Manual-II: Administration Guide for QX Gateways

This manual is effective for all QX Gateways: QXE1T1, QXFXO4, QXISDN4 and QXFXS24.

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

Emergency 911 Calls

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

Limited Warranty

Epygi Technologies, LTD. ('Epygi') warrants to the original end-user purchaser every Quadro and QX to be free from physical defects in material and workmanship under normal use for a period of one (1) year from the date of purchase (proof of purchase required) or two (2) years from the date of purchase (proof of purchase required) for products purchased in the European Union (EU). If Epygi receives notice of such defects, Epygi will, at its discretion, either repair or replace products that prove to be defective.
This warranty shall not apply to defects caused by (i) failure to follow Epygi's installation, operation or maintenance instructions; (ii) external power sources such as a power line, telephone line or connected equipment; (iii) products that have been serviced or modified by a party other than Epygi or an authorized Epygi service center; (iv) products that have had their original manufacturer's serial numbers altered, defaced or deleted; (v) damage due to lightning, fire, flood or other acts of nature.
In no event shall Epygi's liability exceed the price paid for the product from direct, indirect, special, incidental or consequential damages resulting from the use of the product, its accompanying software or its documentation. Epygi offers no refunds for its products. Epygi makes no warranty or representation, expressed, implied or statutory with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability or fitness for any particular purpose.

Return Policy

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

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

European Limited Warranty

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

Extended Warranty

Extended Warranty Option

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

Extended Warranty Statement

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

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

Epygi Technologies, LTD.

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 the file a complaint with the FCC if you believe it is necessary.

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

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

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

Electrical Safety Advisory

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

Industry Canada Statement

This product meets the applicable Industry Canada technical specifications.

Safety Information

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

- To prevent fire or shock hazard, do not expose your Quadro or QX to rain or moisture.
- To avoid electrical shock, do not open the Quadro or QX. Refer servicing to qualified personnel only.
- Never install wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specified for wet locations.
- Never touch 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 Quadro or QX during an electrical storm.
- Do not use your Quadro, QX or telephone to report a gas leak in the vicinity of the leak.
- An electrical outlet should be as close as possible to the unit and easily accessible.

Emergency Services

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

Music on Hold Copyright

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

Compliance with Laws

You may not use the Epygi Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

Document Edition History

Revision	Date	Description	Valid for Models	Valid for FW
1.0	27-May-16	Initial Release	QX Gateways	6.1.17 and higher
1.1	24-Mar-17	Updated	QXFXO4, QXISDN4, QXE1T1	6.1.17 and higher
			QXFXS24	6.1.40 and higher
1.2	11-Dec-17	Updated	QXE1T1, QXFXO4, QXISDN4 and QXFXS24	6.2.1 and higher

Table of Contents

1 About Administration Guide

This guide is intended for administrators who need to prepare for install, configure and operate QX Gateways (herein QX). In this guide, we describe the functionality and configuration of QXs with reference to other guides, manuals and complementary resources.

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

2 Conventions Used in this Guide

Following conventions are used in this guide:

- Add – this button is used to create and add new entry.
- Edit – this button is used to modify the selected entry(s).
- Delete – this button is used to remove the selected entry(s).
- Save – this button is used to apply changes.
- Start – this button is used to start a service, connection, etc.
- Stop – this button is used to start a service, connection, etc.
- Enable/Disable – this button is used to enable/disable the selected entry(s).
- Move Up/Move Down – are used to sort the entries in the specific table in the order they need to be accessed.
- Generate Password – this button is used to generate a system defined strong password.
- Show Hot Desking Settings/Hide Hot Desking Settings – these links are used to show/hide the Hot Desking settings respectively.
- Hide extensions attached to disabled IP lines / Show all extensions – these links 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 QXFXS24).
  - Auto – calls to a destination resolved by the Call Routing Table.
- Address (Redirect Address, Calling Address or Call to) – this 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 – this field is used to enter any optional information about the entry.
- Wildcard supported – 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 the QX to select the way custom voice message will be provided:
  - File – is used to upload/record the file for the message.
  - RTP Channel – is used to stream the massage (hold music, ringing announcements, queue messages, etc.) through the RTP Channels.

- Upload file – show the available methods in case if File is selected from the options mentioned above:
  - Click Choose File next to the Upload file field to open a file chooser window to upload the file.

Once the message has been uploaded/recorded the following links will appear:

- Download … message – used to download the uploaded message.
- Remove … message – used to remove the uploaded message or restore the default one.

Note:

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

3 QX's Graphical Interface

The following top menus and links are available on the QX Management page when logged in as an administrator:

- Dashboard
- Setup
- Extensions
- Interfaces
- Telephony
- Firewall
- Network
- Status
- Maintenance
- Go To Extension – allows quick access to the User Settings for the selected extension.
- Pending Events – allows quick access to the system events and event settings.
- Language – available when a custom Language Pack has been installed. Is used to enable the custom language for GUI or revert back to the default English.
- Date/Time – displays the device's current time.
- Hostname – displays the device's hostname.
- Renew WAN IP Address – will be shown if the WAN IP address for QX 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 QX. The **Active Calls** table includes information about the calling/called parties, call start time and duration.

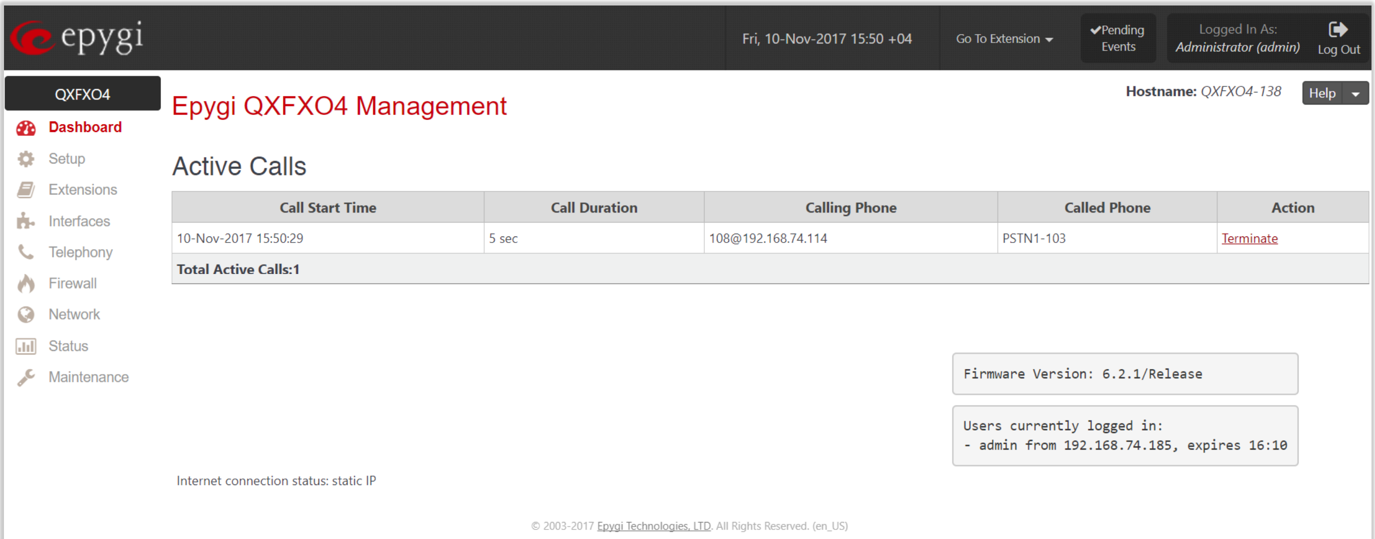


Figure 1: Dashboard menu

- The **Terminate** link is used to terminate the active call.
- 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 QX's firmware are presented as well. The idle session timeout is set to 10 minutes. If no action is performed within 10 minutes, the user will be automatically logged out.

5 Setup Menu

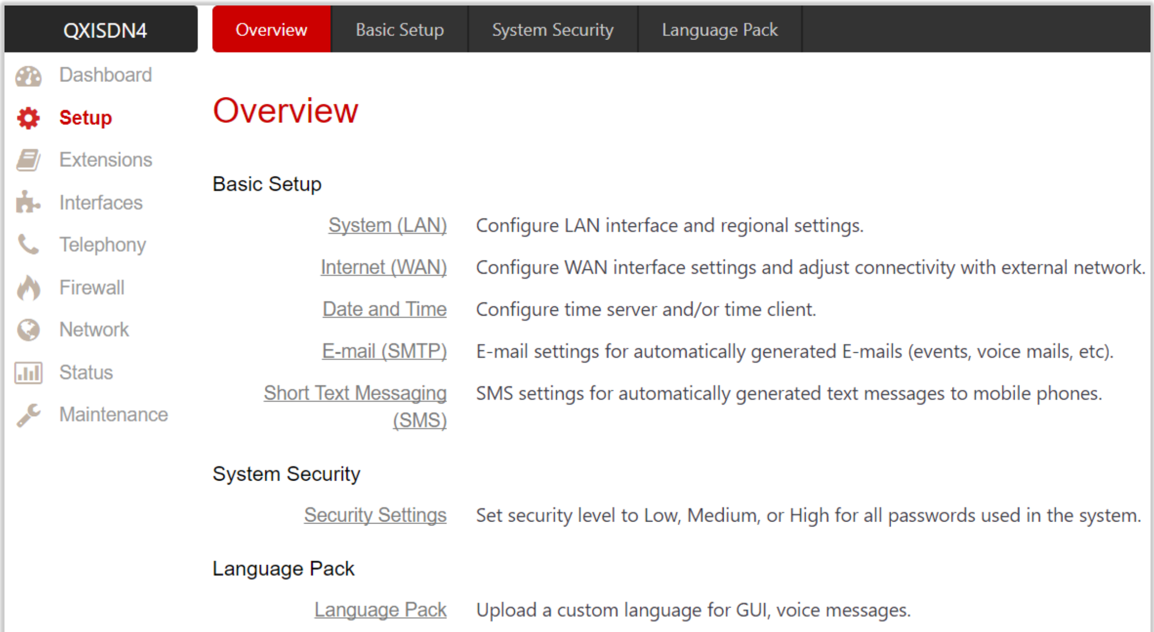


Figure 2: Setup Menu overview

5.1 Basic Setup

5.1.1 System (LAN)

You can login the QX WEB GUI through the LAN interface using the default IP address, which is 172.28.0.1. Go to the Setup→Basic Setup→System (LAN) to adjust the network parameters for the LAN interface. The System Configuration Wizard navigate you through the following parameters and settings:

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

System Configuration

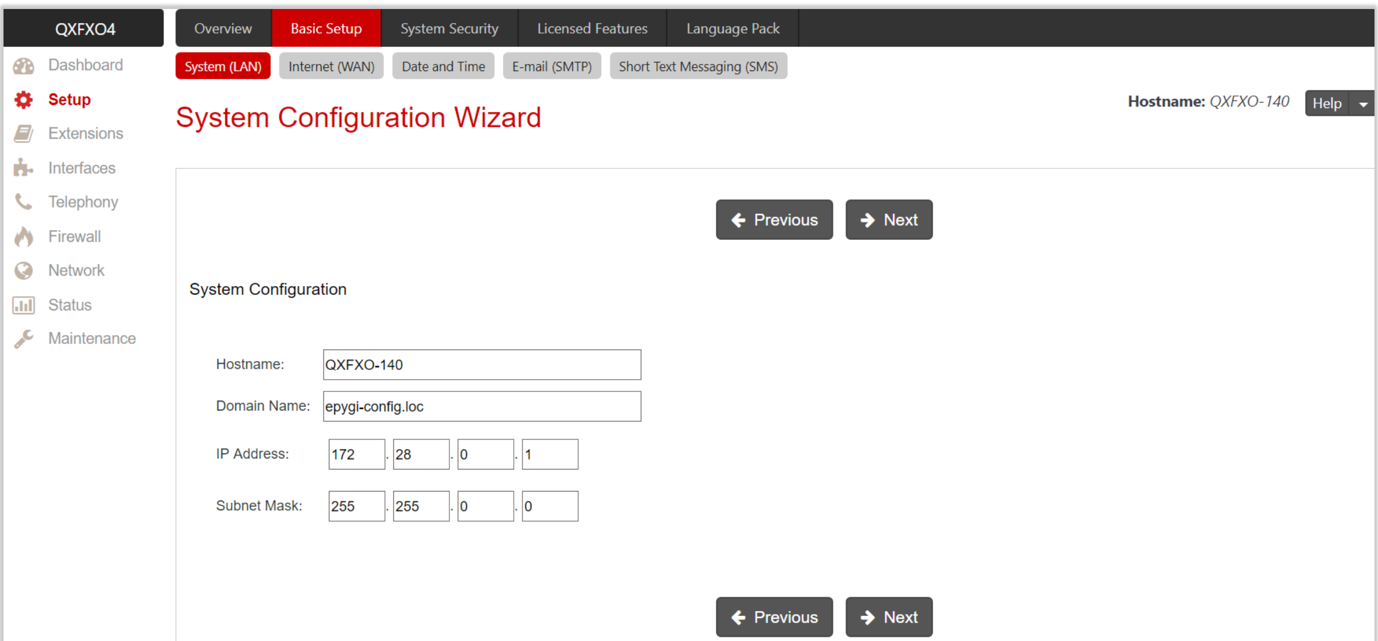


Figure 3: System Configuration section

- Hostname – set the host name for QX.
- Domain Name – set domain name which the QX belongs to.
- IP Address – set the LAN IP address.
- Subnet Mask – set the subnet mask.

