP Tunneling** feature provides means for building network on QX IP PBXs. This network is based on many "slave" QXs in satellite offices and one or more "master" QXs in the main office(s) with SIP tunnels configured between "slave" and "master" devices. One possible scenario for using SIP Tunneling is routing SIP calls through the remote QX device. Another scenario is building a redundant distributed PBX system based on many slave QXs in satellite offices and two or more master QXs in the main office.

For more information on how to configure and use **SIP Tunnels**, refer to the [SIP Tunneling Feature on QX IP PBXs](#) guide.

### 8.2.5 Class of Service

QX **Class of Service** (CoS) is used to define the permissions that extensions (**User** or **Conference**) will have when using certain call routing rules to make a call.

The CoS provides the ability to set restrictions on the call routing rules for each extension, thus allowing to permit or deny the extensions to use call routing rules

For example, the following restrictions can be applied for extensions:

- **Only Internal** – internal calls to other extensions on the QX are only allowed from this extension(s). Calls to SIP and PSTN are not allowed.
- **Only Local PSTN** – calls to the local PSTN are only allowed from this extension(s).
- **Long-distance IP-PSTN only** – long distance IP-PSTN calls are only allowed from this extension(s).
- **International only** – international calls are only allowed from this extension(s).

The above defined abstract restrictions, they should be implemented as service classes on the call routing patterns in the **Call Routing Table**. For example, to implement the long-distance service class, select all call routing rule on the QX that can be used for making long distance PSTN calls and assign them to the **Long-distance IP-PSTN only CoS**.

Pay close attention to the configuration of call routing rules on QX. To avoid from ambiguities, create a call routing rule for each CoS.

Configure a **CoS** as follows:

1. Assign the specified CoS(s) to a certain call routing rule(s).
2. Assign the specified CoS(s) to the extension (**User** or **Conference**).

**Note:**

- CoS is applicable only for call routing rules with **PBX** source type
- If there is no CoS assigned to the call routing rule, that rule will be generally available for any extension (**User** or **Conference**) whether it is attached to a CoS or not.
- If the **Enable Class of Service** option is disabled, call routing rules that are assigned to a certain CoS(s) will be available for any extension (**User** or **Conference**), if there are no any other filtering limitations.

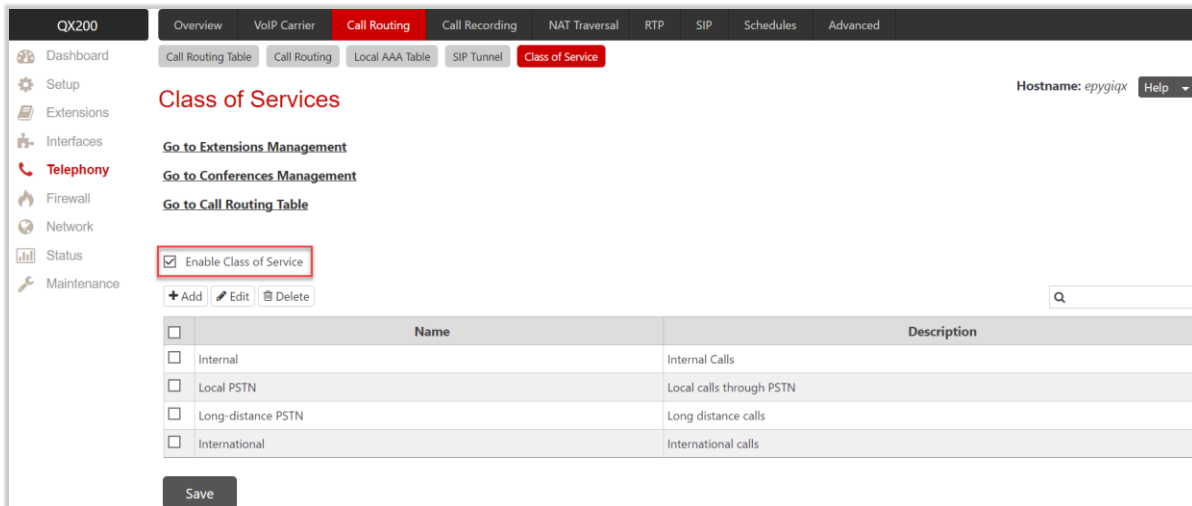


Figure 87: Class of Services page



To create a new **Class of Service** and activate **CoS** functionality:

1. Click the **Add** button.
  - Enter a **Name** for the CoS.
  - Enter a **Description**, if needed.
2. Click **Save** to add the newly created **CoS** to the **Class of Services** table.
3. Tick the **Enable Class of Service** option to activate the **Class of Service** functionality on the QX.

## 8.2.6 Best Matching Algorithm

All calls from QX extensions, as well as some calls from external sources, are being routed in QX according to call routing rules (records) that specify the destination based on the dialed number. When a user dials a number, the QX matches the dialed number against the destination number patterns in call routing records.

- If the dialed number matches only with a single pattern, then the rule with respective pattern will be used to set up the call.
- If multiple patterns have been found to match the dialed number, the system uses the **Best Matching Algorithm** to prioritize the matching patterns.

Once the patterns are prioritized, the rule with the highest priority will be used as a preferred one for call setup. The order of the **call routing rules** is important. The **rule** has a higher priority over those located below in the table. **Move Up** moves the selected rule one level up, increasing the rule priority and the **Move Down** moves the selected rule one level down, decreasing the rule priority.

**Note:** The subsequent prioritized pattern will be used only if the destination specified by a pattern with higher priority is unreachable and the **Failover(s)** is configured.

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 criterion: that is, Criterion 3 is calculated only for patterns that take the same value for Criterion 1 and Criterion 2.

### Criteria list

- **Criterion 1** shows the available asterisks (\*) in a pattern. The patterns without (\*) have a higher priority.
- **Criterion 2** is 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** is the number of matching digits/symbols outside the braces/brackets. The more matching digits outside braces/brackets a pattern contains, the higher its priority. **TIP:** This criterion is only used if several patterns take an equal but non-zero value for **Criterion 2**.
- **Criterion 4** is 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** is the number of question marks (?) outside braces/brackets. The more question marks outside braces/brackets a pattern contains, the higher its priority. **TIP:** This criterion is only used if several patterns take an equal but non-zero value for **Criterion 4**.
- **Criterion 6** is the number of square brackets ([]). The more brackets a pattern contains, the higher its priority.
- **Criterion 7** is the number of braces ({}). The more braces a pattern contains, the higher its priority.
- **Criterion 8** is the number of asterisks (\*). The fewer asterisks a pattern contains, the higher its priority.
- **Criterion 9** is the value of the metric. The lower the metric of a pattern is, the higher its priority.
- **Criterion 10** is the position in the routing table. The higher the position of a pattern in the routing table is, the higher its priority.

**For example:** User dials 1231, the following matching patterns are found in the **Call Routing Table**.

Pattern Position	Routing Pattern
1	*1*
2	123*
3	{11-15}3*
4	?2?1
5	[1-3]*
6	{100-150, asd, \*\?}1
7	1[1-3]3[0-8]
8	123?
9	*2*1
10	*

Table 2: Example – The list of Patterns

**Step 1:** The list is sorted and the patterns with asterisks (\*) are pushed back to the end of the list, due to lower priority (**Criterion 1**).

Position after Step1	Routing Pattern
1	?2?1
2	{100-150, asd, \*\?}1
3	1[1-3]3[0-8]
4	123?
5	*1*
6	123*
7	{11-15}3*
8	[1-3]*
9	*2*1
10	*

Table 3: Example – The list of Patterns after the Step 1

**Step 2:** The list is sorted and the patterns with fewer number of matching digits inside and outside the braces/brackets are pushed back to the end of the list, due to lower priority (**Criterion 2**). The patterns that contain the same number of matching digits are grouped into sub-lists.

Position after Step2	Routing Pattern	Matching Digits
1	1[1-3]3[0-8]	4
2	{100-150, asd, \*\?}1	4
3	123?	3
4	{11-15}3*	3
5	123*	3
6	?2?1	2
7	*2*1	2
8	[1-3]*	1
9	*1*	1
10	*	0

Table 4: Example – The list of Patterns after the Step 2

**Step 3:** Each consecutive criterion is calculated only for the patterns that take the same value for the preceding criterion: that is **Criterion 3** is calculated only for patterns that take the same value for **Criterion 1** and **Criterion 2**.

The list is sorted and the patterns with the fewer number of matching digits outside the braces/brackets are pushed back to the end of the list, due to lower priority (**Criterion 3**).

Position after Step2	Routing Pattern	Matching Digits
1	1[1-3]3[0-8]	2
2	{100-150, asd, \*\?}1	1

Table 5: Example – The list of the Patterns after Step 3

The **Best Matching Algorithm** will stop after executing **Step 3** and the dialed number **1231** will pass through **1[1-3]3[0-8]** routing pattern.

## 8.2.7 Allowed Characters and Wildcards

Below is the complete list of the characters and wildcards supported in the QX. Not all characters and wildcards are supported for all options and settings. Thus, depending on the meaning of the option some limitations can be applied.

### Characters

- **Numbers** – 0...9
- **Letters** – A...Z, a...z
- **Special symbols** – =; +; -; \$; /; ~; \_; -; .; &; (); ' ; ! ; \* ; ? ; { } ; [ ]

### **Note:**

- The symbols (\*, ?, -, ! and ,) should be prefixed with a slash (\) symbol if they are used as ordinary characters; otherwise the system will interpret them as wildcards.
- 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
- [] – a character from the specified set of characters and strings
- **Note:** You can use the wildcard ? within the braces, but not \*.

The following control symbols are used to specify a set:

- Use a comma (,) to separate the elements of a set. **For example:** The pattern is: 9{1,3,11,a}. Numbers matching the pattern will be: 91, 93, 911, 9a. **Note:** No spaces are allowed within braces.
- 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. **For example:** The pattern is: 2{11-15,a-d}5 Numbers matching the pattern will be: 2115, 2125, 2135, 2145, 2155, 2a5, 2b5, 2c5, 2d5.
- Use an exclamation point (!) to exclude a character or a string from a set. **For example:** The pattern is: 2{11-15,a-d,!14,!c}5. Numbers matching the pattern will be: 2115, 2125, 2135, 2145, 2155, 2a5, 2b5, 2d5. **Note:** The exclamation point (!) cannot be used to exclude a range of symbols.

- Use a slash (\) before control symbols (\*, ?, -, ! and ,) to use them as an ordinary character. **For example:** The pattern is: 1\[1-3]. Numbers matching the pattern will be: 1\*1, 1\*2, 1\*3
- Use an at sign (@) to indicate full SIP address (for 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. **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 PBX extension is sip\_number@ip\_address\_of\_QX, e.g. 20233@192.168.35.25), only the sip number part of the pattern will be parsed among other entries with @ symbol in the **Call Routing Table**.

### Allowed SIP Addresses

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

SIP address needs to be entered in one of the following formats:

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

The display name and 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**. The **SIP address** may contain wildcards. 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

## 8.3 Call Recording Settings

The **Call Recording** feature allows to record all inbound and outbound calls, including calls that pass through the QX, keep the recordings locally or send them to the FTP server.

For more information on how to configure and use **Call Recording** feature, refer to the [Call Recording Feature on QX IP PBXs](#) guide.

## 8.4 NAT Traversal

NAT Traversal is divided into separate pages that are used to configure the **General NAT Traversal Settings**, SIP, RTP and STUN parameters for NAT as well as configuring **Exceptions List** for NAT Traversal.

### 8.4.1 General

The **NAT Traversal Settings** page is used to select the NAT Traversal mode which will be used for the SIP traffic. The following modes are available:

- **Automatic** – if selected, the system will analyze the QX WAN IP address. If the address is in the IP range specified for the private networks (according to RFC), the SIP traffic (any incoming and outgoing SIP messages from/to QX) will be routed through the NAT router. Otherwise no SIP traffic will be routed through the NAT router.
- **Force** – if selected, all SIP traffic will be routed through the NAT router.
- **Disable** – if selected, no SIP traffic will be routed through the NAT router.

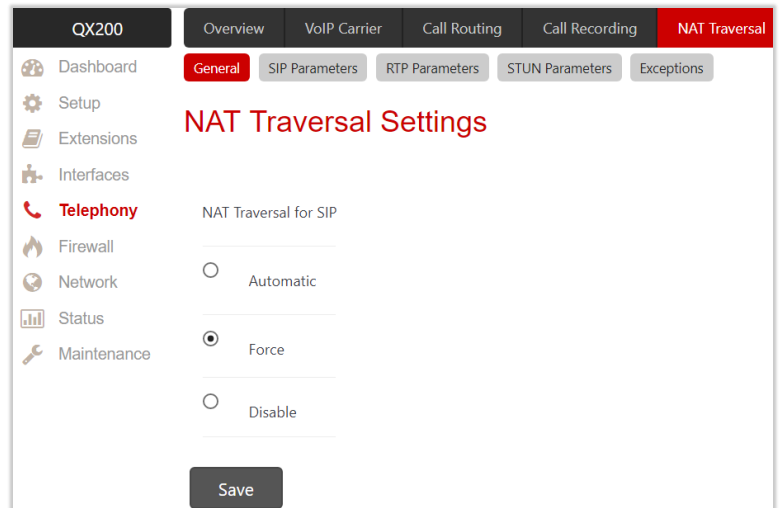


Figure 88: NAT Traversal Settings page

## 8.4.2 SIP Parameters

The **NAT Traversal – SIP Parameters** page is used to configure the NAT specific settings for SIP and offers two independent groups of settings.

The **UDP Parameters** section allows to select the type of connection over NAT as follows:

- **Use STUN** is used to automatically discover the mapped settings for the SIP UDP traffic over NAT. STUN settings are configured on the **STUN Parameters** page.
- **Use Manual NAT Traversal** is used to manually set the mapped settings for the SIP UDP traffic over NAT:
  - **Mapped Host** is used to set the IP address of the mapped host for SIP UDP traffic over NAT.
  - **Mapped Port** is used to set the port number on the mapped host for the SIP UDP traffic over NAT.

The **TCP/TLS Parameters** section allows to set TCP/TLS ports for the connection over NAT as follows:

- **Mapped TCP Host** is used to set the IP address of the mapped host for SIP TCP traffic over NAT.
- **Mapped TCP Port** is used to set the port number on the mapped host for the SIP TCP traffic over NAT.
- **Mapped TLS Host** is used to set the IP address of the mapped host for SIP TLS traffic over NAT.
- **Mapped TLS Port** is used to set the port number on the mapped host for the SIP TLS traffic over NAT.

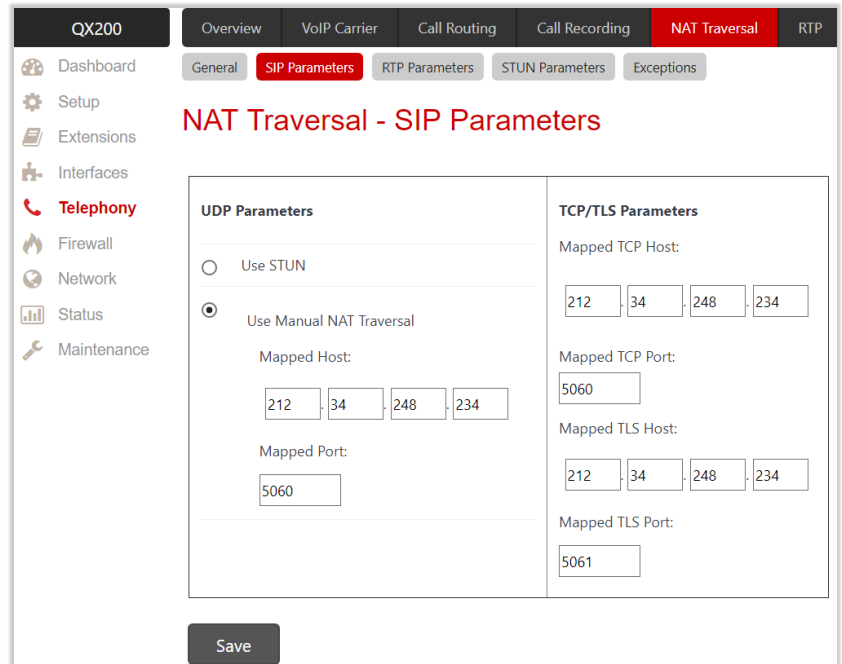


Figure 89: NAT Traversal – SIP Parameters page

### 8.4.3 RTP Parameters

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

- **Use STUN** is used to automatically discover the mapped settings for the RTP UDP traffic over NAT. STUN settings are configured on the **STUN Parameters** page.
- **Use Manual NAT Traversal** is used to manually define the RTP/RTCP port ranges for the RTP traffic over NAT:
  - **Mapped Host** is used to set the mapped host IP address for RTP traffic over NAT.
  - **Min** and **Max** are used to set the port numbers on the mapped host for RTP and RTSP traffic.

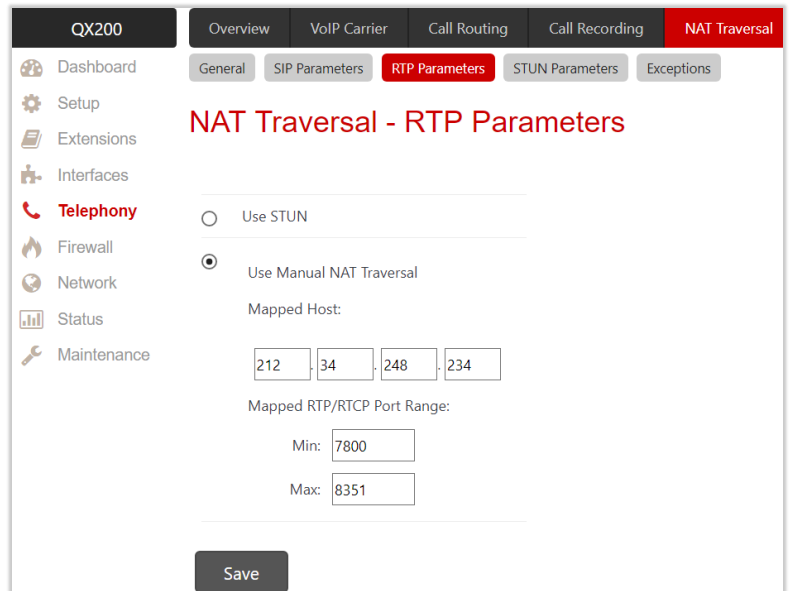


Figure 90: NAT Traversal – RTP Parameters page

### 8.4.4 STUN Parameters

The **NAT Traversal – STUN Parameters** page is used to enable automatic NAT configuration through the STUN server and is used to configure the STUN client on QX as follows:

- **Primary STUN Server** is used to set the STUN server hostname or IP address.
- **Primary STUN Port** is used to set the STUN server port number.
- **Secondary STUN Server** and **Secondary STUN Port** are used to set the respective parameters of the secondary STUN server.
- **Polling Interval** is used to select the possible time intervals between referrals to the STUN server.
- **Keep-alive Interval** is used to set the time interval for keeping NAT mapping alive.
- **NAT IP checking Interval** is used to set the interval between the NAT IP checking attempts (used to distinguish the possible NAT IP address changes and to perform registration on the new host).

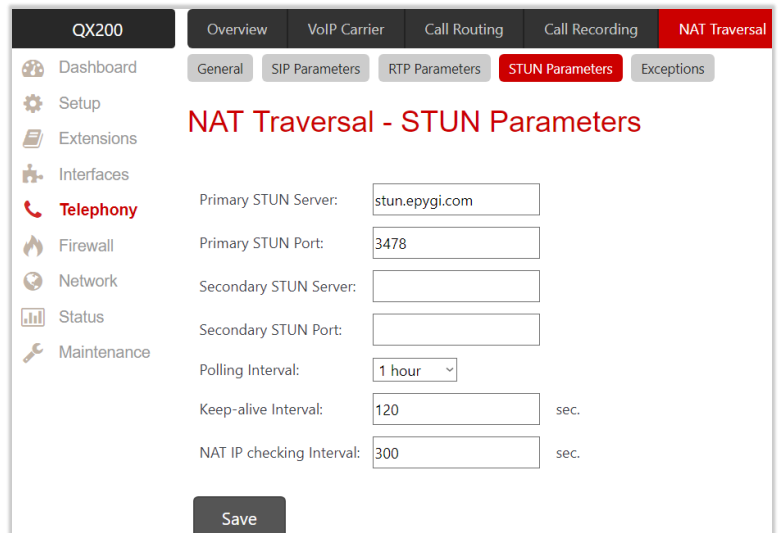
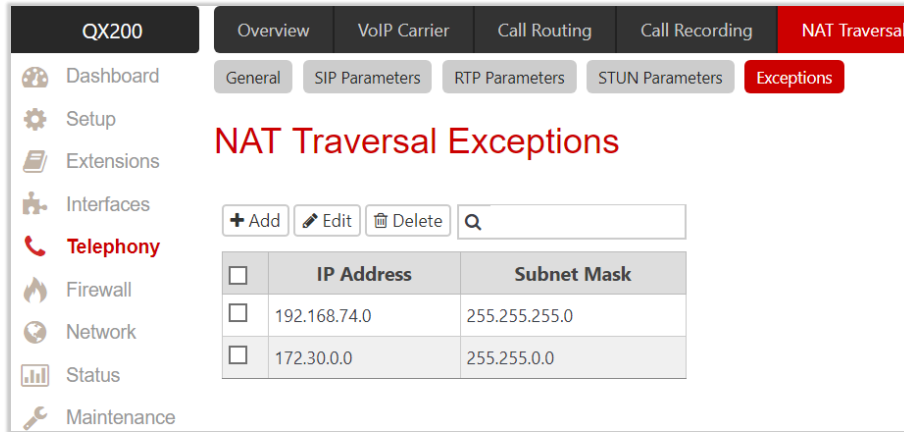


Figure 92: NAT Traversal – STUN Parameters page

## 8.4.5 Exceptions

The **NAT Traversal Exceptions** page displays all possible IP ranges that are not included in the NAT process. IP addresses that are not listed in the **NAT Traversal Exceptions** are accessed over NAT. For example, if a QX user needs to make SIP calls within the local network as well as outside that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table.



	IP Address	Subnet Mask
<input type="checkbox"/>	192.168.74.0	255.255.255.0
<input type="checkbox"/>	172.30.0.0	255.255.0.0

Figure 93: NAT Traversal Exceptions page

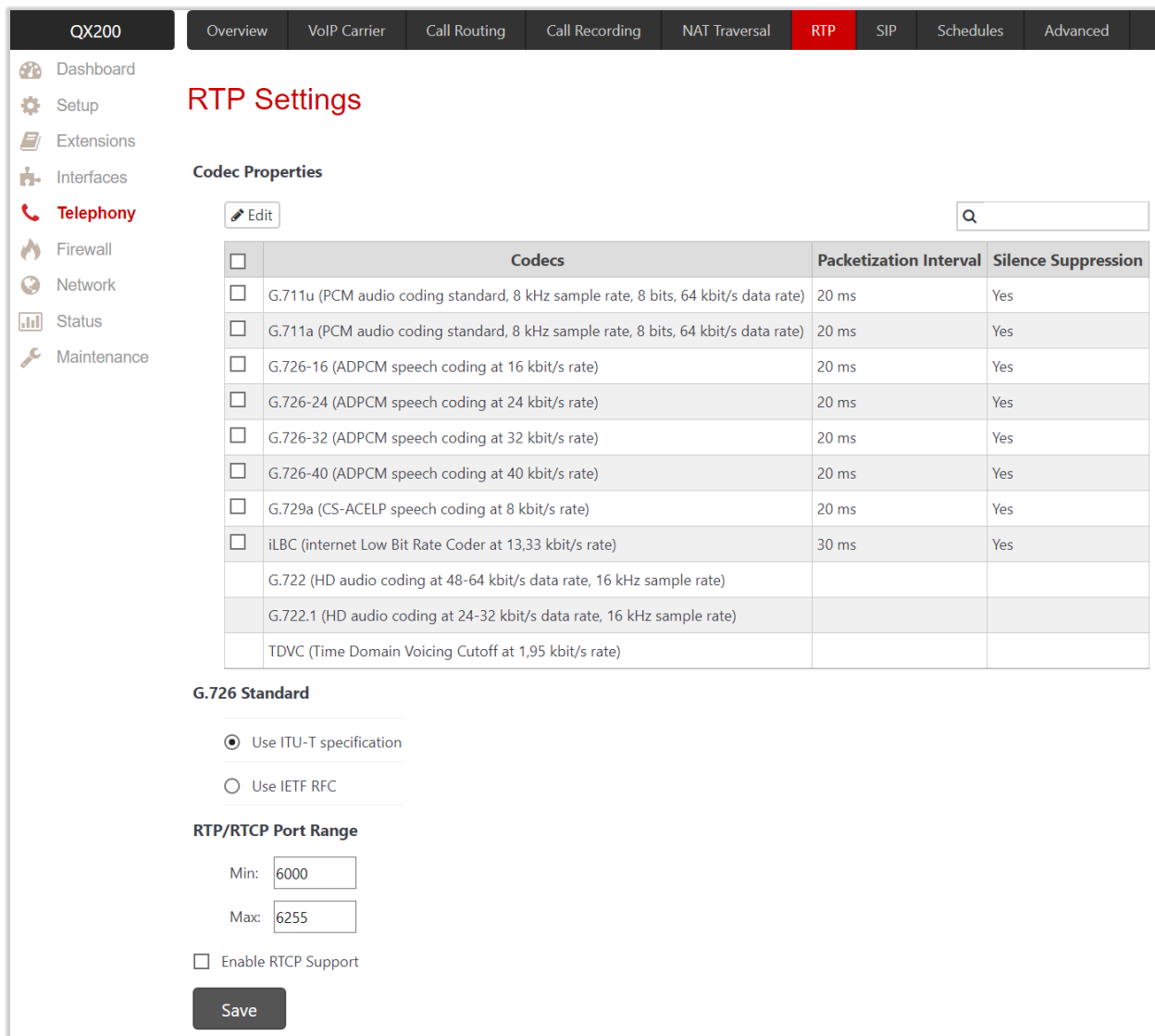
To add a new **exception**:

1. Click **Add** and enter the following information:
  - Enter the **IP Address**.
  - Enter the **Subnet Mask**. **TIP:** Enter **255.255.255.255** as a Subnet Mask to add only the IP address in exception list.
2. Click **Save** to add the new exception entry to the **NAT Traversal Exceptions** table.

## 8.5 RTP

The **RTP Settings** page is used to configure the packet size and silence suppression for each voice codec. The **Codec Properties** table lists all codecs with the packetization interval and silence suppression associated to each.





**RTP Settings**

**Codec Properties**

<input type="checkbox"/>	Codecs	Packetization Interval	Silence Suppression
<input type="checkbox"/>	G.711u (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)	20 ms	Yes
<input type="checkbox"/>	G.711a (PCM audio coding standard, 8 kHz sample rate, 8 bits, 64 kbit/s data rate)	20 ms	Yes
<input type="checkbox"/>	G.726-16 (ADPCM speech coding at 16 kbit/s rate)	20 ms	Yes
<input type="checkbox"/>	G.726-24 (ADPCM speech coding at 24 kbit/s rate)	20 ms	Yes
<input type="checkbox"/>	G.726-32 (ADPCM speech coding at 32 kbit/s rate)	20 ms	Yes
<input type="checkbox"/>	G.726-40 (ADPCM speech coding at 40 kbit/s rate)	20 ms	Yes
<input type="checkbox"/>	G.729a (CS-ACELP speech coding at 8 kbit/s rate)	20 ms	Yes
<input type="checkbox"/>	iLBC (internet Low Bit Rate Coder at 13,33 kbit/s rate)	30 ms	Yes
<input type="checkbox"/>	G.722 (HD audio coding at 48-64 kbit/s data rate, 16 kHz sample rate)		
<input type="checkbox"/>	G.722.1 (HD audio coding at 24-32 kbit/s data rate, 16 kHz sample rate)		
<input type="checkbox"/>	TDVC (Time Domain Voicing Cutoff at 1,95 kbit/s rate)		

**G.726 Standard**

Use ITU-T specification

Use IETF RFC

**RTP/RTCP Port Range**

Min:

Max:

Enable RTCP Support

Figure 94: RTP Settings page

To modify the **Codec** parameters:

1. Tick the checkbox next to the codec and click **Edit**. The following settings (options) are available:
  - **Packetization Interval** is used to set the time interval between two RTP packets of the same stream. If this interval is increased, the overhead will decrease, but the voice quality may deteriorate as a result. If the interval is decreased, the network load will increase and the delay will reduce.
  - **Enable Silence Suppression** is used to stop RTP packet transmission in case of no voice activity. This option helps to avoid extra traffic if the RTP stream contains no voice activity. It is activated after two seconds of silence and restarts immediately in case of any audio.
2. Click **Save** to apply changes.

The following settings (options) are available:

- **G.726 Standard** is used to select between packaging method of the G.726 code words into octets.
  - **Use ITU\_T specification** – if selected, the ITU I.366.2 (AAL2 type 2 service specific convergence sublayer for narrow-band services) type packaging of code words is used, where packing code words into octets start from the most significant rather than the least significant positions in the octet.
  - **Use IETF RFC** – if selected, the IETF RFC (RTP Profile for Audio and Video Conferences with Minimal Control) type packaging of code words is used, where packing code words start from the least significant positions in the octet.
- **RTP/RTCP Port Range** is used to set the port numbers for RTP/RTCP traffic.
- **Enable RTCP Support** is used to enable **Real Time Control Protocol (RTCP)** support and allows the RTCP packets transmission. RTCP is used for monitoring the RTP streams and changing RTP characteristics depending on network conditions.

## 8.6 SIP

### 8.6.1 SIP Settings

The **SIP Settings** page allows to configure SIP ports (UDP, TCP and TLS), the DNS Server for SIP and the SIP timers scheme. The following settings (options) are available:

- **UDP Port** indicates the SIP UDP receive port. By default, **5060** is selected and used.
- **TCP Port** indicates the SIP TCP receive port. By default, **5060** is selected and used. QX will not use TCP protocol as a transport for SIP messages if the TCP port is left blank.
- **TLS Port** indicates the SIP TLS receive port. By default, **5061** is selected and used.
- **Realm** is used to set the messaging level information to be included in SIP messages sent by QX. This information might be used by remote side for authentication purposes.
- **Enable Session Timer** is used to enable advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.
- **DNS Server for SIP** allows to choose between regular DNS servers configured in the [DNS](#) page and specific DNS servers for SIP traffic.
  - **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 fields.
- **SIP Timers** is used to set the timeouts of the SIP messages retransmission.
  - **RFC 3261** is used to apply standard SIP timers described in the corresponding specification.
  - **High Availability** is used to 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 QX.
  - **Custom** is used to manually define the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session Refresh Timeout** timers.

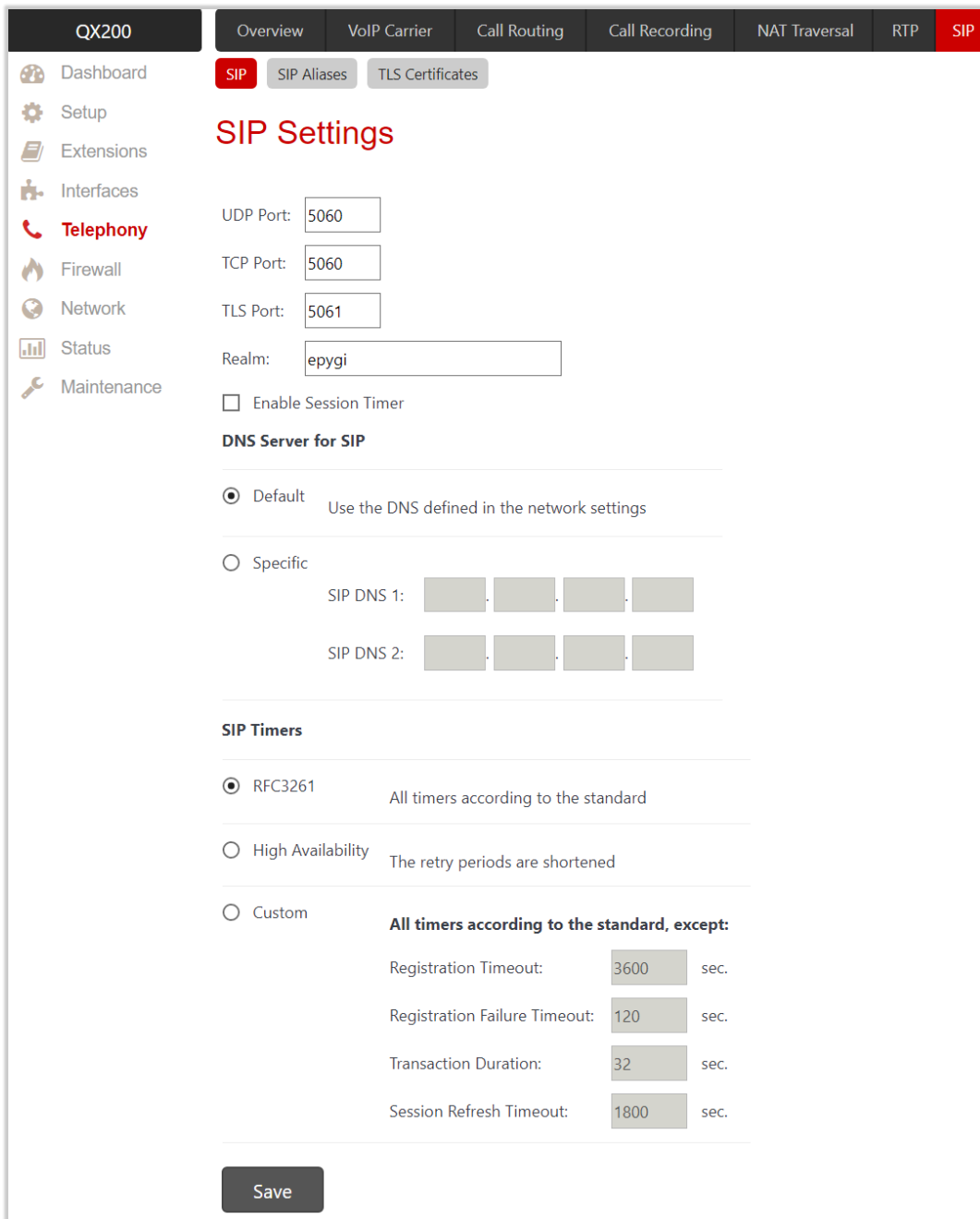


Figure 95: SIP Settings page

## 8.6.2 SIP Aliases

The **Host Aliases for SIP** page is used to add the hostname(s) registered on remote DNS server to the **Host Aliases for SIP** list. This list will be used to identify SIP packets received from remote servers where QX is registered with different names.

### 8.6.3 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 specific information on root certificate.

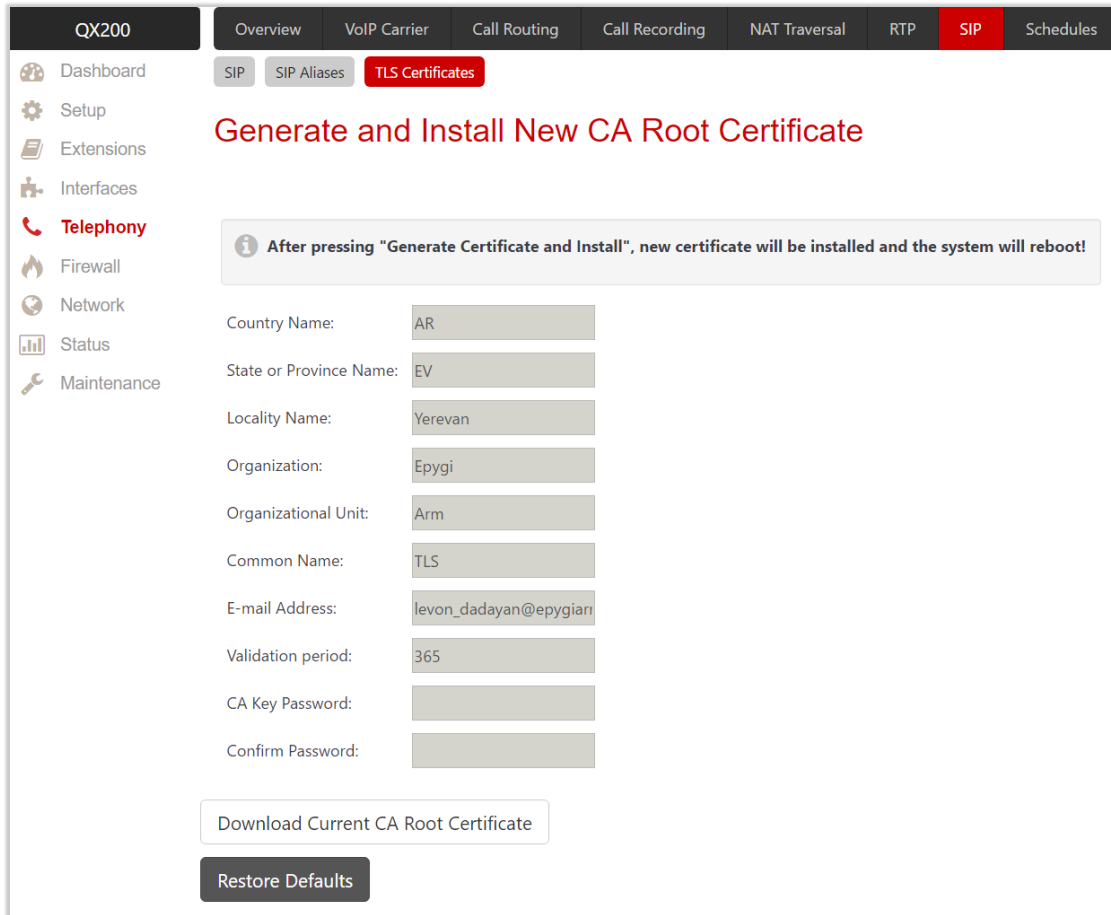


Figure 96: Generate and Install New CA Root Certificate page

- **Generate Certificate and Install** generates a new CA root certificate based on the defined data and installs it on QX. QX will reboot automatically once the new certificate is installed. You may download the actual copy of the certificate from [SIP Settings](#) page.
- **Download Current CA Root Certificate** is used to download the actual CA root certificate in (\*.**cert**) file format.

To ensure a secure TLS connection with QX, 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 QX. If the end user is a server or other device, you may download the certificate from QX and apply it manually on the remote side.

## 8.7 Schedules

The **Schedules** feature is designed for creating flexible weekly working schedule(s). The preconfigured schedules then can be applied to the **Call Routing** and **auto attendant**. The **Day/Night Switching** service allows to control and change the state of schedules manually by using the phone handset instead of going into the GUI.

For more information on how to configure and use **Schedules**, refer to the [Scheduling Feature on QX IP PBXs](#) guide.

## 8.8 Advanced

### 8.8.1 Voice Mail

The **Voice Mail Common Settings** page is mainly used to select the codec for the **Voice Mail** recording.

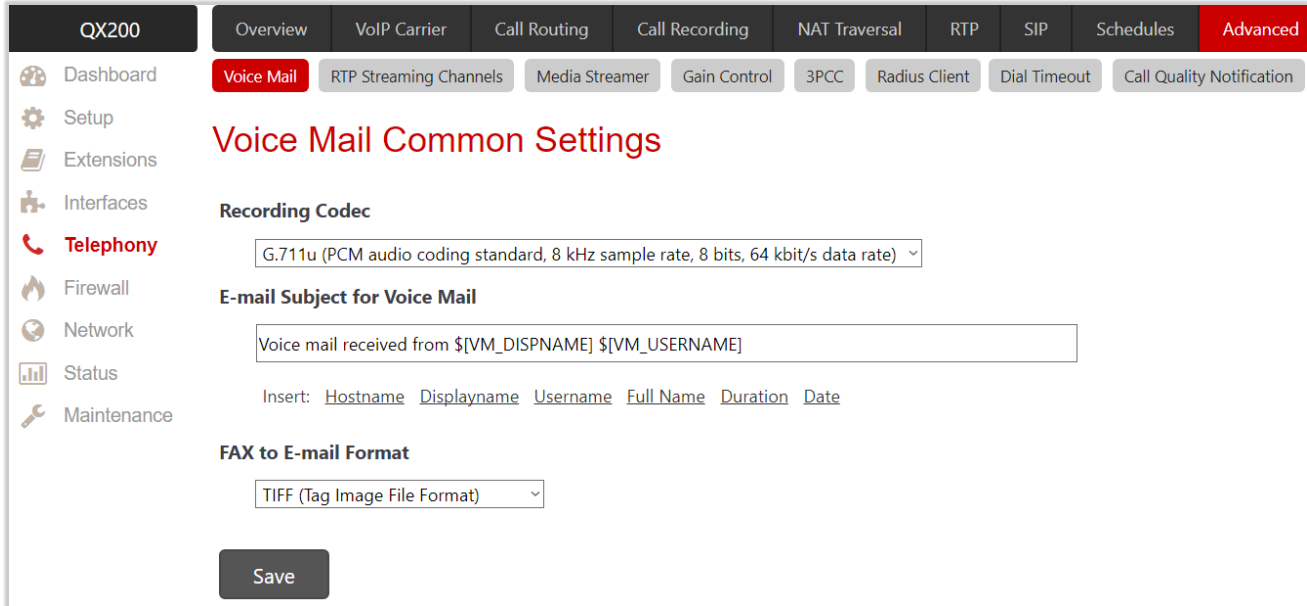


Figure 97: Voice Mail Common Settings page

The following settings (options) are available:

- **Recording Codec** is used to select the codec for voice mail recording. Changing the **Voice Mail** recording codec will directly affect the allocated memory size for extensions.
- **E-mail Subject for Voice Mail** is used to define a flexible subject for all e-mails sent from the QX and carrying the voice mails.