DHCP Settings for the LAN Interface

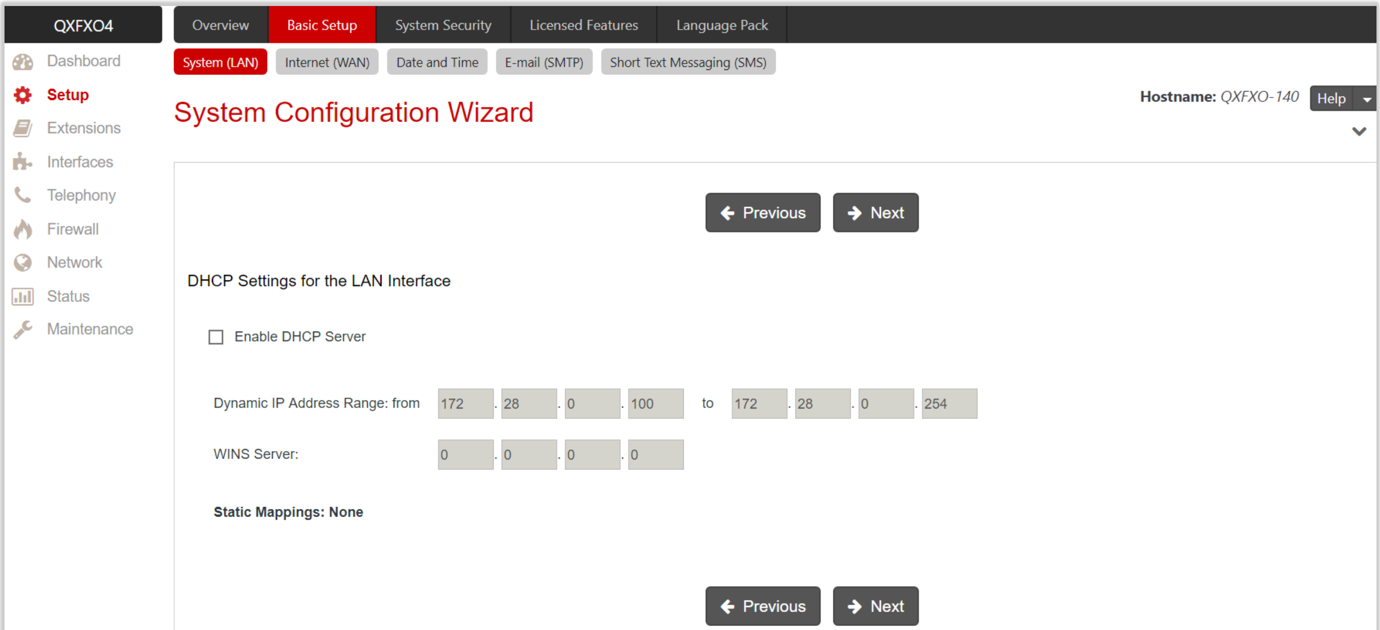


Figure 4: DHCP Settings for the LAN Interface section

- Enable DHCP Server – enable/disable DHCP server capability on the QX.
- Dynamic IP Address Range: (from - to) – set the IP address pool.
- WINS Server – set the IP address for the WINS server.

Regional Settings and Preferences

The regional settings are important for the functionality of the QX voice subsystem.

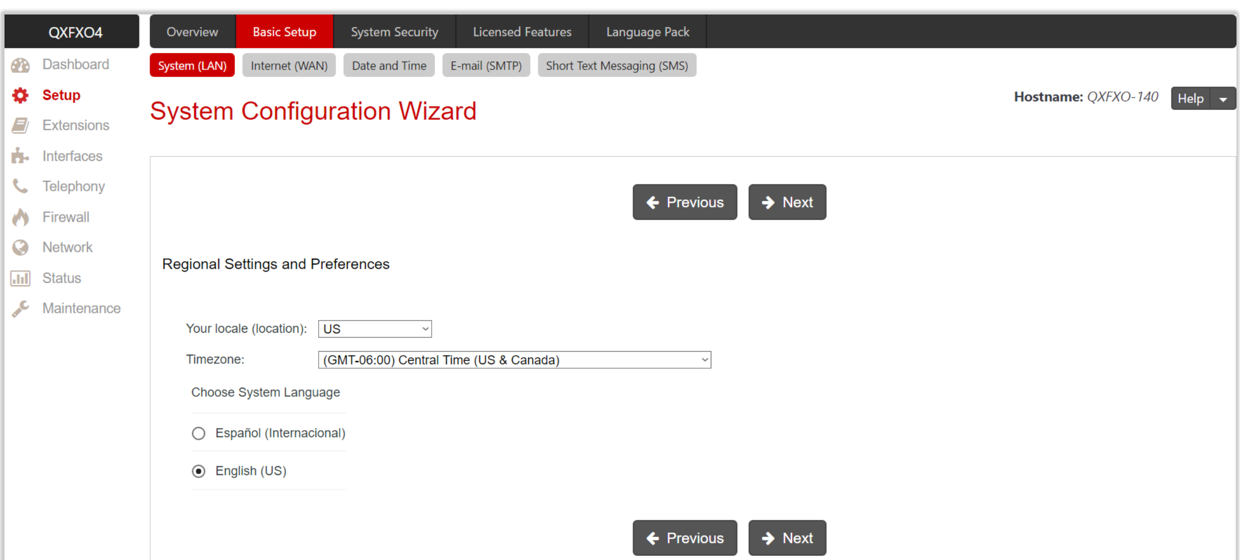


Figure 5: Regional Settings and Preferences section

- Your Locale (location) – select the location and timezone of QX.
- Timezone – select the proper time zone so the QX can display correct time accordingly. TIP: The QX supports Daylight Savings (DST) correction if it is available for the selected time zone.

- Choose System Language – select the language for system voice messages: custom or default English. TIP: This selection is available when a custom Language Pack has been uploaded.

Note:

- ➢ Finish the wizard and click "OK" to apply the changes made in any section 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 not change the factory default settings if their meanings are not fully clear to you.

5.1.2 Internet (WAN) – Internet Configuration Wizard

Go to the Setup→Basic Setup→Internet (WAN) to configure or adjust the network parameters for the QX WAN interface. The Internet Configuration Wizard navigates through the following basic configuration parameters and settings:

- Uplink Configuration
- WAN Interface Protocol
- WAN Interface Configuration
- DNS Settings

<u>Uplink Configuration</u>

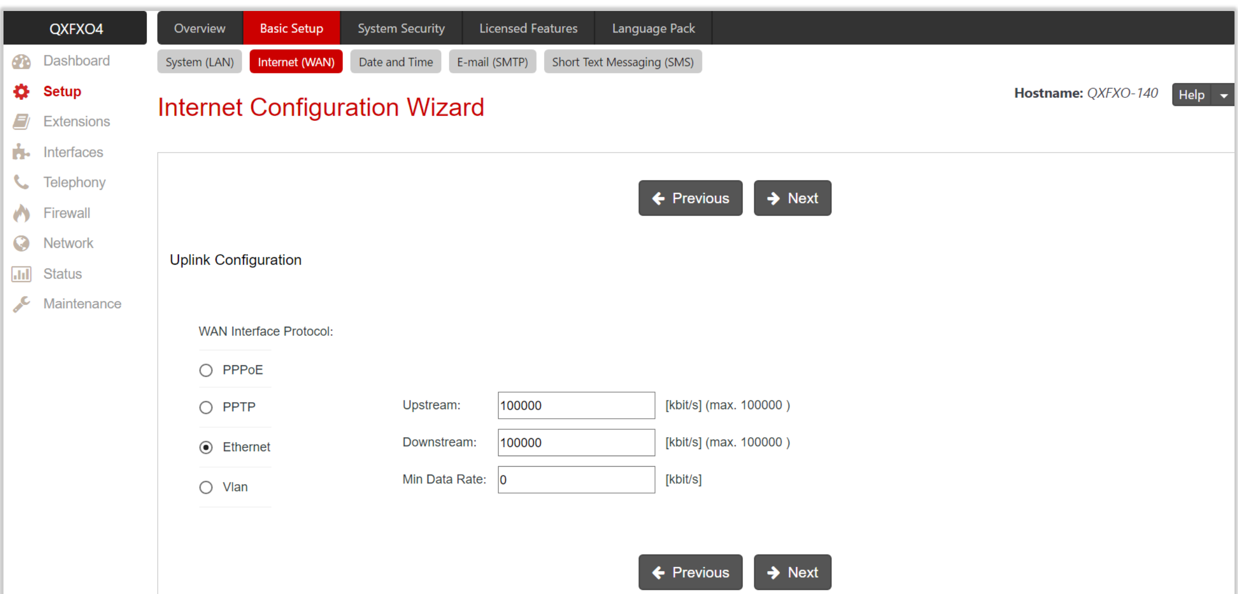


Figure 6: Uplink Configuration section

- WAN Interface Protocol – select the protocol for the WAN interface. Based on this selection the wizard's configuration pages may differ. The following connection protocols are available:
- ➢ PPPoE
- ➢ PPTP
- ➢ Ethernet
- ➢ VLAN (TIP: This option becomes available only when VLAN is configured on the QX.)
- ➢ WAN interface bandwidth settings 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 approaching the limits of a bandwidth capacity, another IP call will be declined.

- Min Data Rate – 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 – keeps the connection alive by sending control packets for the link state verification.
- Authentication Settings – enter the authentication parameters (Username and Password) to register on the ISP server.
- Dial Behavior – select the Dial Behavior type.
  - Dial manually – if selected, a button will be displayed in the top WEB management window to switch the connection on/off.
  - Always connected – if selected, the QX will always stay connected.
- IP Address Assignment – select the IP Address assignment type for the PPPoE interface:
  - Obtain an IP Address automatically – with this option QX will get an IP address dynamically.
  - Use the following IP Address – set the IP address manually.

PPTP

- Obtain an IP Address automatically – with this option selected, QX will use DHCP to get an available IP address from your local network or ISP.
- Use the following IP Address – if selected, manually provide the settings for the WAN interface.

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

- PPTP Server – enter the IP address of the PPTP server.
- Encryption – select the encryption for the traffic over the PPTP interface.
- Keep Connection Alive – keeps the connection alive by sending control packets for the link state verification.
- Authentication Settings – enter the authentication parameters (Username and Password) to register on the ISP server.
- Dial Behavior – select the Dial Behavior type.
  - Dial manually – if selected, a button will be displayed in the top WEB management window to switch the connection on/off.
  - Always connected – if selected, the QX will always stay connected.
- IP Address Assignment – select the IP Address assignment type for the PPPoE interface:
  - Obtain an IP Address automatically – with this option QX will get an IP address dynamically.
  - Use the following IP Address – set the IP address manually.

Ethernet

- Obtain an IP Address automatically – with this option selected, QX will use DHCP to get an available IP address from your local network or ISP.
- Use the following IP Address – if selected, manually provide the settings for the WAN interface.

VLAN

- VLAN ID – 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 – with this option selected, QX will use DHCP to get an available IP address from your local network or ISP.
- Use the following IP Address – if selected, manually provide the settings for the VLAN interface.

WAN Interface Configuration

This section is used to modify the MAC address of the QX. This might be necessary if the ISP requires a specified MAC address (e.g. for authentication).

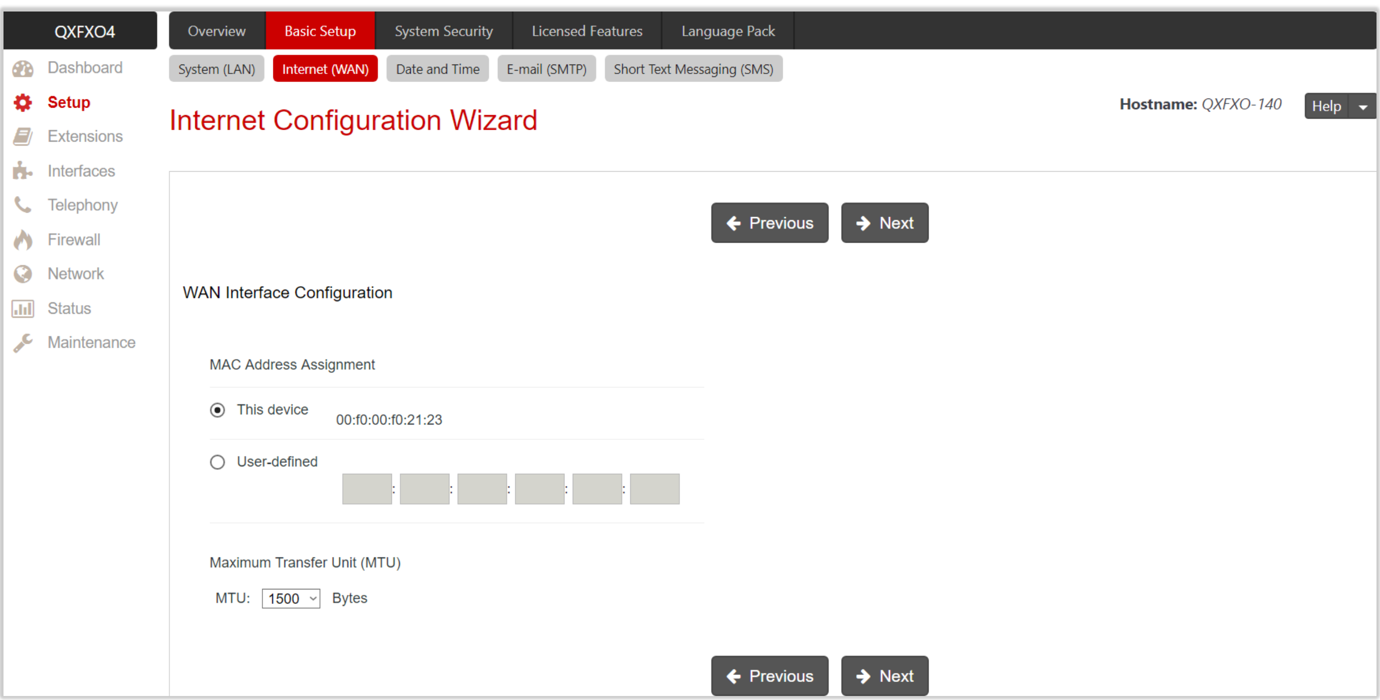


Figure 7: WAN Interface Configuration section

- This device – selects the default MAC address of the WAN interface.
- User-defined – enter the MAC Address manually.
- MTU – 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