Besides using a static text in the subject line, you may use the predefined tags to combine the needed subject:

- **Hostname** is the hostname of QX.
- **Displayname** is the caller's display name. This value is not displayed for PSTN callers.
- **Username** is the caller's SIP username. For PBX callers, this is the caller's extension number and for PSTN callers, this is the caller's PSTN number.
- **Full Name** is the caller's full SIP address (SIP username and the SIP server). For PBX callers, this is the caller's extension number and for PSTN callers, this is the caller's PSTN number.
- **Duration** is the voice mail duration.
- **Date** is the date the voice mail has been received.

To enter 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**" which is followed by the display name of the caller and the date the voice mail has been received.

- **FAX to E-mail Format** is used to set the format of the FAX document received in the extension's voice mailbox and send as an attachment to the e-mail (in case if **Send new voice messages via e-mail** option is enabled for the extension). The **(\* .tiff)** or **(\* .pdf)** formats may be selected here.

## 8.8.2 RTP Streaming Channels

The **RTP Streaming Channels** page is used to define the channels for the RTP streaming. These channels may be then used when configuring RTP channel streaming for **Music on Hold (MoH)**, auto attendant ringing announcement and for other custom messages.

For more information on how to configure and use **RTP Streaming Channels**, refer to the [Customizing Voice Messages on QX IP PBXs](#) guide.

## 8.8.3 Media Streamer

The **Media Streamer** service expand the audio streaming capacity of QX. Audio files uploaded on QX can be streamed out to specified destinations, thus allowing to play music on hold or other messages to callers while they are placed on hold. Audio files can be played either to remote destinations in network, or to extensions on the same QX.

The **Media Streamer** page allows to add and manage playlists for media streamer, start and stop audio streaming with playlists. The configured playlists can be used to stream audio to the extensions through the **RTP Streaming Channels**.

For more information on how to configure and use **Media Streamer**, refer to the [Customizing Voice Messages on QX IP PBXs](#) guide.

## 8.8.4 Gain Control

The **Gain Control** settings are used to set the **Transmit** and **Receive** gains. The **Gain Control** page consists of **Transmit Gain** and **Receive Gain** drop-down lists for each line that contains allowed gain values, which can be set up for every line.

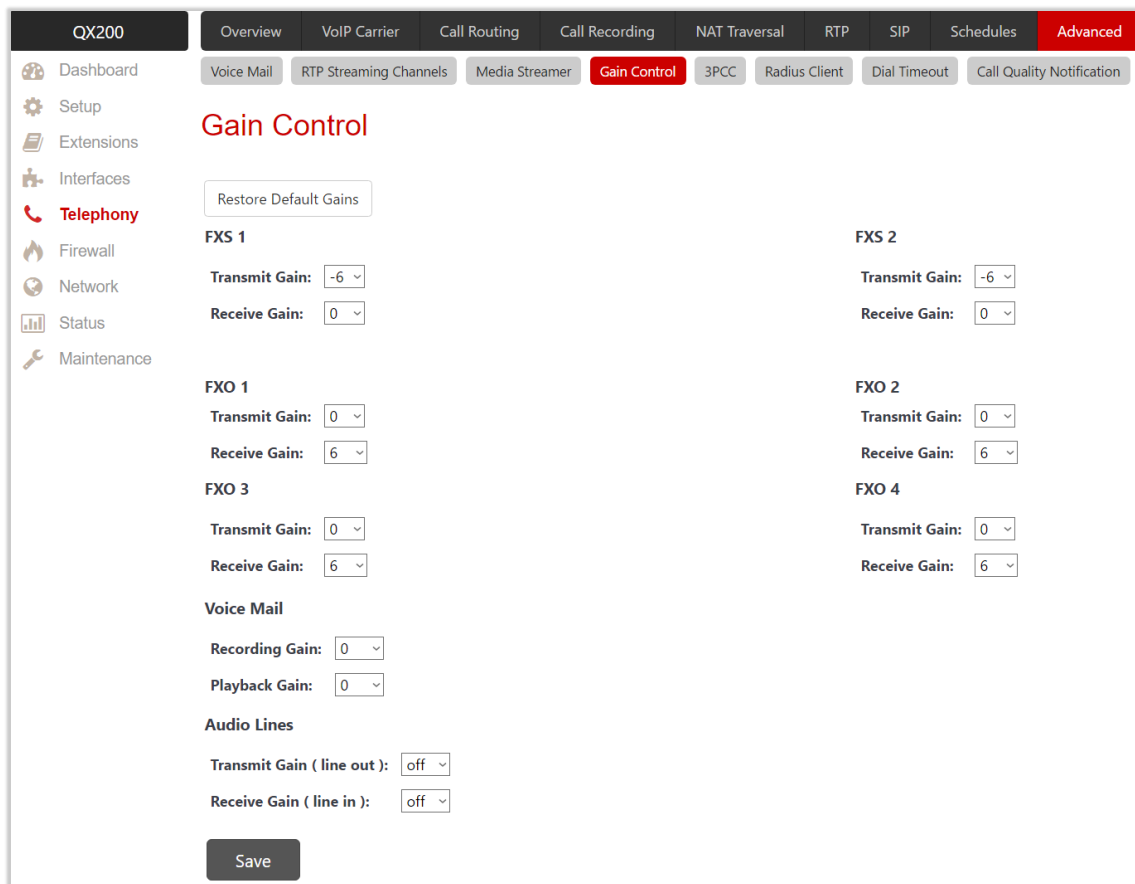


Figure 98: Gain Control page

- For **FXS** lines:
  - **Transmit Gain** is used to set the phone speaker volume on the call.
  - **Receive Gain** is used to set the volume of the phone microphone on the call.
- For **FXO** lines:
  - **Transmit Gain** is used to set the level of voice transmitted from QX to the FXO network.
  - **Receive Gain** is used to set the volume of voice received by QX from the FXO network.
- For **ISDN** trunks:
  - **Transmit Gain** is used to set the level of voice transmitted from QX to the ISDN network.
  - **Receive Gain** is used to set the volume of voice received by QX from the ISDN network.
- For **Voice Mail**:
  - **Recording Gain** is used to set the volume of the phone microphone upon playing voice mails or system messages.
  - **Playback Gain** is used to set the phone speaker volume upon playing voice mails or system messages.
- For **Audio Lines**:
  - **Transmit Gain (line out)** is used to set the level of voice transmitted from QX to the **Audio Line Out** port.
  - **Receive Gain (line in)** is used to set the volume of voice received by QX from the **Audio Line In** port.
- **Restore Default Gains** is used to restore the default values.

## 8.8.5 3PCC

The **3PCC Settings** page is used to adjust the **3<sup>rd</sup> party call controlling** (3PCC) settings. 3PCC service allows call controlling applications to remotely initiate and handle calls on QX and subscribe for certain event notifications from QX.

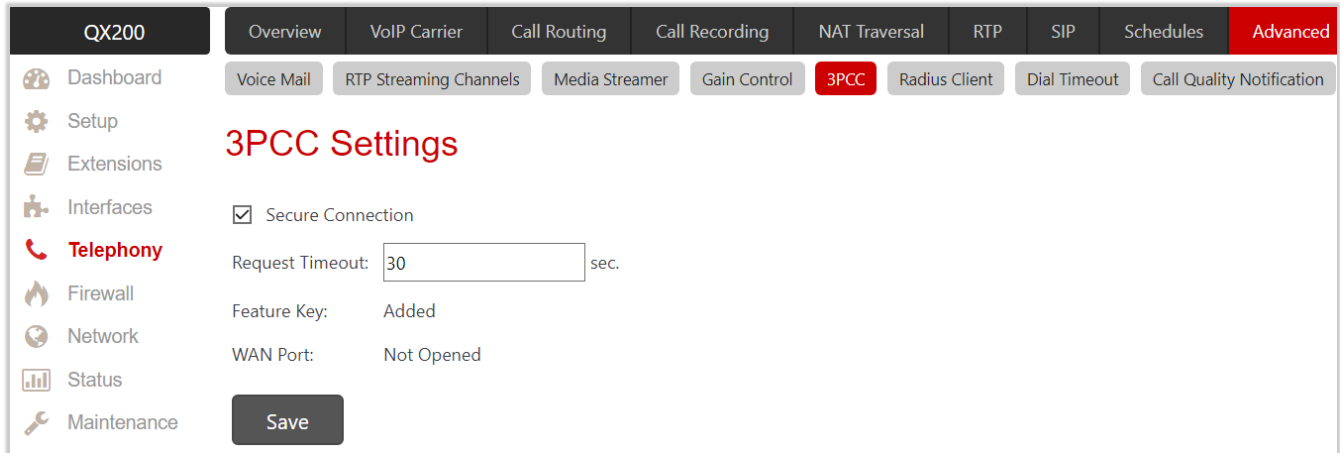


Figure 99: 3PCC Settings page

The following settings (options) are available:

- **Secure Connection** – if selected, a secure encrypted connection will be used between the call controlling application and QX. The **Secure Connection** must be set up in the same way on both sides for successful connection.
- **Request Timeout** is used to set the timeout during which QX should receive a response to the request from the call control application. If no response is received during this timeout, QX will perform a request according to default action. Let's say the call control application is configured to handle incoming calls on QX. Once incoming call is received, QX will try to transfer the call to the call control application. If the call control application does not respond within the mentioned timeout, QX will answer the call or perform an action configured for missed incoming calls. This setting depends on the network conditions therefore consult with your network administrator before changing the default value.
- **Feature Key** indicates whether the feature key for the **3PCC support** is installed on the system or not. The system will not accept connections from 3PCC applications if no key is found. The **3PCC support** is a licensable feature and can be activated from the **Licensed Features** page.
- **WAN Port** indicates whether there is a filtering rule specified for the [Call Control Access](#) or not. If a 3PCC application connects to QX from the WAN interface, a filtering rule should be created on the **Call Control Access** page to allow remote access. Creating a filtering rule is not required if the firewall is not setup on QX. The field shows **Opened** if there is at least one enabled filtering rule for the **Call Control Access**.

## 8.8.6 RADIUS Client

**Remote Authentication Dial in User Service** (RADIUS) is a networking protocol that provides centralized **Authentication, Authorization, and Accounting** (AAA) management for users who connect and use a network service. The RADIUS server provides the option for a caller from/through QX to make calls after passing authentication.

When a RADIUS client is enabled on QX, 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 RADIUS client and server are authenticated through the use of a shared **Secret Key**, which is never sent over network. In addition, user passwords are encrypted when sent between the client and server. If no response from the RADIUS server is returned once the **Receive Timeout** expires, the authentication request will be resent. The client can also forward requests to the secondary server if the primary server is down or unreachable. The secondary server can be used after a number of failed attempts to the primary server.

Once the RADIUS server receives the request from client, it determines the client's validity. If the client is valid, the RADIUS server addresses the user database to find the user whose name matches the request. The user entry in the database contains a list of parameters (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.

The following settings (options) are available:

- **Enable RADIUS Client** is used to activate service on QX. **TIP:** This service cannot be disabled if the **RADIUS Authentication and Authorization** or **RADIUS Accounting** options are enabled at least on one call routing rule.

### Registration Settings

- **Primary Server** is used to set the IP address of the primary RADIUS server.
- **Secondary Server** is used to set the IP address of the secondary RADIUS server.
- **NAT Station IP** is used to set the IP address of the NAT station. If no IP address is set, QX IP address will be sent to the RADIUS server.
- **Secret Key** is used to specify the secret key.
- **Retry Count** is used to select the number of unsuccessful requests before canceling the authentication on RADIUS server.
- **Receive Timeout** is used to select the timeout between two attempts to authenticate.
- **Encoding Type** is used 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 RADIUS server.
- **Authorization Port** is used to set the port number on the RADIUS server where QX is to send the authentication requests.

- **Accounting Port** is used to set the port number on the RADIUS server where QX is to send the accounting messages.

### Authentication Settings

- **Enable common login for all users in time of by phone authentication** is used to activate phone authentication service. This checkbox enables **Username** and **Password** fields to set common authentication parameters.
- **Authentication on Destination RADIUS Server** is used to set the authentication parameters. Leave these fields blank if you want to use the original authentication parameters.

### Accounting Settings

- **Username** is used to set the identification parameter for accounting services only. The source username will be used if no username is specified.
- **Send Accounting messages** is used to select sending **Both Start and Stop** or **Only Stop** accounting message.

QX200
Overview
VoIP Carrier
Call Routing
Call Recording
NAT Traversal
RTP

Voice Mail
RTP Streaming Channels
Media Streamer
Gain Control
3PCC
Radius Client

- Dashboard
- Setup
- Extensions
- Interfaces
- Telephony
- Firewall
- Network
- Status
- Maintenance

## RADIUS Client Settings

Enable RADIUS Client

**Registration Settings**

Primary Server:

Secondary Server:

NAT Station IP:

Secret Key:

Confirm Secret Key:

Retry Count:

Receive Timeout:  sec.

Encoding Type:

Authorization Port:

Accounting Port:

**Authentication Settings**

Enable common login for all users in time of by phone authentication

Username:

Password:

Authentication on the destination RADIUS server:

Username:

Password:

Confirm Password:

**Accounting Settings**

Use this username if accounting only is required.

Username:

Send Accounting Messages:

Both Start and Stop

Only Stop

Figure 100: Radius Client Settings page

## 8.8.7 Dial Timeout

The **Dial Timeout Settings** page is used to adjust the timeout setting when dialing on the phone. The **Routing Dial Timeout** option is used to set timeout 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 completed and starts processing the dialed number. This option is also applicable to all supported IP phones. The modified value will take effect after rebooting IP phone.

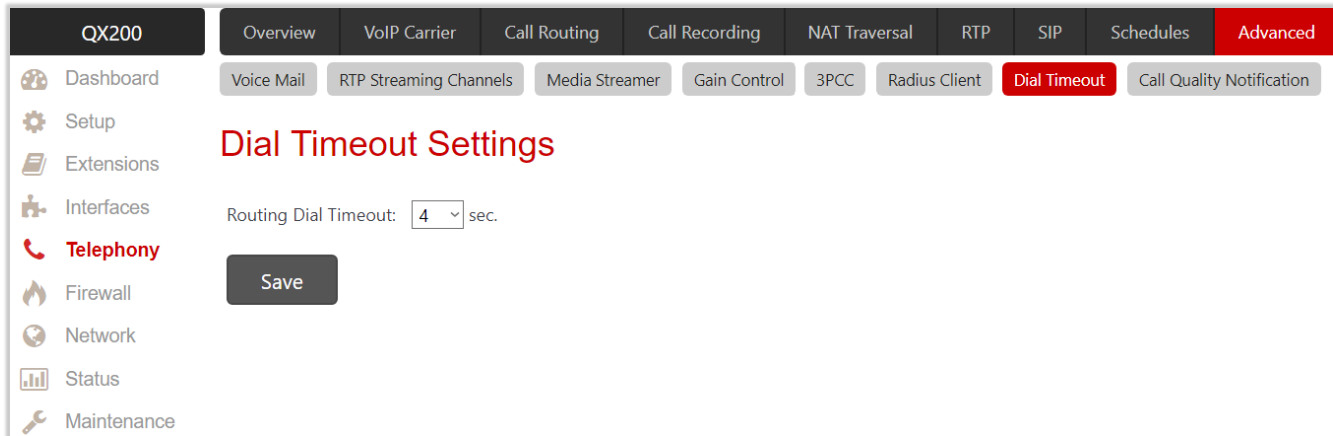


Figure 101: Dial Timeout Settings page

## 8.8.8 Call Quality Notification

The **Configure Call Quality Event Notification** page is used to configure the policy for event notification when the call quality is lower than the selected level.

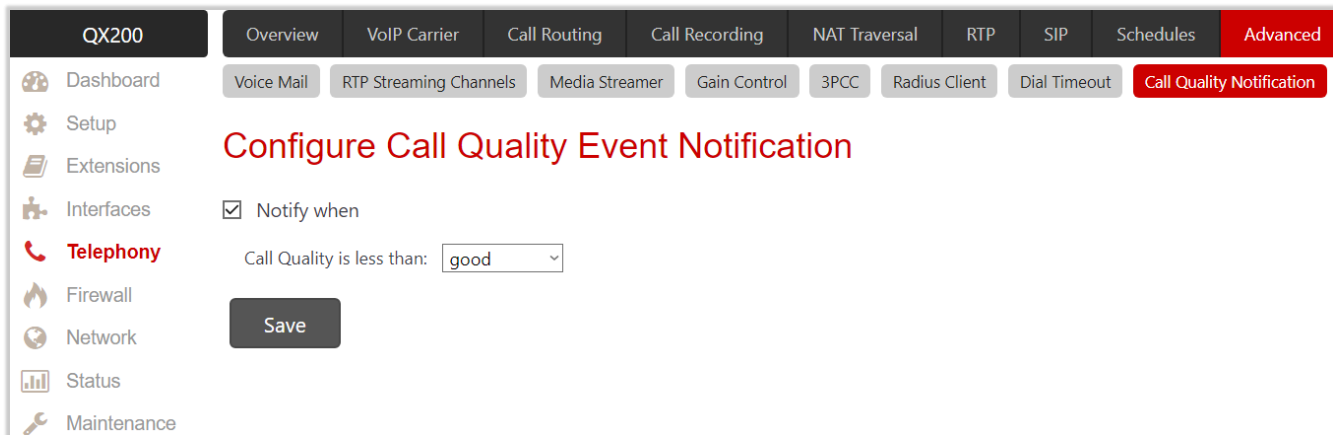
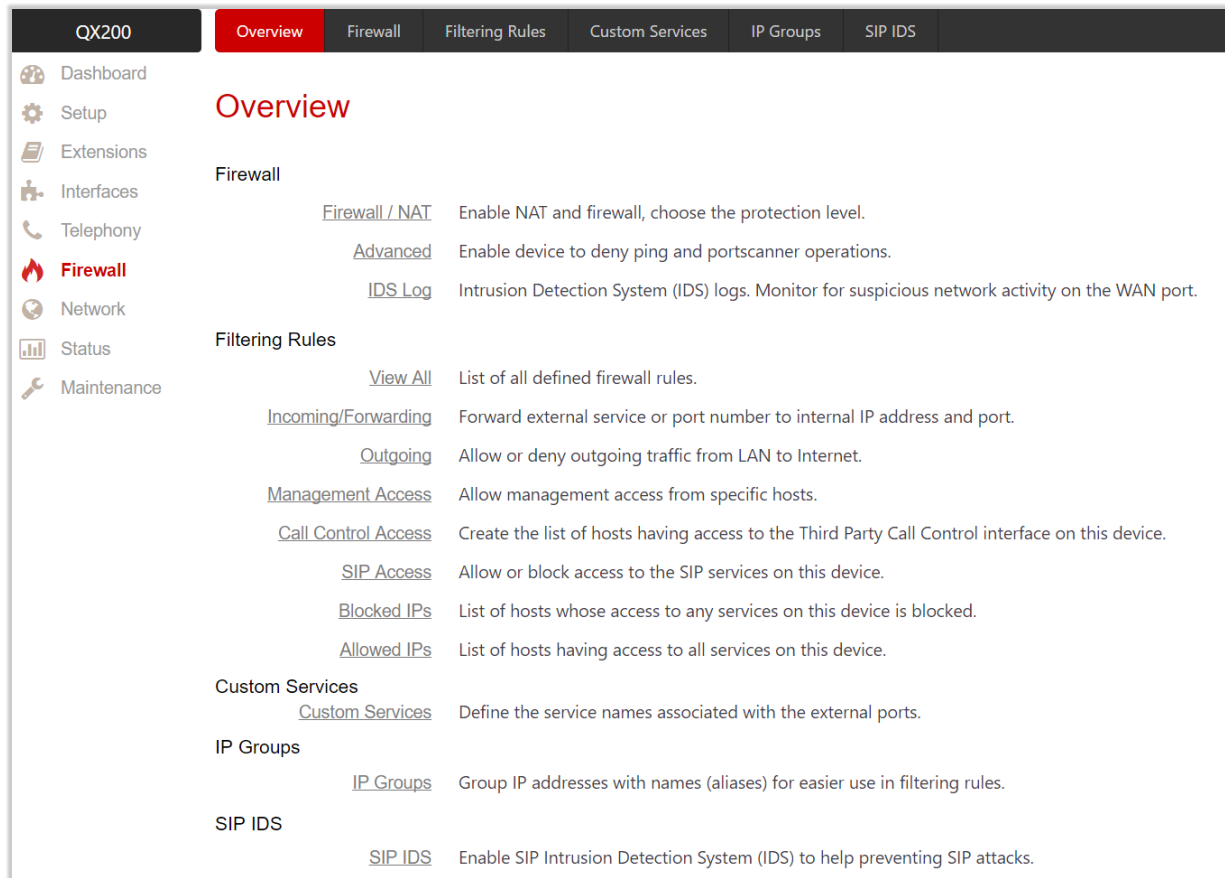


Figure 102: Configure Call Quality Event Notification page

To activate **Call Quality Event Notification** service:

1. Tick the **Notify when** option to enable the call quality monitoring mechanism.
2. Select the **call quality level** below which the notification will be generated and displayed in **System Events**.
3. Click **Save** to apply changes.

## 9 Firewall Menu



QX200	Overview	Firewall	Filtering Rules	Custom Services	IP Groups	SIP IDS
Dashboard	<b>Overview</b>					
Setup	<b>Firewall</b>					
Extensions		<a href="#">Firewall / NAT</a>	Enable NAT and firewall, choose the protection level.			
Interfaces		<a href="#">Advanced</a>	Enable device to deny ping and portscanner operations.			
Telephony		<a href="#">IDS Log</a>	Intrusion Detection System (IDS) logs. Monitor for suspicious network activity on the WAN port.			
<b>Firewall</b>	<b>Filtering Rules</b>					
Network		<a href="#">View All</a>	List of all defined firewall rules.			
Status		<a href="#">Incoming/Forwarding</a>	Forward external service or port number to internal IP address and port.			
Maintenance		<a href="#">Outgoing</a>	Allow or deny outgoing traffic from LAN to Internet.			
		<a href="#">Management Access</a>	Allow management access from specific hosts.			
		<a href="#">Call Control Access</a>	Create the list of hosts having access to the Third Party Call Control interface on this device.			
		<a href="#">SIP Access</a>	Allow or block access to the SIP services on this device.			
		<a href="#">Blocked IPs</a>	List of hosts whose access to any services on this device is blocked.			
		<a href="#">Allowed IPs</a>	List of hosts having access to all services on this device.			
	<b>Custom Services</b>					
		<a href="#">Custom Services</a>	Define the service names associated with the external ports.			
	<b>IP Groups</b>					
		<a href="#">IP Groups</a>	Group IP addresses with names (aliases) for easier use in filtering rules.			
	<b>SIP IDS</b>					
		<a href="#">SIP IDS</a>	Enable SIP Intrusion Detection System (IDS) to help preventing SIP attacks.			

Figure 103: Firewall Menu overview

## 9.1 Firewall

The **Firewall Configuration** page allows setting up the **Firewall** and activating **Network Address Translation (NAT)** and **Intrusion Detection System (IDS)** services on QX.

Firewall is a security service configurable through various criteria. It has three level of security policies: low, medium and high. QX Firewall allows or blocks traffic based on the policies, services and/or IP addresses. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level. Additional service-based rules can be added as well.

NAT is used to connect the QX LAN devices (IP phones, PCs, etc.) to Internet using QX WAN IP address. NAT also forwards incoming packets from the WAN to the QX LAN devices.

IDS is a type of firewall. The latter deletes dangerous packets or packets containing intrusion attacks, also generates a log file containing information about the dropped packets and senders responsible for those packets. The log can be viewed on the [IDS Log](#) page. Users can be notified about the generated logs through an email, flashing LED display notification, etc.

### 9.1.1 Firewall and NAT

The **Firewall Configuration** page is used to configure the following settings (options):

- **Enable IDS** is used to enable service on QX.
- **Enable NAT** is used to enable service on QX.
- **Enable Firewall** is used to enable service on QX. To activate Firewall, the firewall security level should be selected. The **Firewall Security** levels 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.

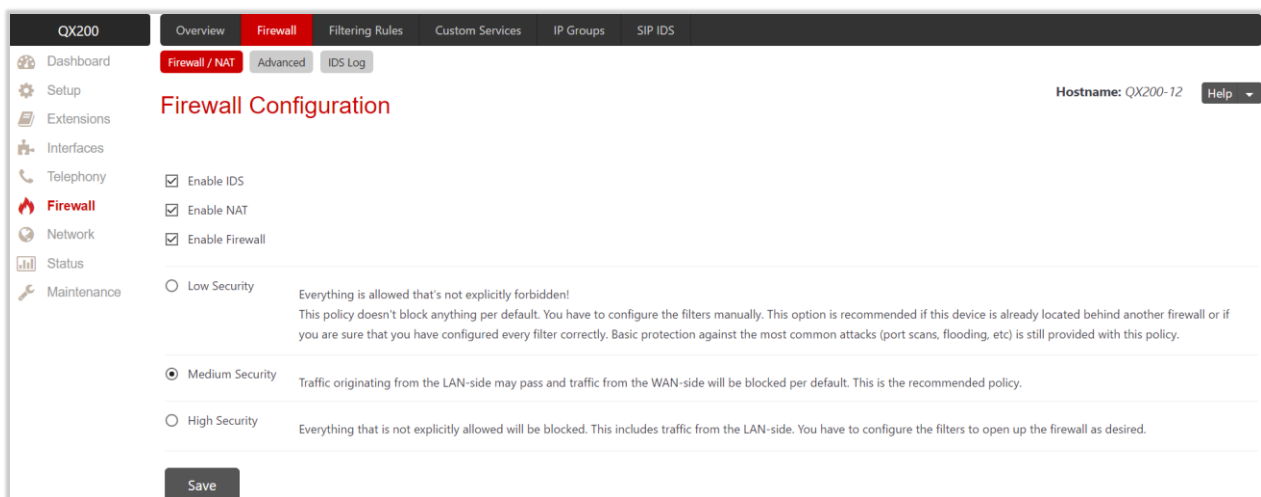


Figure 104: Firewall Configuration page

## 9.1.2 Advanced Firewall Settings

**Advanced Firewall Settings** is used to activate **Ping Stealth** and **Fool Portscanner** services to enhance system security. These services will be activated when Firewall is enabled on QX.

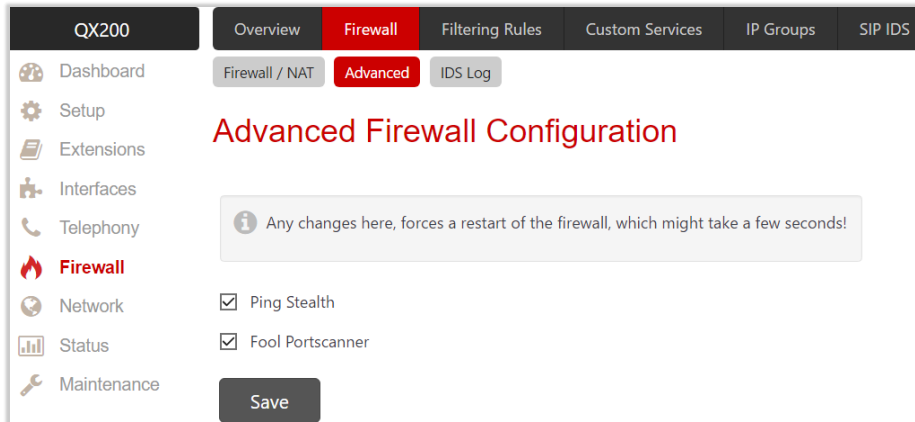


Figure 105: Advanced Firewall Settings page

## 9.1.3 IDS Log

The **IDS Logs** page contains information on dropped packets and the senders responsible for those packets. The system discards dangerous packets or packets including intrusion attacks. It generates a table with the IDS log report. Administrator can be notified about newly logged entries in various ways (e-mail, display notification, etc.) depending on the settings in the **System Events** page. IDS logs will be reported as soon as IDS is enabled from the **Firewall Configuration** page. The **IDS Logs** table shows the IDS entries and descriptions referring to them.

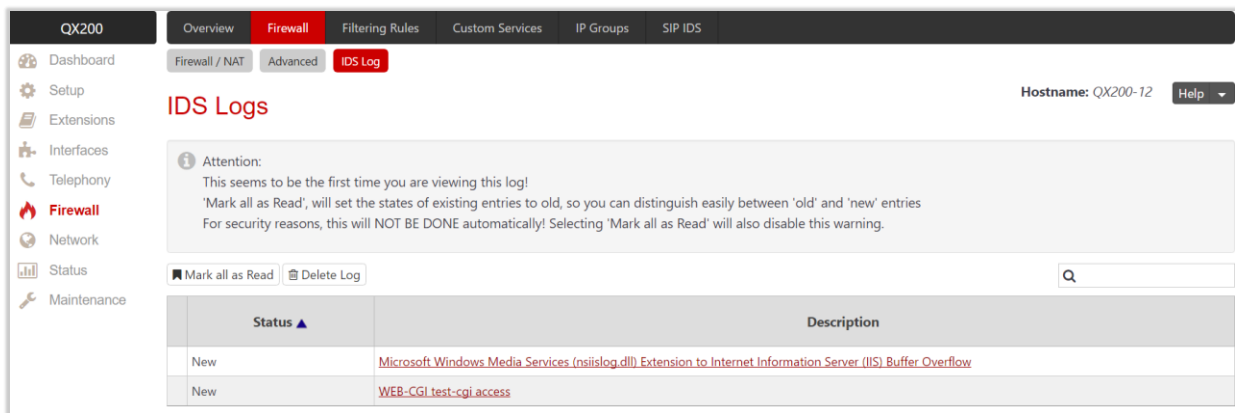


Figure 106: IDS Logs page

Click on the desired entry to see its detailed log in the **IDS Detailed Logs** table. The **IDS Logs** table shows the detailed log: additional information about the access protocol, IP address and port number as well as date and time of the event.

## 9.2 Filtering Rules

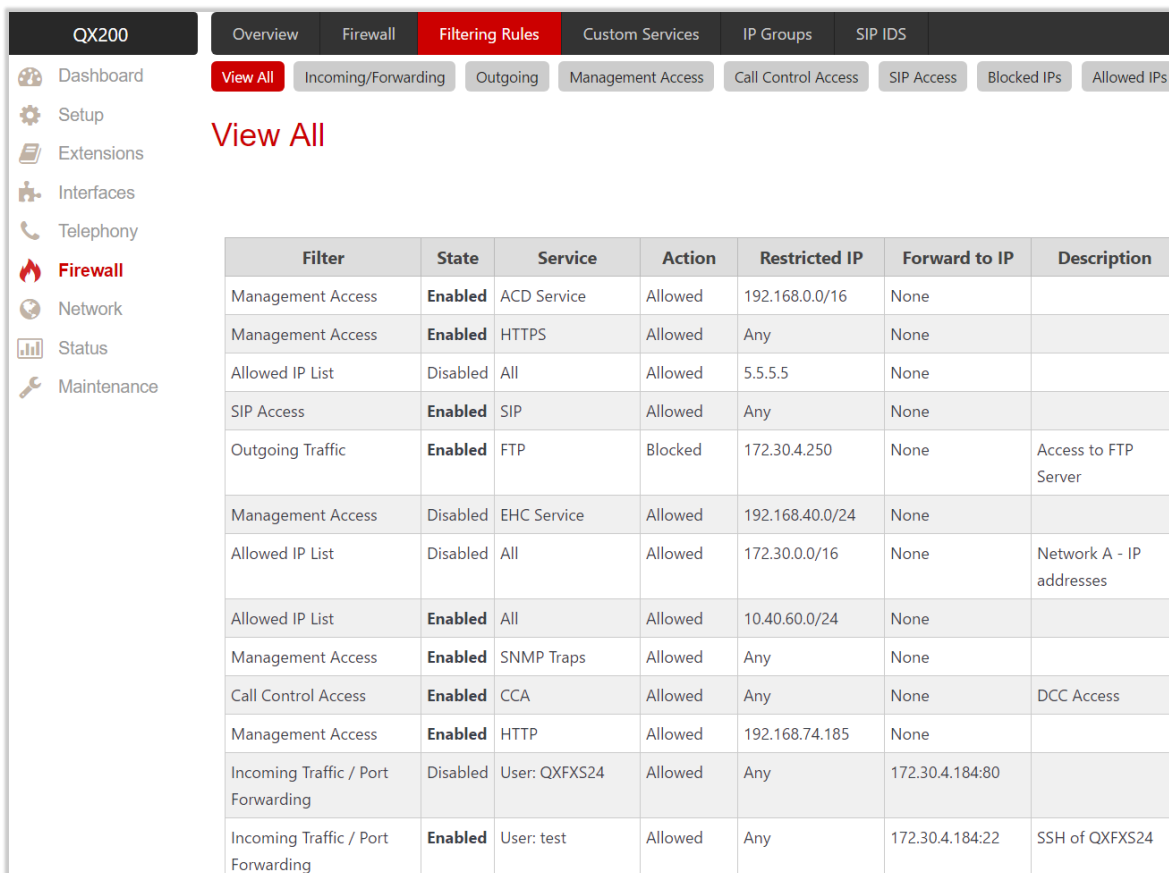
The **Filtering Rules** pages are used to configure the filters for incoming and outgoing traffic. It is allowed to create only one rule per service to prevent inaccurate configuration. You may use IP groups to include several IP addresses for any rule. Since the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled (also NAT is 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 regardless of the type of selected security level.

### 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.
- The newly created blocking filtering rules will take effect immediately only if the IP address(es) is added into the [Blocked IPs](#).

### 9.2.1 View All Filtering Rules

The **View All** table presents all configured filters, specified by their **State** (enabled or disabled), selected **Service**, type of **Action** (allowed or blocked), **Restricted IP** addresses and **Destination** of port forwarding.

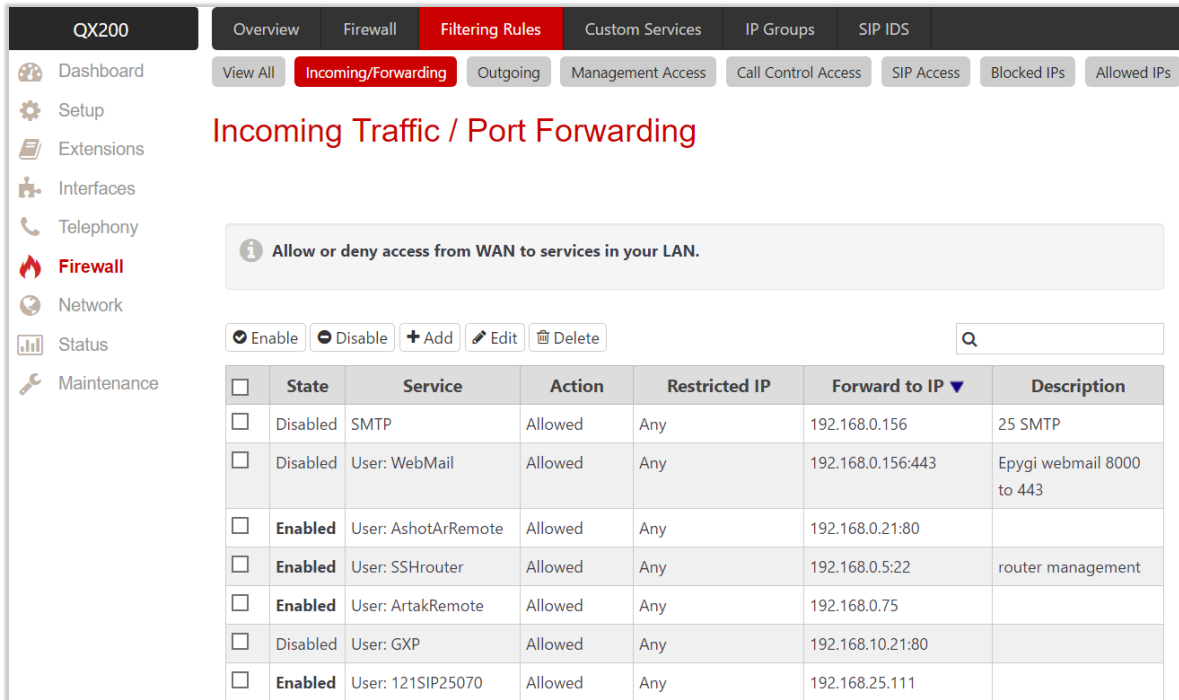


Filter	State	Service	Action	Restricted IP	Forward to IP	Description
Management Access	Enabled	ACD Service	Allowed	192.168.0.0/16	None	
Management Access	Enabled	HTTPS	Allowed	Any	None	
Allowed IP List	Disabled	All	Allowed	5.5.5.5	None	
SIP Access	Enabled	SIP	Allowed	Any	None	
Outgoing Traffic	Enabled	FTP	Blocked	172.30.4.250	None	Access to FTP Server
Management Access	Disabled	EHC Service	Allowed	192.168.40.0/24	None	
Allowed IP List	Disabled	All	Allowed	172.30.0.0/16	None	Network A - IP addresses
Allowed IP List	Enabled	All	Allowed	10.40.60.0/24	None	
Management Access	Enabled	SNMP Traps	Allowed	Any	None	
Call Control Access	Enabled	CCA	Allowed	Any	None	DCC Access
Management Access	Enabled	HTTP	Allowed	192.168.74.185	None	
Incoming Traffic / Port Forwarding	Disabled	User: QXFXS24	Allowed	Any	172.30.4.184:80	
Incoming Traffic / Port Forwarding	Enabled	User: test	Allowed	Any	172.30.4.184:22	SSH of QXFXS24

Figure 107: Filtering Rules – View All page

## 9.2.2 Incoming Traffic/Port Forwarding

The **Incoming Traffic/Port Forwarding** rules are used to allow or deny incoming traffic to reach to QX LAN. Enable the **NAT** service on QX to allow **Port Forwarding** in the **Incoming/Forwarding** filtering rules.

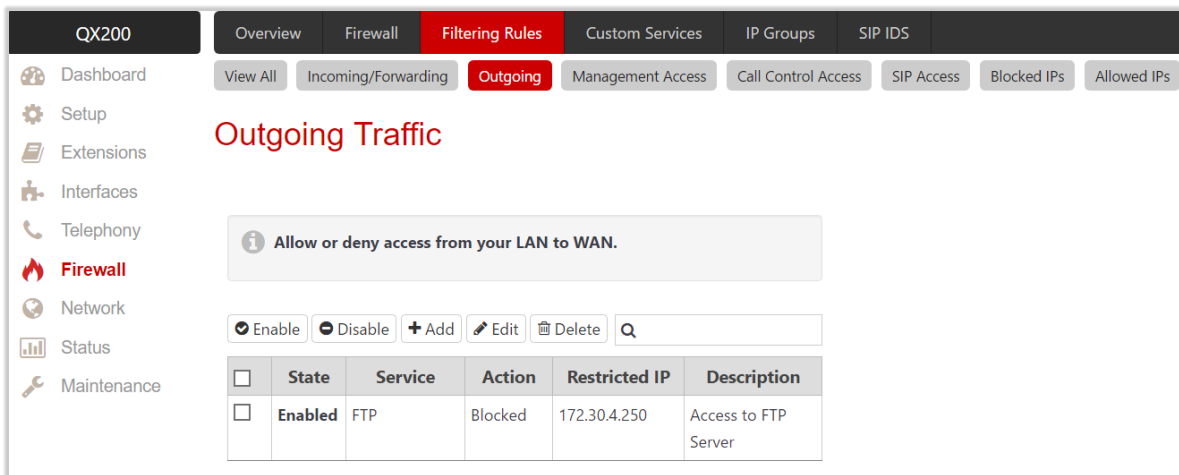


<input type="checkbox"/>	State	Service	Action	Restricted IP	Forward to IP ▼	Description
<input type="checkbox"/>	Disabled	SMTP	Allowed	Any	192.168.0.156	25 SMTP
<input type="checkbox"/>	Disabled	User: WebMail	Allowed	Any	192.168.0.156:443	Epygi webmail 8000 to 443
<input type="checkbox"/>	Enabled	User: AshotArRemote	Allowed	Any	192.168.0.21:80	
<input type="checkbox"/>	Enabled	User: SSHrouter	Allowed	Any	192.168.0.5:22	router management
<input type="checkbox"/>	Enabled	User: ArtakRemote	Allowed	Any	192.168.0.75	
<input type="checkbox"/>	Disabled	User: GXP	Allowed	Any	192.168.10.21:80	
<input type="checkbox"/>	Enabled	User: 1215IP25070	Allowed	Any	192.168.25.111	

Figure 108: Filtering Rules – Incoming Traffic / Port Forwarding page

## 9.2.3 Outgoing Traffic

The **Outgoing Traffic** rules are used to allow or deny access to the external services for QX LAN users.



<input type="checkbox"/>	State	Service	Action	Restricted IP	Description
<input type="checkbox"/>	Enabled	FTP	Blocked	172.30.4.250	Access to FTP Server

Figure 109: Filtering Rules – Outgoing Traffic page



## 9.2.4 Management Access

The **Management Access** rules are used to allow or deny WEB GUI access to QX.