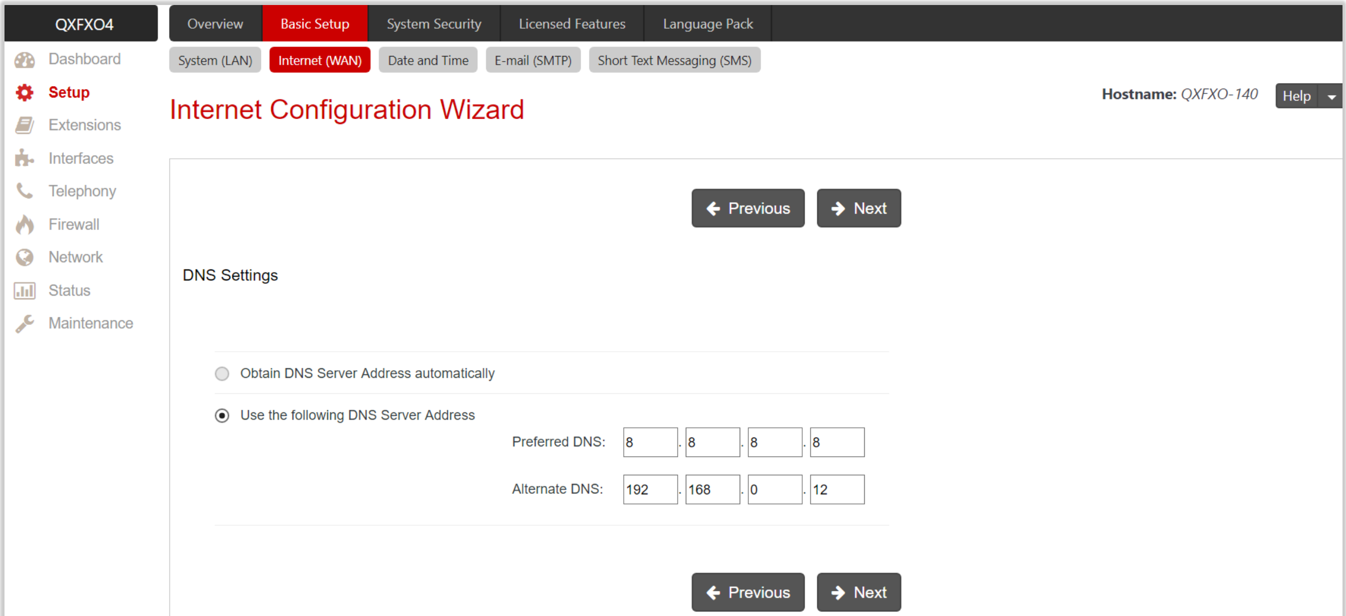


Figure 8: DNS Settings section

- Obtain DNS Server Address automatically – automatically configures the assignment of the name server address from the provider party.
- Use the following DNS Server Address – is used to manually assign a name server as follows:
  - Preferred DNS – enter the IP address of an external name server.
  - Alternate DNS – enter the IP address of the secondary name server that will be used if the main name server cannot be accessed.

Note:

- Finish the wizard and click "OK" to apply the changes made in any section 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 not change the factory default settings if their meanings are not fully clear to you.

5.1.3 Date and Time

The QX **Date and Time** settings may be updated through the international time servers.

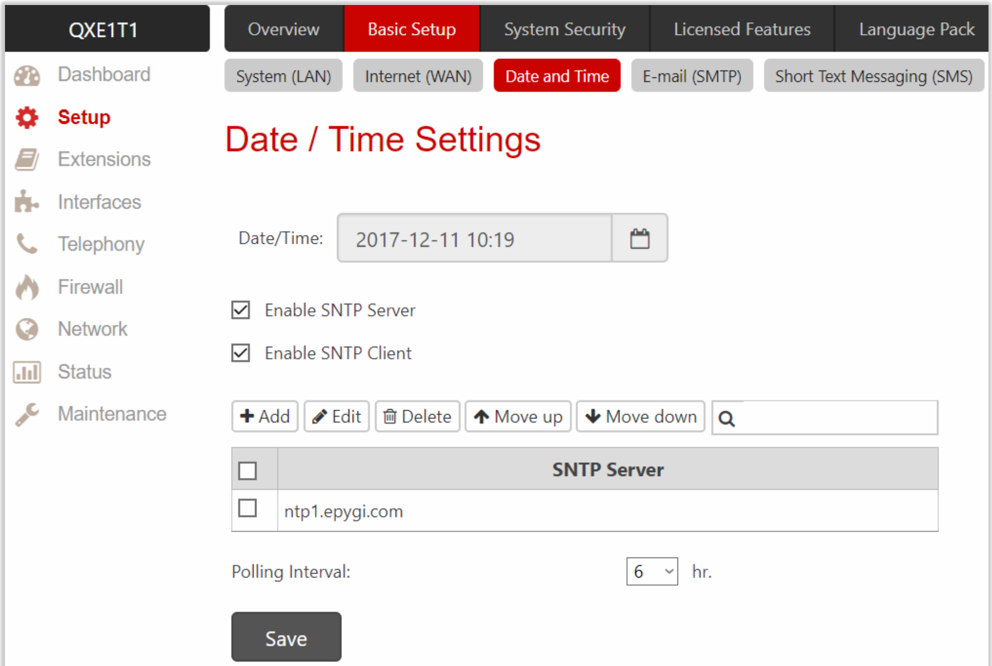


Figure 9: Time/Date Settings page

- **Date/Time** – displays the current system time.
- **Enable SNTP Server** – enable or disable SNTP server capability on the QX.
- **Enable SNTP Client** – enable or disable SNTP client on the QX. If not selected, the current system time can be configured manually.
- **Polling Interval** – select the time interval for the periodical synchronization between the timeserver and QX.

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

1. Click **Add**. Define new server parameters:
   - **Manual** – enter the SNTP server's FQDN (Full Qualified Domain Name) or IP address.
   - **Predefined** – select the SNTP server's host address from the drop-down list.
2. Click **Save**, to add the new SNTP server in 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 Servers** table does not answer, NTP server in the next position will be attempted to reach.

5.1.4 E-mail (SMTP)

Simple Mail Transfer Protocol (SMTP) service allows QX to automatically generate and send alert and notification e-mails as specified in the Event Settings.

- Enable SMTP Service – activates the SMTP service.
- SMTP Host – IP address or hostname of the SMTP server.
- E-mail Sender Address – e-mail address that is either registered on the selected SMTP server or has permission to use the 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) – 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 – select if the specified SMTP server requires authentication. Then enter the Username and Password configured on the SMTP server.

Shown below is the sample e-mail settings on the QX, assuming the e-mail is using smtp.gmail.com as the SMTP server.

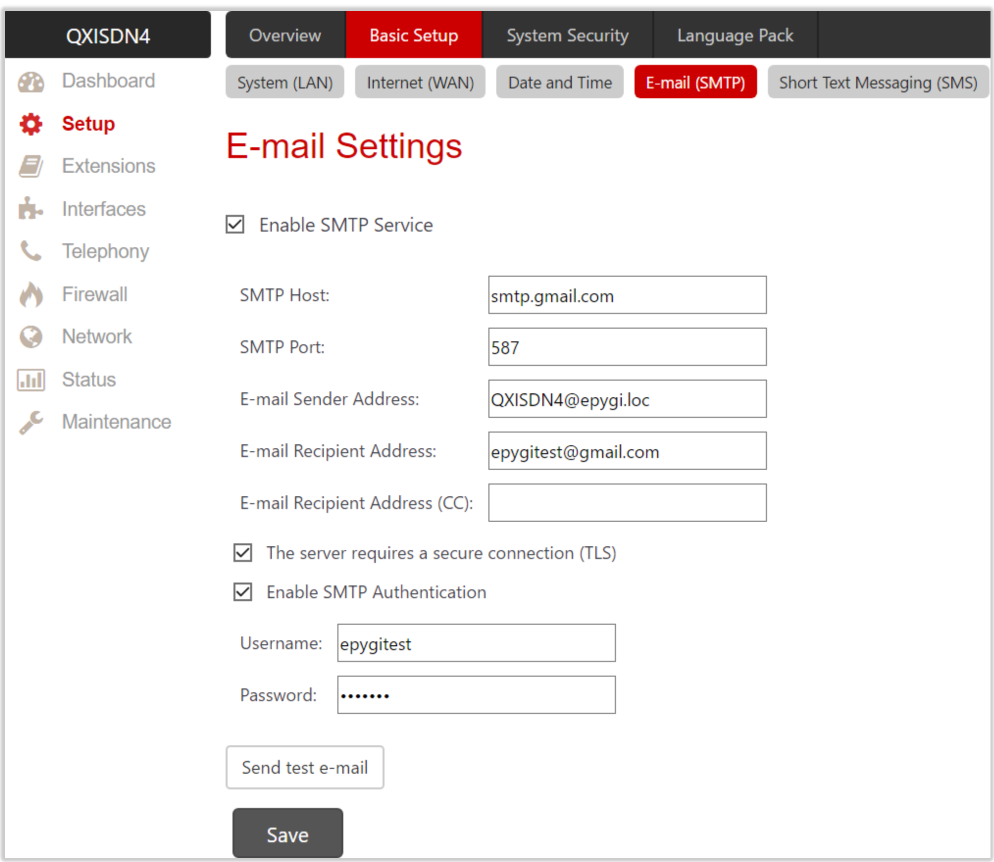


Figure 10: E-mail Settings page

Once the configuration is finished, 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.

- **Enable SMS Service** – activates SMS service.
- **Username** and **Password** – authentication parameters configured on the SMS server.
- **SMS Sender Address** – sms sender's address.
- **SMS Recipient Address** – sms recipient's address. TIP: Use a space, semicolon or a comma to separate mobile numbers in case of multiple recipients.

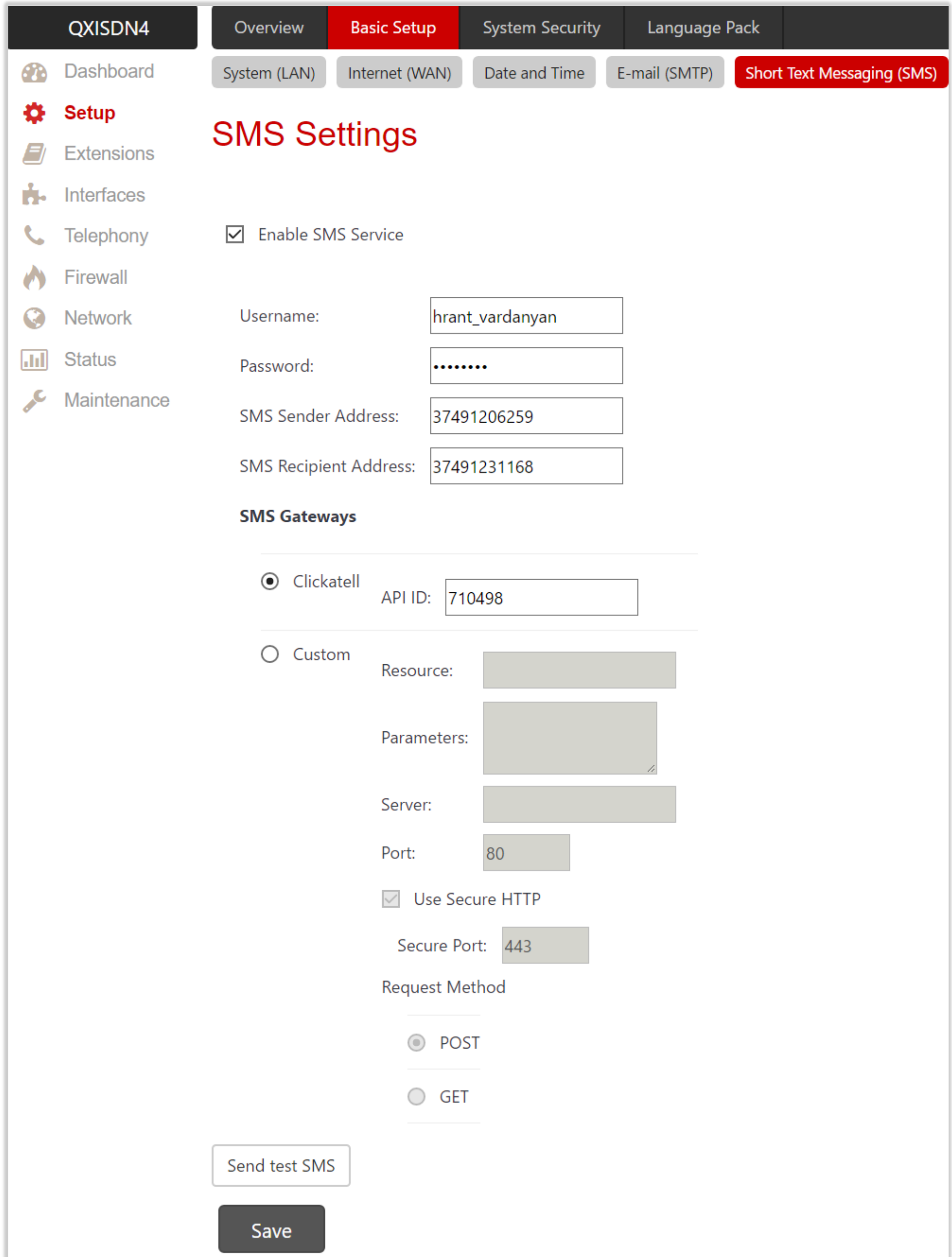


Figure 11: SMS Settings page

You may either use predefined SMS gateway (Clickatell) or define a custom service.

- **Clickatell** – select to use the predefined SMS gateway. Then enter the Clickatell specific parameter provided by the server in the activated **API ID** field. This parameter must be identical on both sides.
  - **Custom** – select to define a custom gateway as follows:
  - **Resource** – enter the HTTP resource name on the SMS gateway.
  - **Parameters** – enter 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 defined in the field Username.
    - **%password%** – indicates the password defined in the field Password.
    - **%to%** – indicates the password defined in the field SMS Recipient Address.
    - **%from%** – indicates the password defined in the field SMS Sender Address.
    - **%text%** – indicates the SMS text generated by QX (voice mail notification, event notification, etc.).

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

- Server – IP address or hostname of the SMS gateway.
- Port – port number of the SMS gateway.
- Use Secure HTTP to access the SMS server via HTTPS. Then define the port number for HTTPS traffic in the activated Secure Port field.

- Select one of the HTTP request's methods (POST or GET) through the Request Method buttons. The QX uses one of methods to access to the SMS gateway.

Once the configuration is finished, click "Send test SMS" to send a test sms to the defined mobile number to verify the settings.

5.2 System Security

The System Security Management is used to manage the QX's global security.