The screenshot shows the 'Management Access' page in the QX200 web interface. The page title is 'Management Access' and it contains a table of rules. The table has the following data:

<input type="checkbox"/>	State	Service	Action	Restricted IP	Description
<input type="checkbox"/>	Enabled	ACD Service	Allowed	192.168.0.0/16	
<input type="checkbox"/>	Enabled	HTTPS	Allowed	Any	
<input type="checkbox"/>	Disabled	EHC Service	Allowed	192.168.40.0/24	
<input type="checkbox"/>	Enabled	SNMP Traps	Allowed	Any	
<input type="checkbox"/>	Enabled	HTTP	Allowed	192.168.74.185	

Figure 110: Filtering Rules – Management Access page

## 9.2.5 Call Control Access

The **Call Control Access** rules are used to allow or deny devices to access QX Call Control interface. It can be used to enable access from the call controlling applications (DCC, HotCall Add-In, etc.) to QX.

The screenshot shows the 'Call Control Access' page in the QX200 web interface. The page title is 'Call Control Access' and it contains a table of rules. The table has the following data:

<input type="checkbox"/>	State	Service	Action	Restricted IP	Description
<input type="checkbox"/>	Enabled	CCA	Allowed	Any	DCC Access

Figure 111: Filtering Rules – Call Control Access page

## 9.2.6 SIP Access

The **SIP Access** rules are used to allow or deny SIP traffic to QX from SIP servers and other SIP devices. It can be used to allow incoming/outgoing SIP calls from IP phones and SIP servers.

The screenshot shows the 'SIP Access' configuration page. At the top, there are tabs for 'View All', 'Incoming/Forwarding', 'Outgoing', 'Management Access', 'Call Control Access', 'SIP Access' (selected), 'Blocked IPs', and 'Allowed IPs'. Below the tabs is a red header 'SIP Access' and a grey box with an information icon stating: 'Allow or deny access to or from SIP servers and other SIP devices in WAN.' Below this is a control bar with 'Enable' (checked), 'Disable', '+ Add', 'Edit', and 'Delete' buttons, along with a search field. A table below shows the following rule:

<input type="checkbox"/>	State	Service	Action	Restricted IP	Description
<input type="checkbox"/>	Enabled	SIP	Allowed	Group: LAN	

Figure 112: Filtering Rules – SIP Access page

## 9.2.7 Blocked IPs

The **Blocked IP List** rules are used to deny access for special devices. Traffic to or from these devices will be blocked in any case, no matter what services are configured in other pages. The **Blocked IP List** has a higher priority over the **Allowed IP List**: if the same host is listed in both tables, it will be blocked.

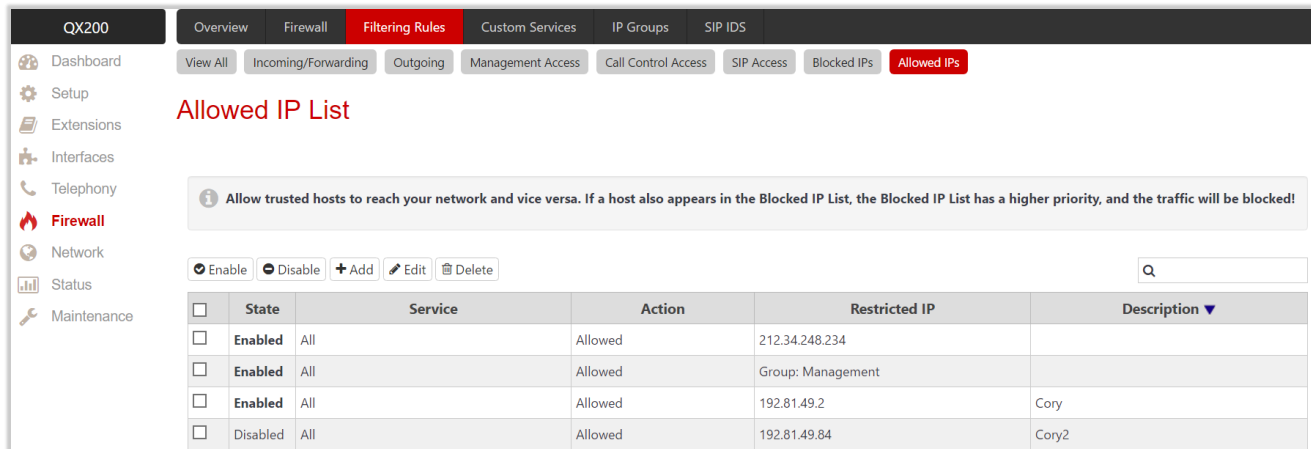
The screenshot shows the 'Blocked IP List' configuration page. At the top, there are tabs for 'View All', 'Incoming/Forwarding', 'Outgoing', 'Management Access', 'Call Control Access', 'SIP Access', 'Blocked IPs' (selected), and 'Allowed IPs'. Below the tabs is a red header 'Blocked IP List' and a grey box with an information icon stating: 'Deny access for special hosts. Traffic to or from these hosts will be blocked in any case!' Below this is a control bar with 'Enable' (checked), 'Disable', '+ Add', 'Edit', and 'Delete' buttons, along with a search field. A table below shows the following rules:

<input type="checkbox"/>	State	Service	Action	Restricted IP	Description
<input type="checkbox"/>	Enabled	All	Blocked	195.154.251.58	
<input type="checkbox"/>	Enabled	All	Blocked	169.254.50.74	Blocked by SIP UA. Reason: Authorization failure. Date:03-Nov-2016 13:26:56
<input type="checkbox"/>	Enabled	All	Blocked	10.26.0.22	Blocked by SIP UA. Reason: Authorization failure. Date:03-Oct-2016 16:15:00
<input type="checkbox"/>	Enabled	All	Blocked	10.26.0.26	Blocked by SIP UA. Reason: Authorization failure. Date:03-Oct-2016 16:18:16

Figure 113: Filtering Rules – Blocked IP List page

## 9.2.8 Allowed IPs

The **Allowed IP List** rules are used to allow trusted devices to reach your network and vice versa. **TIP:** If the IP address of the device also appears in the **Blocked IP List**, then the traffic will be blocked as the **Blocked IP List** has a higher priority.



<input type="checkbox"/>	State	Service	Action	Restricted IP	Description ▼
<input type="checkbox"/>	Enabled	All	Allowed	212.34.248.234	
<input type="checkbox"/>	Enabled	All	Allowed	Group: Management	
<input type="checkbox"/>	Enabled	All	Allowed	192.81.49.2	Cory
<input type="checkbox"/>	Disabled	All	Allowed	192.81.49.84	Cory2

Figure 114: Filtering Rules – Allowed IP List page

### To add a Filtering Rule

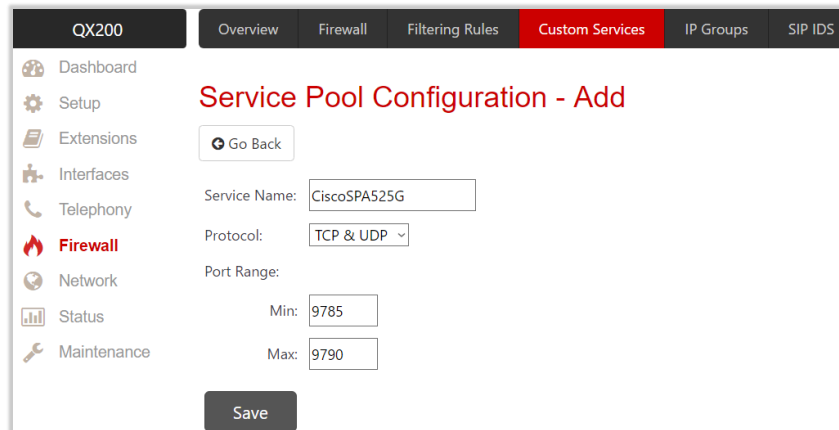
1. Go to the **Filtering Rules** (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, Call Control Access, SIP Access, Blocked IP List or Allowed IP List) page to add a rule.
2. Click **Add** on the corresponding filtering rule page.
  - Select the **Service** to configure a rule for it.
  - Select an **Action** to setup the rule.
  - Enter the destination **IP address** in the **Forward to IP** where traffic should be transferred to if it comes from the restricted host (**Incoming Traffic/Port Forwarding** rule).
  - Enter a **port number** in the **Port Translation** field which will stand instead of the original port number when incoming packet is being forwarded (**Incoming Traffic/Port Forwarding** rule).
  - 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**.
  - Enter a **Description**, if needed.
3. Click **Save** to create a rule with the given parameters. The newly created filtering rule will be shown in the corresponding **Filtering Rule** table and in the **View All** page.
4. Click **Enable** to activate the newly created filtering rule from the corresponding table.

## 9.3 Custom Services

The **Service Pool Configuration** page is used to create new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or allowance upon creating a new filtering rule.

To add a new **service**:

1. Click **Add**.
  - Enter a **Service Name**.
  - Select a **Protocol** type.
  - Set the **Port Range**.
2. Click **Save** to add the new service to the **Service Pool Configuration** table.



The screenshot shows the 'Service Pool Configuration - Add' page. The breadcrumb navigation includes 'QX200', 'Overview', 'Firewall', 'Filtering Rules', 'Custom Services', 'IP Groups', and 'SIP IDS'. The 'Custom Services' tab is active. On the left is a sidebar menu with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall (highlighted), Network, Status, and Maintenance. The main content area has a 'Go Back' button and a form with the following fields:
 

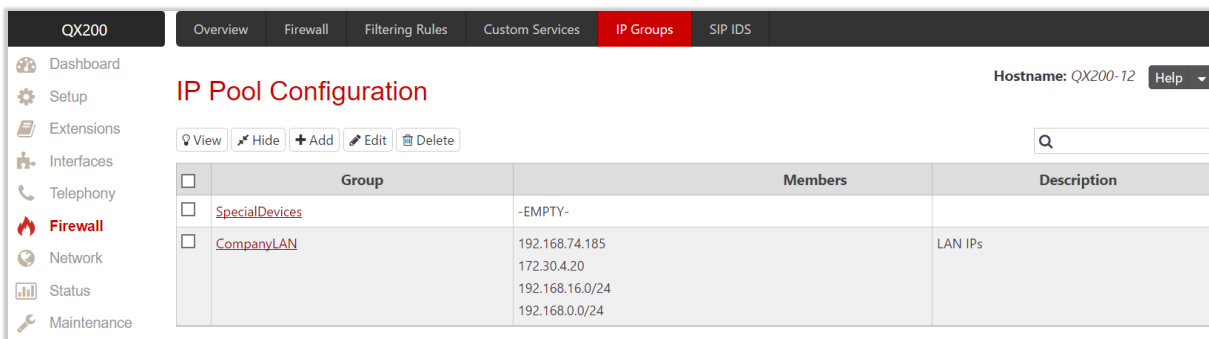
- Service Name: CiscoSPA525G
- Protocol: TCP & UDP
- Port Range: Min: 9785, Max: 9790

 A 'Save' button is located at the bottom of the form.

Figure 115: Service Pool Configuration – Add Service page

## 9.4 IP Groups

The **IP Pool Configuration** page is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, a group can be used instead of several IP addresses. **TIP:** Changing a group name will also change the references to this group, including filtering rules and member relations to the other groups. Deleting a group will also delete any reference to the corresponding group, including filtering rules and member relations to the other groups.



The screenshot shows the 'IP Pool Configuration' page. The breadcrumb navigation includes 'QX200', 'Overview', 'Firewall', 'Filtering Rules', 'Custom Services', 'IP Groups', and 'SIP IDS'. The 'IP Groups' tab is active. The page title is 'IP Pool Configuration' and the hostname is 'QX200-T2'. There are buttons for 'View', 'Hide', '+ Add', 'Edit', and 'Delete'. A search bar is present. Below is a table with the following data:

Group	Members	Description
<a href="#">SpecialDevices</a>	-EMPTY-	
<a href="#">CompanyLAN</a>	192.168.74.185 172.30.4.20 192.168.16.0/24 192.168.0.0/24	LAN IPs

Figure 116: IP Pool Configuration page

Click **Group** name link to display the **IP Pool Group Configuration** page with the **Members** list for the current group.

To add a new **Group** with **Members**:

1. Click **Add** on the IP Pool Configuration page.
2. Enter a **Group Name** and fill out the **Group Description**, if needed.
3. Click **Save** to add the group. The newly added group will be shown on the IP Pool Configuration table.
4. Open the **IP Pool Group Configuration** page by clicking on the group name.
5. Click **Add** on the **IP Pool Group Configuration** page. A page opens where new members can be added to the group.
  - Choose the member addition type by selecting **IP Address**, **IP Subnet** and enter the required information in the text fields or select **A user-defined Group**.
  - Enter a **Member description**, if needed.
6. Click **Save** to add the new member to the **Current Group** table.

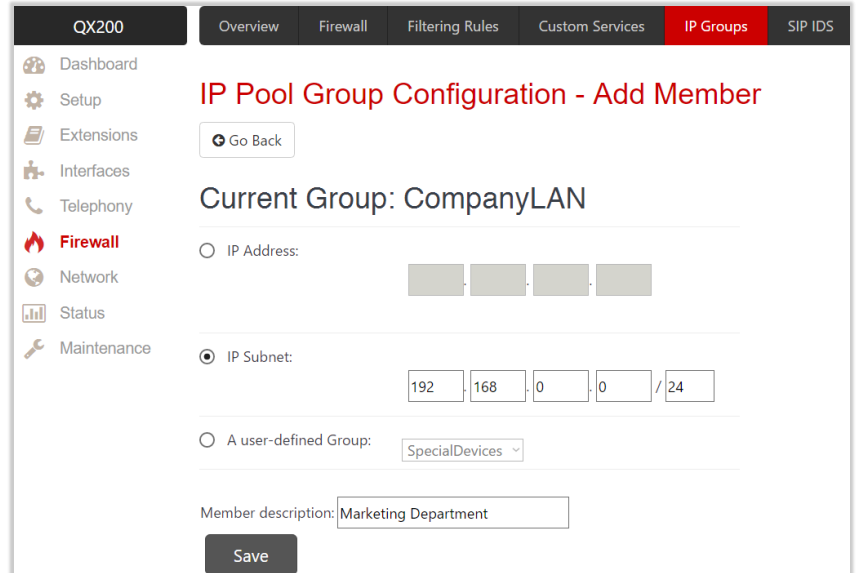


Figure 117: IP Pool Group Configuration – Add Member

## 9.5 SIP IDS

The SIP IDS service is used to prevent SIP attacks. If enabled, SIP IDS will detect repetitive SIP authorization requests and automatically block the offenders by adding their IP addresses to the Blocked IP List of Firewall or discard the SIP messages from those IP addresses, depending on your choice of settings.

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

- **Enable SIP IDS** - is used to activate SIP IDS system for preventing SIP attacks.
- **Do not Block In Firewall** - if selected, the system will not block the SIP attacker by adding its IP address to the [Blocked IP List](#) of Firewall. The IDS system will discard the SIP messages from that IP address within a preconfigured period (32 seconds by default).
- **Permanently add to Blocked IP List** - if selected, the system will block the SIP attacker's IP address by adding it to the [Blocked IP List](#) of Firewall. This action will take effect if the **Firewall** is enabled on the Epygi QX50.
- **Block in Firewall for xx sec** - if selected, the system will block the attacker IP address for the defined period (60 seconds by default).

**Note:** if the IP is blocked by SIP IDS for some period of time, disabling SIP IDS will not allow that IP until the expiration of that period or the firewall is restarted.

- **SIP IDS Exceptions** link leads to the [SIP IDS Exceptions](#) page where you can specify the trusted IP address(es) that shouldn't be blocked.

The IDS system discards suspicious packets or packets containing intrusion attacks, and also generates a log file containing information about the dropped packets and the senders of those packets. The log can be viewed on the IDS Log page. Users can be notified about the generated logs through an email, a flashing LED, display notification, etc.

### 9.5.1 The Bad IP detection logic

The **Bad IP** detection logic is the following:

- 2 failures of SIP authorization/authentication from the same IP during **250** milliseconds of each other.
- 2 messages causing **Non-self-Request-URI** from the same IP during **250** milliseconds of each other.
- If there are **30** failures in a row during any period of time from the same IP, then the IP will be blocked.

**Note:** any successful registration attempt from that IP will reset the counter. For example, if IP=xxx.xxx.xxx.xxx failed to register **29** times and then successfully registered on the **30th** attempt, then it resets the counter to **0**. Next time the same IP can make another **29** unsuccessful attempts before being blocked.

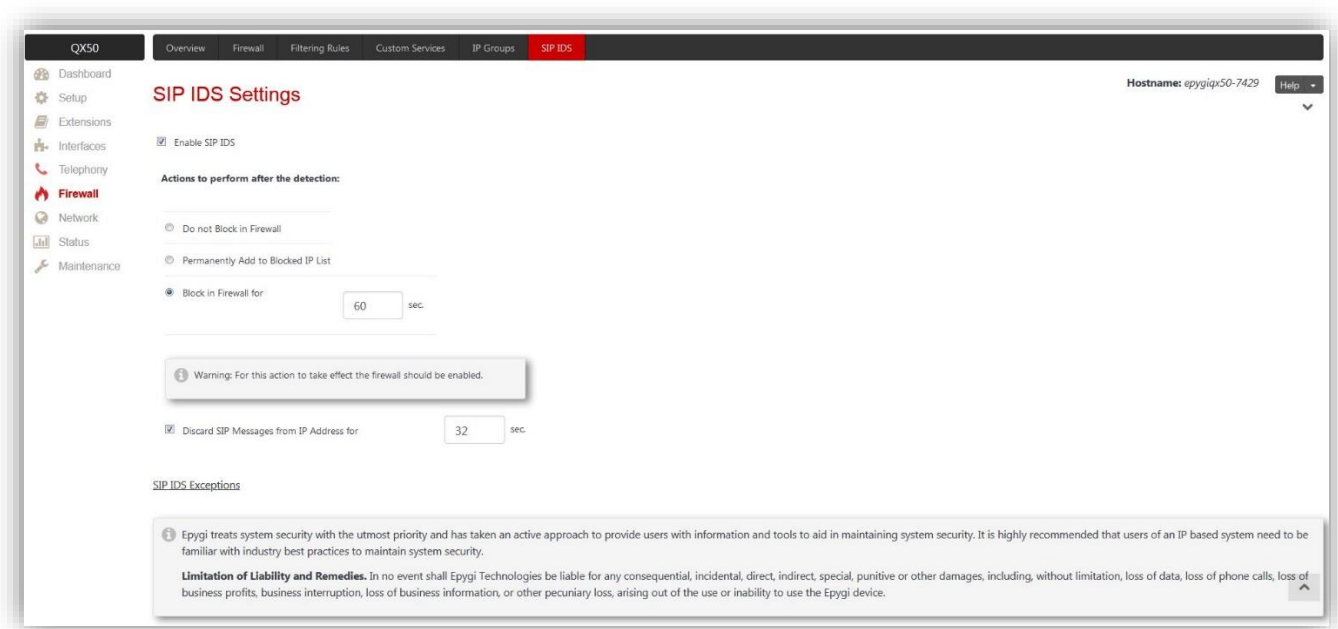
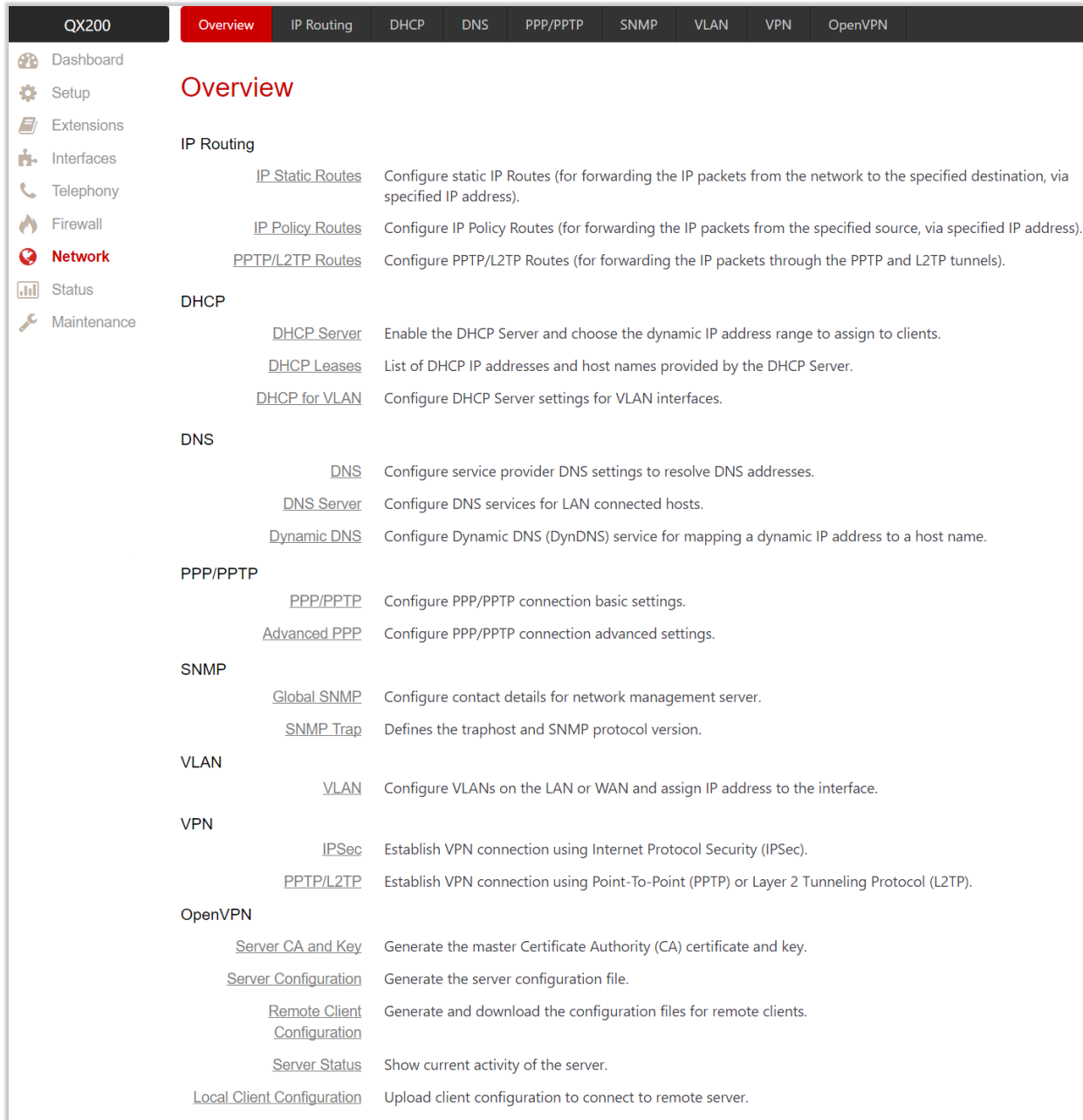


Figure 118: SIP IDS Settings page

## 10 Network Menu



QX200	Overview	IP Routing	DHCP	DNS	PPP/PPTP	SNMP	VLAN	VPN	OpenVPN
Dashboard	<b>Overview</b>								
Setup	<b>IP Routing</b>								
Extensions		<a href="#">IP Static Routes</a>	Configure static IP Routes (for forwarding the IP packets from the network to the specified destination, via specified IP address).						
Interfaces		<a href="#">IP Policy Routes</a>	Configure IP Policy Routes (for forwarding the IP packets from the specified source, via specified IP address).						
Telephony		<a href="#">PPTP/L2TP Routes</a>	Configure PPTP/L2TP Routes (for forwarding the IP packets through the PPTP and L2TP tunnels).						
Firewall		<b>DHCP</b>							
<b>Network</b>		<a href="#">DHCP Server</a>	Enable the DHCP Server and choose the dynamic IP address range to assign to clients.						
Status		<a href="#">DHCP Leases</a>	List of DHCP IP addresses and host names provided by the DHCP Server.						
Maintenance		<a href="#">DHCP for VLAN</a>	Configure DHCP Server settings for VLAN interfaces.						
		<b>DNS</b>							
		<a href="#">DNS</a>	Configure service provider DNS settings to resolve DNS addresses.						
		<a href="#">DNS Server</a>	Configure DNS services for LAN connected hosts.						
		<a href="#">Dynamic DNS</a>	Configure Dynamic DNS (DynDNS) service for mapping a dynamic IP address to a host name.						
		<b>PPP/PPTP</b>							
		<a href="#">PPP/PPTP</a>	Configure PPP/PPTP connection basic settings.						
		<a href="#">Advanced PPP</a>	Configure PPP/PPTP connection advanced settings.						
		<b>SNMP</b>							
		<a href="#">Global SNMP</a>	Configure contact details for network management server.						
		<a href="#">SNMP Trap</a>	Defines the trap host and SNMP protocol version.						
		<b>VLAN</b>							
		<a href="#">VLAN</a>	Configure VLANs on the LAN or WAN and assign IP address to the interface.						
		<b>VPN</b>							
		<a href="#">IPSec</a>	Establish VPN connection using Internet Protocol Security (IPSec).						
		<a href="#">PPTP/L2TP</a>	Establish VPN connection using Point-To-Point (PPTP) or Layer 2 Tunneling Protocol (L2TP).						
		<b>OpenVPN</b>							
		<a href="#">Server CA and Key</a>	Generate the master Certificate Authority (CA) certificate and key.						
		<a href="#">Server Configuration</a>	Generate the server configuration file.						
		<a href="#">Remote Client Configuration</a>	Generate and download the configuration files for remote clients.						
		<a href="#">Server Status</a>	Show current activity of the server.						
		<a href="#">Local Client Configuration</a>	Upload client configuration to connect to remote server.						

Figure 119: Network Menu overview



## 10.1 Second LAN Interface

The **Second LAN Interface Settings** page is used to activate second interface on the QX2000, QX3000 and QX5000.

Figure 120: Second LAN Interface Settings page

This following settings (options) are available:

- **Enable Interface** is used to activate the second interface.
- **IP Address** is used to set the LAN IP address.
- **Subnet Mask** is used to set the subnet mask.
- **DHCP Settings** button is used to configure [DHCP Settings](#) on the second interface.

**Note:** The network for the second LAN interface shouldn't be overlapped with the main LAN interface.

## 10.2 IP Routing

QX **IP Routing** service allows to route IP packets from one destination to another (or to a specified router) through QX or QX VPN. The **IP Routing** is used to make IP Static, IP Policy and PPTP/L2TP routes for IP packets routing.

### 10.2.1 IP Static Routes

**IP Static Routes** are used to forward IP packets from the network (the QX is connected) to a specified destination.

	Target State	Actual State	Route to	Via IP Address
<input type="checkbox"/>	enabled	up	172.30.20.0/24	172.30.0.1
<input type="checkbox"/>	disabled	down	192.168.10.0/26	172.30.4.1
<input type="checkbox"/>	enabled	erroneous - Network is unreachable	10.10.40.0/24	172.16.5.1

Figure 121: IP Static Routes page

To add a new **IP Static Route**:

1. Click **Add** and enter the following information:
  - **Route to** is used to set the IP address and subnet mask of the destination the IP packet will be routed to.
  - **Via IP Address** is used to set the IP address of the router that will forward the IP packet to the specified destination.
2. Click **Save** to add the new route to the **IP Static Routes** table.
3. Click **Enable** to activate the newly created route.

**Note:** 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.

### 10.2.2 IP Policy Routes

**IP Policy Routes** allows to forward IP packets to a specified router depending on the source IP address as well as set the priority for the current routing rule.

To add a new **IP Policy Route**:

1. Click **Add** and enter the following information:
  - **Priority** is used to set the priority of the routing rule. Enter any numeric value from the 1-252 range. The lower the number, the sooner the routing rule will take effect (higher priority).
  - **From** is used to set the packet source IP address and subnet mask of the specified destination to match with the rule.
  - **Via IP Address** is used to set the IP address of the subsequent router to forward the IP packet to.
2. Click **Save** to add the new route to the **IP Policy Routes** table.
3. Click **Enable** to activate the newly created route.
4. Click **Raise Priority** or **Lower Priority** to increase/decrease the priority of the selected policy route by one.

### 10.2.3 PPTP/L2TP Routes

**PPTP/L2TP Routes** allows to forward IP packets through the PPTP and L2TP tunnels of QX. VPN routes cannot be generated if PPTP/L2TP connections do not exist on QX.

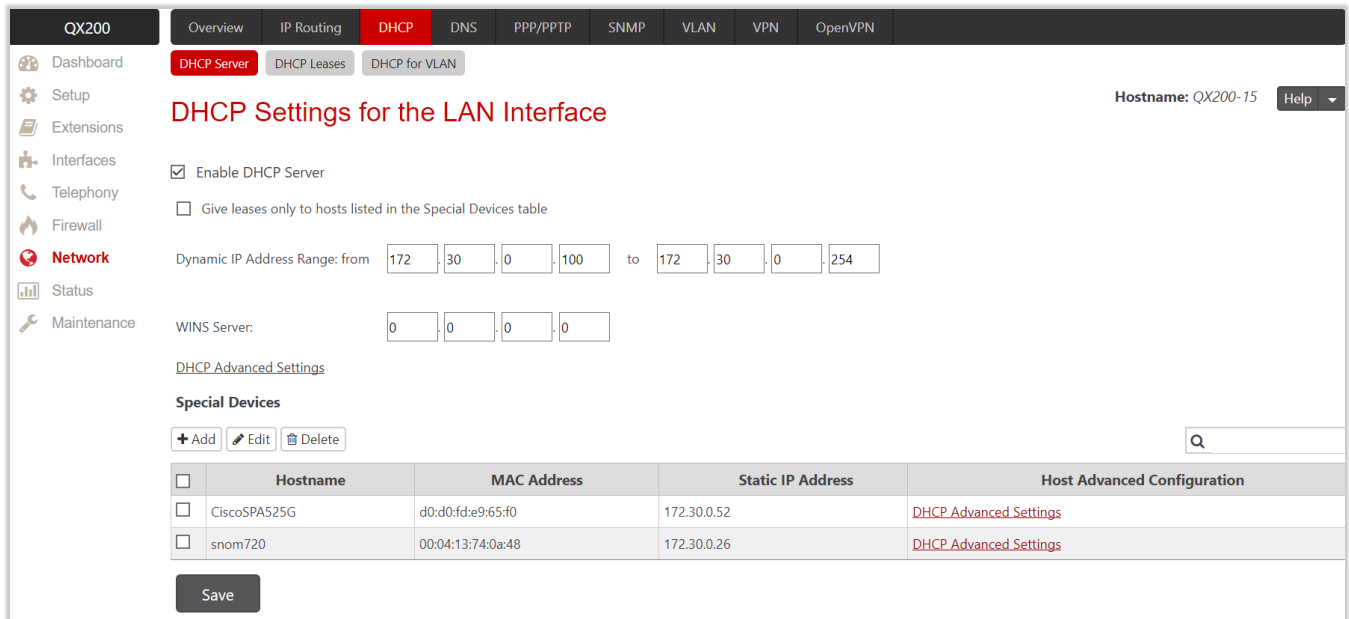
To add a new **PPTP/L2TP Route**:

1. Click **Add** and enter the following information:
  - **Route via** is used to select the available PPTP or L2TP connection from the drop-down list. A connection selected from this list will be used to route the IP packet from the QX LAN to the peer behind the PPTP/L2TP tunnel.
  - **Route to** is used to set the IP address range of the possible peers behind the PPTP/L2TP tunnel the IP packets should be routed to.
2. Click **Save** to add the new route to the **PPTP/L2TP Routes** table.
3. Click **Enable** to activate the newly created route.

## 10.3 DHCP

### 10.3.1 DHCP Server

The DHCP Settings for the LAN Interface page is used to enable DHCP server and configure network parameters for DHCP server.



The screenshot shows the 'DHCP Settings for the LAN Interface' page. It includes a navigation menu on the left with 'Network' selected. The main content area has the following elements:

- Navigation tabs: Overview, IP Routing, **DHCP**, DNS, PPP/PPTP, SNMP, VLAN, VPN, OpenVPN.
- Sub-tabs: **DHCP Server**, DHCP Leases, DHCP for VLAN.
- Page title: DHCP Settings for the LAN Interface. Hostname: QX200-15.
- Options:
  - Enable DHCP Server
  - Give leases only to hosts listed in the Special Devices table
- Dynamic IP Address Range: from 172.30.0.100 to 172.30.0.254
- WINS Server: 0.0.0.0
- Link: [DHCP Advanced Settings](#)
- Section: **Special Devices**
  - Buttons: + Add, Edit, Delete
  - Search: Q
- Table:
 

<input type="checkbox"/>	Hostname	MAC Address	Static IP Address	Host Advanced Configuration
<input type="checkbox"/>	CiscoSPA525G	d0:d0:fd:e9:65:f0	172.30.0.52	<a href="#">DHCP Advanced Settings</a>
<input type="checkbox"/>	snom720	00:04:13:74:0a:48	172.30.0.26	<a href="#">DHCP Advanced Settings</a>
- Save button

Figure 122: DHCP Settings page for the LAN interface page

The following settings (options) are available:

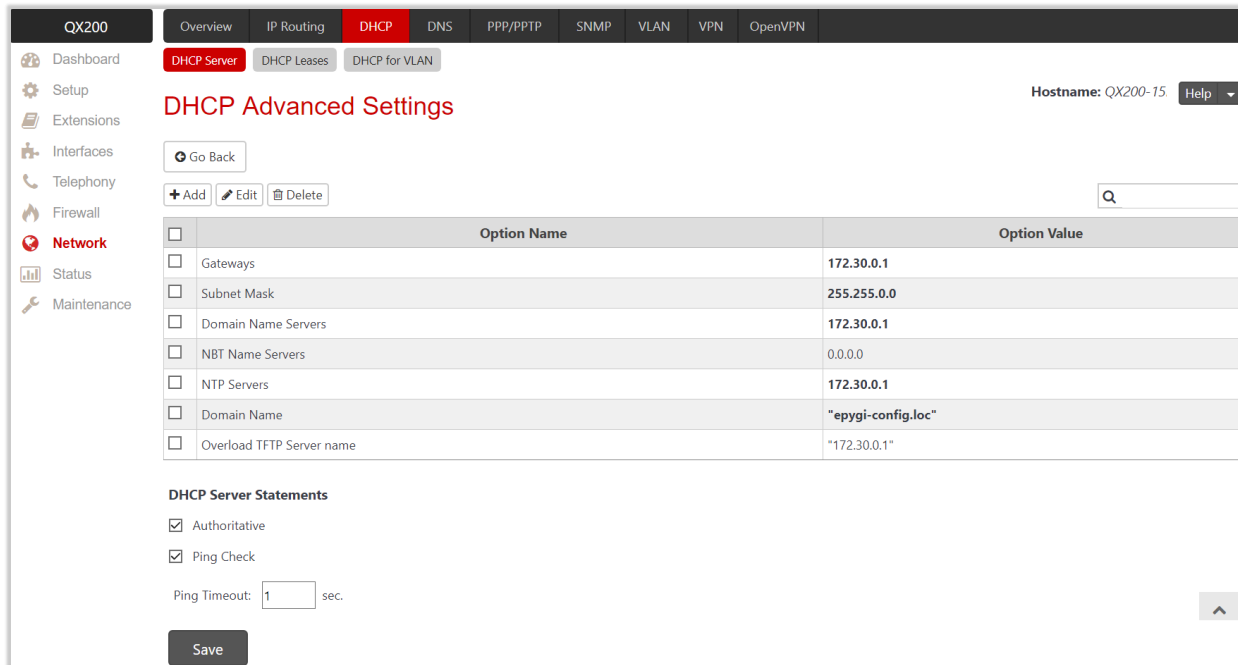
- **Enable DHCP Server** is used to activate DHCP service on LAN interface. If selected, the QX will be able to assign dynamic IP addresses to devices in QX LAN.
- **Give leases only to hosts listed in the Special Devices table** – if selected then DHCP services will be provided only to devices listed in the **Special Devices** table.
- **Dynamic IP Address Range (from to)** is used to set the range of IP addresses that will be assigned to devices (IP phones, PCs, etc.).
- **WINS Server** is used to set an IP address of WINS server.
- **DHCP Advanced Settings** leads to the [DHCP Advanced Settings](#) page to configure the advanced options for DHCP server.
- **Special Devices** allows to set a static IP address binding on the MAC address of the device. When this table is configured, the devices (with defined hostname and MAC address) will always get the same IP address from DHCP server. Devices not listed in this table will get dynamic IP addresses.

To add a new **Host**:

1. Click **Add** and enter the following information:
  - **Hostname**
  - **MAC Address**
  - **Static IP Address** is used to set a fixed IP address. **TIP:** If you leave this field blank, the device will get the first available IP address from the range defined in the **DHCP Settings** page.
2. Click **Save** to add the new host to the **Special Devices** table.

## DHCP Advanced Settings

The **DHCP Advanced Settings** page is used to add new advanced options of the DHCP server and modify the existing ones. The **DHCP Advanced Settings** table lists DHCP server default options. All options will be sent to the DHCP clients.



	Option Name	Option Value
<input type="checkbox"/>	Gateways	172.30.0.1
<input type="checkbox"/>	Subnet Mask	255.255.0.0
<input type="checkbox"/>	Domain Name Servers	172.30.0.1
<input type="checkbox"/>	NBT Name Servers	0.0.0.0
<input type="checkbox"/>	NTP Servers	172.30.0.1
<input type="checkbox"/>	Domain Name	"epygi-config.loc"
<input type="checkbox"/>	Overload TFTP Server name	"172.30.0.1"

**DHCP Server Statements**

Authoritative

Ping Check

Ping Timeout:  sec.

Figure 123: DHCP Advanced Settings page

To add a new DHCP option:

- Click **Add** and enter the following information:
  - Select one of the predefined DHCP server options or define a custom one.
  - **Predefined Options** is used to select one of the predefined DHCP server options.
    - ◆ **Option Name** is used to select DHCP server option.
    - ◆ **Option Value** is used to set the value for the selected option. **Type** and **format** of the value depends on the option selected from the **Option Name** list.
  - **Custom Options** is used to define a new DHCP server option. The following parameters must be entered for a new option:
    - ◆ **Option Code** is used to set a code for the option. It may have values in a range from **0** to **255**.
    - ◆ **Option Type** is used to select the type of the option value. It may be an IP address, a Boolean or integer value, etc.
    - ◆ **Option Value** is used to set the value of the option. This value depends on the selected **Option Type**.
- Click **Save** to add a new DHCP option to the **DHCP Advanced Settings** table.

### Note:

- Use commas to separate values in case of multiple entries.
- The changes made through the **System Configuration Wizard** regarding the DHCP server options will not immediately reflect on the **DHCP Advanced Settings** if option parameters of DHCP server are modified, so you will have to reconfigure changes in the **DHCP Advanced Settings** manually. The settings will be changed automatically if the parameters in DHCP server options are in "**bold**". In this case, the **DHCP Advanced Settings** will be changed automatically if you make changes through the **System Configuration Wizard**.

The following **DHCP Server Statements** are available:

- **Authoritative** is used to enable authoritative mode on DHCP server. **TIP:** If several DHCP servers are used on the network and QX has to provide network parameters to IP phones only, then disable this option.
- **Ping Check** – if selected, verifies the availability of an IP address on the network before providing it to a client. QX will first ping the IP address retrieved from the IP pool and wait for a reply. If no reply is received within a timeout specified in the **Ping Timeout**, the retrieved IP address will be provided to the client. Otherwise, a new IP address will be retrieved from the IP pool and the procedure will be repeated. If not selected, QX will provide an IP address immediately when requested.

### 10.3.2 DHCP Leases

The **DHCP Leases** table shows the list of clients that obtain a lease for an IP address from DHCP server. Before the lease expires, DHCP server will renew the lease for the client or the client will obtain a new lease. By default, the **DHCP address lease time** is 7 days.

IP Address	MAC Address	Lease Start	Lease End	Binding State	Hostname
172.30.4.183	d0:d0:fd:e9:65:f0	Mon Aug 07 20:08:41 2017	Mon Aug 14 20:08:41 2017	active	SEPD00DFDE965F0
172.30.4.182	00:08:5d:13:bc:15	Mon Aug 07 11:24:43 2017	Mon Aug 14 11:24:43 2017	active	6739i00085D13BC15
172.30.4.180	00:04:f2:81:3e:ef	Sun Aug 06 05:37:25 2017	Sun Aug 13 05:37:25 2017	active	Polycom_0004f2813eef

Figure 124: DHCP Leases page for LAN interface

### 10.3.3 DHCP for VLAN

The **DHCP Settings for the VLAN Interface** page is used to enable DHCP server and configure network parameters for DHCP server.

Enable DHCP Server

<input type="checkbox"/>	Vlan ID	IP Address Range	WINS Server
<input type="checkbox"/>	44	10.10.44.3 - 10.10.44.254	10.10.44.2
<input type="checkbox"/>	<b>30 ( Active )</b>	<b>10.10.30.2 - 10.10.30.254</b>	<b>10.10.30.1</b>

VLAN Settings

Figure 125: DHCP Settings for the VLAN Interface

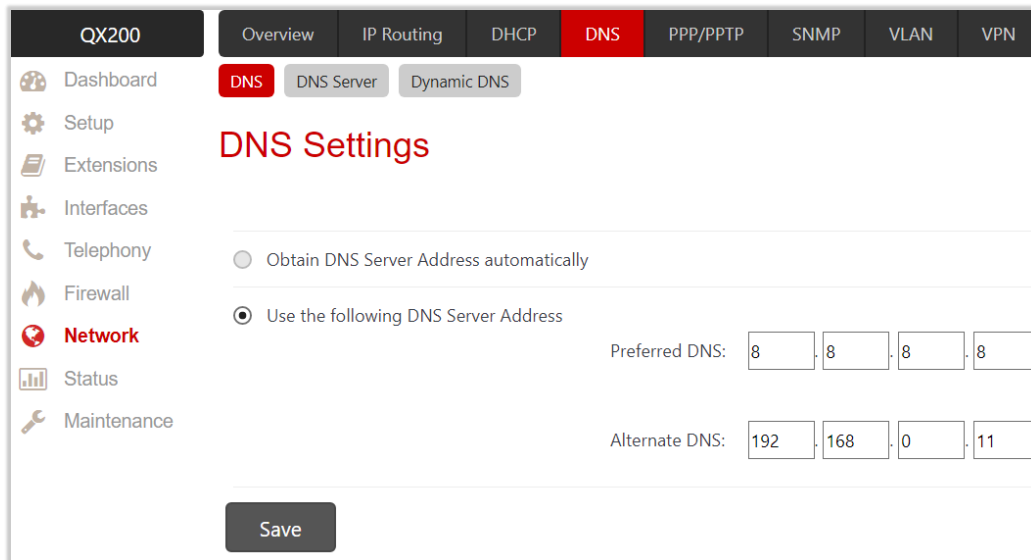
The **DHCP Settings for the VLAN Interface** table lists all **enabled** VLAN interfaces created in the **VLAN Settings** page. The following settings (options) are available:

- **Enable DHCP Server** is used to activate the DHCP service. If selected, QX will be able to assign dynamic IP addresses to devices (e.g. IP phones, PCs, etc.).
- **Activate** is used to activate the DHCP server for the selected VLAN interface. **TIP:** The DHCP server can be activated only for one VLAN interface at once.
- **Edit** is used to modify the selected VLAN interface. This page contains all the same settings and options as the [DHCP Server](#) page.
- **Go to VLAN Settings** leads to the [VLAN Settings](#) page to create a new VLAN or modify existing ones.

## 10.4 DNS

### 10.4.1 DNS

The **DNS Settings** page allows to set up name server(s) for QX.



The screenshot shows the 'DNS Settings' page in the QX200 interface. The top navigation bar includes 'QX200', 'Overview', 'IP Routing', 'DHCP', 'DNS' (highlighted), 'PPP/PPTP', 'SNMP', 'VLAN', and 'VPN'. Below this, there are sub-tabs for 'DNS', 'DNS Server', and 'Dynamic DNS'. The main content area is titled 'DNS Settings' and contains two radio button options: 'Obtain DNS Server Address automatically' (unselected) and 'Use the following DNS Server Address' (selected). Under the selected option, there are two rows of input fields: 'Preferred DNS' with values 8, 8, 8, 8 and 'Alternate DNS' with values 192, 168, 0, 11. A 'Save' button is located at the bottom of the form.

Figure 126: DNS Settings page

The following settings (options) are available:

- **Obtain DNS Server Address automatically** – if selected, QX will get the IP address of DNS server from local network or ISP automatically.
- **Use the following DNS Server Address** is used to manually assign a name server as follows:
  - **Preferred DNS** is used to set the IP address of name server.
  - **Alternate DNS** is used to set the IP address of the secondary name server that will be used if the main name server cannot be accessed.

## 10.4.2 DNS Server

The **DNS Server** returns the correct IP address to the requested domain name, so that any device located in the LAN side 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 and define a list of aliases for the devices.

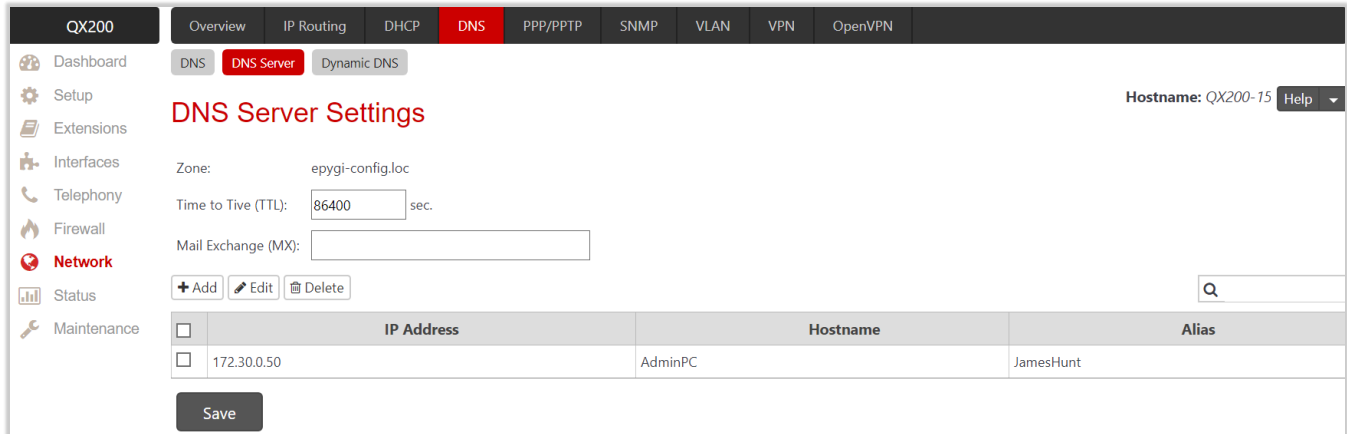


Figure 127: DNS Server Settings page

The following settings (options) are available:

- **Zone** displays the QX domain name as it is configured in the **System Configuration Wizard**.
- **Time to Live (TTL)** – 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. Once the timeout expires, the requested address will be resolved newly.
- **Mail Exchange (MX)** – 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 external network. The value in this field will be used in the MX record in the DNS server on the QX.

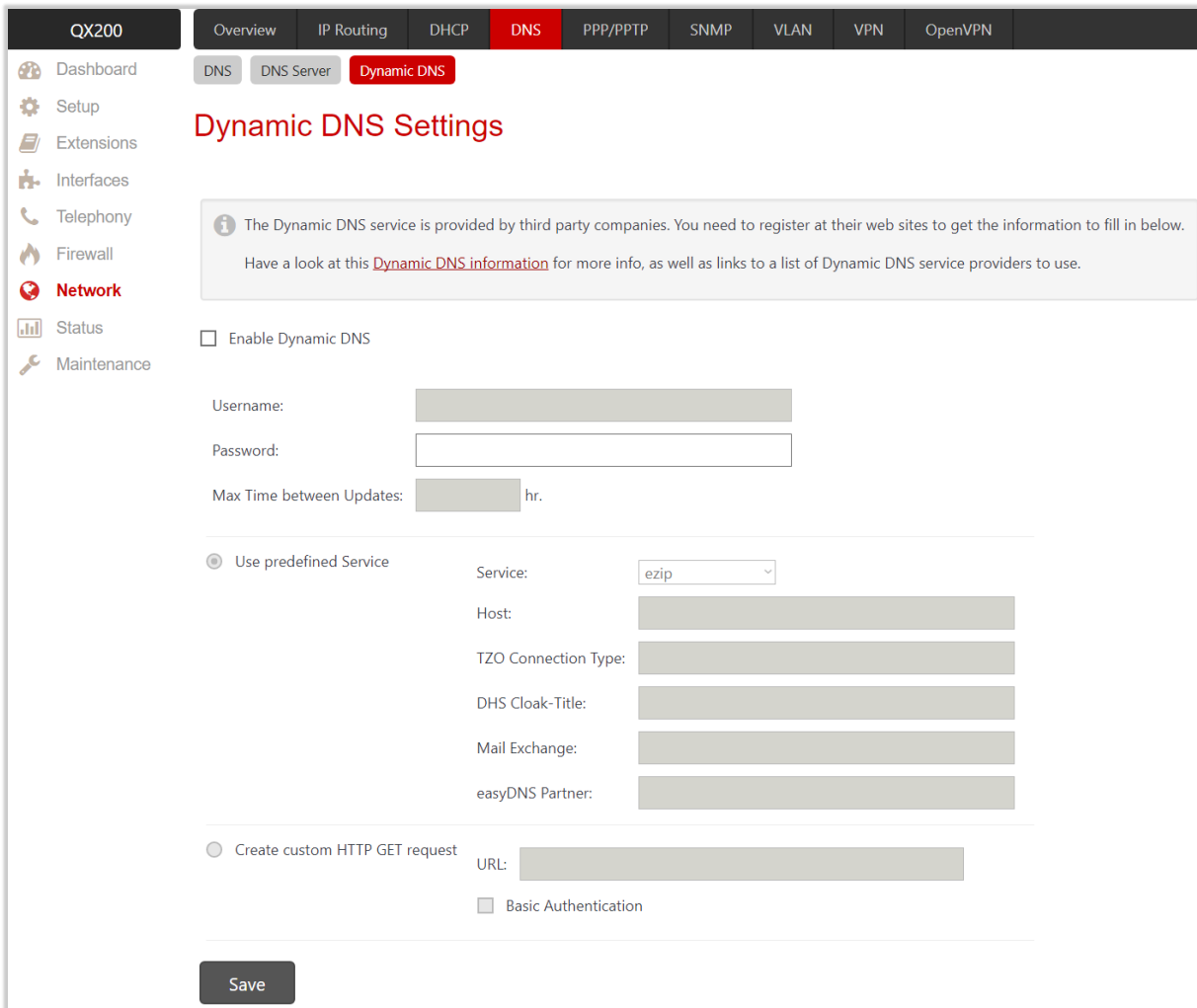
The **DNS Server Settings** table lists aliases for each host (device).

To add a new **Host**:

1. Click **Add** and enter the following information:
  - **IP Address**
  - **Hostname**
  - **Alias** is used to enter up to 5 alias names by which the device will be resolved.
2. Click **Save** to add the new host to the **DNS Server Settings** table.

### 10.4.3 Dynamic DNS

**Dynamic DNS** (DynDNS) associates your address with a consistent domain name without the need to buy a pricey static IP. Dynamic DNS can help by assigning a custom domain name to your IP address that will update automatically as your IP continues to change.



The screenshot shows the 'Dynamic DNS Settings' page in the QX200 web interface. The page has a dark header with navigation tabs: Overview, IP Routing, DHCP, DNS (selected), PPP/PPTP, SNMP, VLAN, VPN, and OpenVPN. A left sidebar contains a navigation menu with items: Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network (selected), Status, and Maintenance. The main content area is titled 'Dynamic DNS Settings' and features a warning box stating: 'The Dynamic DNS service is provided by third party companies. You need to register at their web sites to get the information to fill in below. Have a look at this [Dynamic DNS information](#) for more info, as well as links to a list of Dynamic DNS service providers to use.' Below the warning box, there is a checkbox for 'Enable Dynamic DNS'. Underneath, there are input fields for 'Username:', 'Password:', and 'Max Time between Updates:' (with a unit of 'hr.'). There are two radio button options: 'Use predefined Service' (selected) and 'Create custom HTTP GET request'. The 'Use predefined Service' section includes a 'Service:' dropdown menu (set to 'ezip'), and input fields for 'Host:', 'TZO Connection Type:', 'DHS Cloak-Title:', 'Mail Exchange:', and 'easyDNS Partner:'. The 'Create custom HTTP GET request' section includes a 'URL:' input field and a 'Basic Authentication' checkbox. A 'Save' button is located at the bottom left of the form area.

Figure 128: Dynamic DNS Settings page

The following settings (options) are available:

- **Enable Dynamic DNS** is used to activate service on QX. **TIP:** To activate the DynDNS service on ecQX, first, choose a DynDNS provider and register at the provider's website.
- **Username** and **Password** are used to set the authentication parameters specified during registration at the DynDNS provider.
- **Max Time between updates** is used to set the interval between two updates. The values entered in these fields should be greater than **24**. Normally, whenever you set up a connection to the Internet, the DynDNS is updated at least once in the period indicated in this field.
- **Use predefined Service** enables the manual configuration of the DynDNS service.
  - **Service** is used to select the provider to be subscribed to.
  - **Host** is used to set the name of the host on the Internet.
  - **TZO Connection Type** is used to set the special parameter required by the **TZO** provider.
  - **DHS Cloak-Title** is used to set the special parameter required by the **DHS** provider.



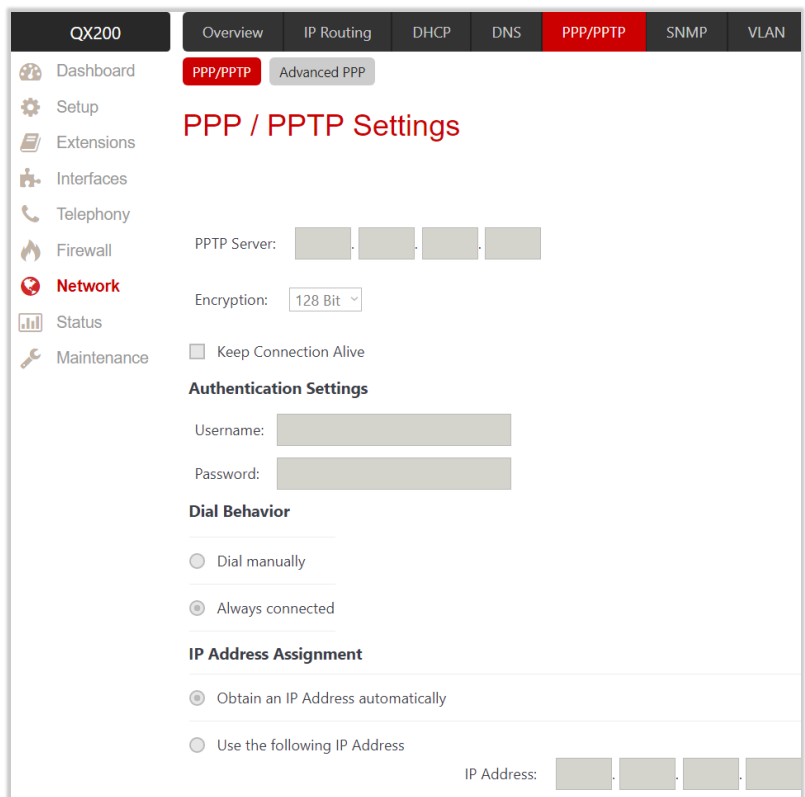
- **Mail Exchange** is used to set the address of the e-mail server the DynDNS service provider will relay e-mails to. If this service is used, ensure that port forwarding is configured for SMTP to the internal e-mail server.
- **easyDNS Partner** is used to enter a special parameter required by the DynDNS provider easyDNS.
- **Create Custom HTTP GET Request** is used to 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, click **Create Custom HTTP GET Request** and enter the appropriate value into the URL field.
- **URL** is used to set the complete request to be sent to the DynDNS server. The request modifies the name server database so that the hostname will be resolved to the new IP address.
- **Basic Authentication** 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's authentication settings. Most of the DynDNS providers require an authentication for security. Authentication parameters can be provided in the URL field to be used for the HTTP GET request. Select **Basic Authentication** if no authentication parameters are provided.

## 10.5 PPP/PPTP

### 10.5.1 PPP/PPTP

The **PPP/PPTP Settings** page is used to establish a connection over the DSL link, or any other type of uplink, to 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 and the provider, QX users will be able to make and receive calls at any time. The following settings (options) are available:

- **PPTP Server** is used to set the IP address of the PPTP server.
- **Encryption** is used to select the encryption for the traffic over the PPTP interface.
- **Keep Connection Alive** is used to keep the connection alive by sending control packets to verify the link state.
- **Authentication Settings** is used to set the authentication parameters (Username and Password) to register on the ISP server.
- **Dial manually** – if selected, a button will be displayed on the **Dashboard** to switch the connection on/off.
- **Always connected** – if selected, the connection will always stay active and connected.
- **IP Address Assignment** is used to select the IP address assignment type:
  - **Obtain an IP Address automatically** – if selected, QX will get the IP address from local network or ISP automatically.



The screenshot shows the 'PPP/PPTP Settings' page in the QX200 web interface. The page is titled 'PPP / PPTP Settings' and has a sub-tab 'Advanced PPP'. The settings are as follows:

- PPTP Server:** [Empty IP address field]
- Encryption:** 128 Bit
- Keep Connection Alive:**
- Authentication Settings:**
  - Username:** [Empty text field]
  - Password:** [Empty text field]
- Dial Behavior:**
  - Dial manually
  - Always connected
- IP Address Assignment:**
  - Obtain an IP Address automatically
  - Use the following IP Address
- IP Address:** [Empty IP address field]

Figure 129: PPP/PPTP Settings page

- Use the following IP Address is used to set the IP address manually.

## 10.5.2 Advanced PPP

The **Advanced PPP Settings** page is used to enable certain settings (options) of the negotiation process during connection establishment. These settings are available only if QX has a PPPoE WAN interface.

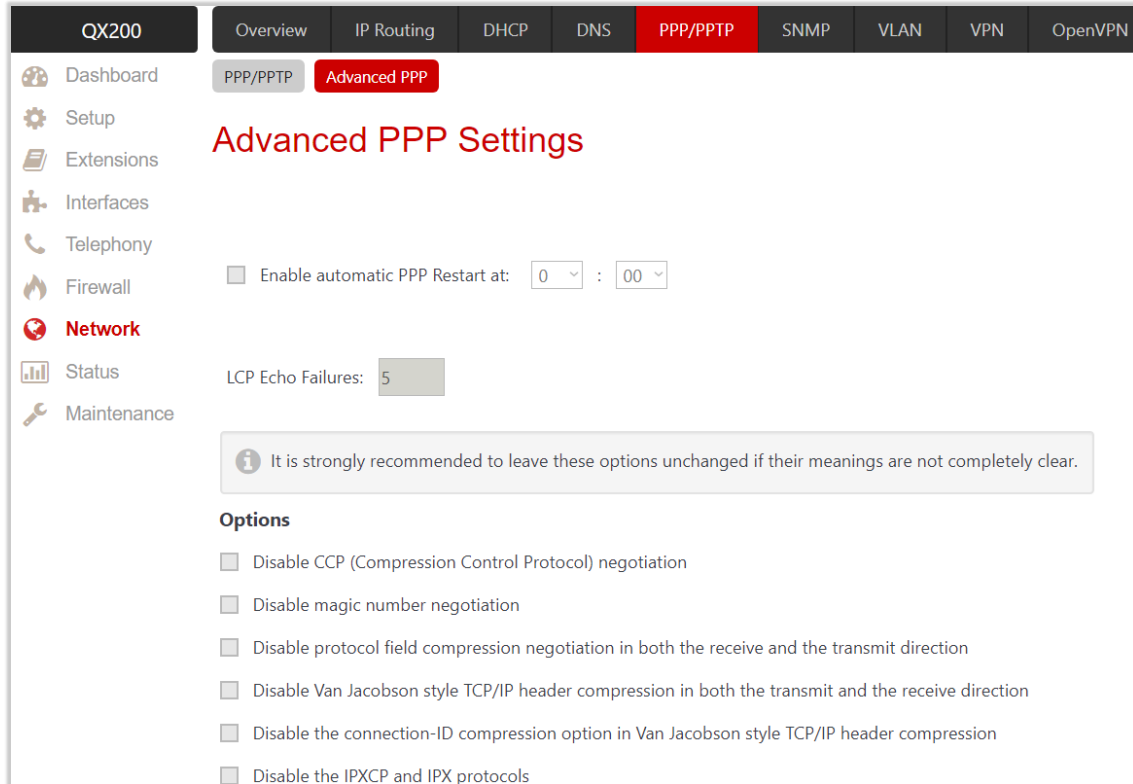


Figure 130: Advanced PPP Settings page

The following settings (options) are available:

- **Enable automatic PPP Restart** is used to select the time when the PPP connection will automatically be restarted.
- **LCP Echo Failures** shows 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** is used to select if the peer system is not working properly. For example, if it is not accepting requests from the PPPD (Point-to-Point Daemon) for CCP negotiation.
- **Disable magic number negotiation** is used to select if the peer system is not working properly. If selected, PPP cannot detect a looped-back line.
- **Disable protocol field compression negotiation in both the receive and the transmit direction** – if selected, no protocol field compression will take place.
- **Disable Van Jacobson style TCP/IP header compression in both the transmit and the receive direction** – if selected, 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** – if selected, PPPD will not compress the connection-ID byte from Van Jacobson and will not ask the peer to do so.

- **Disable the IPXCP and IPX protocols** is used to select if the peer is not working properly and cannot handle requests from PPPD for IPXCP negotiation.

**Note:** It is strongly recommended to leave these switches unchanged if their meanings are not completely clear.

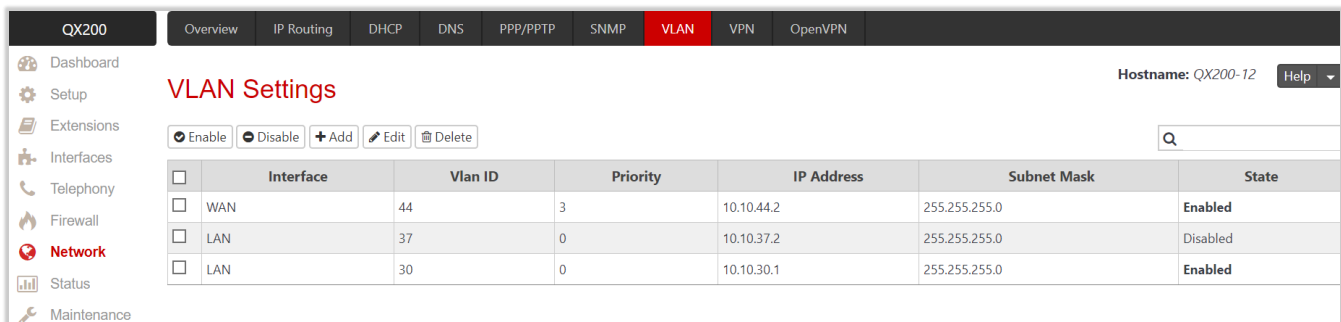
## 10.6 SNMP

**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. The SNMP agent is running to allow administrators to remotely manage QX network and device configuration.

For more information on how to configure and use **SNMP**, refer to the [Configuring SNMP Agent on QX IP PBXs](#) guide.

## 10.7 VLAN

The **VLAN Settings** page is used to create new VLAN interface(s) or modify the existing ones. The **VLAN Settings** table lists all existing virtual interfaces on QX.



<input type="checkbox"/>	Interface	Vlan ID	Priority	IP Address	Subnet Mask	State
<input type="checkbox"/>	WAN	44	3	10.10.44.2	255.255.255.0	Enabled
<input type="checkbox"/>	LAN	37	0	10.10.37.2	255.255.255.0	Disabled
<input type="checkbox"/>	LAN	30	0	10.10.30.1	255.255.255.0	Enabled

Figure 131: VLAN Settings page

To configure a new **VLAN interface**:

1. Click **Add** and enter the following information:
  - **Enable** is used to activate virtual interface after creating it.
  - **Interface Type** is used to select whether the virtual interface will be created on LAN or WAN interface.
  - **VLAN ID** is used to set the virtual network ID from the range of **0** to **4094**.
  - **Priority** is used to select the priority of packets in the corresponding interface. Packets with the lower priority (**0**) will be delivered first.
  - **IP Address** is used to set the IP address.
  - **Subnet Mask** is used to set the subnet mask.
2. Click **Save** to add the new interface to the **VLAN Settings** table.

## 10.8 VPN

**Virtual Private Network (VPN)** is used to connect two local networks (intranets) securely over the Internet. The VPN routers manage authentication between servers and clients and handle data encryption for the connection. In general, VPN connection is similar to Internet connection, both of them are based on IP detection.

VPN gateway must authenticate the IP addresses of the partner VPN gateway(s). Each time a specific VPN is to be established, the same IP addresses are usually expected. This will not create problems if both VPN partners have fixed WAN IP addresses. In some cases, you may use dynamically allocated IP addresses. Devices that use a dynamic IP address as part of a VPN, are turned into **Road Warriors** once they are enabled. Every VPN needs at least one VPN gateway with a fixed IP address.

The endpoints of a VPN must have different WAN IP addresses, and if they are connected to LAN, the LAN must have different IP addresses. As all QX 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.

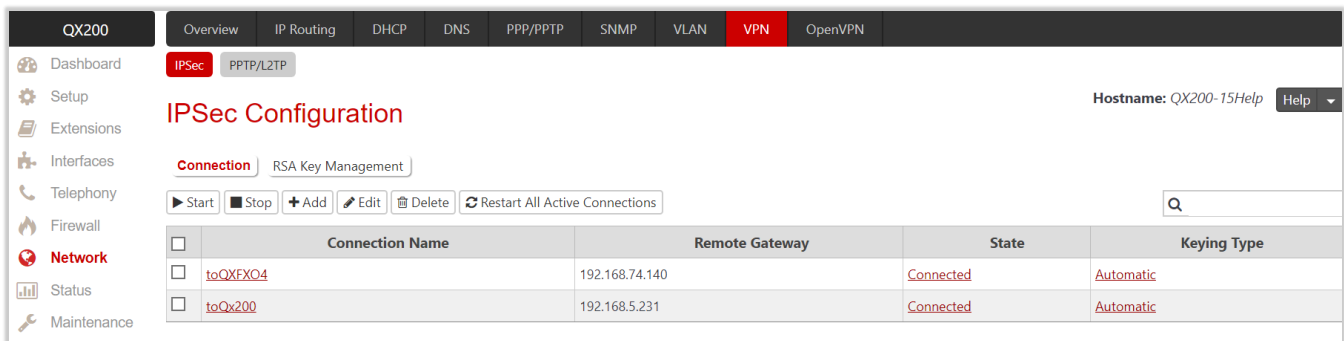
QX supports the following VPN connections: **IPSec**, **PPTP** and **L2TP**. **Note:** It is strongly recommended not to run different types of VPN tunnels between the same endpoints simultaneously.

### 10.8.1 IPSec

**Internet Protocol security (IPSec)** is a framework of open standards which aim to ensure private, secure communications over IP networks through the use of cryptographic security services. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. As IPSec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and as IPSec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP.

#### Connection

The **Connection** sub-page is used to create a new IPSec connection or manage the existing ones.



	Connection Name	Remote Gateway	State	Keying Type
<input type="checkbox"/>	toQXFX04	192.168.74.140	Connected	Automatic
<input type="checkbox"/>	toQx200	192.168.5.231	Connected	Automatic

Figure 132: IPSec Configuration – Connection Settings page

Click **Add** to run **IPSec Configuration Wizard** and configure a new connection. The wizard consists of the following sections:

- [New IPSec Connection](#)
- [IPSec Keying Properties](#)
- [Automatic Keying](#)
- [IPSec Connection Properties](#)
- [Summary](#)

#### New IPSec Connection

- **Connection Name** is used to enter the name of a new IPSec connection.
- **Peer Type** is used to select the remote machine type for the connection. If the required type of machine is not listed, choose **Other**.

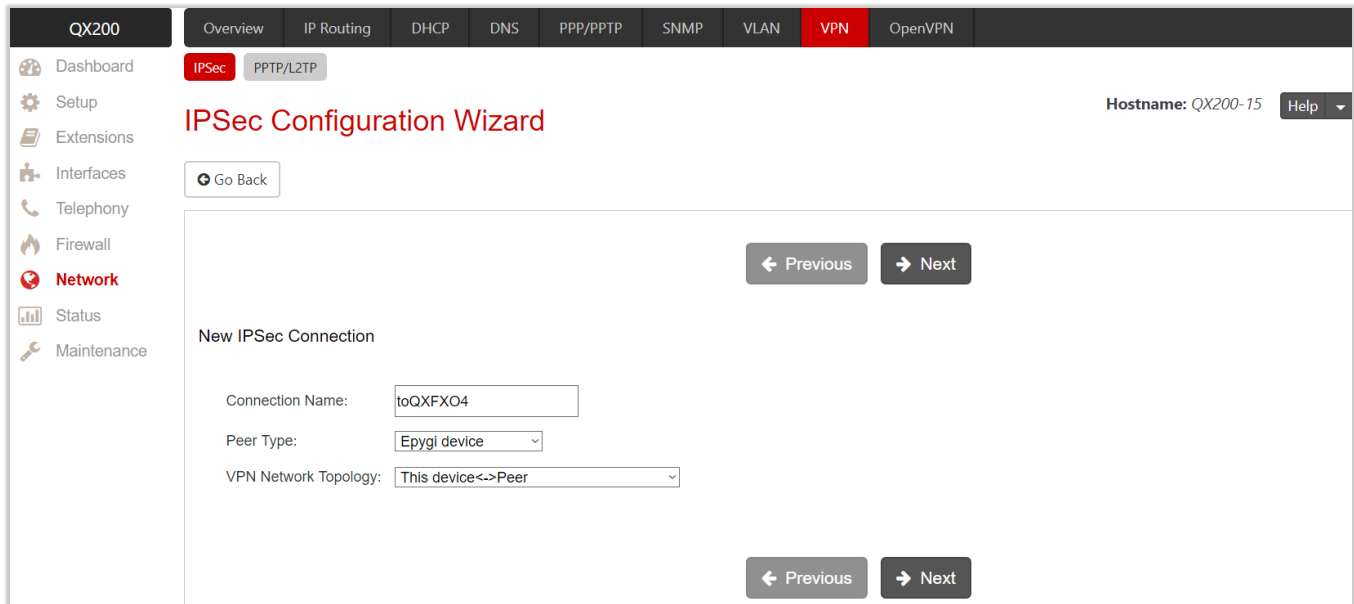


Figure 133: New IPsec Connection section

- **VPN Network Topology** is used to select the location of the peers participating to the VPN connection. The following options are available:
  - **This device<->Peer** – direct connection between QX and peer.
  - **This device<->[Internet]<->Peer** – connection between QX and peer over Internet.
  - **This device<->NAT<->[Internet]<->Peer** – connection between QX and peer over Internet through QX provider's NAT.
  - **This device<->[Internet]<->NAT<->Peer** – connection between QX and peer over Internet through peer provider's NAT.

### IPsec Keying Properties

The **Internet Key Exchange (IKE)** and **Encapsulated Security Payload (ESP)** parameters are used to define the security of your IPsec tunnel.

The IKE parameters group is used to set up **Security Association (SA)** in the IPsec protocol suite.

- **Encryption** is used to select encryption standard. The following standards are available:
  - **Triple DES** uses three different keys on a single data block 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.

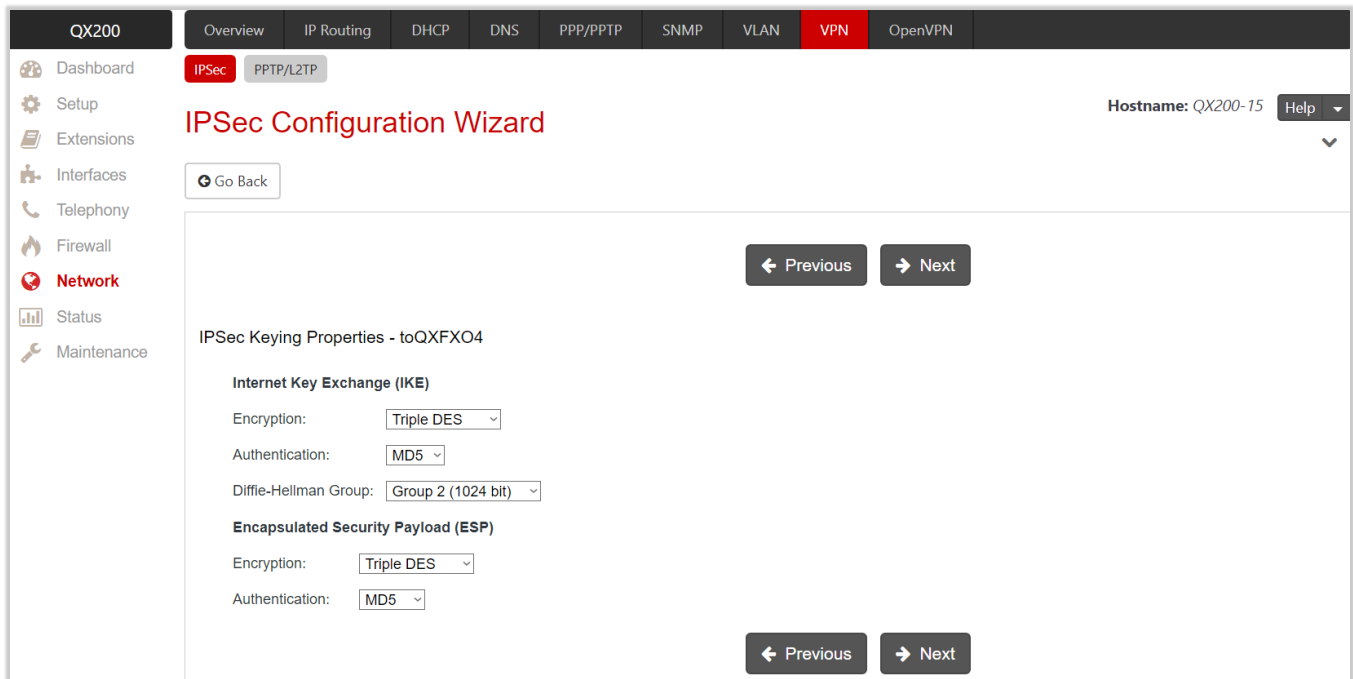


Figure 134: IPsec Keying Properties section

- **Authentication** is used to select authentication type:
  - **SHA (Secure Hash Algorithm)** is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPsec.
  - **MD5 (Message Digest)** is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.
- **Diffie-Hellman Group** 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 ESP parameters group is used to provide authenticity, integrity and confidentiality protection of packets. The same IKE encryption and authentication parameters are used.

## Automatic Keying

The **Automatic Keying** section is used to specify a **Shared Secret** password or RSA public key to secure the IPsec connection.

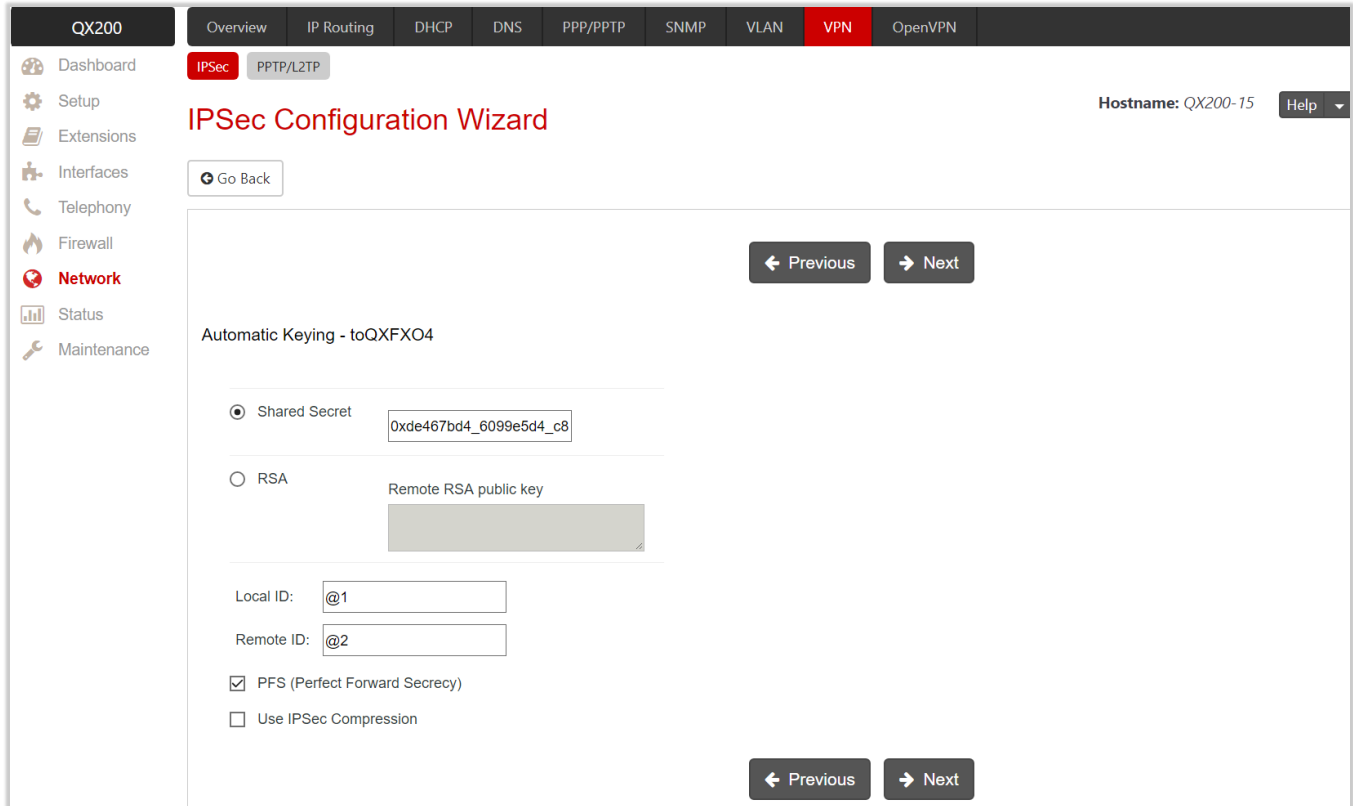


Figure 135: Automatic Keying section

- **Shared Secret** is a type of password 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.
- **RSA** is used to define the public RSA key of your IPsec connection partner.
- **Local ID** is used to set the QX **Fully Qualified Domain Name (FQDN)** that is resolved to an IP address, or any @-ed string that is used in the same way.
- **Remote ID** is used to set the remote endpoint FQDN that is resolved to an IP address, or any @-ed string that is used in the same way.

The **Local ID** and **Remote ID** fields can have the values in one of the formats presented below:

- ◆ **IP address** – for example: 10.1.19.32.
- ◆ **Hostname** – for example: vpn.epygi.com. This form requires additional resources to resolve the hostname, therefore it is not recommended to use this format.
- ◆ **@FQDN** – for 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** – for example: test1@vpn.epygi.com. This form is also considered as a string and is not being resolved. It has no advantage over the previous form.
- **PFS (Perfect Forward Secrecy)** is a procedure of a 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.

**Note:**

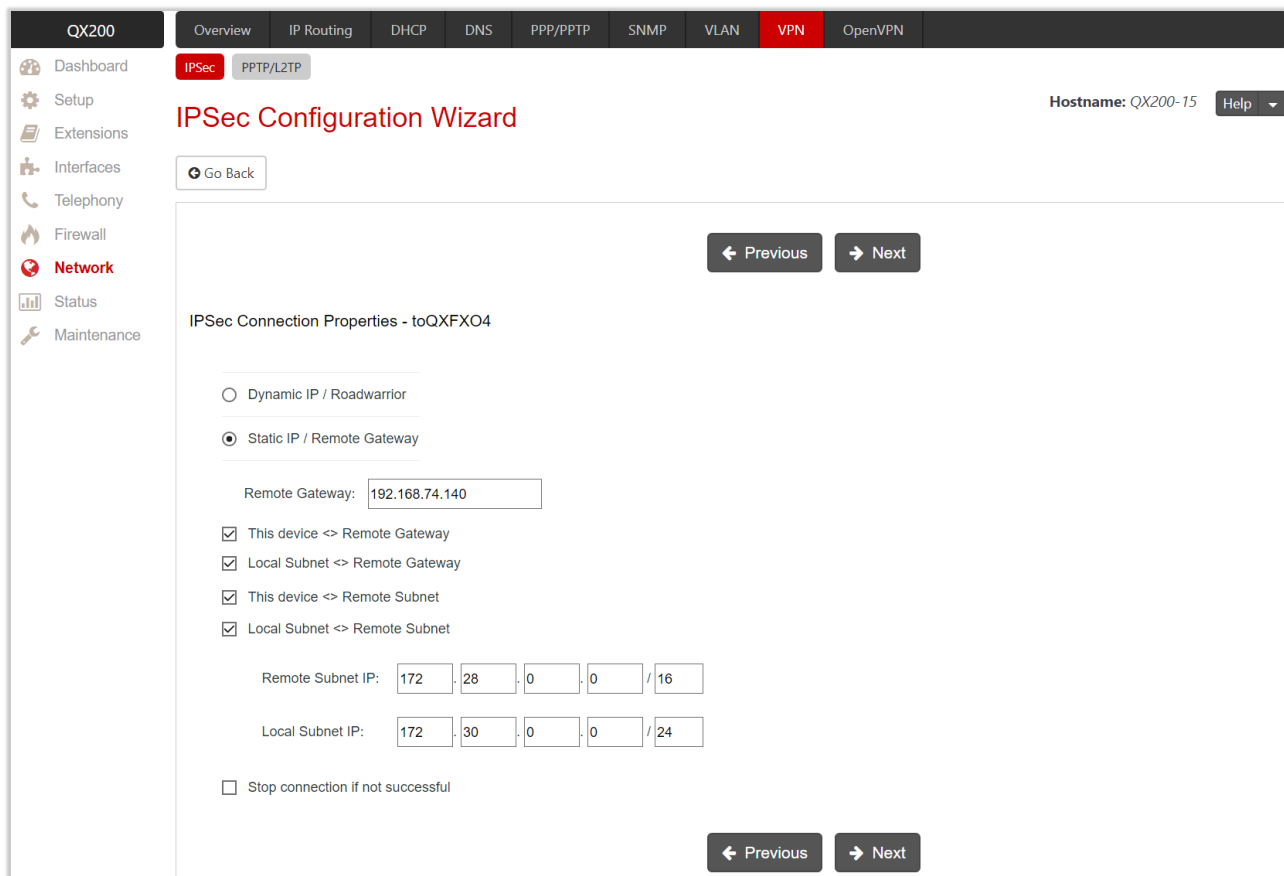
- It is not recommended to start multiple road warrior connections with the **Shared Secret** option selected. In order to start multiple road warriors simultaneously, it is recommended to use **RSA** option with **Local ID** and **Remote ID** fields configured.
- QX will prevent to start a connection with **Shared Secret** option selected if there is already a connection with **RSA** option started, and vice-versa.
- The **Local ID** and **Remote ID** values are mandatory for the **RSA** selection and are optional for **Shared Secret**. However, it is recommended to define the **Local ID** and **Remote ID** values for multiple road-warrior connections.