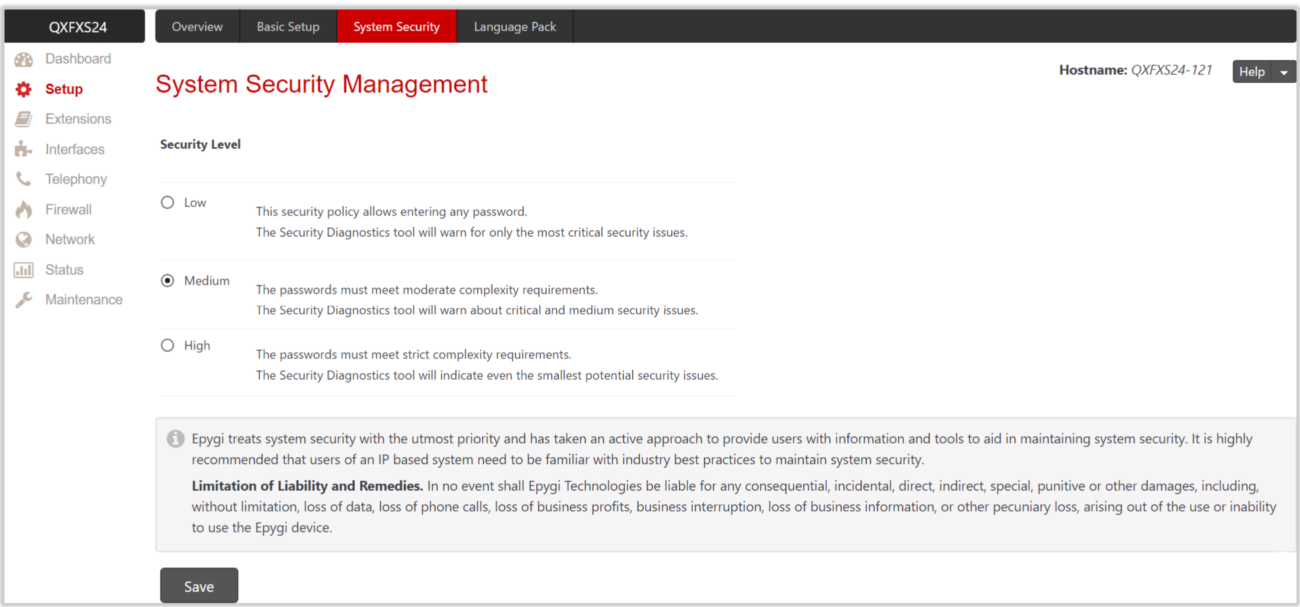


Figure 12: System Security Management page

QX treats the selected security level when checking the passwords strength and when running the security audit to get security reports. The security levels are the following:

- Low – there are no specific restrictions on the strength of the saved password. Only the critical warnings on the Call Routing Rules to PSTN and IP-PSTN, disabled Firewall and IDS will be generated in Security Report.
- Medium – the minimum strength of the passwords must be "moderate". The Security Report will generate warnings on all unsecured Call 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 the passwords must be "strong". The Security Report will generate warnings on the IP Line and extension passwords, disabled IDS, all unsecured Call Routing rules, Firewall level (if it is set below "High"), default administrator passwords etc.

5.3 Licensed Features

5.3.1 Feature Keys

Two types of licensable feature keys are available on the QX:

- Permanent keys – activate licensable features on QX permanently, without time limitation.
- Time limited keys – activate or extend the operation for already activated licensable features temporarily, for the specified period. The feature will be no longer functional after the period expiration date.

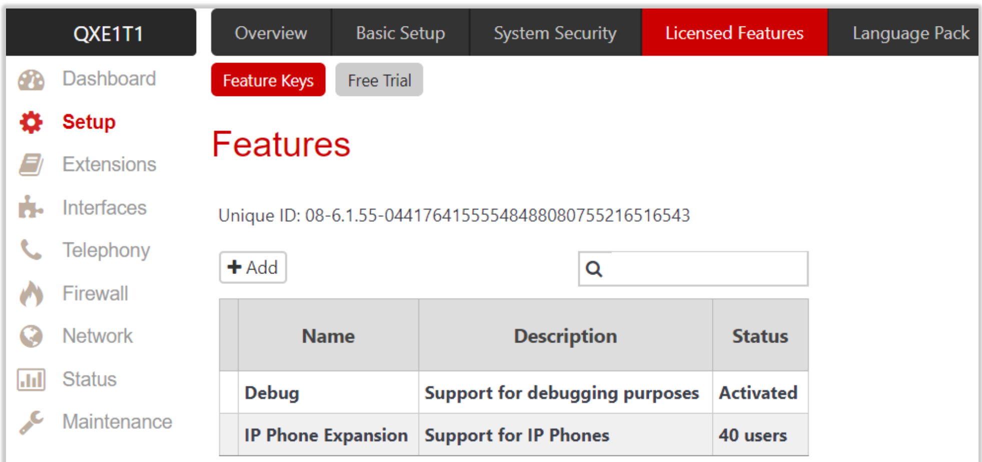


Figure 13: Features page

- Debug – enable SSH connection towards the QX for debugging purposes.
- IP Phone Expansion – enables IP phones support on the QXE1T1/QXFXO4.

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 the feature will turn to "Activated".

Note: Please make sure to have correct Date/Time on the device before adding the license key, otherwise you may have issues with the applied key.

5.3.2 Free Trial

This page lists all QX features that may be activated for a trial period.

Expiration Date/Time – is used to specify the trial period. Upon expiring the specified period, the QX will reboot and trial feature(s) will disable. TIP: The trial option can be activated on the 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. Select the 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 Language Pack

All Epygi supported LPs will change the system voice messages to the custom language, some of LPs will change the device GUI interface as well. For more information on Language Packs, please 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 file for the language pack.
2. Click Save to start uploading the language pack. Clicking Save will stop some vital processes on the QX, therefore it is required to manually reboot the device even if you have cancelled the LP update procedure on the following steps.
3. Click Yes to proceed the upload. The 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 the GUI session from the GUI 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 of the System Configuration Wizard to change the system voice messages.

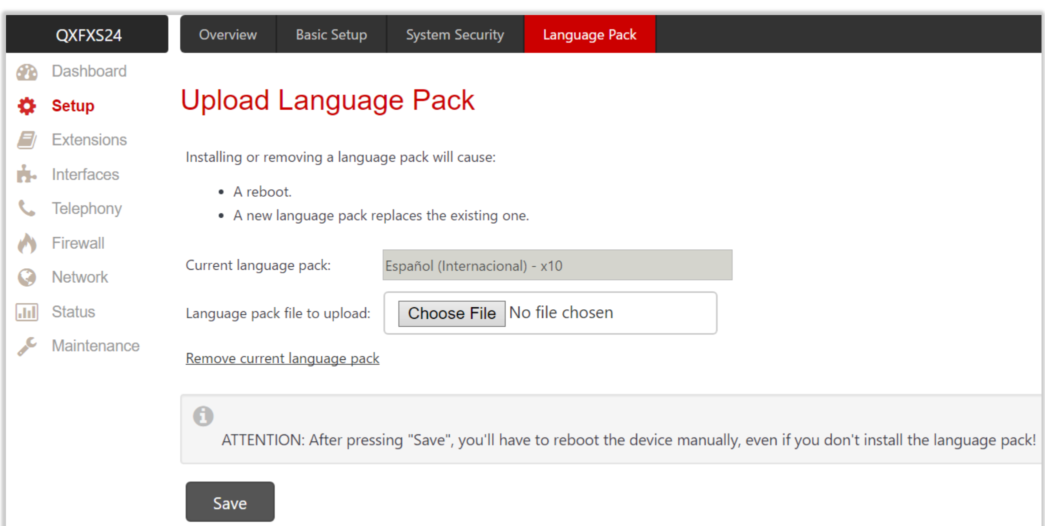


Figure 14: Language Pack page

Remove current language pack – is used to remove the uploaded LP. This link appears only if there is an uploaded LP. Note: Only one custom Language Pack can be uploaded at a time. Thus, the new LP will remove the existing one and reboot the QX.

6 Extensions Menu

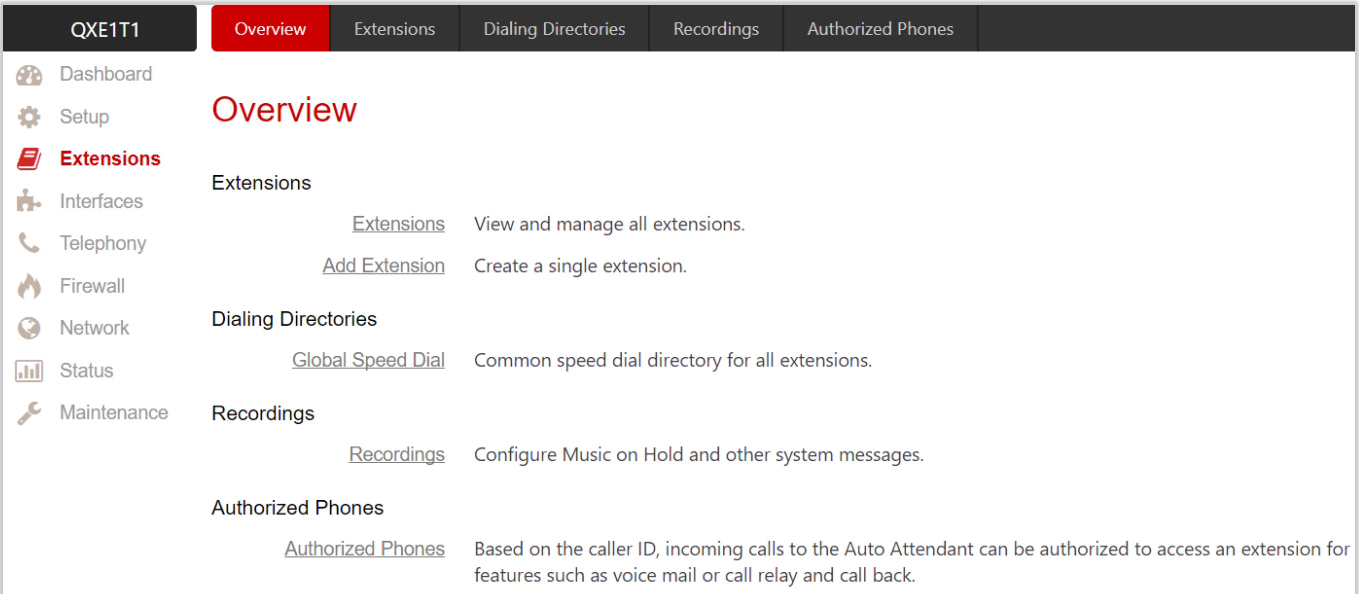


Figure 15: Extensions Menu overview

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.

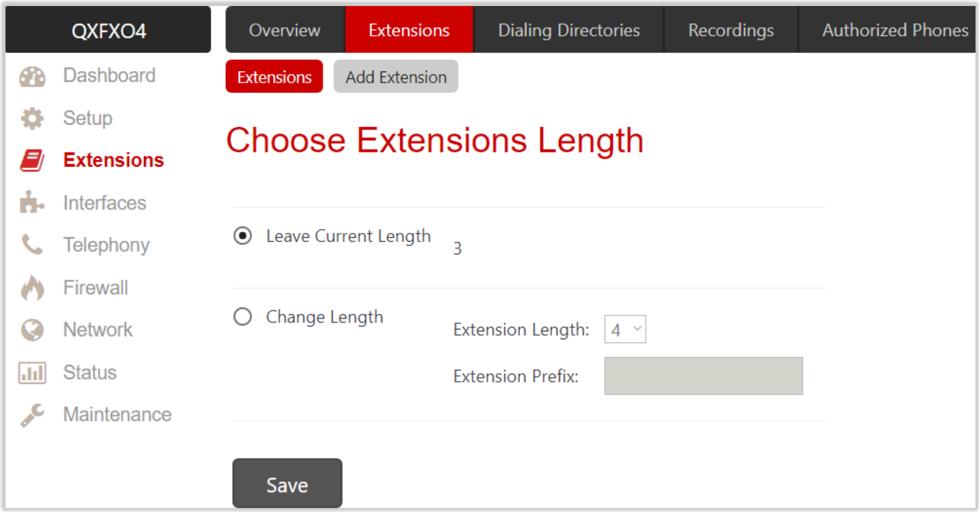


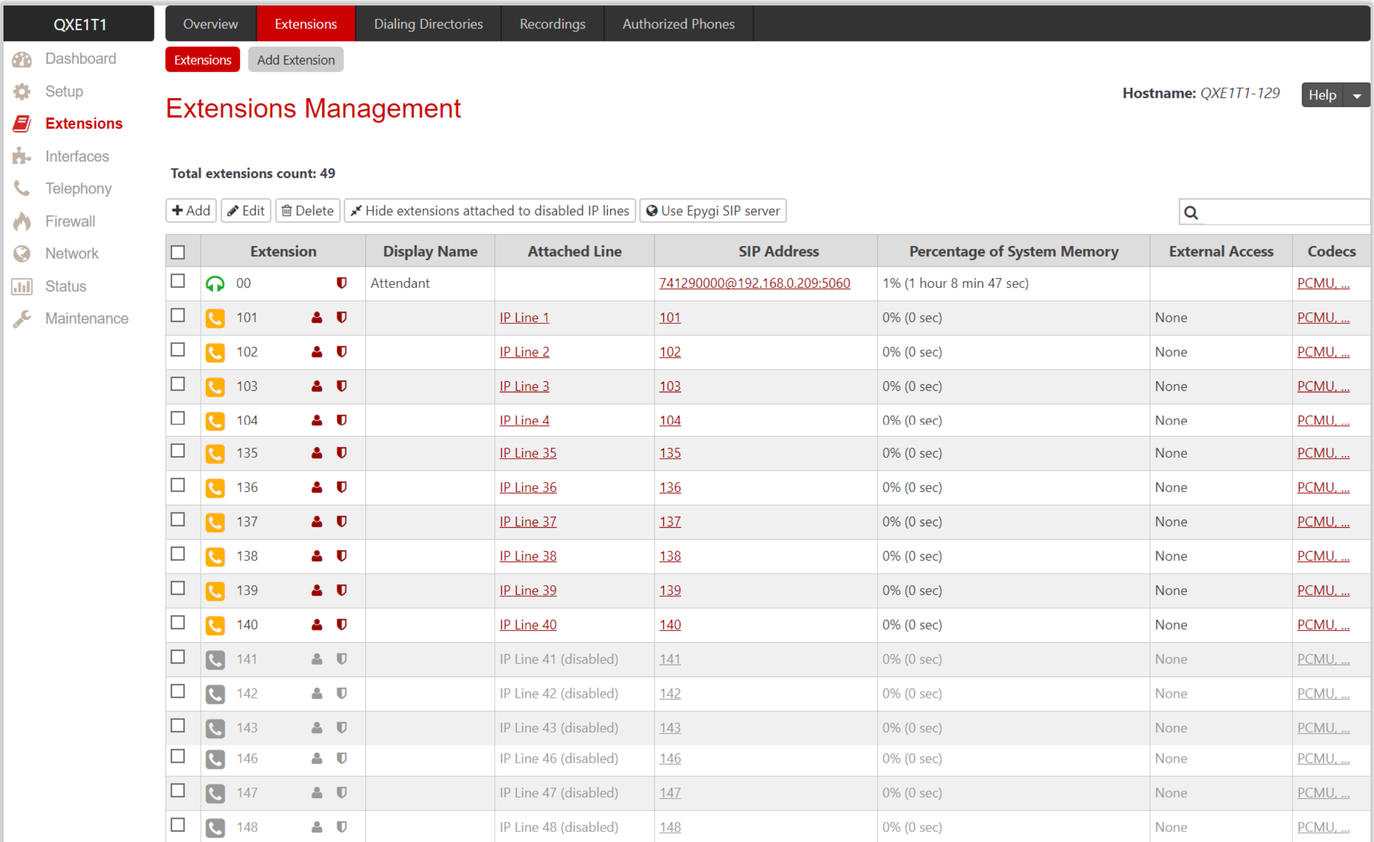
Figure 16: Choose Extensions Length page