### IPSec Connection Properties

The **Dynamic IP/Road Warrior** and **Static IP/ Remote Gateway** radio buttons are used to select whether the remote QX (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**. The following settings (options) is used to configure IPSec connection:

- **Dynamic IP/RoadWarrior** – if selected, the **Remote Gateway IP Address** field will automatically generate the value "any", to allow access regardless of IP address.
- **Static IP/Remote Gateway** is used to set the IP address or hostname of the remote QX (or another VPN gateway device) in the **Remote Gateway** field.
- **This device<>Remote Gateway** allows to access from the local QX to the remote VPN gateway (local subnet and remote subnet are not included). This includes management access. The checkbox is disabled if the **This device<>NAT<>[Internet]<>Peer** or **This device<>[Internet]<>NAT<>Peer** option is selected from the **VPN Network Topology** drop-down list on the **New IPSec Connection** section.
- **Local Subnet<>Remote Gateway** allows to access from all stations connected to the local network to the remote VPN gateway device (local QX and remote subnet are not included). The checkbox is disabled when the **This device<>[Internet]<>NAT<>Peer** option is selected from the **VPN Network Topology** drop-down list on the **New IPSec Connection** section.
- **This device<>Remote Subnet** allows to access from the local QX to all stations of the remote LAN (local subnet and remote VPN gateway devices are not included). The checkbox is disabled when the **This device<>NAT<>[Internet]<>Peer** option is selected from the **VPN Network Topology** drop-down list on the **New IPSec Connection** section.
- **Local Subnet<>Remote Subnet** allows to 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 **Local Subnet IP** and **Remote Subnet IP** fields.
- **Stop connection if not successful** allows to stop the IPSec connection attempts if the partner remains unreachable after the timeout period. If not selected, the system will continue to try to reach the IPSec connection partner.





QX200 Overview IP Routing DHCP DNS PPP/PPTP SNMP VLAN **VPN** OpenVPN

Dashboard IPsec PPTP/L2TP Hostname: QX200-15 Help

Dashboard Setup Extensions Interfaces Telephony Firewall **Network** Status Maintenance

IPSec Configuration Wizard

Go Back

← Previous → Next

IPSec Connection Properties - toQXFXO4

Dynamic IP / Roadwarrior  
 Static IP / Remote Gateway

Remote Gateway: 192.168.74.140

This device <-> Remote Gateway  
 Local Subnet <-> Remote Gateway  
 This device <-> Remote Subnet  
 Local Subnet <-> Remote Subnet

Remote Subnet IP: 172 . 28 . 0 . 0 / 16

Local Subnet IP: 172 . 30 . 0 . 0 / 24

Stop connection if not successful

← Previous → Next

Figure 136: IPsec Connection Properties section

### Note:

- 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 is established first.
- The **Static IP/ Remote Gateway** selection is not applicable if the QX is positioned behind NAT, since the IP address of the remote gateway is not reachable directly in this case.

### Summary

This section displays all configured settings (options) before applying them.

## RSA Key Management

The **RSA Key Management** sub-page is used to generate a new RSA public key. This page also displays the current public RSA key and allows to send it to the IPsec connection partner.

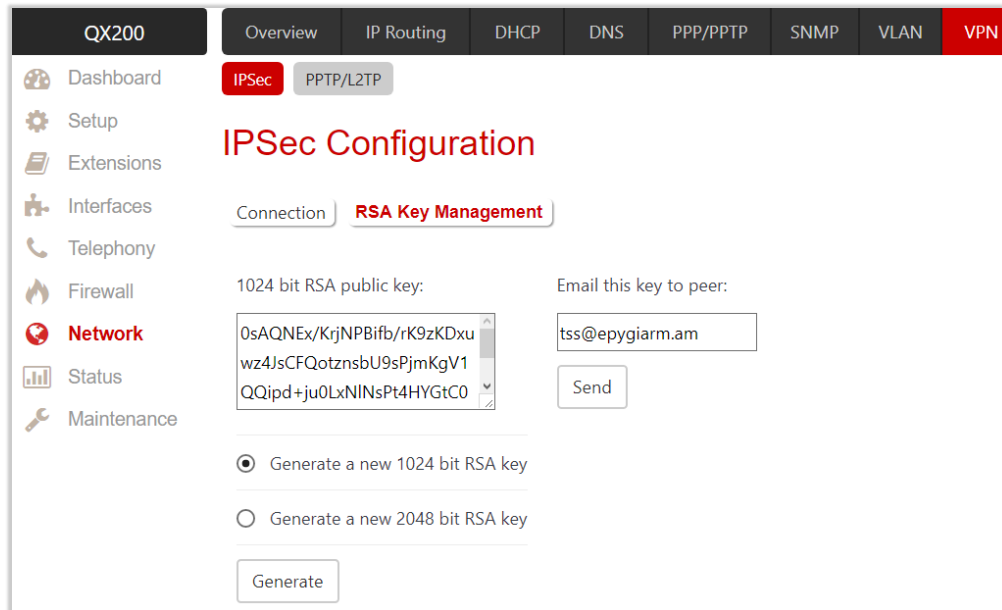


Figure 137: RSA Key Management page

To generate a new **RSA key**:

1. Select one of two available RSA key lengths (1024 or 2048).
2. Click **Generate** to generate the key.
3. Enter the e-mail address and click **Send** to send the generated key to the partner via e-mail.

**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.

### 10.8.2 PPTP/L2TP

**Point-to-Point Tunneling Protocol (PPTP)** is a set of communication rules that govern the secure implementation of VPNs, which allows organizations to extend their own private networks over the public Internet via "**tunnels**". PPTP enables the creation of a secure route of data transfer from a remote client to a server in a private enterprise network through the creation of a VPN over TCP/IP-based networks, such as the Internet. It allows remote users to securely access corporate networks over the Internet, as if the client is physically present in the corporate network.

**Layer 2 Tunneling Protocol (L2TP)** is a networking protocol used by ISPs to enable VPN operations. L2TP is similar to the **Data Link Layer Protocol** in the OSI reference model, but it is actually a session layer protocol.

For **PPTP** and **L2TP** connections, two parties are required: **Client** and **Server**. The client is responsible for establishing connection. The server is waiting for clients; it is not able to initiate the connection itself. Servers define the range of IP addresses that are assigned to the **Server** and **Clients** participating in the connection. Each side is specified by the **Hostname** and **Password**. The client should know the server name and password (QX server has no password) and the server should set the client's hostname and password. The client and server settings have to match on both sides for successful establishment of connection.

**Note:**

- L2TP tunnels have no data encryption mechanism.
- Only one client can be connected to the server in the same network.
- After creating a PPTP server connection, PPTP connections between devices placed on the QX 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.

## Connections

The **Connections** sub-page is used to create a new PPTP or L2TP connection or manage the existing ones.

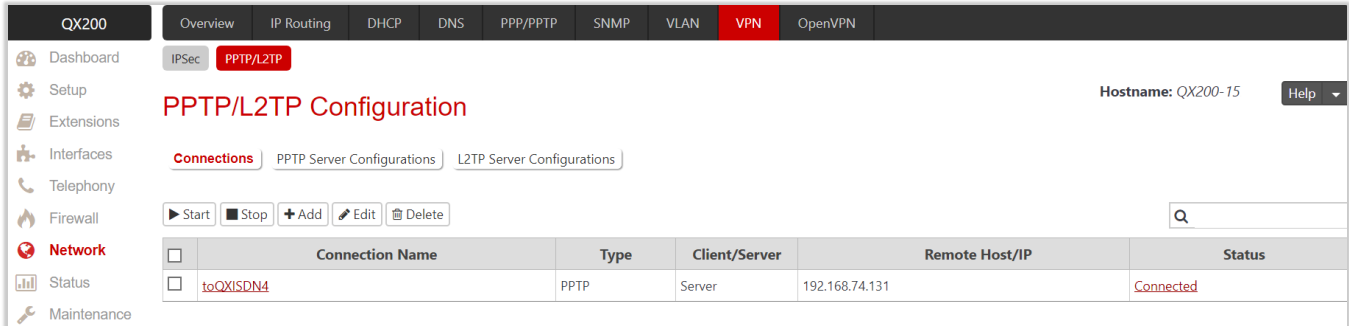


Figure 138: PPTP/L2TP Configuration – Connections page

Click **Add** to run **PPTP/L2TP Connection Wizard** and configure a new connection. The wizard consists of the following sections:

- [New PPTP/L2TP Connection](#)
- [PPTP Connection Properties](#)
- [Summary](#)

### New PPTP/L2TP Connection

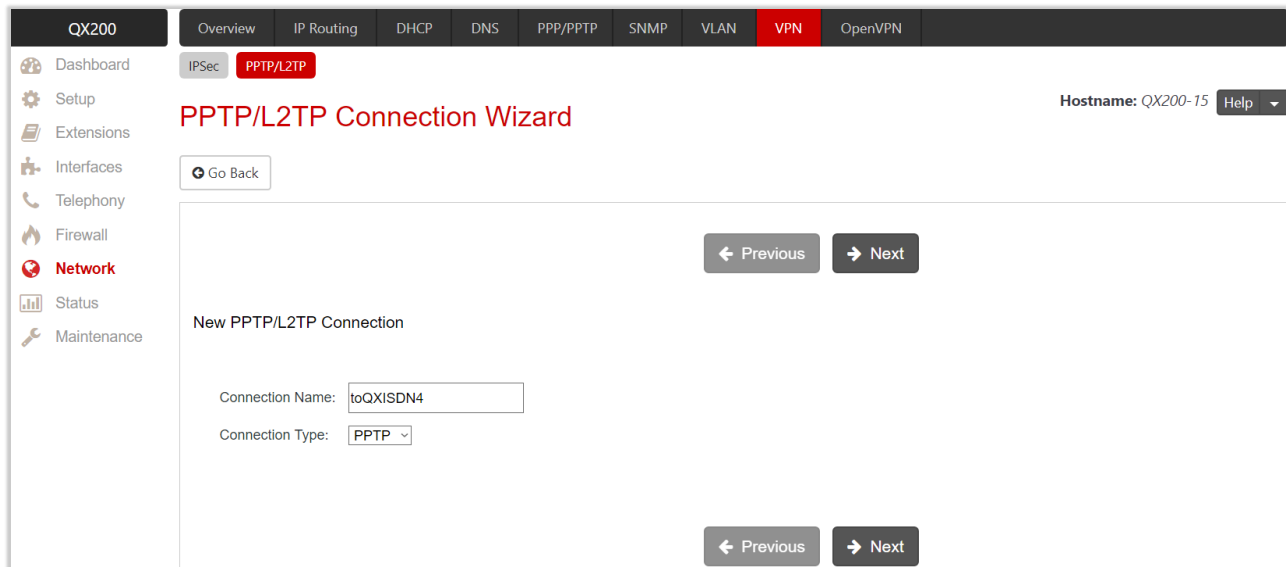
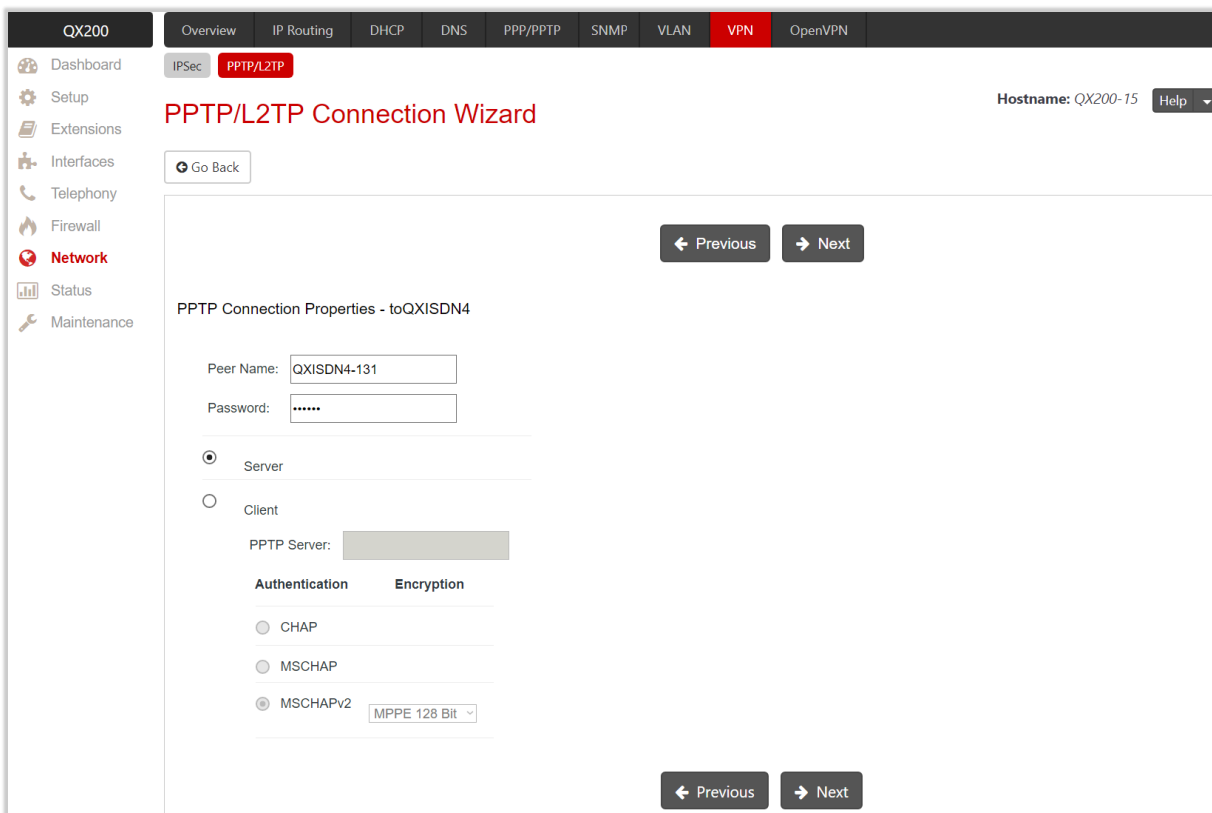


Figure 139: New PPTP/L2TP Connection section

- **Connection Name** is used to enter the connection name.
- **Connection Type** is used to select the type of connection (PPTP or L2TP).

### PPTP Connection Properties

- **Peer Name** is used to enter the connection peer name. **TIP:** The **Peer Name** must be written with Latin characters. When creating a connection with a Windows server, ensure that a user with QX **hostname** and **Dial-in access** exists on the server. When creating a connection with a Windows client, ensure that the specified **Peer Name** matches the **Dial-in connection username**.
- **Password** is used to enter the password.
- **Server/Client** is used to select whether the new connection will be a server or client. The following information should be configured when the **Client** option is selected:
  - **PPTP Server** (if the PPTP connection type is selected) is used to set the IP address or hostname of the PPTP server.
  - **L2TP Server** (if the L2TP connection type is selected) is used to set the IP address of the L2TP server.
- **Authentication** is used to select the authentication protocol. This section is available only if the PPTP connection type is selected on the previous section. The **MSCHAPv2** selection enables the **Encryption** drop-down list where the encryption method can be selected. **TIP:** These authentication settings should be identically configured on both peers for the successful connection.



The screenshot displays the 'PPTP/L2TP Connection Wizard' in the QX200 management console. The main content area is titled 'PPTP Connection Properties - toQXISDN4'. It includes the following fields and options:

- Peer Name:** QXISDN4-131
- Password:** Masked with dots.
- Server/Client Selection:**
  - Server
  - Client
- PPTP Server:** A greyed-out text input field.
- Authentication and Encryption:**
  - Authentication:**
    - CHAP
    - MSCHAP
    - MSCHAPv2
  - Encryption:** A dropdown menu showing 'MPPE 128 Bit'.

Navigation buttons for 'Previous' and 'Next' are located at the top and bottom of the form area.

Figure 140: PPTP/L2TP Connection Properties section

### Summary

This section displays all configured settings (options) before applying them.

## PPTP Server Configurations

The **PPTP Server Configuration** sub-page is used to configure the PPTP server settings.

- **Subnet** is used to set the IP address range for the PPTP server and clients within the PPTP tunnel. **TIP:** 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 must be different from the L2TP server subnet.
- **Authentication** is used to select the authentication protocol through which the client will communicate with the server. **TIP:** The **MSCHAPv2** selection enables **Encryption** drop-down list where the encryption method can be selected.

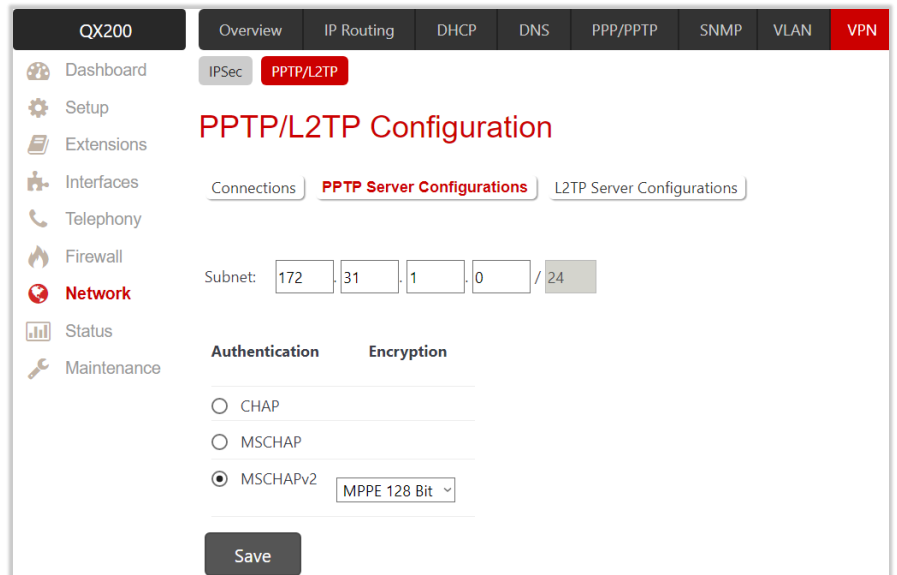


Figure 141: PPTP Server Configuration page

## L2TP Server Configuration

The **L2TP Server Configuration** sub-page is used to configure the L2TP server settings. The **Subnet** is used to set the IP address range for the L2TP server and clients within the L2TP tunnel. **TIP:** 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 must be different from the PPTP server subnet.

## 10.9 OpenVPN

**OpenVPN** allows secure point-to-point or site-to-site connections in routed or bridged configurations between the QX and other devices and remote access facilities. **OpenVPN** supports bidirectional authentication based on certificates, meaning that the client must authenticate the server certificate and the server must authenticate the client certificate before mutual trust is established.

Both server and client will authenticate each other first by verifying if the presented certificate was signed by the certificate authority (CA), then by checking the information in the now-authenticated certificate header, such as the certificate common name or certificate type (client or server).

For information on how to configure and use **OpenVPN** service, refer to the [OpenVPN Service on QX IP PBXs](#) and [Auto Configuration of Epygi Supported IP Phones using OpenVPN](#) guides.

## 11 Status Menu



The screenshot displays the 'Status' menu overview for a QX200 system. The interface includes a top navigation bar with tabs for Overview, System Status, Events, Call History, Conference History, Network Interfaces, and Statistics. A left-hand navigation menu lists various system components, with 'Status' currently selected. The main content area is titled 'Overview' and provides a detailed list of system status categories and their functions.

Category	Item	Description	
System Status	<a href="#">General</a>	Display system host name, uptime duration and firmware release.	
	<a href="#">Network</a>	View system interface settings and active services.	
	<a href="#">Lines</a>	Display status of all available telephony interfaces.	
	<a href="#">Memory</a>	Display available and allocated system memory.	
	<a href="#">Hardware</a>	Display status of various interface ports.	
	<a href="#">SIP Registration</a>	Display extensions registered to an external SIP server.	
	<a href="#">IP Lines Registration</a>	List configured IP lines and the registration status of the IP phone.	
	<a href="#">License</a>	List the software licenses that are assigned/allocated to specific extensions.	
	Events	<a href="#">System Events</a>	View recent system notification messages.
		<a href="#">Event Settings</a>	Determine the action to be taken for events.
Call History		<a href="#">Successful Calls</a>	Display current list of successful calls originated or received.
	<a href="#">Missed Calls</a>	List of missed (unanswered) calls.	
	<a href="#">Unsuccessful Outgoing Calls</a>	Outgoing call attempts that did not complete.	
	<a href="#">Call Cost</a>	Display calculated Call Cost.	
	<a href="#">Settings</a>	Download current call records or configure the number of call records to save.	
	<a href="#">Archive</a>	Chronological display of archived Call Detail Records.	
	<a href="#">Archiving Settings</a>	Options for archiving call records.	
Conference History	<a href="#">Conferences</a>	View call records specific to conference calls.	
	<a href="#">Successful Calls</a>	View call records of outbound calls originated from a conference bridge.	
	<a href="#">Unsuccessful Outgoing Calls</a>	View call records of unsuccessful outgoing call attempts made from a conference bridge.	
	<a href="#">Settings</a>	Download conference call detail records or configure number of call records to save.	
Network Interfaces	<a href="#">LAN</a>	Show current activity of the LAN (Local Area Network).	
	<a href="#">WAN</a>	Show current activity of the WAN (Wide Area Network).	
	<a href="#">VLAN</a>	Show current activity of the VLAN.	
	<a href="#">PPTP/L2TP</a>	Show current activity of the PPTP/L2TP.	
Statistics	<a href="#">Network Transfer</a>	Show the activity of LAN or WAN ports over a period of time.	
	<a href="#">PSTN Channel Usage</a>	Show the activity on the on-board PSTN (FXO, E1/T1 or ISDN) channels over a period of time.	

Figure 142: Staus Menu overview

## 11.1 System Status

### 11.1.1 General

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

- **Uptime Duration** shows the time period the QX is running since last reboot.
- **Device Hostname** shows the device hostname of QX.
- **Firmware Version** shows the version of the QX firmware and the file system.
- **Language Pack** – this information is presented only when a custom language pack is uploaded and indicates the version of language pack.

Name	Status
<b>Uptime Duration</b>	17 hour 1 min 33 sec
<b>Device Hostname</b>	QX200-12
<b>Firmware Version</b>	6.1.55
<b>Language Pack</b>	Español (Internacional) - x10

Figure 143: Status – General Information page

### 11.1.2 Network

The **Network Status** page provides information on available network interfaces and services on the QX.

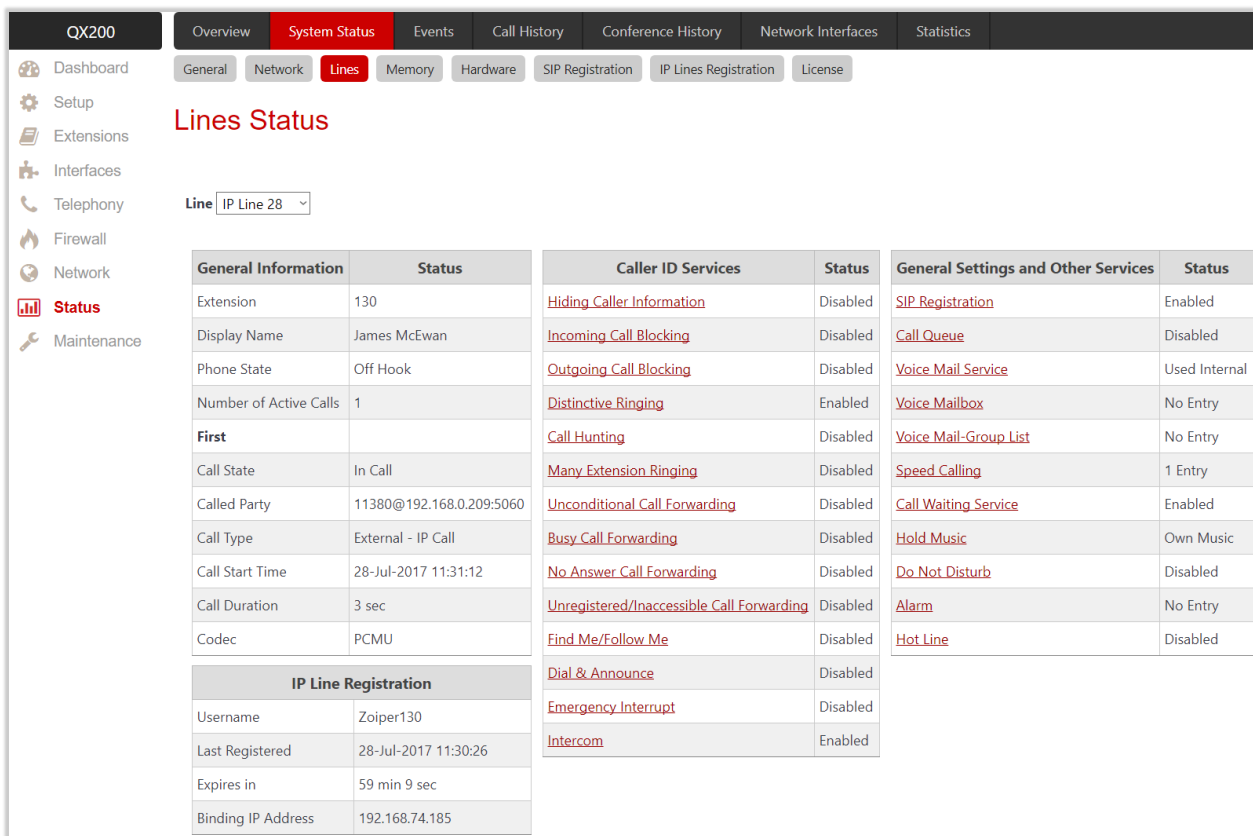
Interface Name	IP Address	Subnet Mask	Properties	Monitor	Service Name	Status	
WAN	192.168.74.12	255.255.255.0	MAC: 00-09-BD-91-01-02	<a href="#">Watch WAN</a>	<a href="#">NTP Server</a>	Running	
TUN0	10.26.0.1	255.255.255.0		<a href="#">Watch TUN0</a>	<a href="#">NTP Client</a>	Running	
LAN0.30	10.10.30.1	255.255.255.0	MAC: 00-09-BD-91-01-01	<a href="#">Watch LAN0.30</a>	<a href="#">DHCP Server for LAN</a>	Running	
WAN0.44	10.10.44.2	255.255.255.0	MAC: 00-09-BD-91-01-02	<a href="#">Watch WAN0.44</a>	<a href="#">DHCP Server for VLAN</a>	Running	
LAN	172.30.4.1	255.255.255.0	MAC: 00-09-BD-91-01-01	<a href="#">Watch LAN</a>	DHCP Client	Stopped	
<b>Default Gateway:</b> 192.168.74.5						<a href="#">DNS</a>	Running
<b>Preferred DNS:</b> 192.168.0.11						<a href="#">Firewall</a>	Low
<b>Alternate DNS:</b> 192.168.0.12						<a href="#">NAT</a>	Running
						<a href="#">PPP</a>	Stopped

Figure 144: Status – Network Status page

### 11.1.3 Lines

The **Lines Status** page displays the current status and general information for the selected **Line** or **Trunk**.

- **FXS Line** contains the following tables:
  - **General Information** shows the attached extension number, display name, the phone state and the number of active calls.
  - **Caller ID Services** shows the status for the **Caller ID Services** (enabled or disabled) on the attached extension.
  - **General Settings and Other Services** shows the settings and services configured on the attached extension.
- **IP Line** contains the following tables:
  - **General Information** shows the number of attached extension, display name, the phone state and the number of active calls.
  - **IP Line Registration** shows the IP line registration status.
  - **Caller ID Services** –shows the status for the **Caller ID Services** (enabled or disabled) on the attached extension.
  - **General Settings and Other Services** shows the settings and services configured on the attached extension.
- **FXO Line** shows the **Allowed Call Type**, the destination for **Incoming Calls** (user extension, auto attendant or Call Routing Table) and the **state** of the line (Free or Busy).
- **ISDN Trunk** shows the status of **B1** and **B2 channels** and the **state of the trunk** (Free or Busy). The table includes a group of static and dynamic parameters. The static parameters are always displayed. The dynamic parameters appear only whenever an event takes place on the channel.



The screenshot shows the 'Lines Status' page for 'IP Line 28'. The page is divided into several sections:

- General Information:** Extension: 130, Display Name: James McEwan, Phone State: Off Hook, Number of Active Calls: 1.
- Caller ID Services:** A table listing services like Hiding Caller Information, Incoming Call Blocking, Outgoing Call Blocking, Distinctive Ringing, Call Hunting, Many Extension Ringing, Unconditional Call Forwarding, Busy Call Forwarding, No Answer Call Forwarding, Unregistered/Inaccessible Call Forwarding, Find Me/Follow Me, Dial & Announce, Emergency Interrupt, and Intercom, with their respective statuses (Disabled or Enabled).
- General Settings and Other Services:** A table listing services like SIP Registration, Call Queue, Voice Mail Service, Voice Mailbox, Voice Mail-Group List, Speed Calling, Call Waiting Service, Hold Music, Do Not Disturb, Alarm, and Hot Line, with their respective statuses.
- IP Line Registration:** Username: Zoiper130, Last Registered: 28-Jul-2017 11:30:26, Expires in: 59 min 9 sec, Binding IP Address: 192.168.74.185.

Figure 145: Status – Lines Status page



### 11.1.4 Memory

The **Memory Status** pages show information on available memory size and memory allocation among the applications and services on the QX. The **Memory Size** is expressed in time units calculated using a [specific codec](#). The following sub-pages are available:

- **General Information** shows the memory size and current memory allocation (usage) between the system messages, voice mails, recorded calls and recorded conferences. The **Databases** table shows the memory size used by different QX services.
- **User Extension** shows the memory size available and currently allocated (used) to voice mails and recorded/uploaded system voice messages for each **user extension**. **Universal Extension Recordings** shows the space used to define the system default voice messages common for all user extensions.
- **Attendant** shows the memory size available and currently allocated (used) to recorded/uploaded system voice messages for each **auto attendant**.
- **Recorded Box** shows the memory size available and currently allocated (used) to recorded calls, recorded/uploaded system messages for each specific **Recording Box**. Only **G711 codec** is used to record calls.
- **ACD Queue** shows the memory size available and allocated (used) to recorded/uploaded system messages for each specific **ACD Queue**.
- **Conference** shows the memory size available and allocated (used) to currently recorded conferences and recorded/uploaded system voice messages for each **Conference**.

The screenshot shows the QX200 web interface. The top navigation bar includes 'Overview', 'System Status' (selected), 'Events', 'Call History', 'Conference History', 'Network Interfaces', and 'Statistics'. Below this, there are sub-tabs: 'General', 'Network', 'Lines', 'Memory' (selected), 'Hardware', 'SIP Registration', 'IP Lines Registration', and 'License'. The main content area is titled 'Memory - General Information' and has sub-tabs for 'General Information', 'User Extension', 'Attendant', 'Recording Box', 'ACD Queue', and 'Conference'. A note states: 'The system memory size is calculated according to the selected [recording codec](#).' Below this, it shows 'Device Memory size: 22 day 22 hour 32 min 50 sec (15484140 kB)'. The main data is presented in two tables:

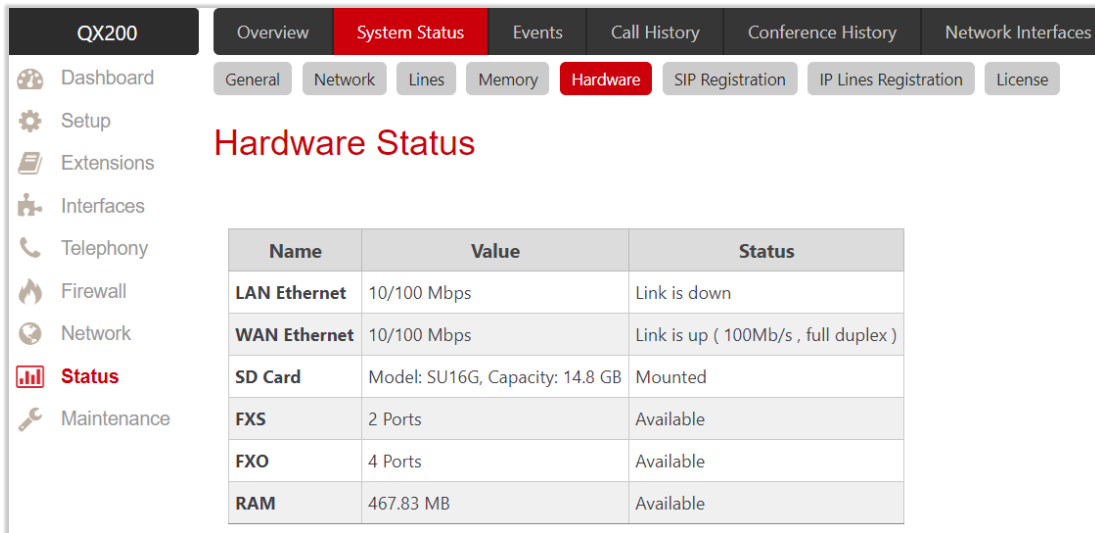
Memory Type	Size	Database	Size(kB)
System Messages	5 min 59 sec	<a href="#">Call History Archive (Used)</a>	412
Voice Mails	11 sec	<a href="#">Call History Archive (Allocated)</a>	154841
Recorded Calls	7 min 41 sec	<a href="#">Media Streamer (Used)</a>	388
Recorded Conferences	0 sec	<a href="#">Media Streamer (Allocated)</a>	15484
<b>Used Memory</b>	<b>13 min 51 sec</b>	ACD	1152
Free Memory	13 day 9 hour 0 min 57 sec	EAC Chat	320
<b>Total Allocated Memory</b>	<b>13 day 9 hour 14 min 48 sec</b>		

Figure 146: Status – Memory Status page

For more information on **Memory Status**, refer to the [Memory Management on QX IP PBXs](#) guide.

### 11.1.5 Hardware

The **Hardware Status** table shows the list of network interfaces, on-board and external devices and parts currently available on the QX with their parameters and statuses.



The screenshot shows the 'Hardware Status' page. The navigation menu on the left includes Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status (highlighted), and Maintenance. The main content area has a 'Hardware Status' heading and a table with the following data:

Name	Value	Status
LAN Ethernet	10/100 Mbps	Link is down
WAN Ethernet	10/100 Mbps	Link is up ( 100Mb/s , full duplex )
SD Card	Model: SU16G, Capacity: 14.8 GB	Mounted
FXS	2 Ports	Available
FXO	4 Ports	Available
RAM	467.83 MB	Available

Figure 147: Status – Hardware Status page

### 11.1.6 SIP Registration

The **SIP Registration Status** page displays information about the registration of QX extensions on SIP server(s). Information about the configured **SIP Tunnels** between Epygi devices is displayed here as well.



The screenshot shows the 'SIP Registration Status' page. The navigation menu on the left includes Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status (highlighted), and Maintenance. The main content area has a 'SIP Registration Status' heading and three tables:

**Registration on SIP Servers**

Extension	Username/DID Number	SIP Server	Registered	Registration Time
<a href="#">130</a>	7415130	192.168.0.209	Yes	28-Jul-2017 11:35:52
<a href="#">117</a>	174117	192.168.0.209	Yes	28-Jul-2017 11:25:10
<a href="#">103</a>	7415103	192.168.0.209	Yes	28-Jul-2017 11:25:10

**SIP Tunnels to Slave Devices**

Tunnel Name	Slave Device IP/Port	Registration State	Registration Date/Time
QX200toQXISDN4	192.168.74.131:5060	Registered	07/28/2017 - 11:38:46

**SIP Tunnels to Master Devices**

Tunnel Name	Master Device IP/Port	Registration State	Registration Date/Time
QX200toQXFXO4	192.168.74.140:5060	Registered	07/28/2017 - 11:35:12

Figure 148: Status – SIP Registration Status page

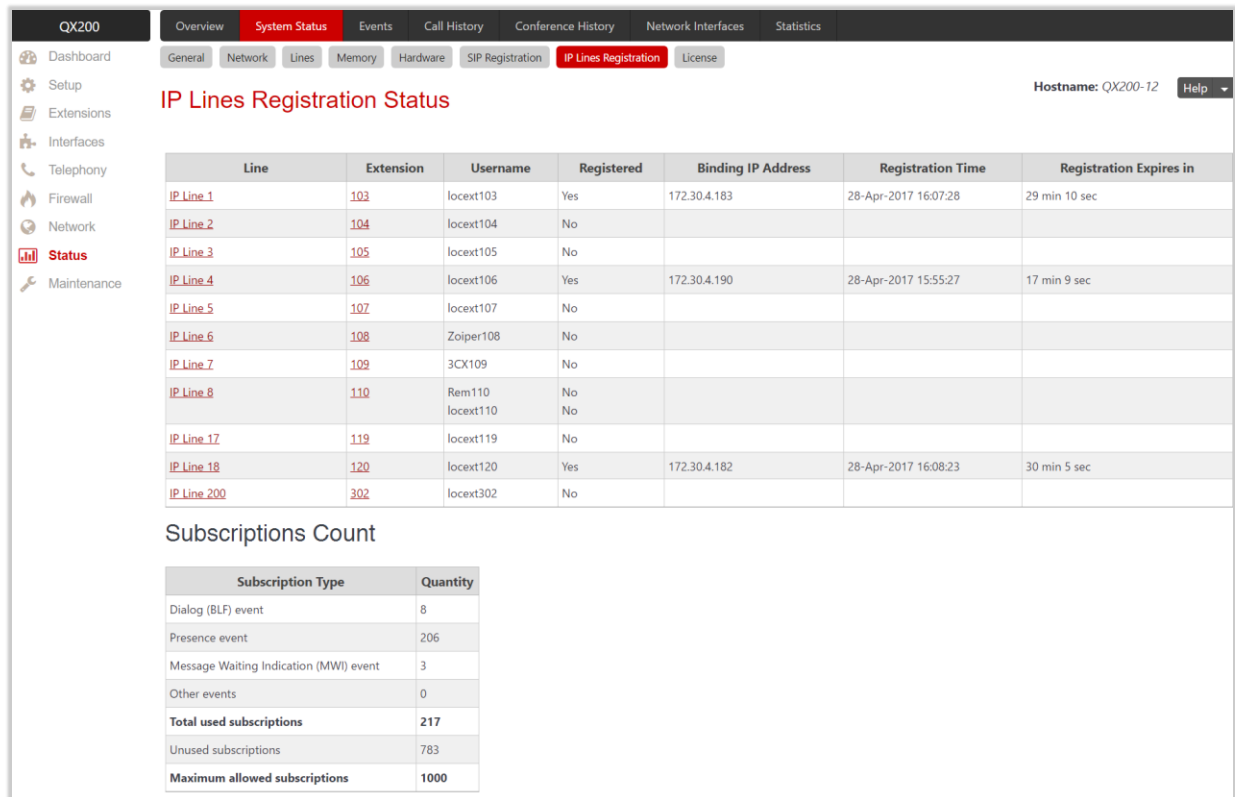
### 11.1.7 IP Lines Registration

The **IP Lines Registration Status** page provides information on IP lines registration and subscriptions used on the QX. The **IP Lines Registration table** lists the IP lines and remote extensions registered on the QX. The **Subscriptions Count** table shows the used and maximum allowed subscriptions on the QX. The subscriptions are events originated by QX services or IP phones. The following information is available:

- **Dialog (BLF) event** – IP phone's **Busy Lamp Field (BLF)** subscriptions, used for watching the extensions, as well as showing the states for other telephony services on the phone.
- **Message Waiting Indication (MWI) event** – IP phone's MWI subscriptions, used for voice mailbox status indication on the phone.
- **Presence event** and **Other events** are used by the QX internal services.

**Note:**

- When the allowed number of subscriptions is reached, new subscriptions are no longer possible. In order to avoid losing subscriptions, make sure the number of subscription is kept reasonably below the maximum allowed number.
- The number of **Maximum allowed subscriptions** can be changed from the `generalconfig.cgi` hidden page. Reboot the QX to apply changes.



Line	Extension	Username	Registered	Binding IP Address	Registration Time	Registration Expires in
IP Line 1	103	locext103	Yes	172.30.4.183	28-Apr-2017 16:07:28	29 min 10 sec
IP Line 2	104	locext104	No			
IP Line 3	105	locext105	No			
IP Line 4	106	locext106	Yes	172.30.4.190	28-Apr-2017 15:55:27	17 min 9 sec
IP Line 5	107	locext107	No			
IP Line 6	108	Zoiper108	No			
IP Line 7	109	3CX109	No			
IP Line 8	110	Rem110 locext110	No No			
IP Line 17	119	locext119	No			
IP Line 18	120	locext120	Yes	172.30.4.182	28-Apr-2017 16:08:23	30 min 5 sec
IP Line 200	302	locext302	No			

Subscription Type	Quantity
Dialog (BLF) event	8
Presence event	206
Message Waiting Indication (MWI) event	3
Other events	0
<b>Total used subscriptions</b>	<b>217</b>
Unused subscriptions	783
<b>Maximum allowed subscriptions</b>	<b>1000</b>

Figure 149: Status – IP Lines Registration Status page

## 11.1.8 License

The **License Status** page provides information about the following licensable features on the QX.

- DCC Basic
- DCC Pro
- iQall Mobile Toggling

License	Total	In Use	Attached Extensions
DCC Basic	6	1	106
DCC Pro	32	1	120
iQall Mobile Toggling	8	2	103 129

Figure 150: Status – License Status page

## 11.2 Events

### 11.2.1 System Events

The **System Events** page lists information about system events that have occurred on the QX. When a new event takes place, a record is added to the **System Event** table.