The following options are available:

- Leave Current Length – keep the current length of QX extensions unchanged. By default, the extension's length is 3 on the QXFXO4, QXE1T1 and is 2 on QXISDN4 and QXFXS24. In front of this selection, the actual configured length of extensions is displayed.
- Change Length – change the length of extensions as follows:
  - Extension Length – select the length of extensions. It will be applied for all existing extensions on the QX. The length of the extension can be 2, 3, 4.
  - Extension Prefix – define the prefix the existing extensions as well as the newly created extensions should start with. The prefix cannot start with the digits 0 or 9.

Attention:

- By saving the settings on the Choose Extensions Length page, all existing extensions will lose the custom voice messages. The device will be rebooted. The Choose Extensions Length page will not appear again unless the default configuration settings will not be restored on the QX.
- QXFXS24 and QXISDN4 is limited to 200, QXFXO4 and QXE1T1 to 400 extensions in total.



Extension	Display Name	Attached Line	SIP Address	Percentage of System Memory	External Access	Codecs
00	Attendant		741290000@192.168.0.209:5060	1% (1 hour 8 min 47 sec)		PCMU, ...
101		IP Line 1	101	0% (0 sec)	None	PCMU, ...
102		IP Line 2	102	0% (0 sec)	None	PCMU, ...
103		IP Line 3	103	0% (0 sec)	None	PCMU, ...
104		IP Line 4	104	0% (0 sec)	None	PCMU, ...
135		IP Line 35	135	0% (0 sec)	None	PCMU, ...
136		IP Line 36	136	0% (0 sec)	None	PCMU, ...
137		IP Line 37	137	0% (0 sec)	None	PCMU, ...
138		IP Line 38	138	0% (0 sec)	None	PCMU, ...
139		IP Line 39	139	0% (0 sec)	None	PCMU, ...
140		IP Line 40	140	0% (0 sec)	None	PCMU, ...
141		IP Line 41 (disabled)	141	0% (0 sec)	None	PCMU, ...
142		IP Line 42 (disabled)	142	0% (0 sec)	None	PCMU, ...
143		IP Line 43 (disabled)	143	0% (0 sec)	None	PCMU, ...
146		IP Line 46 (disabled)	146	0% (0 sec)	None	PCMU, ...
147		IP Line 47 (disabled)	147	0% (0 sec)	None	PCMU, ...
148		IP Line 48 (disabled)	148	0% (0 sec)	None	PCMU, ...

Figure 17: Extensions Management page

The Extensions Management table consists of the following components:

- Extension – lists the numbers for extensions on the QX. These numbers are used for calling the extensions internally.
- Display Name – is an optional name given to extension mainly to identify the extension's owner at the called side.
- Attached Line – indicates the IP line (FXS for QXFXS24) a corresponding extension is attached to.
  TIP: None is displayed when no FXS or IP line is attached to the extension.
- SIP Address – displays the full SIP address of extension, (i.e., username@sipserver:port) when the Registration on SIP Server is enabled. If registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- Percentage of System Memory – indicates the memory size assigned to extension in percentage regarding the total system memory. The actual available duration for the extension's voice mails, uploaded/recorded greetings and blocking messages is also displayed here.
- External Access – indicates whether the GUI Login or Call Relay options are enabled on the extension.
- Codecs – list the short information about extension specific voice Codecs. Extension codec's can be accessed and modified by clicking on the link of the corresponding extension's Codecs. The link leads to the Extension Codecs page.

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: **Attendant** and **User Extension**.
2. Click **Save** to add the new extension to the **Extension Management** table.

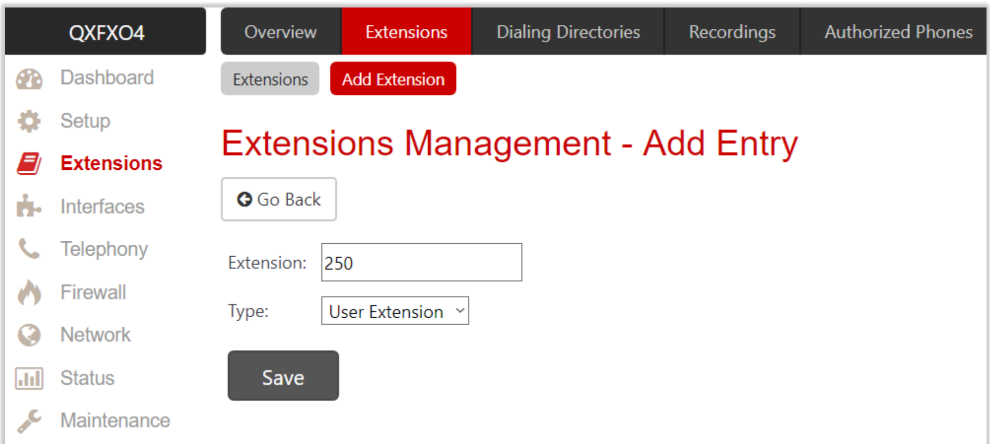


Figure 18: Extensions Management – Add Entry page

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

- **Active extensions** are those that are attached to a line, can place and receive calls and use available telephony services.
- **Inactive extensions** are those that are not attached to the line. They can use some available telephony services, but cannot place and receive calls.

Note:

- Adjust the routing rules for calling extensions with custom length manually since the call routing rule(s) for calling PBX extensions will not be adjusted automatically.
- A maximum extension length is **20** digits.
- Auto Attendant extension type is **NOT** available on QXFXS24.

6.1.3 Edit Extension

The Edit leads to the Extensions Management – Edit Entry page to editing an extension(s). When editing multiple extensions, fields that cannot be edited for multiple records have Multiple values in the Edit Entry page. When editing user and attendant extensions together, the Edit Entry page displays only common fields. Additionally, "Select to modify fields" checkbox to submit changes of the corresponding settings (options), otherwise the changes won't be applied.

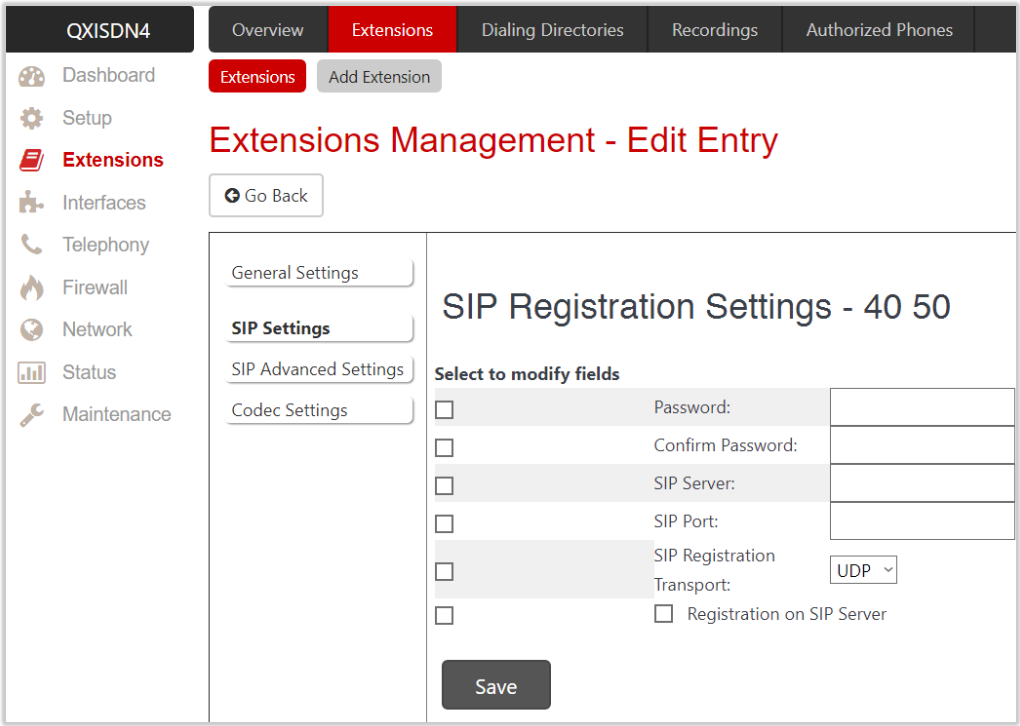


Figure 19: Extensions Management – Edit Entry page for multiple edit operation

6.1.4 User Extension

The following sections are available for configuration:

- General Settings
- SIP Settings
- SIP Advanced Settings

General Settings

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

- Display Name – is the caller ID that will be displayed on the callee's phone.
- Password – assign a password to the extension. TIP: This password will be used for GUI login and Call Relay.
- Attached Line (N/A for QXISDN4) – list all free lines the 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 (herein VE). VEs can't place/receive calls, but allowed to use a limited number of QX telephony services, such as the call forwarding service or the 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.

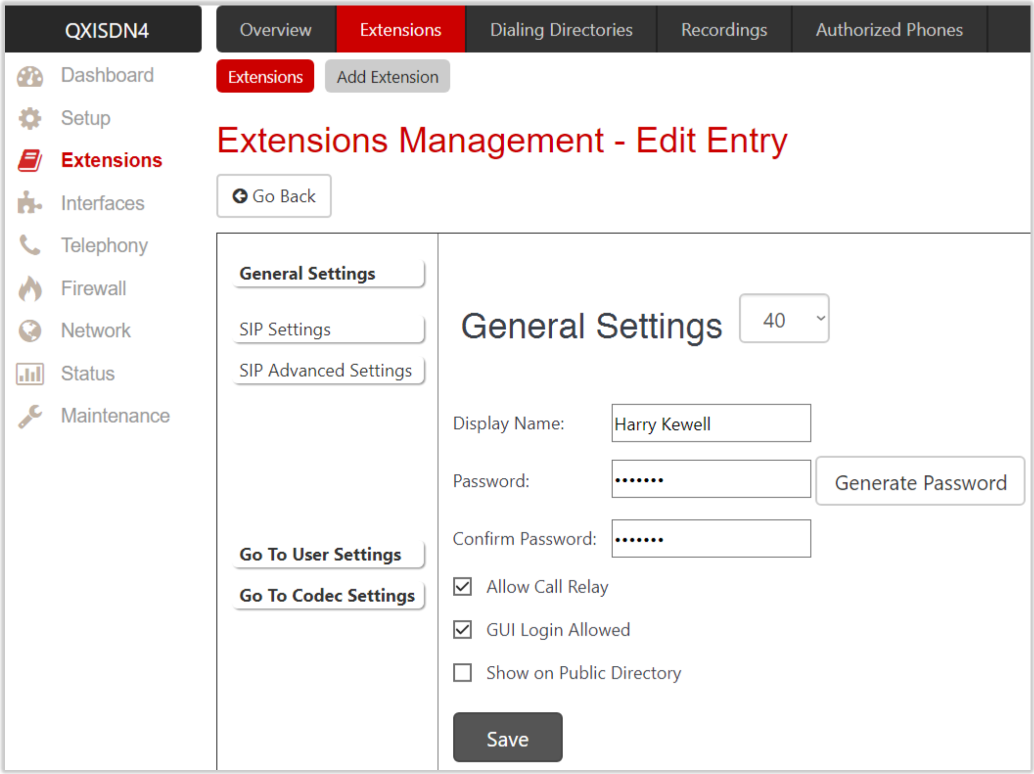


Figure 20: User Extension – General Settings section

- Allow Call Relay (N/A for QXFXS24) – enable the extension to be used to access the Call Relay service in the QX Auto Attendant. It is recommended to define a proper and non-empty password when enabling this service in order to protect it from an unauthorized access.
- GUI Login Allowed (N/A for QXFXS24) – enable GUI access (by extension name and password) for the current extension.
- Show on Public Directory (N/A for QXFXS24) – if selected, allows to display the extension (Display Name, number) on the General Information page.