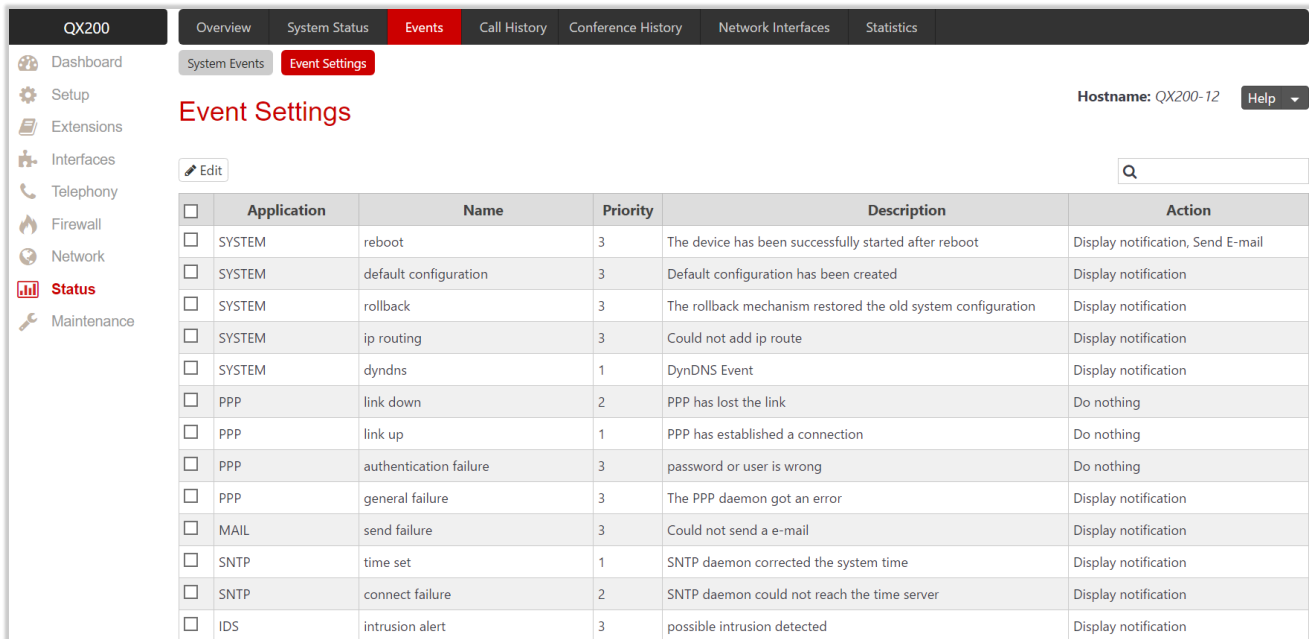
Status	Timestamp	Priority	Application	Name	Description	Reference
New	Mon May 1 17:57:16 2017	3	SIP	ip phone registration rejected	IP phone user SIPTunnel_QX200-74.12 [192.168.74.15:5060]: registration failed. Reason: No Such Line Configured.	IP Lines Registration Status
New	Mon May 1 17:53:09 2017	1	VPN	tunnel started	PPTP-Tunnel to toQX200-74.15 successfully started	VPN connections status
New	Mon May 1 17:16:48 2017	1	SIP	ip phone registration succeeded	IP phone user locext106 [172.30.4.190:5060] has registered.	IP Lines Registration Status
New	Mon May 1 17:16:39 2017	1	DHCPSEVER	distributed lease	IP address 172.30.4.190 given to MAC address 00:15:65:98:5d:d6 via lan0	DHCP Settings for the LAN Interface
New	Mon May 1 17:15:51 2017	3	SIP	ip phone registration lost	IP phone user locext106 [172.30.4.190:5060] has unregistered.	IP Lines Registration Status
New	Mon May 1 16:40:17 2017	1	SNTP	time set	time changed by -1.143350 secs to Mon May 1 16:40:17 2017 (ntp1.epygi.com)	Date / Time
New	Mon May 1 13:40:17 2017	1	SNTP	time set	time changed by -1.134968 secs to Mon May 1 13:40:17 2017 (ntp1.epygi.com)	Date / Time
New	Mon May 1 11:07:58 2017	1	SYSTEM	auto backup	Automatic backup completed.	Backup Configuration Management
New	Mon May 1 11:07:58 2017	1	SYSTEM	backup	Backup configuration complete (file size: 3736183 bytes).	

Figure 151: System Events list

The **System Events** table is the list of new and read system events. Events are marked by different colors 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). This 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 occurred. **TIP:** Once the administrator marks all new events as "read", the **Pending Events** link will disappear from **Top Menu** bar.

## 11.2.2 Event Settings

The **Event Settings** page lists all available events on QX and allows to notify admins/users in case of any event.



<input type="checkbox"/>	Application	Name	Priority	Description	Action
<input type="checkbox"/>	SYSTEM	reboot	3	The device has been successfully started after reboot	Display notification, Send E-mail
<input type="checkbox"/>	SYSTEM	default configuration	3	Default configuration has been created	Display notification
<input type="checkbox"/>	SYSTEM	rollback	3	The rollback mechanism restored the old system configuration	Display notification
<input type="checkbox"/>	SYSTEM	ip routing	3	Could not add ip route	Display notification
<input type="checkbox"/>	SYSTEM	dyndns	1	DynDNS Event	Display notification
<input type="checkbox"/>	PPP	link down	2	PPP has lost the link	Do nothing
<input type="checkbox"/>	PPP	link up	1	PPP has established a connection	Do nothing
<input type="checkbox"/>	PPP	authentication failure	3	password or user is wrong	Do nothing
<input type="checkbox"/>	PPP	general failure	3	The PPP daemon got an error	Display notification
<input type="checkbox"/>	MAIL	send failure	3	Could not send a e-mail	Display notification
<input type="checkbox"/>	SNTP	time set	1	SNTP daemon corrected the system time	Display notification
<input type="checkbox"/>	SNTP	connect failure	2	SNTP daemon could not reach the time server	Display notification
<input type="checkbox"/>	IDS	intrusion alert	3	possible intrusion detected	Display notification

Figure 152: Event Settings page

By default, the notification will be displayed in the **System Events** page. You can modify and select other notification methods (actions) as well.

To change the **Notification** option for the event:

1. Tick the **checkbox** next to the event and click **Edit**. Multiple selection is supported.
2. Tick the **checkbox** next to the available **Action**. The following actions are available:
  - **Display Notification** displays notification in the **System Events** page.
  - **Flash LED** – LED flashes every second. For some events, the LED will start flashing after a delay.
  - **Send Mail** –e-mail will be sent to the e-mail address(es) specified in the [E-mail Settings](#) page.
  - **Send SNMP Trap** – the trap will be sent to the traphost(s) listed in the [SNMP Trap Receiver Settings](#) table.
  - **Send SMS** –SMS will be sent to the mobile number specified in the [SMS Settings](#) page.
  - **Rest Request** – the notification will be sent to the **Monitoring** server(s) specified in the <https://xxx.xxx.xxx.xxx/ecmon> hidden page.
3. Click **Save** to apply changes.

**Note:**

- Actions that are not allowed for the selected event (e.g. mail notification if the PPP link is down or the mail server is configured improperly) are hidden. When editing multiple events, **Actions** that are not appropriate for one of the selected events will be hidden.
- In case of the IDS intrusion alert, only the first intrusion in each 10-minute period will raise an event.
- If QX cannot receive an IP address (from the DHCP or PPP servers) or cannot register an extension on the SIP server or cannot reach an NTP server, it raises only one event for the entire period the action has failed but will continue to try.

## 11.3 Call History

**Call History** allows to track and report the **Call Detail Records (CDRs)** for calls originated and terminated on QX, as well as for calls passed through QX.

### 11.3.1 Successful Calls, Missed Calls and Unsuccessful Outgoing Calls

The **Successful Calls**, **Missed Calls** and **Unsuccessful Outgoing Calls** pages list successful, missed and unsuccessful outgoing calls and their parameters. The following components are available:

- **Filter** allows to search for call records based on at least one of the following criteria: **Call Start Time**, **Call Duration**, **Call Cost**, **Caller** and **Called** parties.
- **Clear Filter** is used to remove the filter.
- The **Download** and **Download in CSV format** buttons are used to download the displayed CDRs for each page (Successful, Missed and Unsuccessful Outgoing) in (\*.log) and (\*.csv) formats respectively.

Number of Records	Total Duration	Maximum Duration	Average Duration	Minimum Duration	Total Cost
37	7 min 36 sec	2 min 32 sec	12 sec	0 sec	3.5

Call Start Time	Call Duration	Calling Phone	Called Phone	Billed Extension	Call Cost	Details
30-May-2018 14:46:11	7 sec	"Jack Brown" 105	11380@192.168.0.209:5060	105	1.17	Authenticated by: PIN code Close Reason: Got BYE message
23-May-2018 15:35:40	9 sec	"James Hunt" 103	11380@192.168.0.209:5060	103	1.5	Codec: PCMU, Quality: 1 (excellent) Close Reason: Got BYE message
30-May-2018 14:48:05	5 sec	"Jack Brown" 105	11380@192.168.0.209:5060	105	0.83	Codec: PCMU, Quality: 1 (excellent) Authenticated by: PIN code Close Reason: Got BYE message
30-May-2018 14:48:06	4 sec	"Jack Brown" 105	"Jack Brown" 105			Codec: PCMU, Quality: 1 (excellent)
30-May-2018 14:47:55	5 sec	"Jack Brown" 105	"James Hunt" 103			Codec: PCMU, Quality: 1 (excellent) call transferred
30-May-2018 14:47:48	0 sec	103	"Jack Brown" 105			call forwarded
30-May-2018 14:47:41	0 sec	116	"Jack Brown" 105			call forwarded
30-May-2018 14:47:26	0 sec	106	"Jack Brown" 105			call forwarded
30-May-2018 14:47:15	4 sec	"Amanda Pitt" 106	"Amanda Pitt" 116			Codec: PCMU, Quality: 1 (excellent)

Figure 153: Call History – Successful Calls page

CDRs listed in the **Call History – Successful Calls** table are characterized by the following parameters:

- Call Start Time
- Call Duration

- Calling Phone
- Called Phone
- **Billed Extension** shows the extension which is charged for the call (if available).
- **Call Cost** shows the calculated call cost (if available).
- **Details** provides the following additional information:
  - **Details** shows information on the call quality, audio codec and the call close reason. The call close reason appears to provide more information about the call termination, such as a network problem, call termination by one of the parties, **Voice Mail Service** activation, etc. The **Codec** link leads to the [RTP Statistics](#) page where the **RTP parameters** of the call are shown.
  - **Authenticated By** shows the authentication parameters (e.g. **login** or **PIN code**) used to pass the authentication when making a call.
  - Information about **FAX statistics** for the calls that have a FAX transmission handled. The **FAX** link leads to the [FAX Statistics](#) page where the **FAX parameters** of the call are shown.

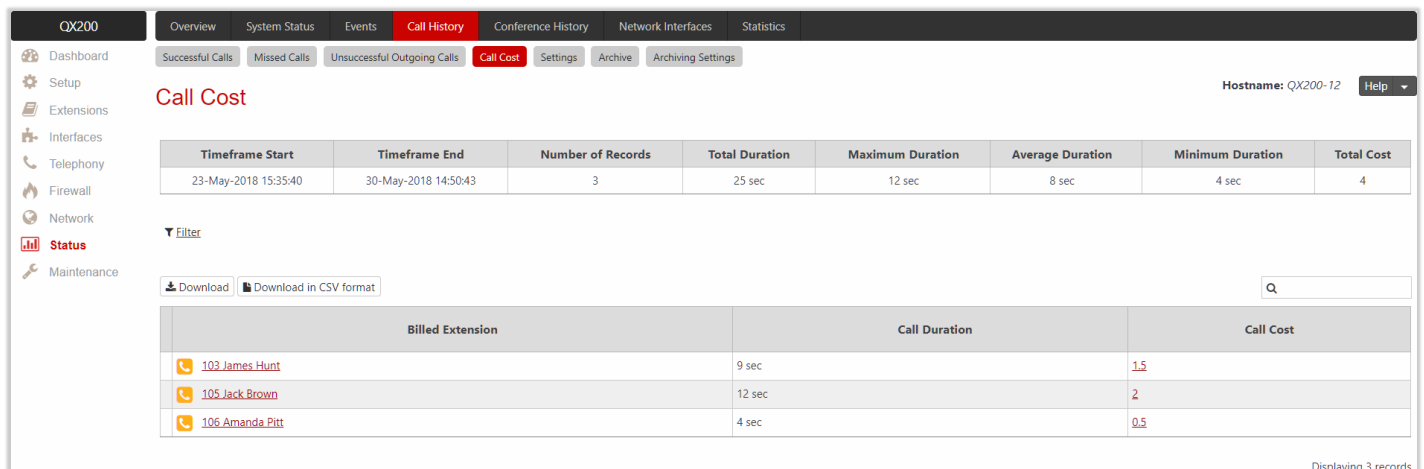
### 11.3.2 Call Cost

The **Call Cost** page shows the summarized information regarding the chargeable calls. The following components are available:

- **Filter** allows to search for call records based on at least one of the following criteria: **Timeframe**, **Duration**, **Call Cost** and **Billed Extension**.
- **Clear Filter** is used to remove the filter.
- The **Download** and **Download in CSV format** buttons are used to download the displayed CDRs in the (\*.log) and (\*.csv) formats respectively.

The **Call Cost** table is characterized by the following parameters:

- **Billed Extension** shows the extension which is charged for the call.
- **Duration** shows the total duration of all chargeable calls for the extension.
- **Cost** shows the total cost of all chargeable calls for the extension.



Timeframe Start	Timeframe End	Number of Records	Total Duration	Maximum Duration	Average Duration	Minimum Duration	Total Cost
23-May-2018 15:35:40	30-May-2018 14:50:43	3	25 sec	12 sec	8 sec	4 sec	4

Billed Extension	Call Duration	Call Cost
103 James Hunt	9 sec	1.5
105 Jack Brown	12 sec	2
106 Amanda Pitt	4 sec	0.5

Figure 154: Call Cost page

### 11.3.3 Settings

The **Call History – Settings** page is used to configure specific parameters for displaying **Call History**. The following settings (options) are available:

- **Enable Call Reporting** is used to activate service and allows to select the maximum number of CDR entries to be displayed in the **Call History** tables respectively.
- **Maximum Number of Successful/Missed/Unsuccessful Call Records** is used to select the maximum number of CDR entries to be displayed in the **Call History** tables. When the number of CDRs exceeds the defined numbers, the oldest entries will be automatically deleted. To keep the **Call History** safe, configure and use the [Archiving Settings](#) service.
- **CDR Parameters** section provides the full list for CDR parameters on QX. You can select the specific parameters to be excluded from the downloaded/archived CDR files to make them more compact, thus more readable. For detailed information about **CDR parameters**, refer to the [Call Detail Records on QX IP PBXs](#) guide.

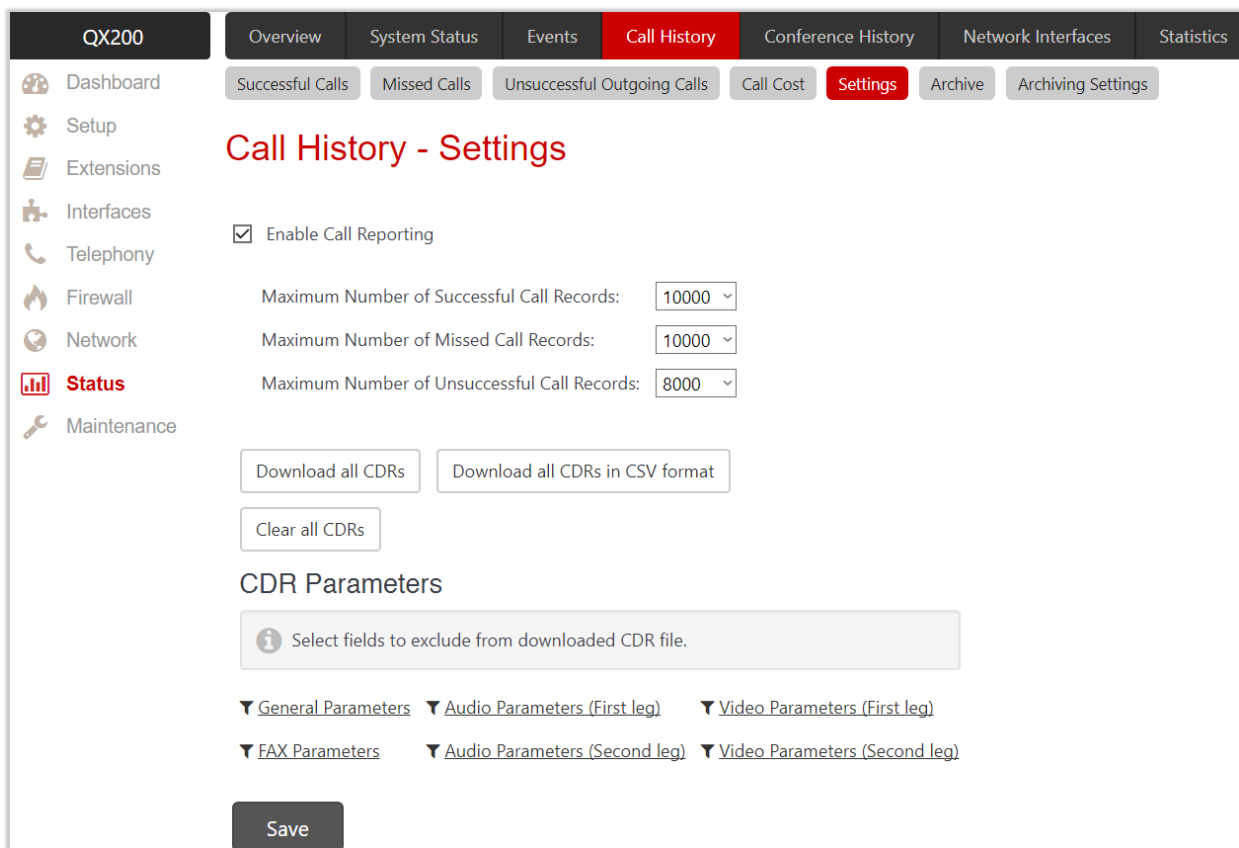


Figure 155: Call History – Settings page

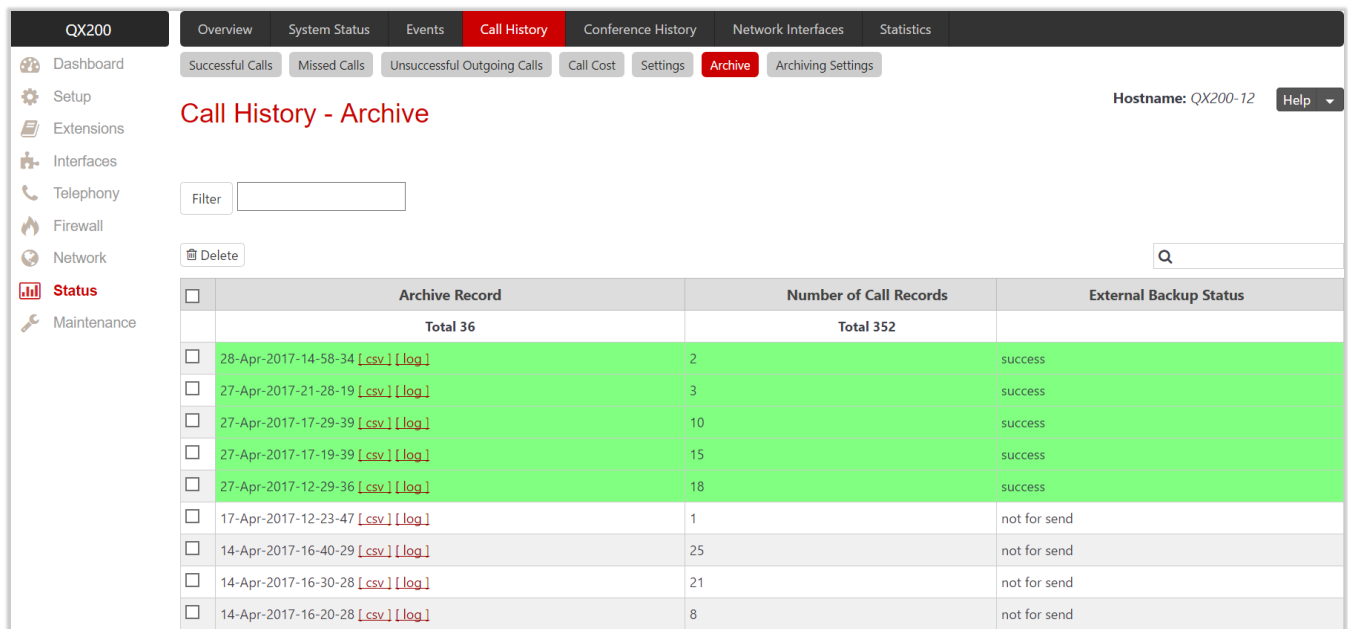
### 11.3.4 Archive

The **Call History – Archive** page shows the archived CDR files and allows the user to download them either in (\*.log) and (\*.csv) format.

The following functions are available on this page:

- **Filter** allows to search for specific archived CDR records in the **Archive** table by the record's full name or some part of the name.
- **Delete** is used to remove the selected record(s) from the **Archive**.
- **Clear all Records** is used to remove all archived files.





	Archive Record	Number of Call Records	External Backup Status
	<b>Total 36</b>	<b>Total 352</b>	
<input type="checkbox"/>	28-Apr-2017-14-58-34 [ csv ] [ log ]	2	success
<input type="checkbox"/>	27-Apr-2017-21-28-19 [ csv ] [ log ]	3	success
<input type="checkbox"/>	27-Apr-2017-17-29-39 [ csv ] [ log ]	10	success
<input type="checkbox"/>	27-Apr-2017-17-19-39 [ csv ] [ log ]	15	success
<input type="checkbox"/>	27-Apr-2017-12-29-36 [ csv ] [ log ]	18	success
<input type="checkbox"/>	17-Apr-2017-12-23-47 [ csv ] [ log ]	1	not for send
<input type="checkbox"/>	14-Apr-2017-16-40-29 [ csv ] [ log ]	25	not for send
<input type="checkbox"/>	14-Apr-2017-16-30-28 [ csv ] [ log ]	21	not for send
<input type="checkbox"/>	14-Apr-2017-16-20-28 [ csv ] [ log ]	8	not for send

Figure 156: Call History – Archive page

CDRs listed in the **Call History – Archive** table are characterized by the following specifications:

- **Archive Records** shows the archived record (file) name which is actually the archiving date and time. Click the hyperlinked [ csv ] or [ log ] to download the archived file.
- **Number of Call Records** shows the number of call records in the archived file.
- **External Backup Status** shows the status of the archived file backup. The following statuses are available:
  - **Success** shows that the archived file has been successfully backed up.
  - **Failed** shows that the archived file failed to be backed up. The **Try to send now** link will appear next to this status allowing to repeat the backup process.

### 11.3.5 Archiving Settings

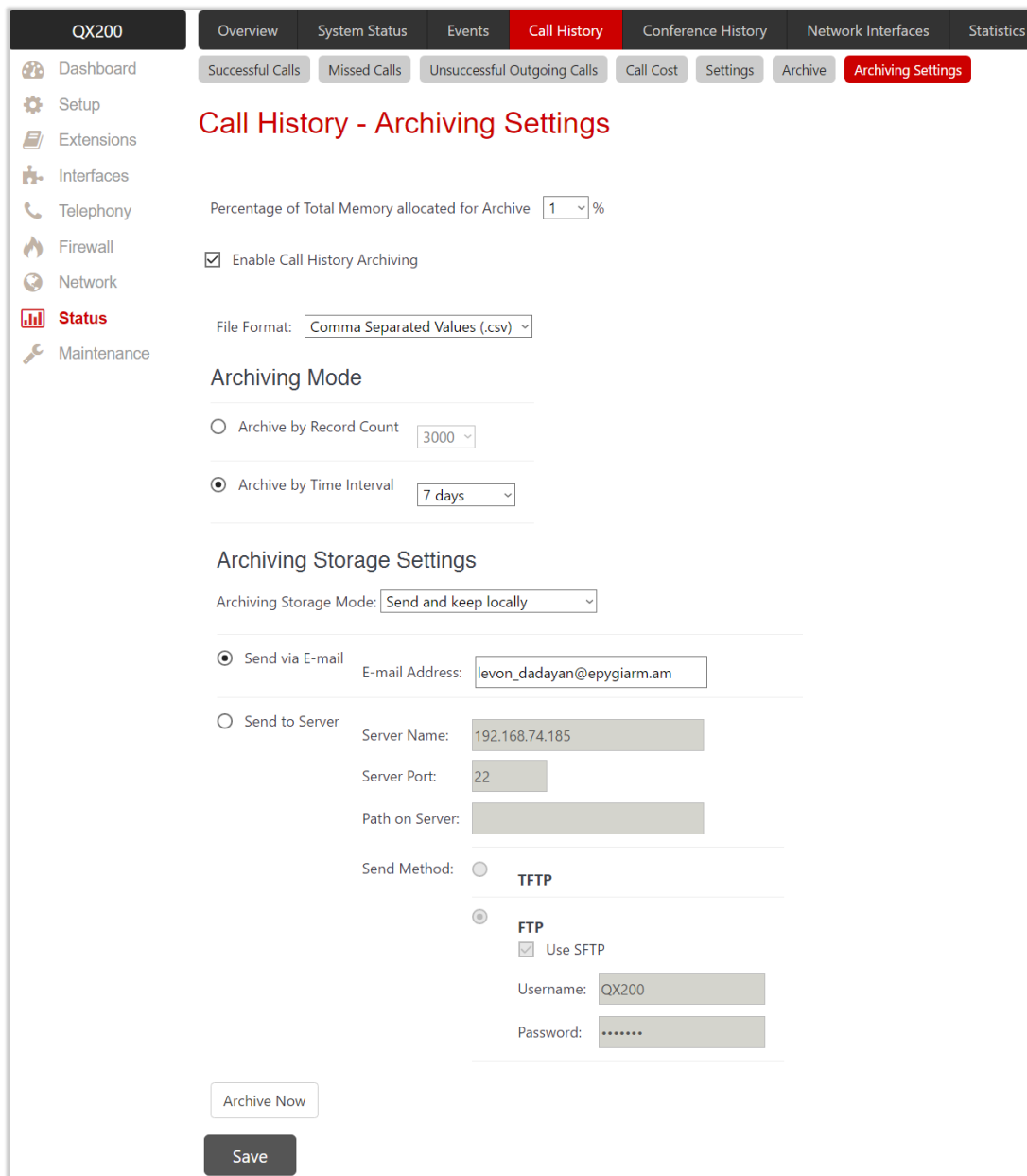
The **Call History Archiving** service is used to configure the automatic archiving of **Call History**. The following settings (options) are available:

- **Percentage of Total Memory allocated for Archive** is used to allocate memory for archiving.
- **Enable Call History Archiving** is used to activate service on QX.
- **File Format** is used to select the format of archived file as (\*.log) and (\*.csv).

#### Archiving Mode

This section is used to select the archiving mode. The following modes are available:

- **Archive by Record Count** – if selected, the file will be archived as soon as the number of records specified in the drop-down list is collected.
- **Archive by Time Interval** – if selected, the file will be archived as soon as the timeframe specified in the drop-down list is elapsed from the last archiving. If no CDRs were produced during that timeframe, archived file for that period will not be generated.



**QX200** | Overview | System Status | Events | **Call History** | Conference History | Network Interfaces | Statistics

Successful Calls | Missed Calls | Unsuccessful Outgoing Calls | Call Cost | Settings | Archive | **Archiving Settings**

## Call History - Archiving Settings

Percentage of Total Memory allocated for Archive:  %

Enable Call History Archiving

File Format:

### Archiving Mode

Archive by Record Count:

Archive by Time Interval:

### Archiving Storage Settings

Archiving Storage Mode:

Send via E-mail  
E-mail Address:

Send to Server

Server Name:

Server Port:

Path on Server:

Send Method:  TFTP

FTP

Use SFTP

Username:

Password:

Figure 157: Call History – Archiving Settings page

## Archiving Storage Settings

This section is used to select archiving storage and configure the backup settings.

- **Archiving Storage Mode** is used to select one of the following archiving modes:
  - **Do not send** – if selected, the CDRs will be archived and kept locally only.
  - **Send and keep locally** – if selected, the CDRs will be sent to the server and kept locally.
  - **Send and delete from archive** – if selected, the CDRs will be sent to the server and removed from the archive.
- The following options are available for storing archived CDRs:
  - **Send via E-mail** allows to send the archived files via e-mail. The destination e-mail address has to be entered in the **E-mail Address** field.
  - **Send to Server** allows to send the archived files to the external server. This selection enables the following fields to be filled:

- ◆ **Server Name** is used to set the IP address or hostname of the server.
- ◆ **Server Port** is used to set the port of the server.
- ◆ **Path on Server** is used to enter the path on the server.
- ◆ **Send Method** – the server type: **TFTP** or **FTP**. Specify the **Username** and **Password** in case of the **FTP**. If these fields are left blank, anonymous authentication will be used. **TIP:** Select the **Use SFTP** option to enable **SFTP** support.
- **Archive Now** is used to archive CDRs immediately.

### 11.3.6 RTP Statistics

The **RTP Statistics** page provides detailed information about the established call. When QX serves as an RTP proxy, this page displays two groups (legs) of RTP statistics. Normally, one leg describes the RTP stream from caller to the QX and the other leg describes the RTP stream from QX to the destination. The following parameters are available:

- **Quality** indicates the call quality, which depends on RTP statistics. Below is the legend for **Call Quality**:
  - **excellent** – RX Lost Packets < 1% and RX Jitter < 20
  - **good** – RX Lost Packets < 5% and RX Jitter < 80
  - **satisfactory** – RX Lost Packets < 10% and RX Jitter < 150
  - **bad** – RX Lost Packets < 20% and RX Jitter < 200
  - **very bad** – RX Lost Packets > 20% or RX Jitter > 200
- **Local** and **Remote** indicate the two peers the RTP stream is transmitted in between. The table below describes the characteristics of RTP stream between these peers.
  - **Rx/Tx Codec** is the codec for received and transmitted RTP stream respectively.
  - **Rx/Tx Packets** is the number of RTP packets received and transmitted respectively.
  - **Rx/Tx Packet Size** is the size of RTP packets (payload) received and transmitted respectively.
  - **Rx Lost Packets** is the number of lost RTP packets for received stream.
  - **Rx 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:

$$D(i,j) = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i)$$

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

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

- **Rx Maximum Delay** is the 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:

$$V(i) = |(R_i - R_1) - (S_i - S_1)| = |(R_i - S_i) - (R_1 - S_1)|$$

$$\text{Rx Maximum Delay} = \max V(i) / 8$$

- **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.
- **Configure Call Quality Event Notification** leads to the **Call Quality Notification** page to configure call quality control notifications.

- **Configure System Events** leads to the **Event Settings** page to configure the methods of notification for each system event.

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

- Calls from or addressed to the IP lines or remote extension.
- Calls from an external user are routed to another external user through call routing rules.

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

### 11.3.7 FAX Statistics

The **FAX statistics** page provides information on received and transmitted packets, lost, bad and duplicated packets. These statistics only refer to **T.38 FAX** transmission. FAX statistics are not available for the FAX transmitted with other protocols.

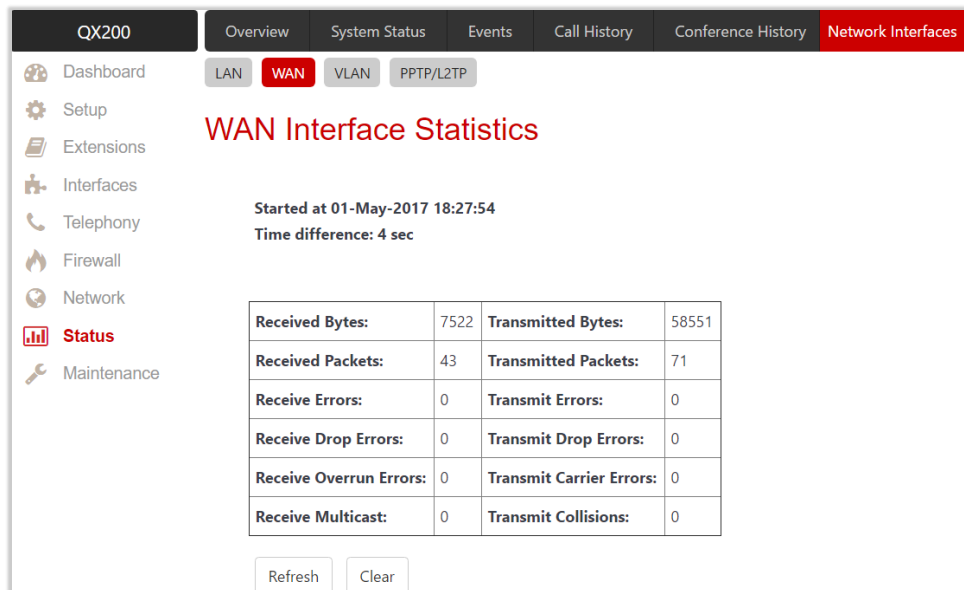
## 11.4 Conference History

**Conference History** allows to track and report the details of conference calls that have been activated on QX.

For more information on **Audio-Video conferencing**, refer to the [Audio-Video Conferencing on QX IP PBXs](#) guide.

## 11.5 Network Interfaces

The **Interface Statistics** pages display statistics (e.g. the number of received and transmitted packets, errors, etc.) for each interface.



The screenshot shows the 'WAN Interface Statistics' page. At the top, there are navigation tabs for 'Overview', 'System Status', 'Events', 'Call History', 'Conference History', and 'Network Interfaces'. Below these are sub-tabs for 'LAN', 'WAN', 'VLAN', and 'PPTP/L2TP'. The main content area displays the title 'WAN Interface Statistics' and the start time 'Started at 01-May-2017 18:27:54' with a 'Time difference: 4 sec'. A table of statistics is shown below:

Received Bytes:	7522	Transmitted Bytes:	58551
Received Packets:	43	Transmitted Packets:	71
Receive Errors:	0	Transmit Errors:	0
Receive Drop Errors:	0	Transmit Drop Errors:	0
Receive Overrun Errors:	0	Transmit Carrier Errors:	0
Receive Multicast:	0	Transmit Collisions:	0

At the bottom of the statistics section, there are 'Refresh' and 'Clear' buttons.

Figure 158: LAN Interface Statistics page

## 11.6 Statistics

### 11.6.1 Network Transfer

The **Transfer Statistics** page is used to generate charts with the transmit/receive values (criteria), interface type and time period. Select the desired criteria and click **Show** to generate the **Transfer Statistics** 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 chart show the total number of specified criteria.

Figure 159: Transfer Statistics page

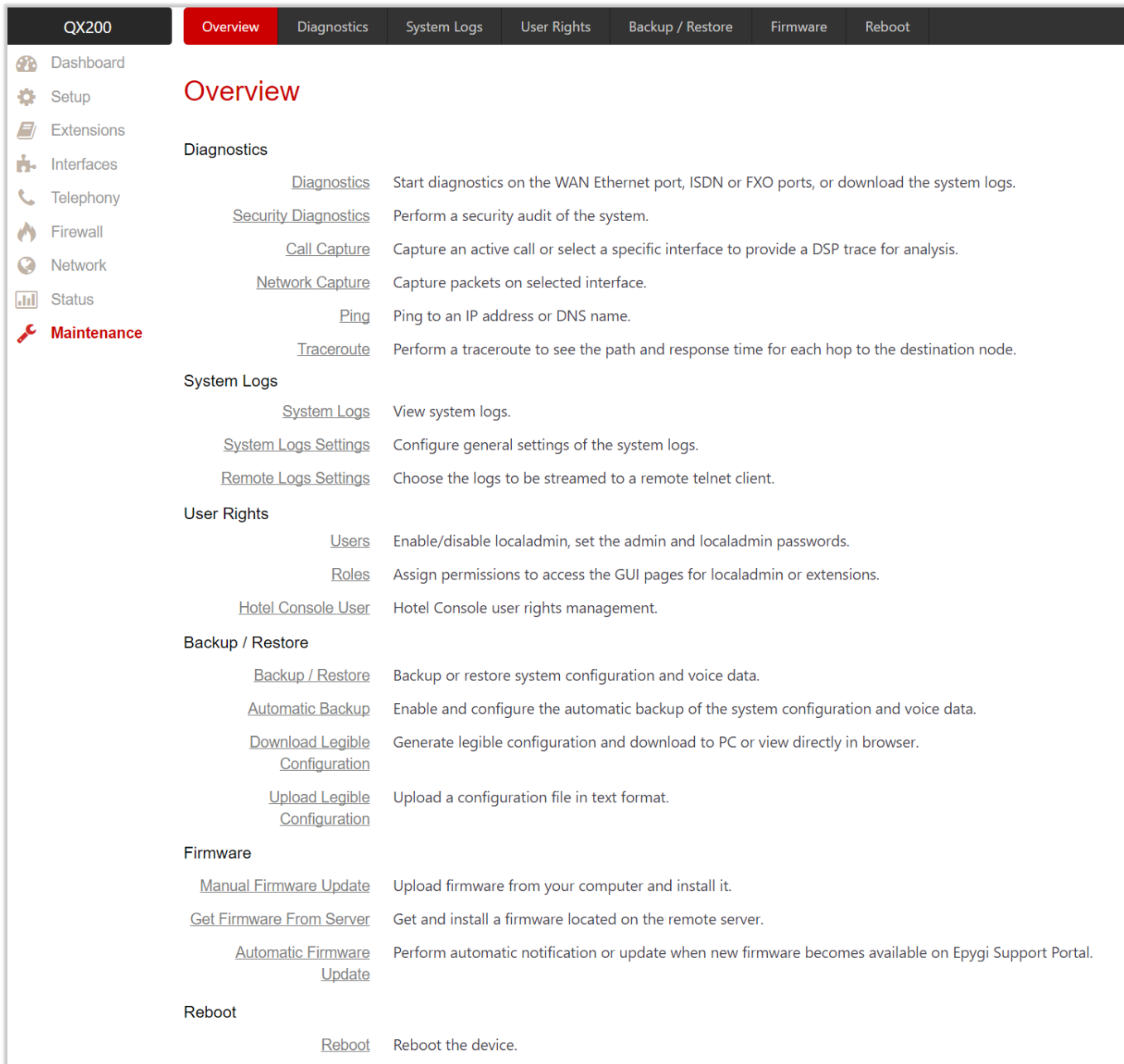
### 11.6.2 PSTN Channel Usage

The **PSTN Channel Usage** page is used to generate charts with the incoming/outgoing calls and maximum active calls (criteria) and time period for the selected on-board lines or trunks.

Figure 160: FXO Channel Usage Statistics page

Select the desired criteria and click **Show** to generate the **Channel Usage Statistics** chart.

## 12 Maintenance Menu



Category	Sub-Category	Description
Diagnostics	<a href="#">Diagnostics</a>	Start diagnostics on the WAN Ethernet port, ISDN or FXO ports, or download the system logs.
	<a href="#">Security Diagnostics</a>	Perform a security audit of the system.
	<a href="#">Call Capture</a>	Capture an active call or select a specific interface to provide a DSP trace for analysis.
	<a href="#">Network Capture</a>	Capture packets on selected interface.
	<a href="#">Ping</a>	Ping to an IP address or DNS name.
	<a href="#">Traceroute</a>	Perform a traceroute to see the path and response time for each hop to the destination node.
System Logs	<a href="#">System Logs</a>	View system logs.
	<a href="#">System Logs Settings</a>	Configure general settings of the system logs.
	<a href="#">Remote Logs Settings</a>	Choose the logs to be streamed to a remote telnet client.
User Rights	<a href="#">Users</a>	Enable/disable localadmin, set the admin and localadmin passwords.
	<a href="#">Roles</a>	Assign permissions to access the GUI pages for localadmin or extensions.
	<a href="#">Hotel Console User</a>	Hotel Console user rights management.
Backup / Restore	<a href="#">Backup / Restore</a>	Backup or restore system configuration and voice data.
	<a href="#">Automatic Backup</a>	Enable and configure the automatic backup of the system configuration and voice data.
	<a href="#">Download Legible Configuration</a>	Generate legible configuration and download to PC or view directly in browser.
	<a href="#">Upload Legible Configuration</a>	Upload a configuration file in text format.
Firmware	<a href="#">Manual Firmware Update</a>	Upload firmware from your computer and install it.
	<a href="#">Get Firmware From Server</a>	Get and install a firmware located on the remote server.
	<a href="#">Automatic Firmware Update</a>	Perform automatic notification or update when new firmware becomes available on Epygi Support Portal.
Reboot	<a href="#">Reboot</a>	Reboot the device.

Figure 161: Maintenance Menu overview

## 12.1 Diagnostics

The **Diagnostics** page allows to run network and on-board lines (trunks) diagnostics to verify QX connectivity and collect system logs for diagnostic purposes.