SIP Settings

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

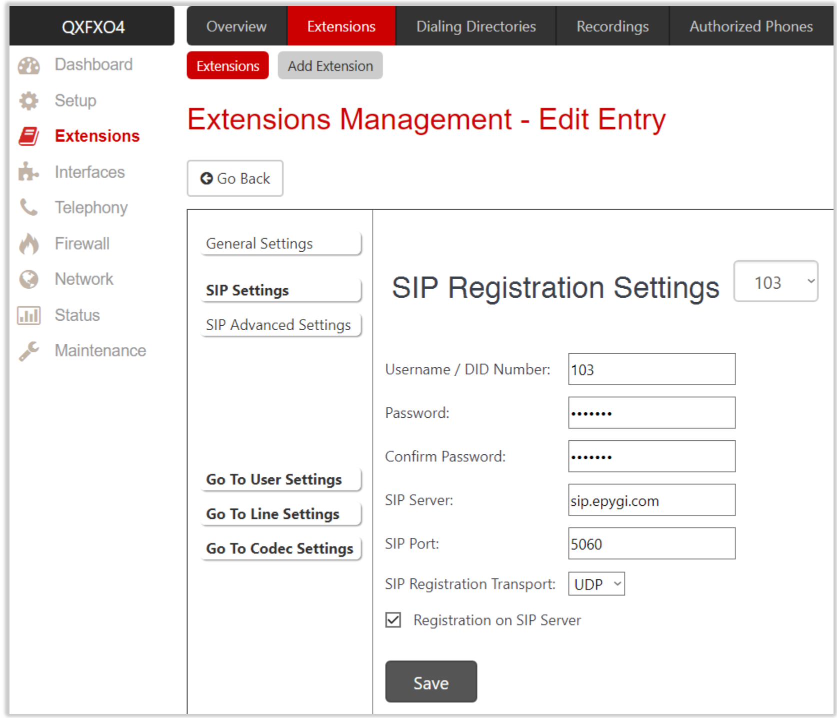


Figure 21: SIP Settings section

- Username / DID Number – is the registration username or the DID number on the external server. TIP: A 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, such as 192.168.0.26 or a host name, such as sip.epygi.com. TIP: A 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.
- Registration on SIP Server – is used to register the current extension on the SIP server.

How it works: Upon receiving a SIP Invite message from an external server, the 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 an external SIP server, then only enter the DID number in the Username/DID Number field and keep the other fields empty.

SIP Advanced Settings

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

- Authentication User Name – enter an identification parameter. It should be provided by the SIP service provider and can be requested for some SIP servers only. For others, the field should be left empty.
- Send Keep-alive Messages to Proxy – enable the SIP registration server accessibility to the verification mechanism.
- Timeout – define 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 – 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 checkbox must be enabled if the remote party does not recognize hold requests initiated from the QX.

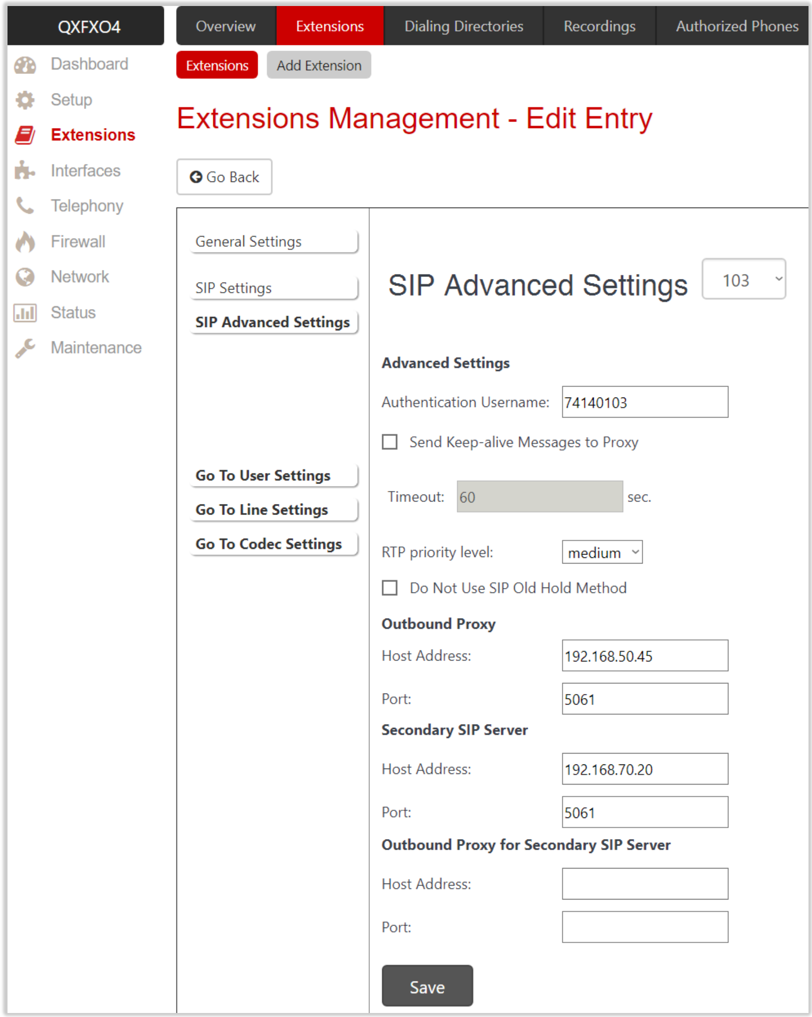


Figure 22: SIP Advanced Settings section

- 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 restrictions of NAT. 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 – act as an alternative SIP registration server when the primary SIP Registration Server becomes inaccessible. If the connection with the primary SIP server fails, the 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 – specify 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 the SIP server providers and are used by QX to reach the selected SIP servers.

6.1.5 Auto Attendant Extension

The Auto Attendant is an IVR system (N/A for QXFXS24) that replaces a receptionist and allows to distribute calls to the QX's extensions or services through prerecorded audio prompts. Remote access to the QX's attendant is possible through IP/PSTN/IP-PSTN calls, by dialing Attendant's SIP or PSTN number.

Note: The SIP Settings, SIP Advanced Settings and Go To Codec Settings sections are the same as for user extensions.

General Settings

This section describes how to configure general settings of the Attendant:

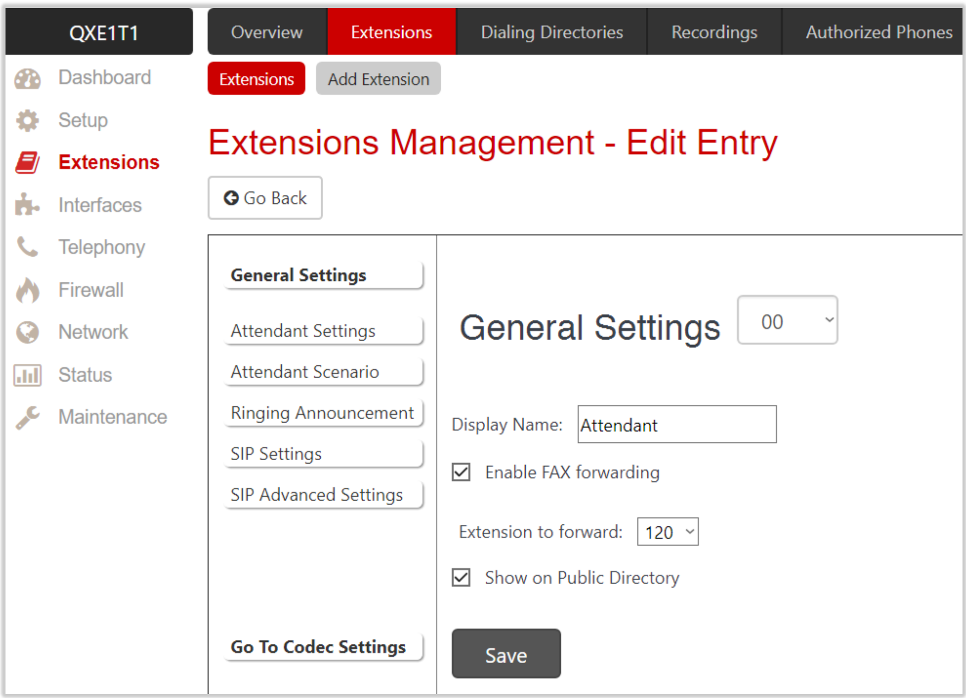


Figure 23: Attendant – General Settings section

- Display Name – is the caller ID that will be displayed on the phone when making call to attendant or from attendant (e.g. when using callback service).
- Enable FAX forwarding – if selected, the system forwards the FAX messages to the selected extension if incoming calls are routed to the Attendant and FAX tone is detected on the Attendant.
- Extension to forward – select the extension where the incoming FAX addressed to the Attendant will be forwarded. The list contains only those extensions that have FAX support enabled. FAX support can be enabled from the Extension Codecs page. TIP: FAX forwarding is applicable only for incoming calls from PSTN and SIP.
- Show on Public Directory – if selected, allows to display the extension (Display Name, number) on the General Information page.

Attendant Settings

This section describes how to manage the attendant scenario (Figure 25). The following settings and options are available:

- Attendant Scenario – select between the auto attendant scenarios. The following scenarios are available:
  - Standard scenario – available and active on the 00 attendant and newly created attendant extensions by default.
  - VXML scenario – allows to upload custom scenario file in VXML format.
- Authorized Phones – leads to the Authorized Phones page. If the external SIP or PSTN caller added to the Authorized Phones, he/she allowed to access the attendant services bypassing the authorization procedure and use the Callback service as well.

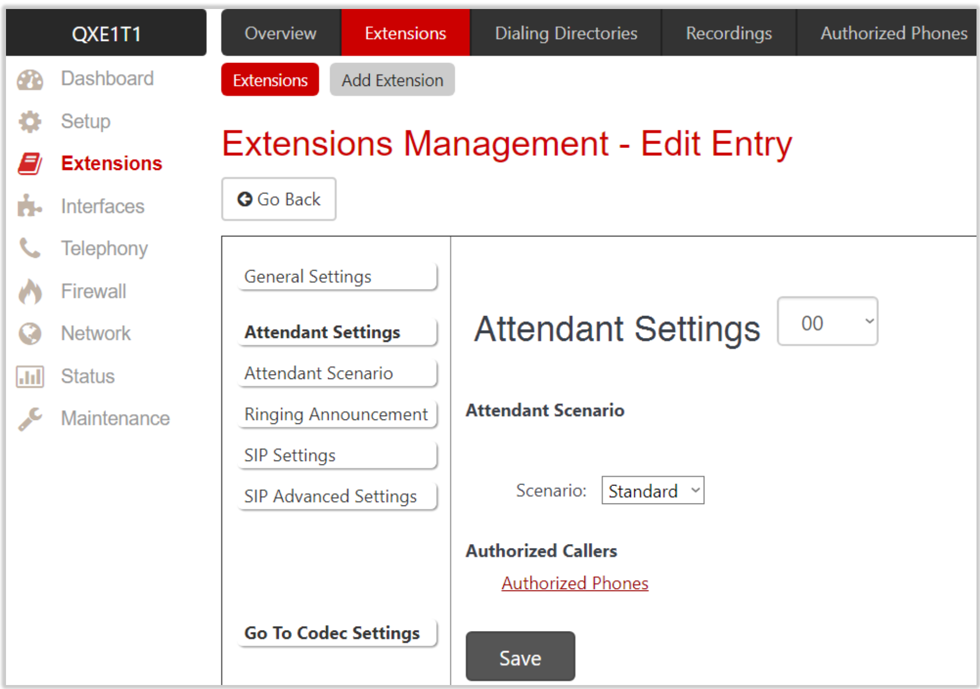


Figure 24: Attendant Settings section

Attendant Scenario

This section is used to configure the selected scenario.

Standard scenario

The following options are available for 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 Attendant Prompt(s). Prompt Repetition is used to define 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.
  - Call Type, Calling Address – (identical for both Call Redirection and ZeroOut Redirection) – allow to redirect the call to the specified destination.

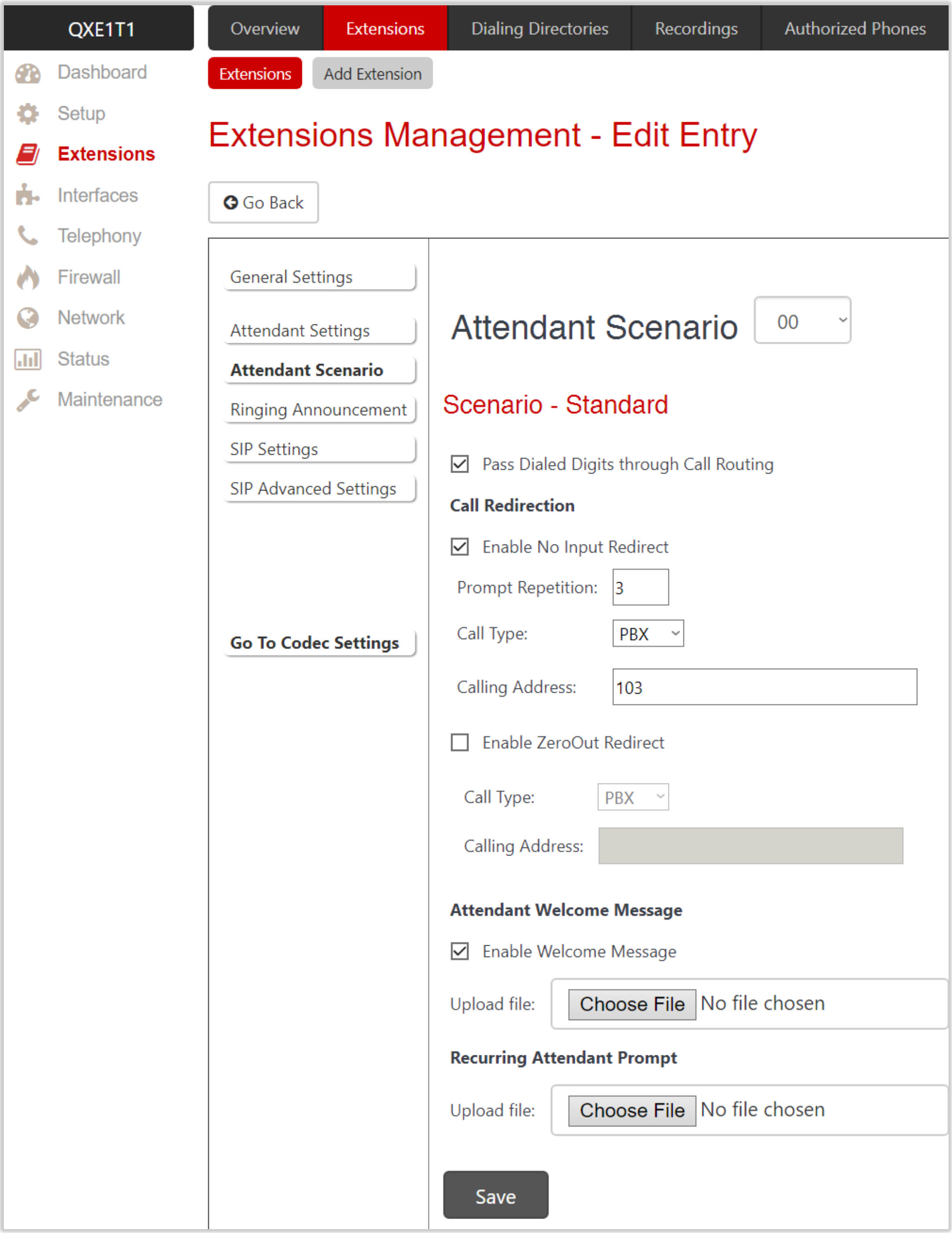


Figure 25: Attendant Scenario section

Note: The routing patterns in the Call Routing Table starting with digit **0** will not work for incoming calls to attendant if both the ZeroOut and Pass Dialed Digits through Call Routing options are enabled. The ZeroOut feature 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.

- Attendant Welcome Message – allows to enable/disable and customize the Attendant welcome message.
- Recurring Attendant Prompt – allows to customize the Attendant active recurring prompt (played after the Welcome Message and then periodically repeated while being in the Attendant).

VXML scenario

The VXML scenario allows to upload custom scenario file and voice messages. Following options are available:

- Upload VXML scenario file – is used to upload a new scenario file. TIP: The uploaded file needs to be in EpygiXML format and is restricted to 20 KB file size.

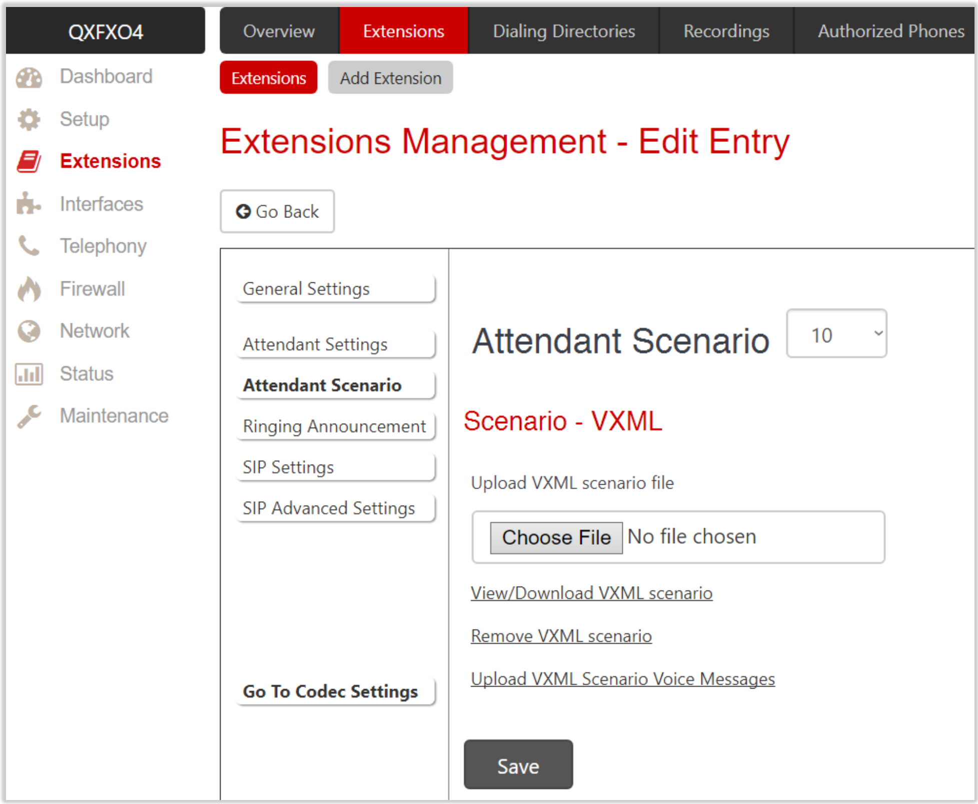


Figure 26: Auto Attendant – VXML scenario

- Upload VXML Scenario Voice Messages – leads to the Upload Custom Scenario Voice Messages page to manage voice messages used in scenario. TIP: It is allowed to upload all voice messages at once. To do this, create an archive file of the (*.tar.gz) type containing all the necessary files and upload it from the Upload VXML Scenario Voice Messages page.
- View/Download VXML scenario – view or download the scenario file.
- Remove VXML scenario – remove the custom scenario file.

Ringing Announcement

The Ringing Announcement section is used to play an optional custom voice message to callers instead of ring-back tones when making calls through the auto attendant.

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

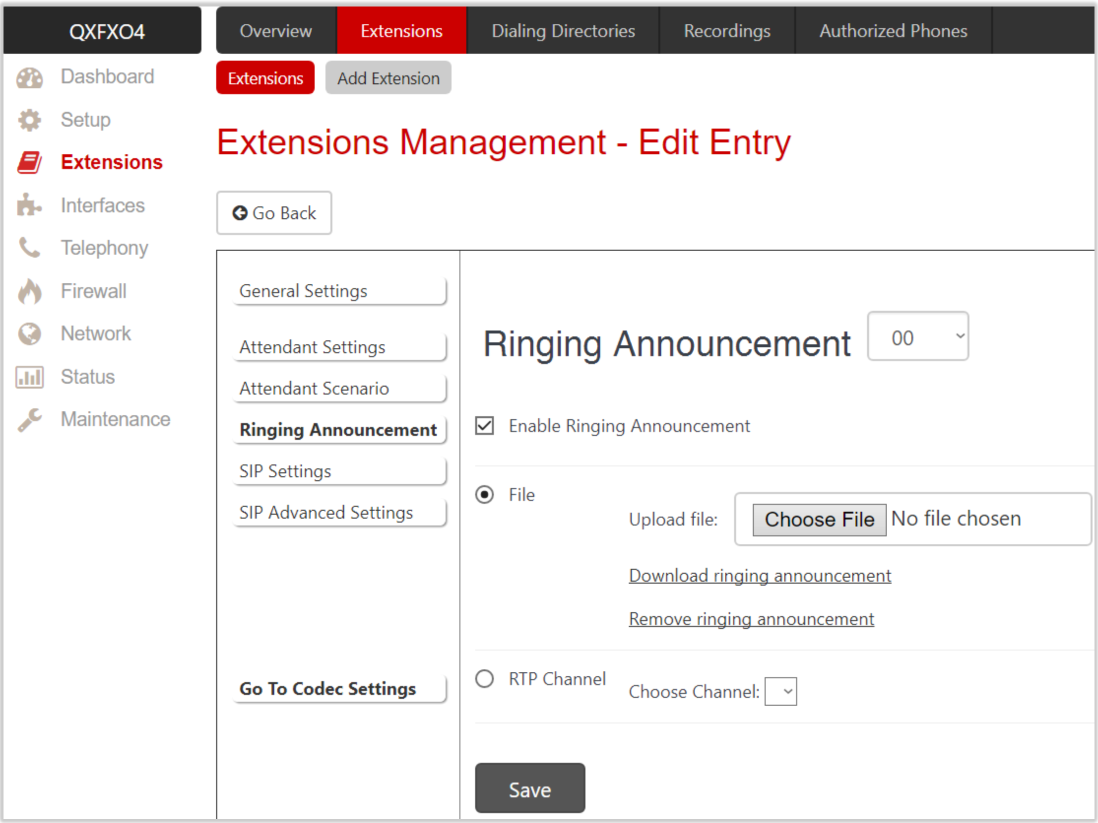


Figure 27: Auto Attendant – Ringing Announcement section

- **Enable Ringing Announcement** – enables/disables the Auto Attendant optional announcement message. If selected but no custom announcement message is uploaded, the system default message will be played to callers.

6.1.6 Bulk Import

Extension Template Management and **Bulk User Extensions Importer** tools are used to create and update multiple user type extensions on the QXFXS24.

The **Extension Template Management** tool is for configuring the common settings, such as SIP server name, SIP port, etc. for the extensions, while the Bulk User Extensions Importer tool for configuring the specific settings, such as Display Name, Extension Password, etc.

For information on how to configure and use **Bulk Import** service, please refer to the [Extensions Bulk Import on QXFXS24] guide.

6.2 Extension Codecs

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

The enabled codecs participate in codec negotiation at the call setup. The order of the enabled codecs is very important. A codec placed at the top of the table is used as the preferred codec. When establishing a call, the system will try this codec first. If the remote party does not support the preferred codec, the following codecs will be tried out strictly in the order given in the Codecs table.

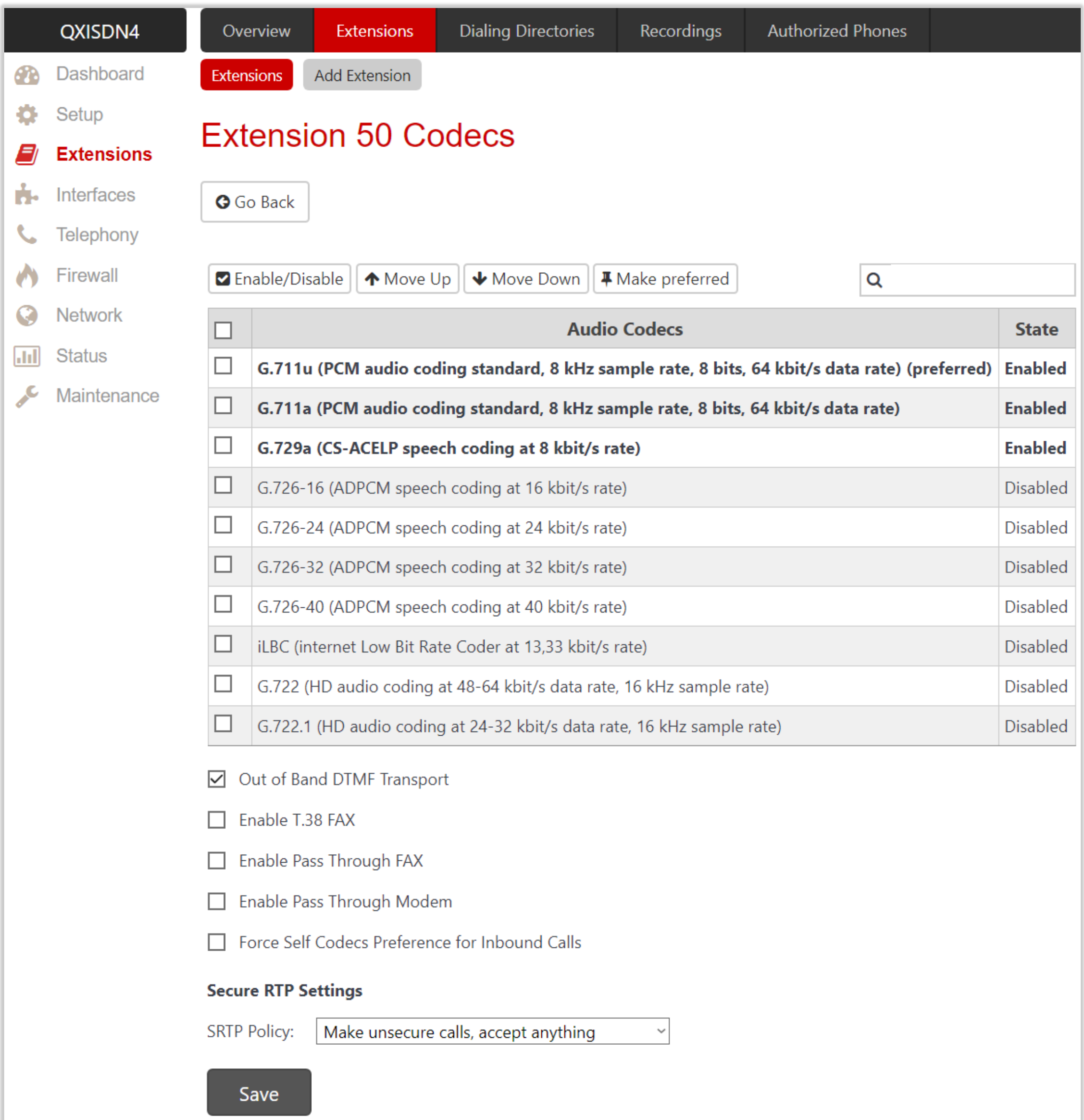


Figure 28: Extension Codecs list

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

- **Move Up/Down** – moves the selected codec one level up/down to increase/decrease the codec's priority.
- **Make preferred** – moves the selected codec to the top of the table, setting its priority to the highest. Pressing **Make preferred** for a disabled codec will first enable the codec and then move it to the top.
- **Out of Band DTMF Transport** – enables the DTMF code transmission in parallel with the voice stream. Destination received the DTMF code will play it locally if it supports the feature as well. This helps avoid DTMFs loss in case of heavy traffic. The feature is valuable for all codecs but it is especially recommended for low bit rate codecs, such as G.729, G.726/16, etc.
- **Enable T.38 FAX** – enables the T.38 codec support of FAX transmission for incoming unified FAX messages (fax to mailbox) and remote IP devices connected to the QX via routing rules that use the target extension user settings (UES).
- **Enable Pass Through FAX** – enables the G.711 codec support for incoming unified FAX messages and IP devices connected to the attached IP line. TIP: If both of the above checkboxes are enabled, the T.38 codec will be used as a preferred codec for FAX transmission. If it is not supported by the peer, the G.711 codec will be used instead.
- **Enable Pass Through Modem** – enables the modem tone detection and G.711 codec support for the data transmission from/to the modem attached to the line. During data transmission, Silence Suppression and **Echo Cancellation** are automatically disabled on the line. The checkbox is available for the Auto Attendant extensions. TIP: If the user extension or attendant is intended to accept modem connections, disable the **Enable T.38 FAX** checkbox to allow the system to identify the modem tones correctly, otherwise the modem connection may fail.
- **Force Self Codecs Preference for Inbound Calls** – allows to use your own preferred codecs (if available on both peers).
- **Secure RTP Settings** – are used to configure secure voice over IP communication on the QX.
- **SRTP Policy** – is used to select the secure IP connection policy.
  - **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** – system will try first to establish secure call, but will fall back to unsecure call if party doesn't accept secure calls. Both secure and unsecure incoming calls will be accepted, as requested by remote party, with the preference given to establishing secure call.
  - **Make unsecure calls, accept anything** – system will establish unsecure outgoing calls, but both secure and unsecure incoming calls will be accepted as requested by remote party.

Note:

- Pay attention when configuring **Auto Attendant** codecs as they are used by virtual extensions for redirecting the incoming calls.
- For bandwidth used by secure calls, see Needed Bandwidth for IP Calls.