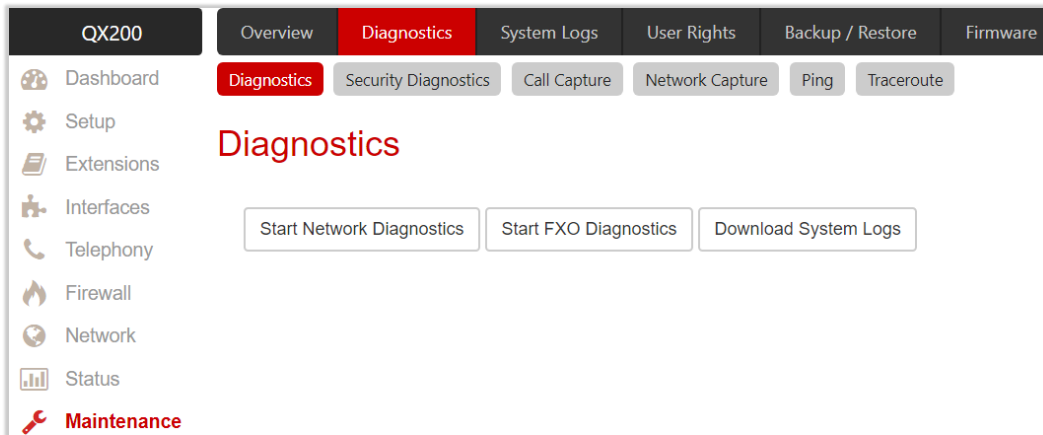


Figure 162: Diagnostics page

- **Start Network Diagnostics** is used to run network diagnostics, i.e., to check the WAN link and network parameters such as IP configuration, Default Gateway, primary and secondary DNS servers' accessibility.
- **Start FXO Diagnostics** is used to run FXO diagnostics to determine the optimal value for the **Country Specific Regional Setting** (CSRS) appropriate to your PSTN provider. Once the FXO diagnostics is complete, the recommended value should be manually set on the <http://xxx.xxx.xxx.xxx/fxocfg> hidden page. Setting this value may resolve echo or poor audio quality issues on FXO lines.
- **Start ISDN Diagnostics** is used to run ISDN diagnostics to initiate ISDN BRI low level diagnostics. With these tests, the ISDN physical link is checked and the **Frame Synchronization** is verified.
- **Download System Logs** is used to download all logs in (\*.tar) file format. These logs can then be used by [Epygi Technical Support](#) to determine the issues that have occurred on QX.

### 12.1.1 Security Diagnostics

The **Security Diagnostics** page allows to run security audit and get security reports.

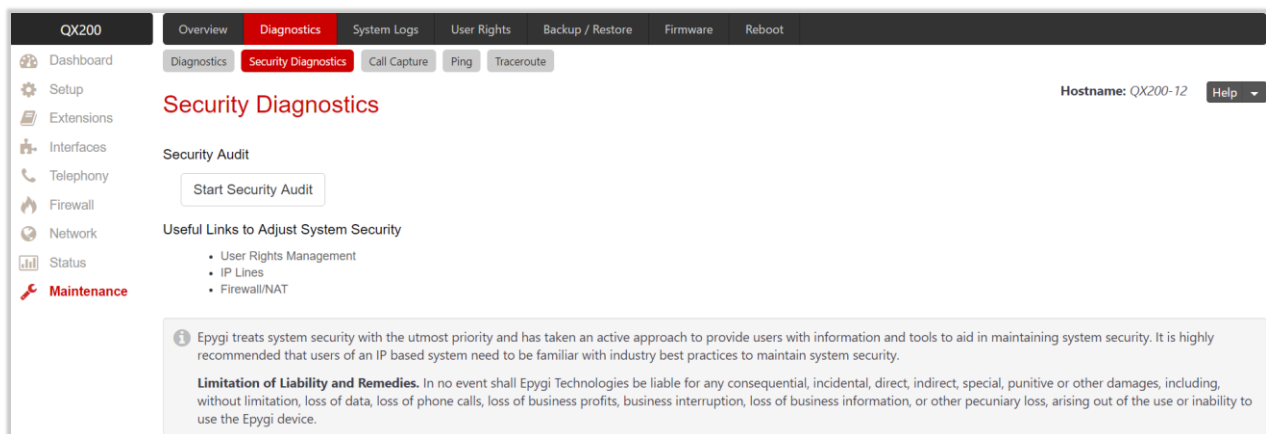


Figure 163: Security Diagnostics page

- **Start Security Audit** is used to run security audit. QX **Security Audit** is a security reporting system, which generates the warnings regarding QX weaknesses for the selected **Security Level**. The warnings may

vary depending on the selected **Security Level**. **Security Audit** will detect configuration issues related to security in Firewall, IDS, IP line passwords, Call Routing and extension settings. **Show Security Report** allows to display the last security audit report.

- The following useful links are available to adjust the system security:
  - [User Rights Management](#)
  - [IP Lines](#)
  - [Firewall/NAT](#)

## 12.1.2 Call Capture

**Call Capture** is used to capture the calls to/from on-board interfaces. You can capture calls on the following interfaces (depending on the QX model): FXS, FXO or ISDN. This page consists of two sub-pages:

- **Active Calls** lists all active calls on the QX for a certain moment.
- **Interfaces** lists all available interfaces on the QX.

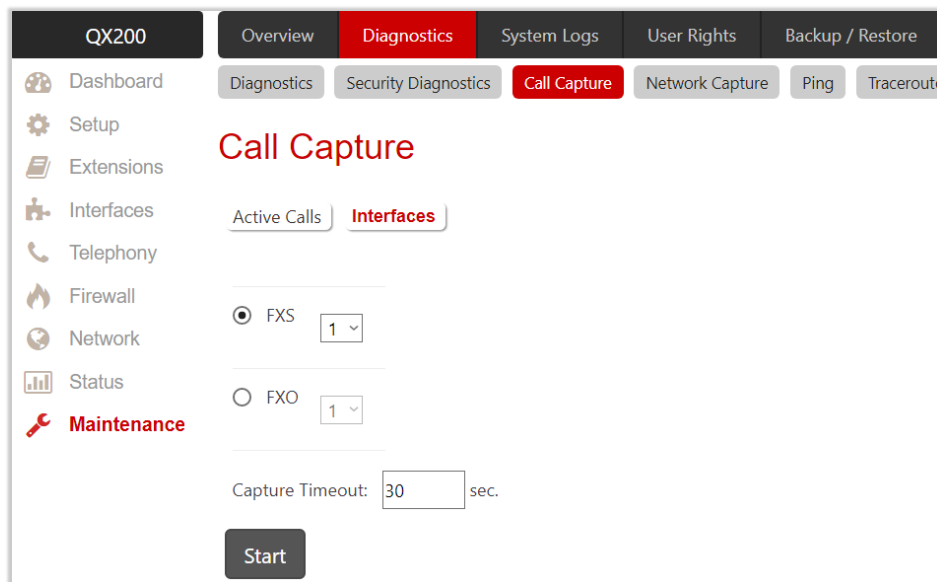


Figure 164: Call Capture - Interfaces subpage

To start **Call Capture**:

1. Tick the checkbox next to the call, which should be captured from **Active Calls** sub-page or select the available interface from **Interfaces** sub-page.
2. Configure the **Capture Timeout**, during which the call will be captured. **TIP:** The call capture will automatically be stopped, when the capture timeout expires.
3. Click **Start** to start a call capture.
4. Click **Stop** to stop a call capture and download the captured file.

The captured call will be downloaded in (\*.tar) format. It contains two streams (receive and transmit) of the captured call. These streams can be then played with an audio player application.

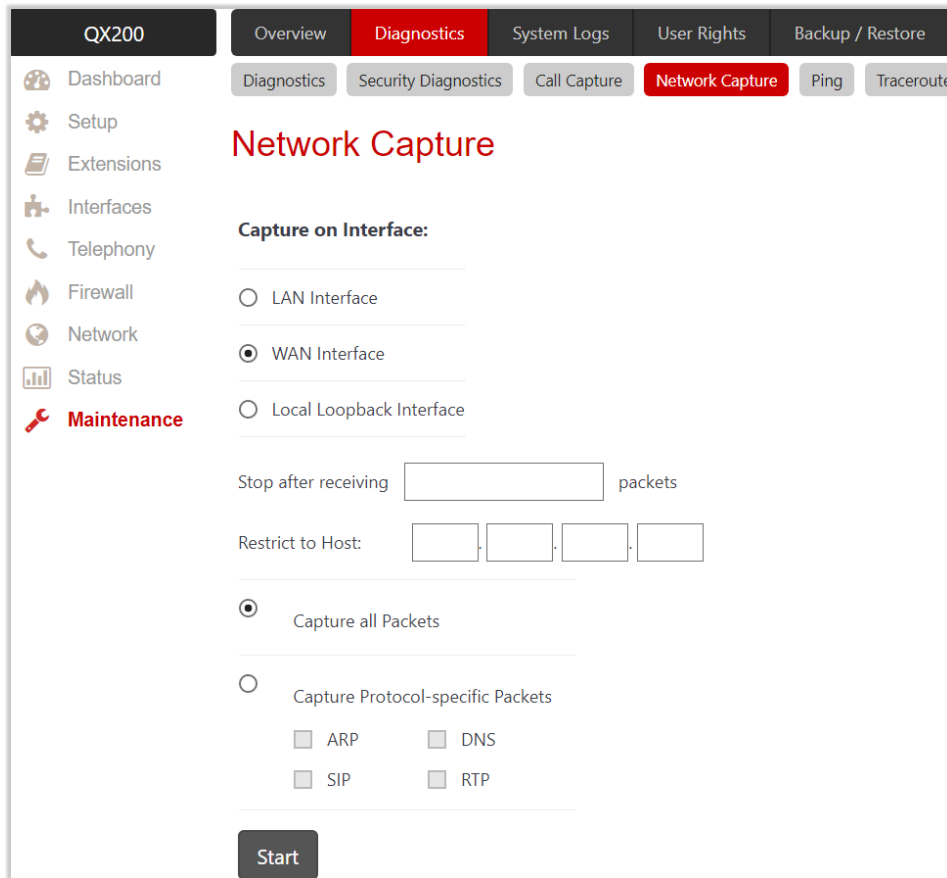
**Note:** The **Call Capture** duration is limited to **160** seconds.



### 12.1.3 Network Capture

**Network Capture** is used to capture packets for the selected network interface. The following options are available:

- **Capture on Interface** is used to select the interface to capture packets. The **Local Loopback Interface** option is used to capture the traffic within the unit.
- **Stop after receiving count packet** is used to enter the number of packets to be captured.
- **Restrict to Host** is used to enter a specific IP address packets should be captured for.



The screenshot shows the 'Network Capture' configuration page. The interface includes a navigation menu on the left with options like Dashboard, Setup, Extensions, Interfaces, Telephony, Firewall, Network, Status, and Maintenance. The main content area has a title 'Network Capture' and several configuration sections:

- Capture on Interface:** Three radio buttons for 'LAN Interface', 'WAN Interface' (selected), and 'Local Loopback Interface'.
- Stop after receiving:** A text input field followed by 'packets'.
- Restrict to Host:** Four text input fields for IP address digits.
- Capture all Packets:** A selected radio button.
- Capture Protocol-specific Packets:** An unselected radio button with four checkboxes for 'ARP', 'DNS', 'SIP', and 'RTP'.
- Start:** A dark button at the bottom.

Figure 165: Network Capture page

- **Capture all Packets** allows capturing all packets on the selected interface.
- **Capture Protocol-specific Packets** is used to restrict capturing specific packets only (ARP, SIP, DNS, and RTP).

To start **Network Capture**:

1. Select the **Interface**.
2. Configure restriction parameters, if needed.
3. Select packets to capture: **all** or **specific ones**.
4. Click **Start** to start a network capture.
5. Click **Stop** to stop a network capture and download the captured file.

**Note:** **Network Capture** size is limited to **24 MB**. This will limit the duration of captured file.

### 12.1.4 Ping

**Ping** is used diagnostically to ensure that a destination (e.g. host computer) the user is trying to reach is operating. Ping works by sending an **Internet Control Message Protocol (ICMP)** Echo Request to a specified interface on the network and waiting for a reply. Ping can be used for troubleshooting to test connectivity and determine response time.

To ping a target:

1. Enter the destination IP address or hostname in the **Ping Target** field.
2. Click **Start Ping**.
3. The results of the ping will be displayed in the **Ping Output** window.

### 12.1.5 Traceroute

**Traceroute** is a utility that records the route (the specific gateway at each hop) through the Internet between your device and a specified destination. It also calculates and displays the amount of time each hop took.

To traceroute a target:

1. Enter the destination IP address or hostname in the **Traceroute Target** field.
2. Tick the **Use ICMP** checkbox to send an ICMP request to the ping destination (MS Windows standard), otherwise a UDP request will be sent (Linux standard).
3. Click **Start Traceroute**.
4. The results of the ping will be displayed in the **Traceroute Output** window.

**Note:** No **Traceroute** is possible if the **Firewall level** is set to "**High**". For the purpose of tracerouting, several IP packets are sent out. UDP is used to send packets and ICMP is used to receive information about the routers. In their headers, the **TTL** value increases from **1** to **30**. When the first IP packet is received by the first router, its IP address will be returned in its acknowledgement.

## 12.2 System Logs

The **System Logs** page shows the logs on QX. System logs are useful to determine any kind of problems on the QX.

You can collect **user logs** from handset. Dial **\*82** to collect the logs. The collected logs will be a part of the **System Logs** when you download them next time. This could be used to collect the logs at the exact moment when a problem occurs.

## 12.2.1 System Logs Settings

The **System Logs Settings** page is used to adjust system logging settings. The following settings (options) are available:

- **Enable User Logging** – this logging contains brief information about events on QX.
- **Enable Developer Logging** – this logging contains detailed information about events on QX.
- **Log Lines to Show** is used to select the maximum number of log lines to display on the **System Logs** page.
- **Mark all Logs** is used to set a line marker in the logs.
- **Comment** is used to describe the problem captured in the following logs.
- **Download all Logs** is used to download all logs in (\*.tar) file format. These logs can then be used by [Epygi Technical Support](#) to determine the issues that has occurred on QX.

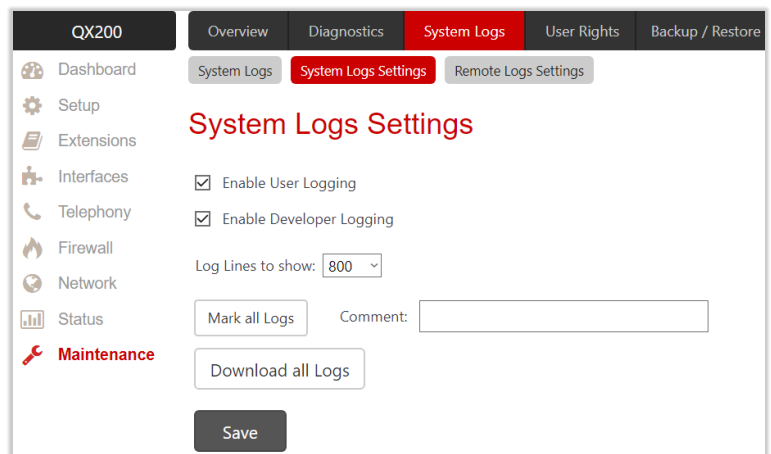


Figure 166: System Logs Settings page

## 12.2.2 Remote Logs Settings

The **Remote Logs Settings** page is used to adjust the system logging settings for collecting the logs remotely. These logs can then be used by [Epygi Technical Support](#) to determine the issues that has occurred on QX.

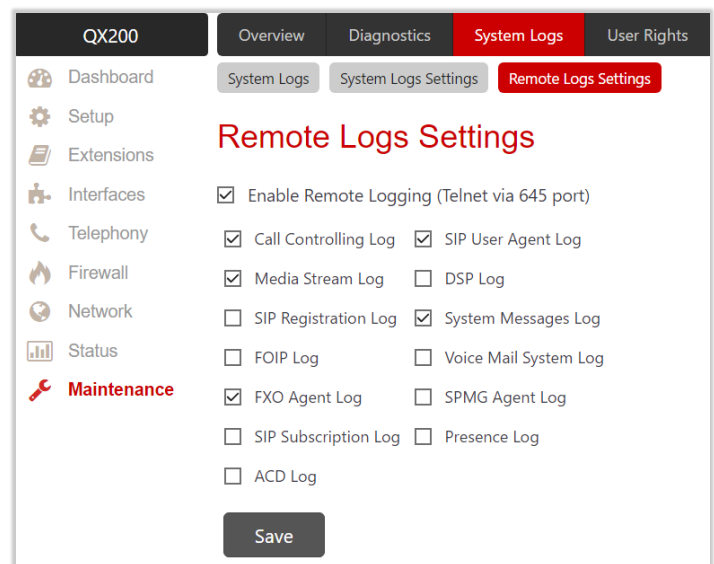
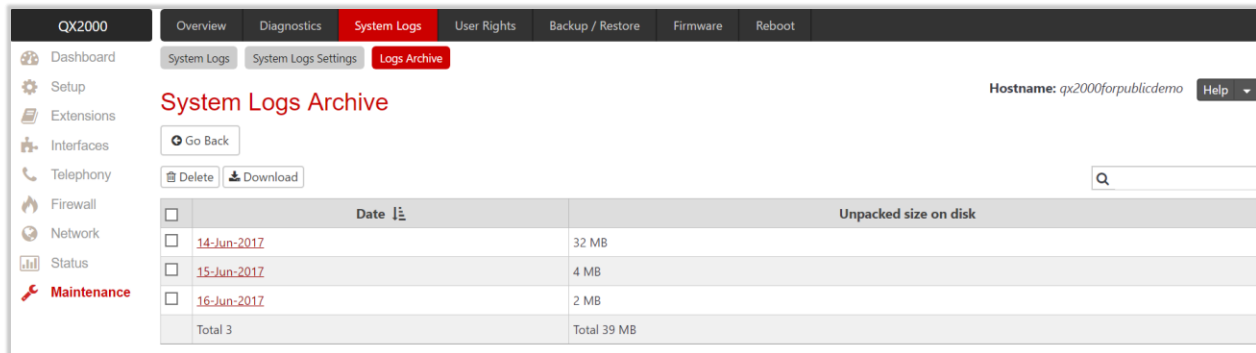


Figure 167: Remote Logs Settings page

## 12.2.3 Logs Archive

The **System Logs Archive** page shows the archived logs table with time period by **Date**. Clicking on the corresponding date will open the archived system logs table on an hourly basis. **Hour** shows the initiation time of the system logs. It can be used to collect the logs at the exact moment when the issue has started.



<input type="checkbox"/>	Date	Unpacked size on disk
<input type="checkbox"/>	14-Jun-2017	32 MB
<input type="checkbox"/>	15-Jun-2017	4 MB
<input type="checkbox"/>	16-Jun-2017	2 MB
Total 3		Total 39 MB

Figure 168: System Logs Archive page

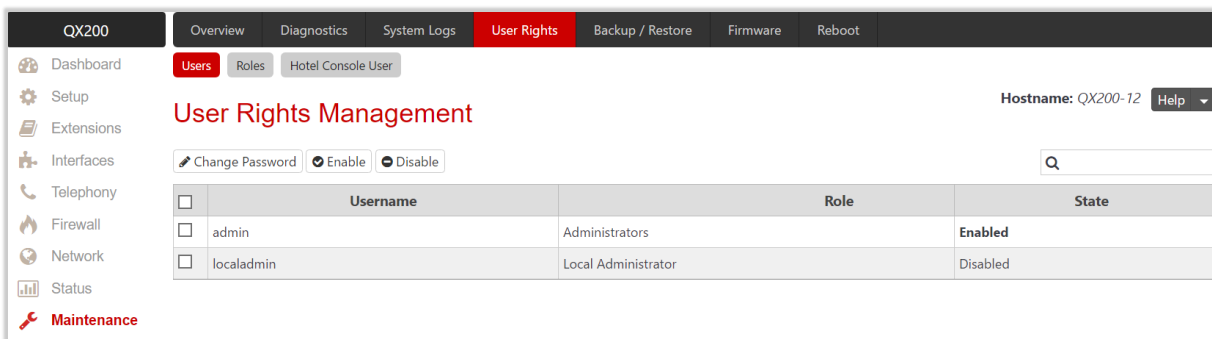
## 12.3 User Rights

The **User Rights** service is used to configure permissions/restrictions on the GUI access for various users.

### 12.3.1 Users

The **Users** page contains a table where the **Administrator** and **Local Administrator** accounts are listed. This page allows to modify the passwords of **Administrator** and **Local Administrator** accounts. Two levels of QX GUI administration are available:

- **admin** – this is the **Administrator** account. The latter has access to all WEB GUI pages. The administrator is responsible for granting access to all other user groups. By default, as well as after factory reset of QX, the **admin password** is set to **19**.
- **localadmin** – this is a common **sub-administrator** account. **Local Administrator** has permission to access and adjust each WEB GUI page. By default, as well as after factory reset of QX, the **localadmin password** is set to **19**. The **localadmin** account is disabled by default.



<input type="checkbox"/>	Username	Role	State
<input type="checkbox"/>	admin	Administrators	Enabled
<input type="checkbox"/>	localadmin	Local Administrator	Disabled

Figure 169: User Rights Management – Users page

To change the **GUI Access Password**:

1. Tick the checkbox next to the **admin** or **localadmin** entry in the table and click **Change Password**.
2. The **Change Password** page appears for the selected user. Select **GUI Access Password** tab.
  - Enter the old password (by default – 19)
  - Enter a new password and then re-enter it to confirm.
3. Click **Save** to change the password.

The **Phone Access Password** is used for authentication purposes (when connecting to 3PCC application using **admin** account) as well as for [Administrator Login](#) (\*75).

To change the **Phone Access Password**:

1. Tick the checkbox next to the **admin** entry in the table and click **Change Password**.
2. The **Change Password** page appears for selected user. Select **Phone Access Password** tab.
  - Enter a new password and then re-enter it to confirm.
3. Click **Save** to change the password.

**Note:**

- The **GUI Access Password** can consist of lowercase and uppercase alphabetic characters, digits and symbols. A maximum password length is **20** characters.
- The **Phone Access Password** can consist of only digits. A maximum password length is **20** characters.
- In order to keep passwords safe, make sure you write it down in a safe place and don't share it with others.

## 12.3.2 Roles

The **Roles** page contains a table where the user roles are listed. This page allows to set access permissions to the GUI pages for each role in the table.

- **Local Administrator** – this role can have permissions to adjust each GUI page.
- **Extension** – this role refers to all user extensions created on QX. Permissions for each GUI page can be adjusted.

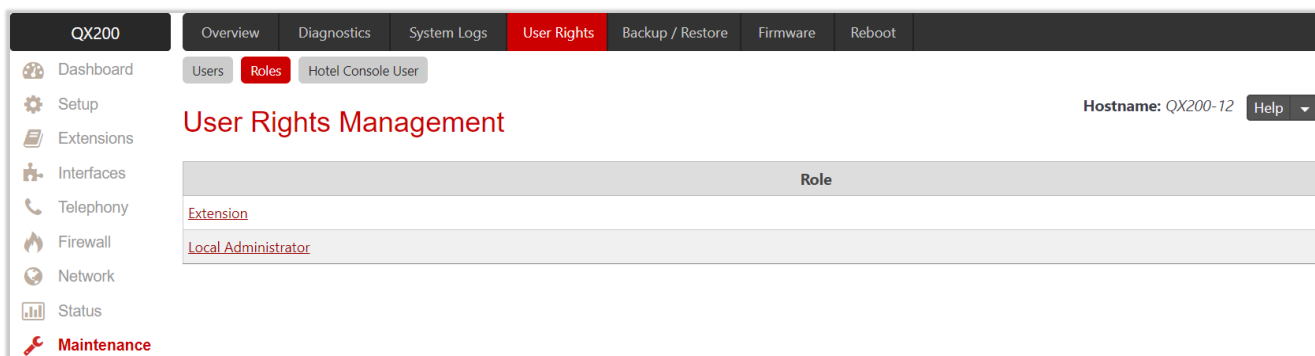


Figure 170: User Rights Management – Roles page

To manage the permissions for the selected role:

1. Click the hyperlinked role (**Extension** or **Local Administrator**). The **Access Rights** page will be opened.
2. Tick the checkbox(es) next to **CGI Name**.
3. Click the **Grant Access** or **Deny Access** to grant/deny access for the selected page(s).

<input type="checkbox"/>	CGI Name	Page Name	Access
<input type="checkbox"/>	addressmanagement	Caller ID Based Services - Add/Edit Entry	Granted
<input type="checkbox"/>	alarm	Basic Services - Alarm Settings	Denied
<input type="checkbox"/>	alarmadd	Alarm Settings - Add/Edit Entry	Denied
<input type="checkbox"/>	dialandannounceadd	Dial & Announce List - Add/Edit Entry	Granted
<input type="checkbox"/>	dnd	Basic Services - Do Not Disturb Settings	Granted
<input type="checkbox"/>	extensionstat	PBX Information	Granted
<input type="checkbox"/>	findfollowadd	FindFollow List - Add/Edit Entry	Granted
<input type="checkbox"/>	forwardadd	Forwarding List - Add/Edit Entry	Granted
<input type="checkbox"/>	grouplist	Group List	Granted
<input type="checkbox"/>	hold	Basic Services - Hold Music Settings	Granted
<input type="checkbox"/>	hotline	Basic Services - Hot Line Settings	Granted

Figure 171: Access Rights – extensions page

### 12.3.3 Hotel Console User

The **Hotel Console User Rights Management** page is used for managing the users allowed to connect to the QX from the **Epygi Hotel Console (EHC)** application.

For more information on how to configure and use **EHC** application with QX, refer to the [Epygi Hotel Console \(EHC\) - User Guide](#).

## 12.4 Backup / Restore

### 12.4.1 Backup / Restore

**Configuration Management** includes features that allow to back up and save the current configuration of QX, restore the configuration from backups created earlier, as well as to restore the system default configuration.

Backup / Restore Automatic Backup Download Legible Configuration Upload Legible Configuration

## Configuration Management

Backup and download current configuration:

Backup and download current configuration including EAC Data:

Restore previously backed up configuration:

Restore to Factory Default settings:

Figure 172: Configuration Management page

The following settings (options) are available:

- **Backup and download current Configuration** – this option is used to create a backup file with all current configuration settings and system voice messages (default and customized). Click the **Download** button to back up and download the current configuration. The file will be saved in the (\*.bin) format. The backup filename will have the following format: **config\_[Hostname]\_[Firmware Version]\_[Date/Time].bin**
- **Backup and download current configuration including EAC data** – this option is also used to create a backup file with all current configuration settings and system voice messages (default and customized). Compared to the previous option the current configuration includes the **EAC data**, covering the **EAC Chat** database, **Agents Status** and **Call Statistics**. Click the **Download** button to back up and download the current configuration. The file will be saved in the (\*.bin) format. The backup filename will have the following format: **config\_[Hostname]\_[Firmware Version]\_[Date/Time].bin**

**Note:** **Voice Mails** and **Call Recordings** are not backed up and included in the configuration file.

- **Restore previously backed up configuration** is used to restore earlier created backup file and replace the current configuration settings and system voice messages.
  1. Click the **Upload** button.
  2. Click **Choose File** to open the file chooser window and browse for the file.
  3. Click **Save** to start configuration restore.

**Note:** QX doesn't allow to restore the earlier created backup in case it is running a firmware version lower than the version at the time of configuration backup.

- **Restore to Factory Default settings** is used to reset all configuration settings and restores factory default settings of device.
  1. Click the **Reset** button.
  2. Click **Yes** to proceed the factory reset procedure.

**Note:** Unlike the factory reset done by pressing the **Reset** pin on QX manually, this option will keep the following data:

- The device registration with [Epygi Technical Support](#).
- The installed [license keys](#).

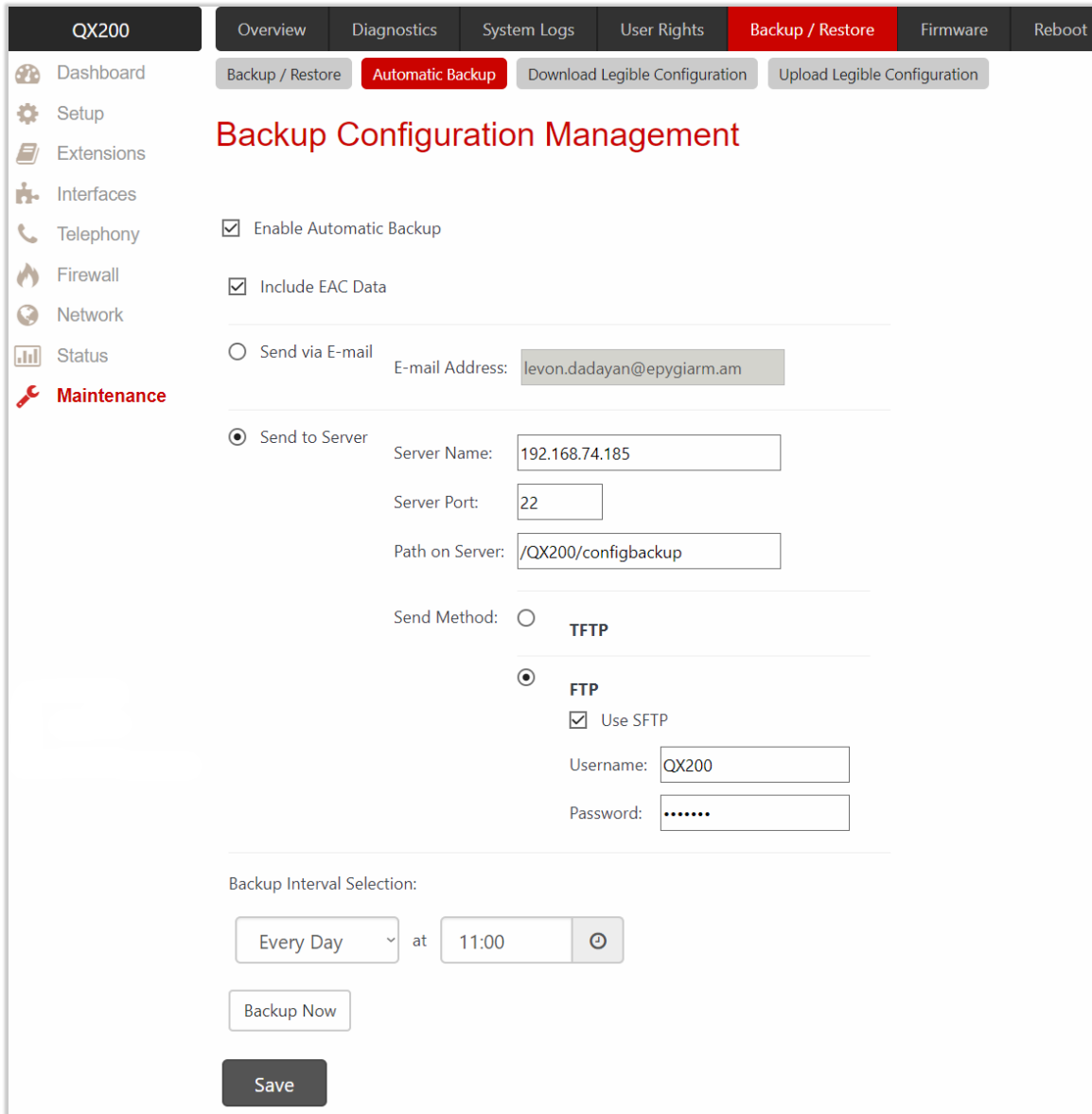
## 12.4.2 Automatic Backup

The **Backup Configuration Management** service allows to activate and configure the automatic backup of the current configuration and system voice messages (default and customized).

The following settings (options) are available:

- **Enable Automatic Backup** is used to activate service on QX.
- **Include EAC Data** is used to include the **EAC data**, covering the **EAC Chat** database, **Agents Status** and **Call Statistics** in the backup file.
- **Send via Email** allows sending the backup file via e-mail. The destination e-mail address has to be entered in the **E-mail Address** field.
- **Send to Server** allows sending the backup file to an external server. This selection enables the following fields to be filled:
  - **Server Name** is used to set the IP address or the hostname of the server.
  - **Server Port** is used to set the port of the server.
  - **Path on Server** is used to set the path on the server.

- **Send Method** – the server type: TFTP or FTP. Specify the **Username** and **Password** in case of the FTP. If these fields are left empty, anonymous authentication will be used. **TIP:** Select the **Use SFTP** option to enable SFTP support.
- **Backup Interval Selection** is used to schedule the automatic backup.
- **Backup Now** is used to back up the configuration immediately.



The screenshot shows the 'Automatic Backup' configuration page for a QX200 device. The page is part of the 'Backup / Restore' section, which also includes options for 'Download Legible Configuration' and 'Upload Legible Configuration'. The main heading is 'Backup Configuration Management'.

Key configuration options include:

- Enable Automatic Backup
- Include EAC Data
- Send via E-mail (E-mail Address: levon.dadayan@epgyiarm.am)
- Send to Server (Server Name: 192.168.74.185, Server Port: 22, Path on Server: /QX200/configbackup)
- Send Method:  TFTP,  FTP (with  Use SFTP, Username: QX200, Password: [masked])
- Backup Interval Selection: Every Day at 11:00
- Buttons: Backup Now, Save

Figure 173: Automatic Backup page



### 12.4.3 Download Legible Configuration

The **Legible Configuration** service allows to generate a piece of QX configuration, download it to review and make necessary changes, then upload back to update the configuration. The downloaded **Legible Configuration File** (LCF) contain QX configuration parameters in (\*.txt) file format. LCF can be edited with any text editor and uploaded back to save the changes on the same or another QX system.

For more information on how to configure and use **Legible Configuration** service, refer to the [Legible Configuration on QX IP PBXs](#) guide.

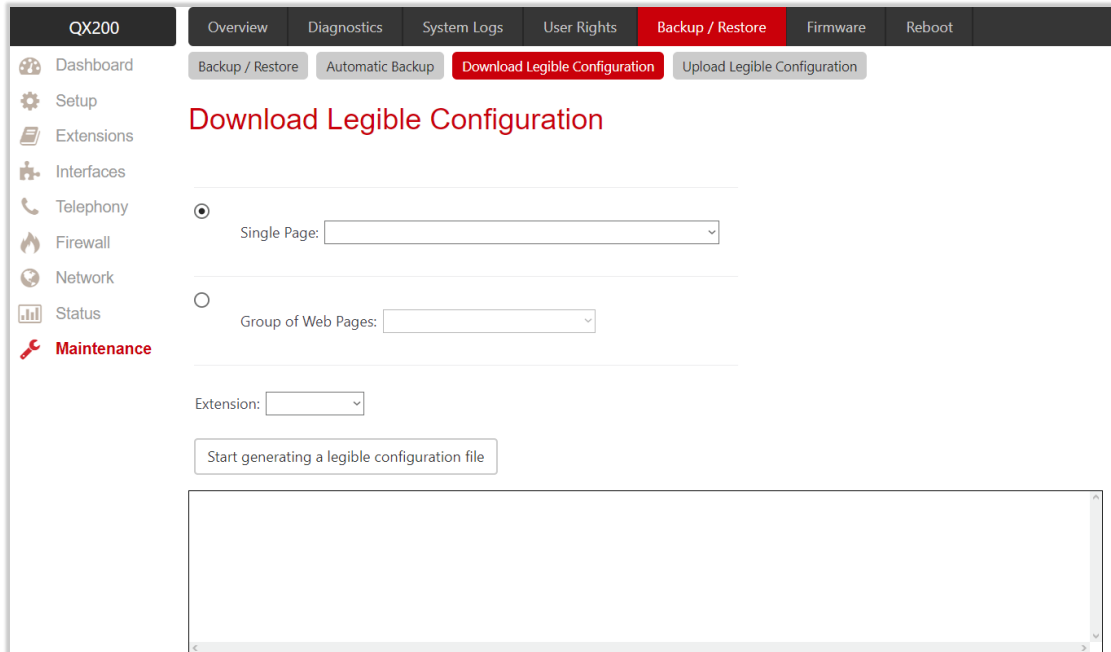


Figure 174: Download Legible Configuration page

The following radio buttons are used to select between a specific CGI or a group of CGIs:

- **Single Page** is used to select a certain page from the list of WEB GUI pages the legible configuration can be manually managed for. **For example:** selecting **RTP Settings** will generate a legible configuration file with parameters present on the RTP Settings page.
- **Group of Web Pages** is used 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.
- **Extension** is used to select the settings in the generated legible configuration file to one specific extension. **For example:** each of the extensions on QX has its 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 LCF will contain the parameter of all available extensions on QX (if the selected parameter applies to the extension and not to the overall system, like RTP settings).

The following functional buttons are available:

- **Start generate a legible configuration file** is used to start parsing the configuration structure of the device for the defined parameters. The progress will be displayed in the window.
- **Cancel generation process** is used to stop the generation procedure. This button appears once the configuration generation procedure has been started.

- **Download generated configuration!** is used to download the generated file in the (\*.txt) format. This button appears when the legible configuration generation is finished. Necessary changes can be made in the downloaded configuration file and then uploaded back to the system.
- **View generated configuration!** is used to view the generated file directly in the browser. This button appears once the legible configuration generation is finished.
- **Restart generation!** is used to cancel the generated configuration file and start over. This button appears once the legible configuration generation is finished.

## 12.4.4 Upload Legible Configuration

The Upload Legible Configuration page is used to upload a configuration file in (\*.txt) file format.

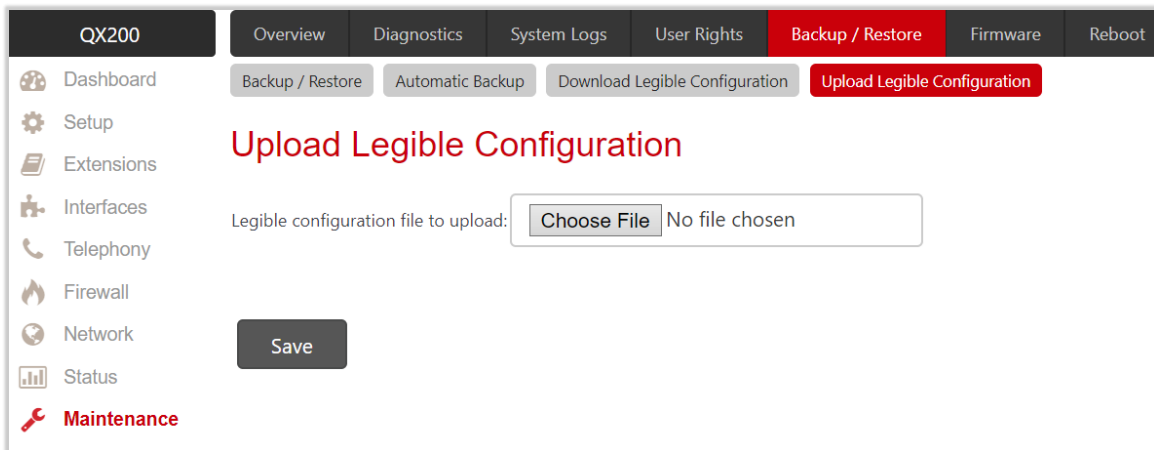


Figure 175: Upload Legible Configuration page

### Checking the Validity of a LCF

Before applying the changes specified in the LCF, QX checks the validity of the uploaded LCF. First, the QX compares the FW version indicated in the LCF with the currently running one on the QX. If they match, the QX will proceed checking the correctness of the specified settings similarly as it does when the user presses **Save** to submit the changes. At any point, the QX detects a mistake (version mismatch, wrong value for a setting, a wrong syntax). It will generate an error and delete the LCF without applying any change. If no mistakes are found in the edited LCF, the QX will start to sequentially apply the changes.

## 12.5 Firmware

The **Firmware** section is used to update the firmware of QXs. The following options are available for updating the current firmware:

- Upload and update firmware manually.
- Download and update firmware manually.
- Download and update firmware automatically

For more information on how to update the QX **firmware**, refer to the [Firmware Update Service on Epygi QX Line](#) guide.

### Attention:

- It is recommended to back up the configuration for **emergency purposes** prior to upgrading the firmware. You can do that by clicking the **Download Configuration** link in the **Manual Firmware Update** page. The current configuration will remain once the firmware has been updated. Moreover, voice mails, call recordings, all custom messages and call history will be saved during the upgrade.
- Firmware installation will take about **5** minutes. During that time, QXs will be in non-operational condition, neither telephony nor Internet access is possible.
- You will not be automatically redirected to the Login page. To access QX WEB GUI, connect to QX again and login.
- QX will factory reset and the system configuration will be lost while downgrading the firmware.
- After the firmware update, all IP phones attached to the QX will be restarted.

### 12.5.1 Manual Firmware Update

The **Manual Firmware Update** page is used to upload and update the QX firmware manually.

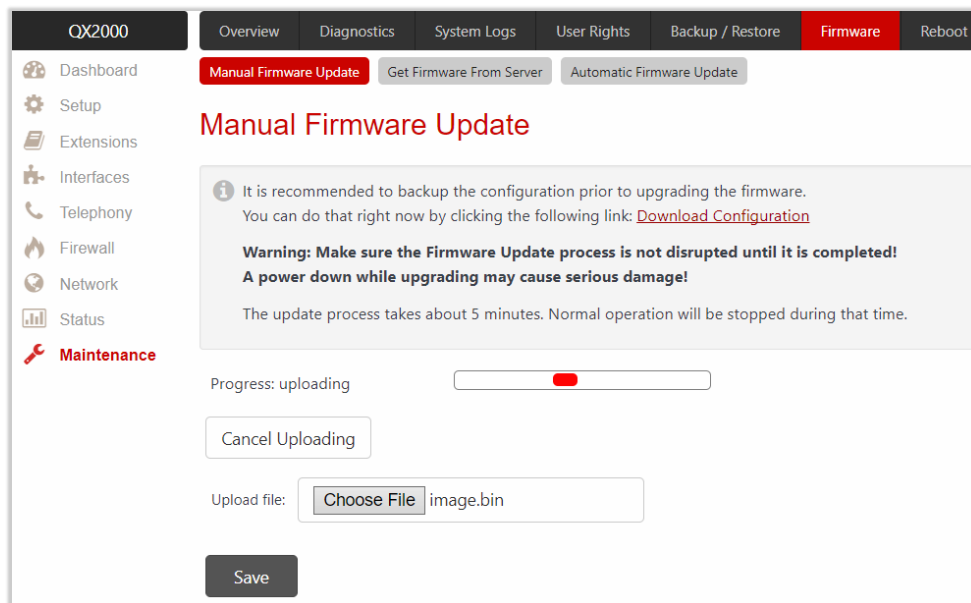


Figure 176: Manual Firmware Update page

To perform **Manual Firmware Update**:

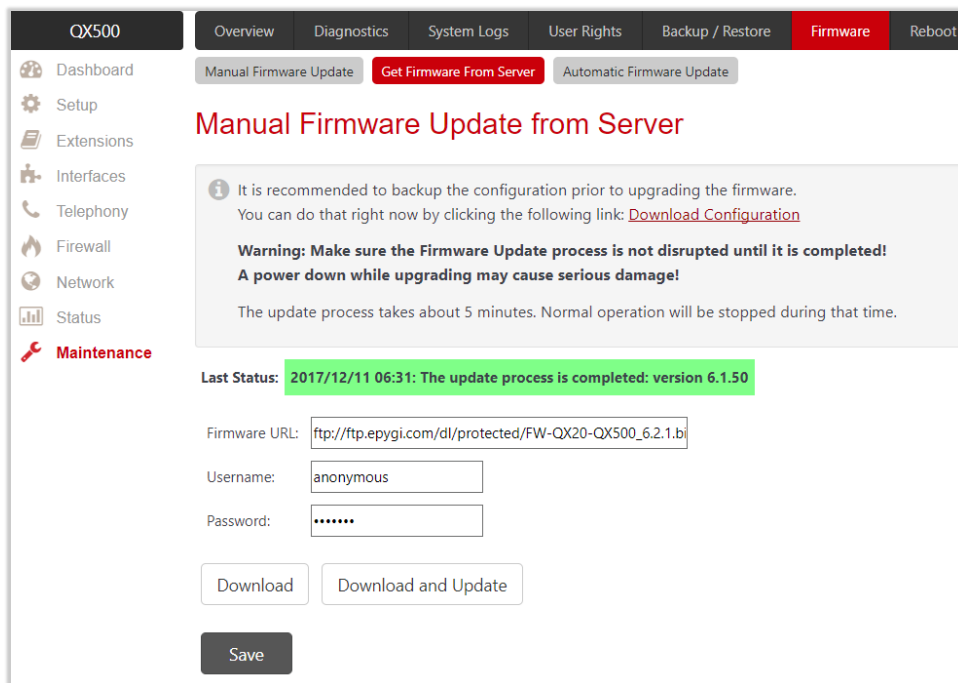
1. Go to the **Maintenance**→**Firmware**→**Manual Firmware Update** page.
2. Click the **Download Configuration** link to back up the current configuration (recommended).
3. Click the **Choose File** button to browse for **image.bin** file.

4. Click **Save** to start uploading the file. The following information will be displayed once the firmware has been uploaded.
  - **Firmware check** shows the status of the uploaded firmware. **Invalid** status means that the uploaded firmware is not compatible with the QX hardware version.
  - **Current Firmware Version/New Firmware Version** shows the current/new firmware versions accordingly.
5. Click **Yes** to proceed the update or click **Discard this firmware** to close the message without updating the device.

**Note:** The update process takes about **5** minutes. Normal operation will be stopped during that time.

## 12.5.2 Get Firmware From Server

The **Manual Firmware Update from Server** page is used to manually download and update the QX firmware from the FTP server.



The screenshot shows the 'Manual Firmware Update from Server' page in the QX500 web interface. The page has a navigation bar with tabs for Overview, Diagnostics, System Logs, User Rights, Backup / Restore, Firmware (selected), and Reboot. Below the navigation bar, there are three buttons: Manual Firmware Update, Get Firmware From Server (highlighted in red), and Automatic Firmware Update. The main content area features a warning message: 'It is recommended to backup the configuration prior to upgrading the firmware. You can do that right now by clicking the following link: [Download Configuration](#). Warning: Make sure the Firmware Update process is not disrupted until it is completed! A power down while upgrading may cause serious damage! The update process takes about 5 minutes. Normal operation will be stopped during that time.' Below the warning, a green status bar indicates: 'Last Status: 2017/12/11 06:31: The update process is completed: version 6.1.50'. The form includes fields for Firmware URL (ftp://ftp.epygi.com/dl/protected/FW-QX20-QX500\_6.2.1.bj), Username (anonymous), and Password (masked with dots). There are 'Download' and 'Download and Update' buttons, and a 'Save' button at the bottom.

Figure 177: Manual Firmware Update from Server page

To perform **Manual Download and Firmware Update**:

1. Go to the **Maintenance**→**Firmware**→**Manual Firmware Update** page.
2. Click the **Download Configuration** link to back up the current configuration (recommended).
3. Set the **Firmware URL** to get the new firmware located in the FTP server.
4. Set the **Username** and **Password** to pass the FTP server authentication (if needed).
5. Click **Save** to apply changes before starting downloading and updating the firmware.
6. Click **Download and Update** to automatically download and update the firmware or click **Download** to start downloading firmware from FTP server.
  - **Firmware check** shows the status of the uploaded firmware. **Invalid** status means the firmware is not compatible with the QX hardware version.
  - **Current Firmware Version/New Firmware Version** shows the current/new firmware versions accordingly.

- Click **Update** to proceed the update or click **Discard** to close the warning message without updating the device.

**Note:** The update process takes about **5** minutes. Normal operation will be stopped during that time.

### 12.5.3 Automatic Firmware Update

The **Automatic Firmware Update** page is used to enable and configure the automatic firmware update settings on QX. When this service is enabled, on the scheduled time the QX will automatically check if a new firmware is available on the server. Then, based on the preconfigured settings, will notify user or update the firmware immediately.

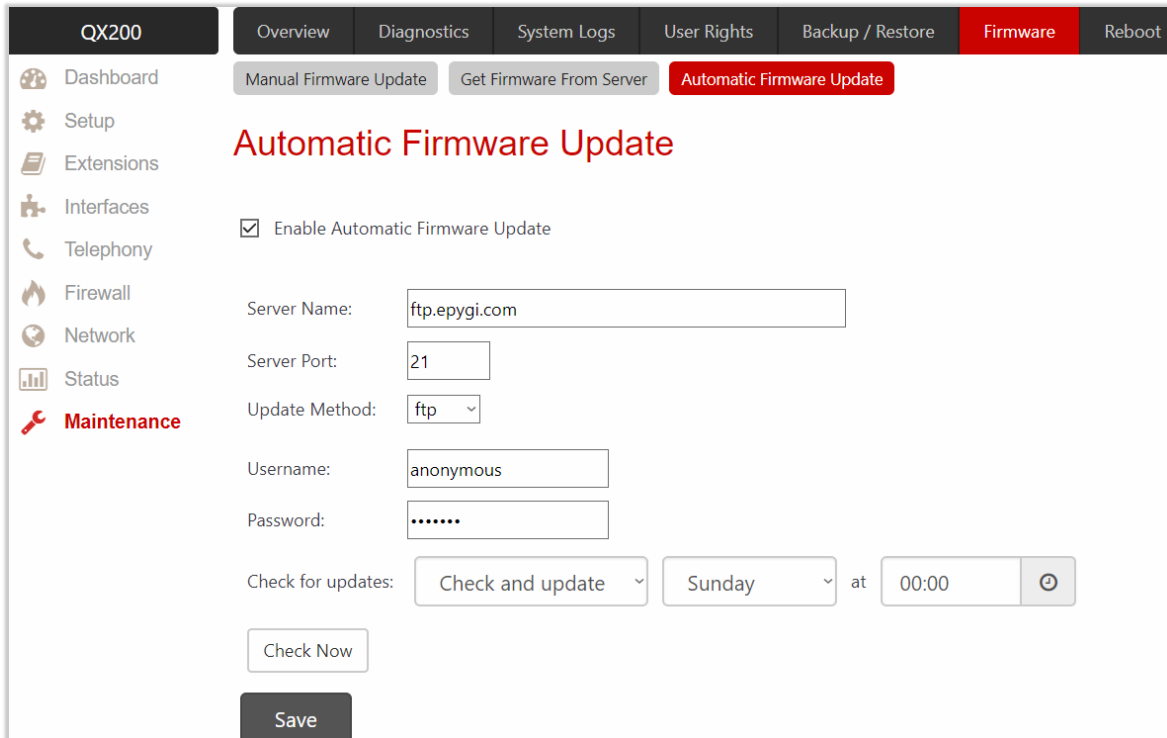


Figure 178: Automatic Firmware Update page

**Note:** The server configuration can be done manually. The recommended and simplest method is to use the Epygi public FTP server.

Check for updates based on one of the following options:

- Select the **Check and notify** option if you want QX to check for a new firmware in the server at the scheduled time and notify.
- Select **Check and update** option if you want QX to check for a new firmware, automatically download and install it on a scheduled time.
- Click **Check Now** to manually initiate the action selected from the **Check for updates** drop-down list.

To perform the automatic firmware update from Epygi FTP server:

- Tick the **Enable Automatic Firmware Update** option.
- Leave the **Server Name**, **Server Port**, **Update Method**, **Username** and **Password** text fields to their default values (ftp.epygi.com, 21, ftp and anonymous respectively, use blank for password) to use Epygi's public ftp server.
- Select the **Check and update** option from the **Check for updates** drop-down list.

4. Configure the **Date/Time** settings.
5. Click **Save**.

The system will check for a new firmware at a scheduled time. If there is a new firmware available, QX will download and update it automatically.

## 12.6 Reboot

The **Yes, Reboot Device** button is used to reboot the QX. **TIP:** The WEB GUI session with the QX will be terminated, i.e., after successful reboot you need to log in again.

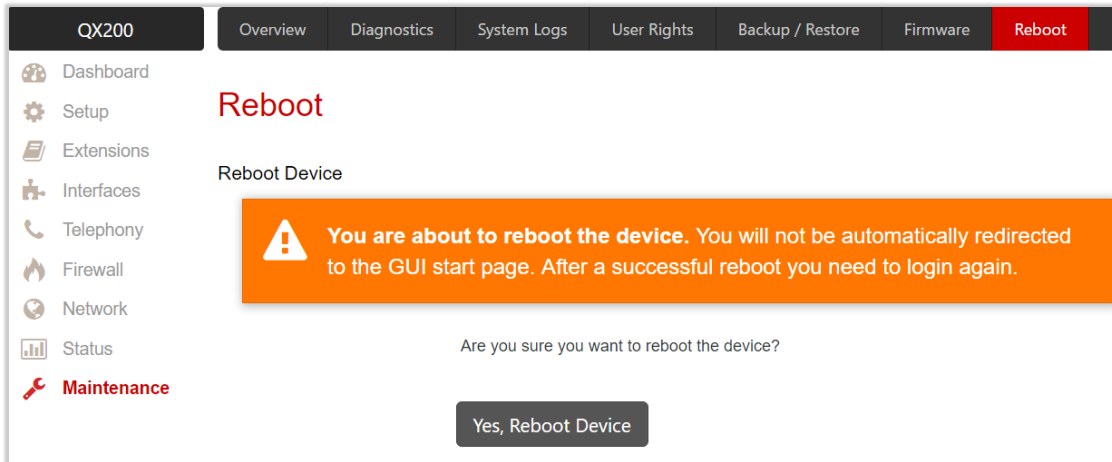


Figure 179: Reboot Device page

## 12.7 Registration Form

The **Register Your Device in Technical Support Center** page appears when configuring the unregistered QX, and it has been created for customer support purposes. The page allows you to register on [Epygi Technical Support](#).



Figure 180: Device Registration page

The following registration options are available:

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

## 13 Appendices

### 13.1 Administrator Login

The **Administrator Login** is used to review and modify the auto attendant greeting and recurring prompt as well as the universal extension messages. Phone Access Password will be required for login.

1. Dial \***75** to log in.
2. Enter the **Phone Access Password**.
3. Follow the voice prompts to review and change system messages.
4. Dial \***0** or **hang up** to logout.

System will notify about the messages that can be reviewed and modified.

Administrator Login menu						
<b>1</b> Review Attendant Greeting	<b>2</b> Review Attendant Recurring Prompt	<b>3</b> Review Universal Extension Messages				
Enter the <b>Attendant Number</b> (in case of multiple AAs)	Enter the <b>Attendant Number</b> (in case of multiple AAs)	<b>1</b> Voice Mail Greeting message	<b>3</b> Incoming Call Blocking message	<b>4</b> Outgoing Call Blocking message	<b>6</b> Out of Office message	<b>7</b> Find Me/ Follow Me message
<b>1</b> Listen to the current greeting	<b>1</b> Listen to the current prompt	<b>1</b> Listen to the current message	<b>1</b> Listen to the current message	<b>1</b> Listen to the current message	<b>1</b> Listen to the current message	<b>1</b> Listen to the current message
<b>2</b> Record a new greeting	<b>2</b> Record a new prompt	<b>2</b> Record a new message	<b>2</b> Record a new message	<b>2</b> Record a new message	<b>2</b> Record a new message	<b>2</b> Record a new message
<b>3</b> Restore system default greeting	<b>3</b> Restore system default prompt	<b>3</b> Restore system default message	<b>3</b> Restore system default message	<b>3</b> Restore system default message	<b>3</b> Restore system default message	<b>3</b> Restore system default message
<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback	<b>#</b> Stop recording or playback

Table 6: Administrator Login menu

## 13.2 Needed Bandwidth for IP Calls

The bandwidth required for an IP call depends on the used **codec**. The codec specifications are listed in the tables below.

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

Table 7: Required Bandwidth for Standard Packets

Codecs	Packet Size (in msec)					
	10	20	30	40	50	60
G.711u/G.711a	114	89	81	76	74	72
G.726-16	66	41	33	28	26	24
G.726-24	74	49	41	36	34	32
G.726-32	82	57	49	44	42	40
G.726-40	90	65	57	52	50	48
G.729a	58	33	26	20	18	16
iLBC	–	–	31	–	–	22
G.722	114	89	81	76	74	72
G.722.1	82	57	49	44	42	40

Table 8: Required Bandwidth for Encrypted Packets when using a SRTP

Codecs	Packet Size (in msec)					
	10	20	30	40	50	60
G.711u/G.711a	148	105	90	85	80	74
G.726-16	95	59	43	38	34	29
G.726-24	108	65	52	45	41	37
G.726-32	118	74	60	53	48	45
G.726-40	124	81	66	61	56	52
G.729a	92	49	35	30	26	22
iLBC	–	–	41	–	–	26
G.722	148	105	90	85	80	74
G.722.1	118	74	60	53	48	45

Table 9: Required Bandwidth for Encrypted Packets when using a VPN



## 13.3 System Default Values

The values are described ONLY for features, services and options which are enabled and preconfigured by default. The following abbreviations are used:

- n/a – not applicable for the selected QX model
- E – the setting (option) is enabled
- D – the setting (option) is disabled
- SA – the service or setting (option) is activated/preconfigured
- SNA – the service or setting (option) is NOT activated/preconfigured
- SDM – system default message

### 13.3.1 System Settings

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>User Rights Management</b>								
Username		admin	admin	admin	admin	admin	admin	admin
GUI Password		19	19	19	19	19	19	19
Phone Access Password		19	19	19	19	19	19	19
admin (role - Administrators)		E	E	E	E	E	E	E
localadmin (role – Local Administrator)		D	D	D	D	D	D	D
Access Rights – user extension	Access for all available pages	granted	granted	granted	granted	granted	granted	granted
Access Rights – localadmin	Access for all available pages	granted	granted	granted	granted	granted	granted	granted
<b>System Configuration Wizard</b>								
LAN IP Address		172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	192.168.0.200	192.168.0.200
LAN Subnet Mask		255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0	255.255.240.0	255.255.240.0
Hostname		epygiqx	epygiqx	epygiqx	epygiqx	epygiqx	epygiqx	epygiqx
Domain Name		epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc
DHCP Server	DHCP Settings for the LAN Interface	SNA	SNA	SNA	SNA	SNA	SNA	SNA
Your locale (location)		US	US	US	US	US	US	US
Timezone		(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)	(GMT-06:00) Central Time (US&Canada)
Emergency Codes		n/a	911	911	911	n/a	n/a	n/a
PSTN Access Code		n/a	9	9	9	n/a	n/a	n/a

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>System Configuration Wizard</b>								
Generate System Event		n/a	SNA	SNA	SNA	SNA	n/a	n/a
Send Notification via E-mail		n/a	SNA	SNA	SNA	SNA	n/a	n/a
Send Notification via SMS		n/a	SNA	SNA	SNA	SNA	n/a	n/a
Leave Voice Message		n/a	SNA	SNA	SNA	SNA	n/a	n/a
<b>Internet Configuration Wizard</b>								
WAN Interface Protocol		Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet
Upstream [kbit/s]		1,000,000	100,000	100,000	100,000	100,000	1,000,000	1,000,000
Downstream [kbit/s]		1,000,000	100,000	100,000	100,000	100,000	1,000,000	1,000,000
Min Data Rate [kbit/s]		0	0	0	0	0	0	0
IP configuration of the WAN interface		Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	n/a	n/a
MAC Address Assignment		This device	This device	This device	This device	This device	n/a	n/a
Maximum Transfer Unit (MTU)		1500	1500	1500	1500	1500	1500	1500
DNS Settings		Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	Obtain an IP Address automatically	Undefined	Undefined
<b>Date / Time Settings</b>								
SNTP Server		E	E	E	E	E	E	E
SNTP Client		E	E	E	E	E	E	E
SNTP Server		ntp1.epygi.com	ntp1.epygi.com	ntp1.epygi.com	ntp1.epygi.com	ntp1.epygi.com	ntp1.epygi.com	ntp1.epygi.com
Polling Interval		6 hr.	6 hr.	6 hr.	6 hr.	6 hr.	6 hr.	6 hr.
<b>System Security Management</b>								
Security Level		Medium	Medium	Medium	Medium	Medium	Medium	Medium
<b>Extensions Management</b>								
Extension Length		3	3	3	3	3	4	4
Extensions attached to FXS lines		n/a	(101-102) to (1-2)	n/a	(101-102) to (1-2)	n/a	n/a	n/a
Extensions attached to IP lines		(101-112) to (1-12)	(103-118) to (1-16)	(101-116) to (1-16)	(103-126) to (1-24)	(101-200) to (1-100)	(101-1200) to (1-200)	(101-1200) to (1-200)
Percentage of System Memory for Extensions attached to FXS lines		n/a	5%	n/a	5%	n/a	n/a	n/a
Percentage of System Memory for Extensions attached to IP lines		0.1%	0.4%	0.4%	0.4%	0.1%	0.04%	0.02%

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Auto Attendant 00 – General Settings</b>								
Display Name		Attendant	Attendant	Attendant	Attendant	Attendant	Attendant	Attendant
Enable FAX forwarding		D	D	D	D	D	D	D
Show on Public Directory		E	E	E	E	E	E	E
Percentage of System Memory		5%	5%	5%	5%	5%	0.08%	0.08%
<b>Auto Attendant 00 – Attendant Settings</b>								
Schedule		D	D	D	D	D	D	D
Attendant Scenario		Standard	Standard	Standard	Standard	Standard	Standard	Standard
<b>Auto Attendant 00 – Attendant Scenario</b>								
Pass Dialed Digits through Call Routing		D	D	D	D	D	D	D
Call Redirection		SNA	SNA	SNA	SNA	SNA	SNA	SNA
ZeroOut Redirection		SNA	SNA	SNA	SNA	SNA	SNA	SNA
Welcome Message		E	E	E	E	E	E	E
Welcome Message and Recurring Prompt	The system default messages are used.	SDM	SDM	SDM	SDM	SDM	SDM	SDM
<b>Auto Attendant 00 – SIP Registration Settings</b>								
Username / DID Number		00	00	00	00	00	00	00
Password		left blank	left blank	left blank	left blank	left blank	left blank	left blank
SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank
SIP Port		5060	5060	5060	5060	5060	5060	5060
SIP Registration Transport		UDP	UDP	UDP	UDP	UDP	UDP	UDP
Registration on SIP Server		D	D	D	D	D	D	D
<b>Auto Attendant 00 – SIP Advanced Settings</b>								
Authentication Username		None	None	None	None	None	None	None
Send Keep-alive Messages to Proxy		D	D	D	D	D	D	D
RTP Priority Level		Medium	Medium	Medium	Medium	Medium	Medium	Medium
Do Not use SIP Old Hold Method		D	D	D	D	D	D	D
Outbound Proxy		left blank	left blank	left blank	left blank	left blank	left blank	left blank
Secondary SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank
Outbound Proxy for Secondary SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Auto Attendant 00 – Codecs</b>								
G711u, G711a and G729		E	E	E	E	E	E	E
Preferred Codec		G711u	G711u	G711u	G711u	G711u	G711u	G711u
G726-16, G726-24, G726-32, G726-40, iLBC, G.722, G.722.1, TDVC		D	D	D	D	D	D	D
H.263, H.263+ and H.264		D	D	D	D	D	D	D
Out of Band DTMF Transport		E	E	E	E	E	E	E
T.38 FAX		E	E	E	E	E	E	E
Pass Through FAX		E	E	E	E	E	E	E
Pass Through Modem		D	D	D	D	D	D	D
Force Self Codecs Preference for Inbound Calls		D	D	D	D	D	D	D
SRTP Policy		Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything
<b>User Extension – General Settings</b>								
Display Name		None	None	None	None	None	None	None
Password		left blank	left blank	left blank	left blank	left blank	left blank	left blank
Use Kickback		D	D	D	D	D	D	D
Allow Call Relay		D	D	D	D	D	D	D
Allow GUI Login Allowed		D	D	D	D	D	D	D
Allow 3pcc/Click2Dial Access		D	D	D	D	D	D	D
Show on Public Directory		D	D	D	D	D	D	D
Use Parent Extension		D	D	D	D	D	D	D
<b>User Extension – SIP Registration Settings</b>								
Username / DID Number		Same as the extension number	Same as the extension number	Same as the extension number	Same as the extension number	Same as the extension number	Same as the extension number	Same as the extension number
Password		left blank	left blank	left blank	left blank	left blank	left blank	left blank
SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank
SIP Port		5060	5060	5060	5060	5060	5060	5060
SIP Registration Transport		UDP	UDP	UDP	UDP	UDP	UDP	UDP
Registration on SIP Server		D	D	D	D	D	D	D

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>User Extension – SIP Advanced Settings</b>								
Authentication Username		None	None	None	None	None	None	None
Send Keep-alive Messages to Proxy		D	D	D	D	D	D	D
RTP Priority Level		Medium	Medium	Medium	Medium	Medium	Medium	Medium
Do Not use SIP Old Hold Method		D	D	D	D	D	D	D
Outbound Proxy		left blank	left blank	left blank	left blank	left blank	left blank	left blank
Secondary SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank
Outbound Proxy for Secondary SIP Server		left blank	left blank	left blank	left blank	left blank	left blank	left blank
<b>User Extension – Voice Mailbox Settings</b>								
Voice Mailbox type		Use Internal Voice Mail	Use Internal Voice Mail	Use Internal Voice Mail	Use Internal Voice Mail	Use Internal Voice Mail	Use Internal Voice Mail	Use Internal Voice Mail
Configuration wizard status		Activated	Activated	Activated	Activated	Activated	Activated	Activated
<b>User Extension – Codecs</b>								
G711u, G711a and G729		E	E	E	E	E	E	E
Preferred Codec		G711u	G711u	G711u	G711u	G711u	G711u	G711u
G726-16, G726-24, G726-32, G726-40, iLBC, G.722, G.722.1, TDVC		D	D	D	D	D	D	D
H.263, H.263+ and H.264		D	D	D	D	D	D	D
Out of Band DTMF Transport		E	E	E	E	E	E	E
T.38 FAX		E	E	E	E	E	E	E
Pass Through FAX		E	E	E	E	E	E	E
Pass Through Modem		D	D	D	D	D	D	D
Force Self Codecs Preference for Inbound Calls		D	D	D	D	D	D	D
SRTP Policy		Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything	Make unsecure calls, accept anything
<b>Universal Extension Recordings</b>								
System Messages	The system default messages are used.	SDM	SDM	SDM	SDM	SDM	SDM	SDM
Percentage of System Memory	Memory allocation	0.1%	1%	1%	1%	0.1%	0.08%	0.08%

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>IP Lines</b>								
IP lines attached to extensions		(1-12) to (101-112)	(1-16) to (103-118)	(1-16) to (101-116)	(1-24) to (103-126)	(1-100) to (101-200)	(1-200) to (101-1200)	(1-200) to (101-1200)
IP line State		Free	Free	Free	Free	Free	Free	Free
<b>IP Line Settings</b>								
PnP for IP lines		E	E	E	E	E	E	E
Firmware Version Control		E	E	E	E	E	E	E
Configure IP phones from		LAN	LAN	LAN	LAN	LAN	LAN	LAN
Phones Default Template		systemdefault	systemdefault	systemdefault	systemdefault	systemdefault	systemdefault	systemdefault
<b>FXS Lines</b>								
FXS lines attached to extensions		n/a	(1-2) to (101-102)	n/a	(1-2) to (101-102)	n/a	n/a	n/a
Caller ID Type		n/a	Standard 2	n/a	Standard 2	n/a	n/a	n/a
Ringer Type		n/a	Type A	n/a	Type A	n/a	n/a	n/a
<b>FXO Line Settings</b>								
FXO lines		n/a	2	n/a	4	n/a	n/a	n/a
Enable Line		n/a	E	n/a	E	n/a	n/a	n/a
Allowed Call Type		n/a	Both incoming and outgoing calls	n/a	Both incoming and outgoing calls	n/a	n/a	n/a
Route incoming FXO call to		n/a	00	n/a	00	n/a	n/a	n/a
<b>ISDN Trunk Settings</b>								
ISDN trunks		n/a	n/a	4	n/a	n/a	n/a	n/a
Interface Type		n/a	n/a	User	n/a	n/a	n/a	n/a
Connection Type		n/a	n/a	PTMP	n/a	n/a	n/a	n/a
Service Type		n/a	n/a	No MSN	n/a	n/a	n/a	n/a
Route incoming call to		n/a	n/a	00	n/a	n/a	n/a	n/a
<b>Call Routing Table</b>								
Call Routing Rule 1	Destination Number Pattern to call <b>00</b> Auto Attendant	00	00	00	00	00	00	00
Call Routing Rule 2	Destination Number Pattern to call <b>PBX</b> extensions	???	???	???	???	???	????	????
Call Routing Rule 3	Destination Number Pattern to call <b>SIP</b> (sip.epygi.com)	8*	8*	8*	8*	8*	8*	8*

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>NAT Traversal</b>								
NAT Traversal for SIP		Automatic	Automatic	Automatic	Automatic	Automatic	Automatic	Automatic
NAT Traversal - SIP Parameters		Use STUN	Use STUN	Use STUN	Use STUN	Use STUN	Use STUN	Use STUN
NAT Traversal - RTP Parameters		Use STUN	Use STUN	Use STUN	Use STUN	Use STUN	Use STUN	Use STUN
<b>NAT Traversal – STUN Parameters</b>								
Primary STUN Server		stun.epygi.com	stun.epygi.com	stun.epygi.com	stun.epygi.com	stun.epygi.com	stun.epygi.com	stun.epygi.com
Primary STUN Port		3478	3478	3478	3478	3478	3478	3478
Polling Interval		1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 hour
Keep-alive Interval		120 sec.	120 sec.	120 sec.	120 sec.	120 sec.	120 sec.	120 sec.
NAT IP checking Interval		300 sec.	300 sec.	300 sec.	300 sec.	300 sec.	300 sec.	300 sec.
<b>RTP Settings</b>								
Packetization Interval for G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a		20	20	20	20	20	20	20
Packetization Interval for iLBC		30	30	30	30	30	30	30
Silence Suppression for G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, iLBC		Yes	Yes	Yes	Yes	Yes	Yes	Yes
G726 Standard		Use ITU-T specification	Use ITU-T specification	Use ITU-T specification	Use ITU-T specification	Use ITU-T specification	Use ITU-T specification	Use ITU-T specification
RTP/RTCP Port Range		6000-6509	6000-6255	6000-6255	6000-6255	6000-6509	6000-7799	6000-8399
Enable RTCP Support		D	D	D	D	D	D	D
<b>SIP Settings</b>								
UDP Port		5060	5060	5060	5060	5060	5060	5060
TCP Port		5060	5060	5060	5060	5060	5060	5060
TLS Port		5061	5061	5061	5061	5061	5061	5061
Realm		epygi	epygi	epygi	epygi	epygi	epygi	epygi
Session Timer		D	D	D	D	D	D	D
DNS Server for SIP		Default	Default	Default	Default	Default	Default	Default
SIP Timers		RFC3261	RFC3261	RFC3261	RFC3261	RFC3261	RFC3261	RFC3261

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Schedules</b>								
Work Hours	for Company's Schedule	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)	09:00-13:00, 14:00-18:00 (from Monday to Friday)
Observe Holidays	for Company's Schedule	D	D	D	D	D	D	D
State	for Company's Schedule	Running on Schedule	Running on Schedule	Running on Schedule	Running on Schedule	Running on Schedule	Running on Schedule	Running on Schedule
<b>Voice Mail Common Settings</b>								
Recording Codec		G711u	G711u	G711u	G711u	G711u	G711u	G711u
E-mail Subject for Voice Mail		Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]	Voice mail received from \$[VM_DISPNA M E] \$[VM_USERNA M E]
FAX to E-mail Format		TIFF	TIFF	TIFF	TIFF	TIFF	TIFF	TIFF
<b>Gain Control</b>								
FXS 1 (Transmit Gain/Receive Gain)		-6/0	-6/0	-6/0	-6/0	-6/0	-6/0	-6/0
FXS 2 (Transmit Gain/Receive Gain)		-6/0	-6/0	-6/0	-6/0	-6/0	-6/0	-6/0
FXO 1 (Transmit Gain/Receive Gain)		0/6	0/6	0/6	0/6	0/6	0/6	0/6
FXO 2 (Transmit Gain/Receive Gain)		0/6	0/6	0/6	0/6	0/6	0/6	0/6
FXO 3 (Transmit Gain/Receive Gain)		0/6	0/6	0/6	0/6	0/6	0/6	0/6
FXO 4 (Transmit Gain/Receive Gain)		0/6	0/6	0/6	0/6	0/6	0/6	0/6
ISDN 1 (Transmit Gain/Receive Gain)		0/0	0/0	0/0	0/0	0/0	0/0	0/0
ISDN 2 (Transmit Gain/Receive Gain)		0/0	0/0	0/0	0/0	0/0	0/0	0/0
ISDN 3 (Transmit Gain/Receive Gain)		0/0	0/0	0/0	0/0	0/0	0/0	0/0
ISDN 4 (Transmit Gain/Receive Gain)		0/0	0/0	0/0	0/0	0/0	0/0	0/0
Audio Line Out (Transmit Gain)		Off	Off	Off	Off	Off	Off	Off
Audio Line In (Receive Gain)		Off	Off	Off	Off	Off	Off	Off
Voice Mail (Recording Gain)		0	0	0	0	0	0	0
Voice Mail (Playback Gain)		0	0	0	0	0	0	0
<b>Dial Timeout Settings</b>								
Routing Dial Timeout		4 sec.	4 sec.	4 sec.	4 sec.	4 sec.	4 sec.	4 sec.



Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Firewall Configuration</b>								
IDS		E	E	E	E	E	n/a	n/a
NAT		E	E	E	E	E	n/a	n/a
Firewall		D	D	D	D	D	D	D
Firewall Security Level		SNA	SNA	SNA	SNA	SNA	SNA	SNA
<b>Advanced Firewall Configuration</b>								
Ping Stealth		E	E	E	E	E	E	E
Fool Portscanner		D	D	D	D	D	n/a	n/a
<b>Filtering Rules</b>								
Management Access	HTTPS service allowed for Any IP	E	E	E	E	E	E	E
SIP Access	SIP service allowed for Any IP	E	E	E	E	E	E	E
<b>SIP IDS Settings</b>								
SIP IDS		E	E	E	E	E	E	E
Add the IP address into the Blocked IP List in Firewall		E	E	E	E	E	E	E
Discard SIP messages from IP address for		32 sec.	32 sec.	32 sec.	32 sec.	32 sec.	32 sec.	32 sec.
<b>Second LAN Interface Settings</b>								
Second LAN Interface		n/a	n/a	n/a	n/a	n/a	E	E
IP Address		n/a	n/a	n/a	n/a	n/a	172.30.0.1	172.30.0.1
Subnet Mask		n/a	n/a	n/a	n/a	n/a	255.255.0.0	255.255.0.0
DHCP Server for the Second LAN interface		n/a	n/a	n/a	n/a	n/a	D	D
<b>DHCP Advanced Settings – DHCP Options</b>								
Gateways		172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	192.168.0.200	192.168.0.200
Subnet Mask		255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0	255.255.0.0	255.255.254.0	255.255.254.0
Domain Name Servers		172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	192.168.0.200	192.168.0.200
NBT Name Servers		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
NTP Servers		172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	192.168.0.200	192.168.0.200
Domain Name		epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc
Overload TFTP Server Name		172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	172.30.0.1	192.168.0.200	192.168.0.200

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>DHCP Advanced Settings – DHCP Server Statements</b>								
Authoritative		D	D	D	D	D	D	D
Ping Check		E	E	E	E	E	E	E
Ping Timeout		1 sec.	1 sec.	1 sec.	1 sec.	1 sec.	1 sec.	1 sec.
<b>DNS Server Settings</b>								
Zone		epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc	epygi-config.loc
Time to Live (TTL)		86400 sec.	86400 sec.	86400 sec.	86400 sec.	86400 sec.	86400 sec.	86400 sec.
Mail Exchange (MX)		Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
<b>PPTP Server Configuration</b>								
Subnet		172.31.1.0/24	172.31.1.0/24	172.31.1.0/24	172.31.1.0/24	172.31.1.0/24	n/a	n/a
Authentication		MSCHAPv2	MSCHAPv2	MSCHAPv2	MSCHAPv2	MSCHAPv2	n/a	n/a
Encryption		MPPE 128-bit	MPPE 128-bit	MPPE 128-bit	MPPE 128-bit	MPPE 128-bit	n/a	n/a
<b>L2TP Server Configuration</b>								
Subnet		172.31.2.0/24	172.31.2.0/24	172.31.2.0/24	172.31.2.0/24	172.31.2.0/24	n/a	n/a
<b>Event Settings</b>								
All available system events		Display notification	Display notification	Display notification	Display notification	Display notification	Display notification	Display notification
PPP	System events concerning PPP application	Do nothing	Do nothing	Do nothing	Do nothing	Do nothing	n/a	n/a
<b>Call History – Settings</b>								
Call Reporting		E	E	E	E	E	E	E
Maximum Number of Successful Call Records		100	100	100	100	100	100	100
Maximum Number of Missed Call Records		100	100	100	100	100	100	100
Maximum Number of Unsuccessful Call Records		100	100	100	100	100	100	100
CDR Parameters	CDR Parameters exclusion from CDR file	D	D	D	D	D	D	D
<b>Call History – Archiving Settings</b>								
Percentage of Total Memory allocated for Archive		0%	0%	0%	0%	0%	0%	0%
Call History Archiving		D	D	D	D	D	D	D

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>System Logs Settings</b>								
User Logging		E	E	E	E	E	E	E
Developer Logging		E	E	E	E	E	E	E
Log Lines to show		1000	1000	1000	1000	1000	1000	1000
<b>Automatic Firmware Update</b>								
Automatic Firmware Update		E	E	E	E	E	D	D
Server Name		ftp.epygi.com	ftp.epygi.com	ftp.epygi.com	ftp.epygi.com	ftp.epygi.com	ftp.epygi.com	ftp.epygi.com
Server Port		21	21	21	21	21	21	21
Update Method		ftp	ftp	ftp	ftp	ftp	ftp	ftp
Username		anonymous	anonymous	anonymous	anonymous	anonymous	anonymous	anonymous
Password		left blank	left blank.	left blank.	left blank.	left blank.	left blank.	left blank.
Check for updates		Check and notify every day at 0:00	Check and notify every day at 0:00	Check and notify every day at 0:00	Check and notify every day at 0:00	Check and notify every day at 0:00	Check and notify every day at 0:00	Check and notify every day at 0:00

## 13.3.2 User Extension Settings

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Voice Mail Settings – General Settings</b>								
Maximum Voice Mail Duration		5 min.	5 min.	5 min.	5 min.	5 min.	5 min.	5 min.
Forward/Rewind Duration		3 sec.	3 sec.	3 sec.	3 sec.	3 sec.	3 sec.	3 sec.
Ask password before granting local access to Voice Mailbox		D	D	D	D	D	D	D
Ask password before granting remote access to Voice Mailbox		E	E	E	E	E	E	E
Play welcome message		D	D	D	D	D	D	D
Play Voice Mail help		E	E	E	E	E	E	E
Automatically play Voice Mail		E	E	E	E	E	E	E
Play Voice Mails count information message		D	D	D	D	D	D	D
Play date/time information message		E	E	E	E	E	E	E
Play beep at the end of message		E	E	E	E	E	E	E
Silent Voice Mail recording		D	D	D	D	D	D	D
Voice Mail Greeting Message		SDM	SDM	SDM	SDM	SDM	SDM	SDM
<b>Voice Mail Settings – VM Notifications</b>								
Send new Voice Mail notifications via E-mail		D	D	D	D	D	D	D
Send new Voice Mail notifications via SMS		D	D	D	D	D	D	D
Send new Voice Mail notifications via phone call		D	D	D	D	D	D	D
Voice Mail Notification Message		SDM	SDM	SDM	SDM	SDM	SDM	SDM
<b>Voice Mail Settings – VM Indication</b>								
Lamp indication		E	E	E	E	E	E	E
Tone indication		n/a	E	n/a	E	n/a	n/a	n/a
Ringing indication		n/a	D	n/a	D	n/a	n/a	n/a
<b>Voice Mail Settings – VM Redirection</b>								
Zero Out Redirect	Calls will be redirected to 00 Auto Attendant.	E	E	E	E	E	E	E
FAX Redirection		D	D	D	D	D	D	D
Automatic Fax Receiving Mode		D	D	D	D	D	D	D

Service / Option / Parameter	Description	QX20	QX50	QXISDN4+	QX200	QX500	QX2000	QX3000
<b>Account Settings</b>								
Display Name		None	None	None	None	None	None	None
User Password Protection	Both for incoming and outgoing calls	D	D	D	D	D	D	D
Remote Extension service		D	D	D	D	D	D	D
User's name for Dial by Name Directory		Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
<b>Basic Services – General Settings</b>								
No Answer Timeout		20 sec.	20 sec.	20 sec.	20 sec.	20 sec.	20 sec.	20 sec.
Call Waiting service		E	E	E	E	E	E	E
Redial Interval		10 sec.	10 sec.	10 sec.	10 sec.	10 sec.	10 sec.	10 sec.
Redial Period		15 min.	15 min.	15 min.	15 min.	15 min.	15 min.	15 min.
<b>Basic Services – Hold Music Settings</b>								
Send Hold Music to Remote IP Party		D	D	D	D	D	D	D
Listen Hold Music		Own_Music	Own_Music	Own_Music	Own_Music	Own_Music	Own_Music	Own_Music
Hold Music		SDM	SDM	SDM	SDM	SDM	SDM	SDM
<b>Basic Services – Do Not Disturb Settings</b>								
Actual Status		SNA	SNA	SNA	SNA	SNA	SNA	SNA
Expires after		30 min	30 min	30 min	30 min	30 min	30 min	30 min
Send Message to Caller		E	E	E	E	E	E	E

## 14 References

---

Refer to the below listed recourses to get more details about the configurations described in this guide:

- Manual-I: Installation Guide for QX IP PBXs
- Manual-III: User Guide for QX IP PBXs
- System Capacity of QX IP PBXs
- QX IP PBX Features on Epygi Supported IP Phones
- Licensable Features on QX IP PBXs
- Language Packs Overview for Epygi QX Line
- Audio-Video Conferencing on QX IP PBXs
- Receptionist Service on QX IP PBXs
- QX IP PBX Remote Extension Configuration
- Extensions Bulk Import on QX IP PBXs
- Auto Configuration of Epygi Supported IP Phones using OpenVPN
- Call Detail Records on QX IP PBXs
- Firmware Update Service on Epygi QX Line
- DCC – User Guide

Find the above listed documents on [Epygi Support Portal](#).

# 15 Software License Agreement

## EPYGI TECHNOLOGIES, LLC. Software License Agreement

### THIS IS A CONTRACT.

CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QX AND 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, LLC. (the "Licensor"), hereby grants to you a non-exclusive right to use the QX or Quadro Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may use the Licensed Materials only in connection with your operation of your QX or Quadro. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.
- 2. Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or the transfer of the Licensed Materials is subject to the terms of this Agreement.
- 3. Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.
- 4. No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language under penalty of law.
- 5. Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your QX or Quadro 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 QX or Quadro 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 2233 Lee Road Suite 201 Winter Park, Florida 32789 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](http://www.gnu.org) ( link to : <http://www.gnu.org/> ) . For a list of free software go to <http://www.epygi.com/about/free-software-list>.