6.3 Dialing Directories

The Global Speed Dial service allows multiple speed dial rules assigned to specific destinations to be composed in a file and imported to the QX. To use these codes, the QX extension should simply dial the code on the phone. The call will pass through the Call Routing Table.

For information on how to configure and use Global Speed Dial service, please refer to the Dialing Directories on QX IP PBXs guide.

6.4 Recordings

The Universal Extension Recordings (N/A for QXFXS24) is used to define the voice messages universal for all extensions on QX. The defined messages become applicable by default to all extensions on QX.

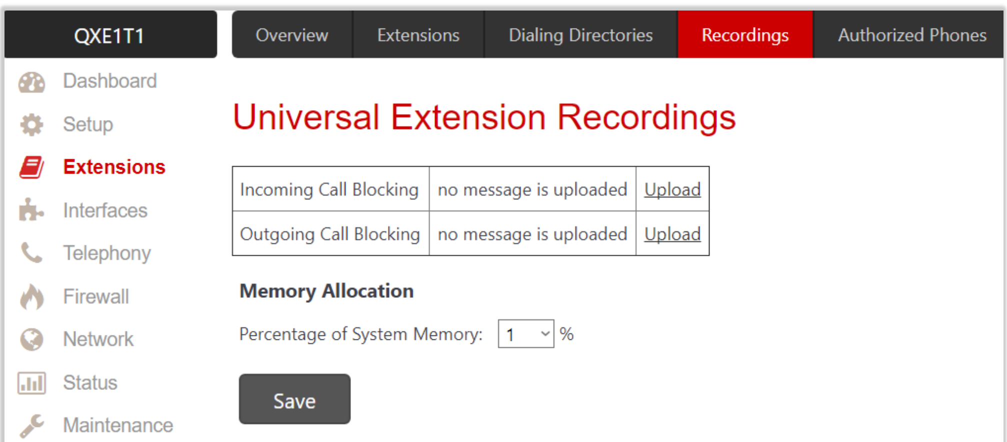


Figure 29: Universal Extension Recordings page

- Incoming Call blocking – message played when calling to the blocked extension.
- Outgoing Call blocking – message played when calling from the blocked extension.

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

- Upload – is used to upload a custom message.
- Download and Remove – are used to download and/or remove the uploaded message.
- Percentage of System Memory – defines the memory space for universal extension recordings.

6.5 Authorized Phones

The **Authorized Phones** (N/A for QXFXS24) is used to create the list of trusted external users allowed to access the QX Auto Attendant services without authentication.

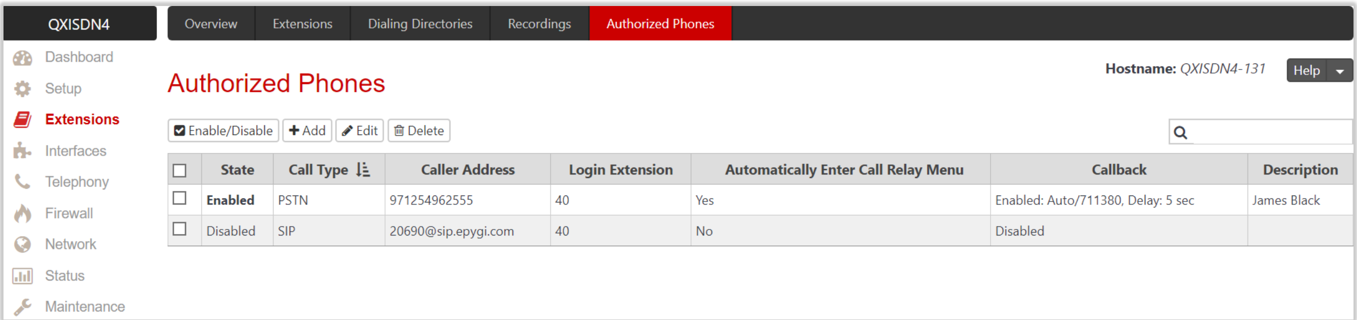


Figure 30: Authorized Phones

To add a new entry:

1. Click **Add**. The **Authorized Phones – Add Entry** page will be opened.
2. Select "**Enable**" checkbox to activate service for the created entry.
3. Enter the caller's SIP address or PSTN number.
4. Select the **Login Extension**. When calling the QX's Auto Attendant, a trusted user will automatically be logged in as the selected extension, i.e., the extension number and password will be automatically submitted by the system and the trusted user will directly access to the Auto Attendant services. The SIP settings of the logged in extension will be used for making IP calls.
5. Select the **Automatically Enter Call Relay Menu** checkbox. If selected allows direct access for the trusted user to Auto Attendant Call Relay menu. If not selected, a trusted caller will be directed to the Auto Attendant's main menu, but still will be able to reach **Call Relay** services without authentication.
6. Configure **Callback Settings** (optional).

- Select **Enable Callback** checkbox to allow the specified caller to use the **Callback** service.
- Specify the Call Back Destination. TIP: If the **Callback Destination** is left empty, the trusted caller address will be implied as a **Callback** destination.
- Define **Callback Response Delay** before the **Callback** will be started.

How it works: When the trusted user calls the Auto Attendant, he/she will be able to use QX services as if a PBX extension. If the **CallBack** service is activated the trusted user will get a call back from Auto Attendant.

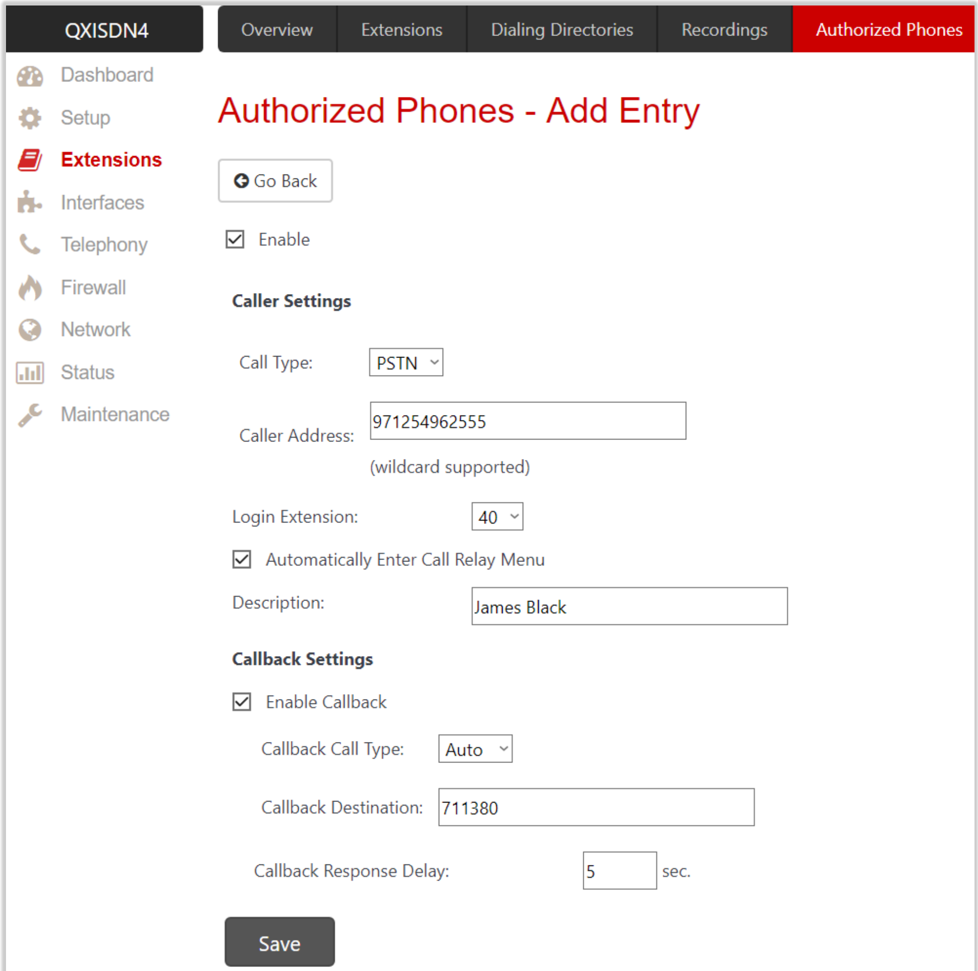


Figure 31: Authorized Phones – Add Entry page

Note:

- Authorized Phones will only work when the trusted caller connects to the Auto Attendant running the Standard scenario configured.
- For more information how to configure and use Callback service, please refer to the Callback Service on QX IP PBXs guide.

7 Interfaces Menu

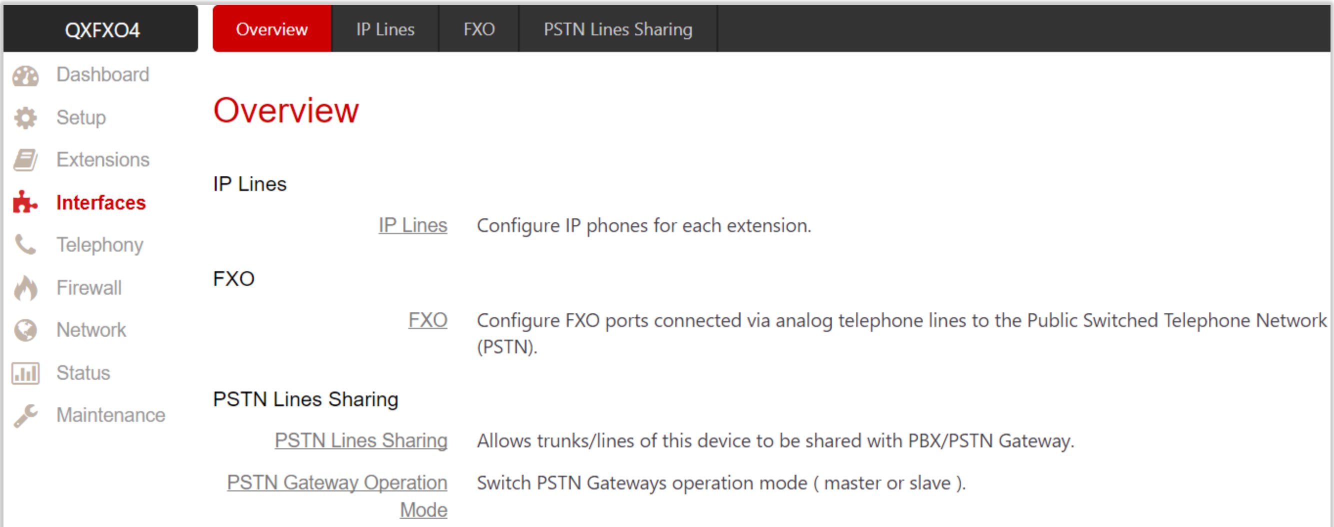


Figure 32: Interfaces Menu overview

7.1 FXS

7.1.1 FXS Lines

The **FXS (On-board) Line Settings** are used to configure on-board FXS lines, define the caller ID detection type, configure remote party disconnect indication and select the ringer type on each of them.

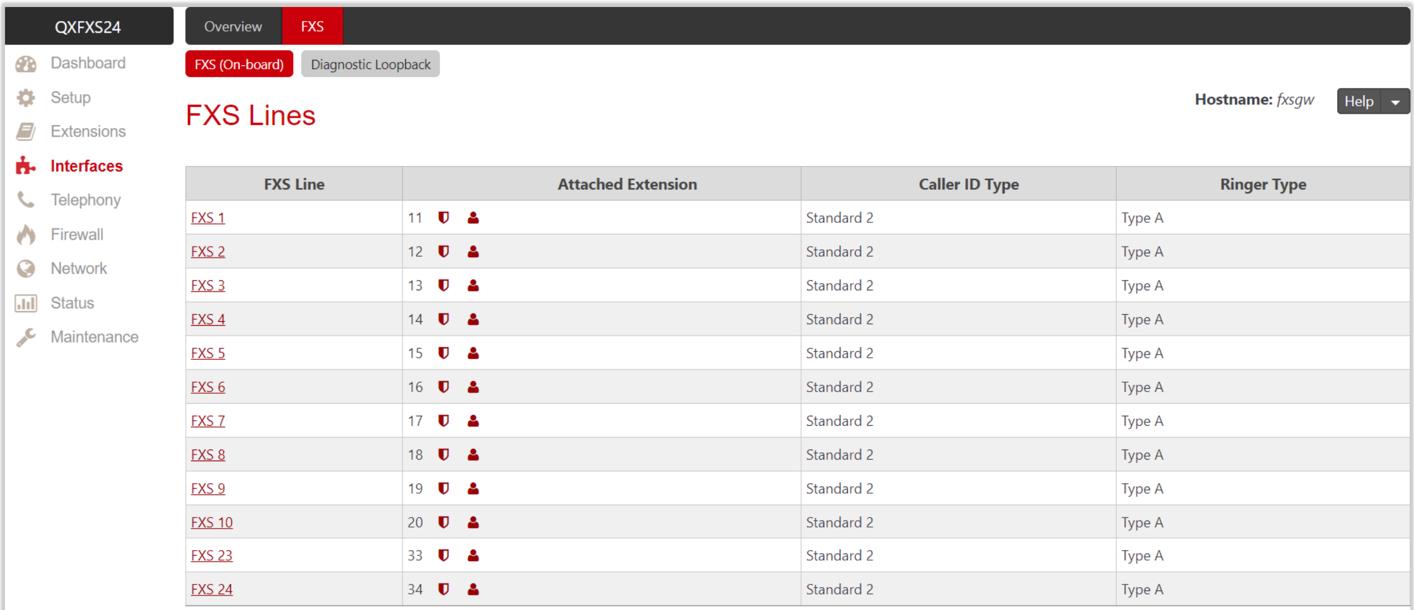


Figure 33: FXS Lines page

- **Available Lines** – displays all FXS lines available on the QXFXS24. Press a hyperlinked FXS line to go to the **Line Settings** page (Figure 34) to configure settings of the selected FXS line.
- **Attached Extension** – displays the extension attached to the corresponding FXS line. Nothing will be displayed if there is no extension attached to that line. Press the hyperlinked extension number to go to the **Extensions Management – Edit Entry** page to configure the extension's settings.

Line Settings – Line

The Line Settings – Line # page is used to configure specific settings for the selected FXS line.

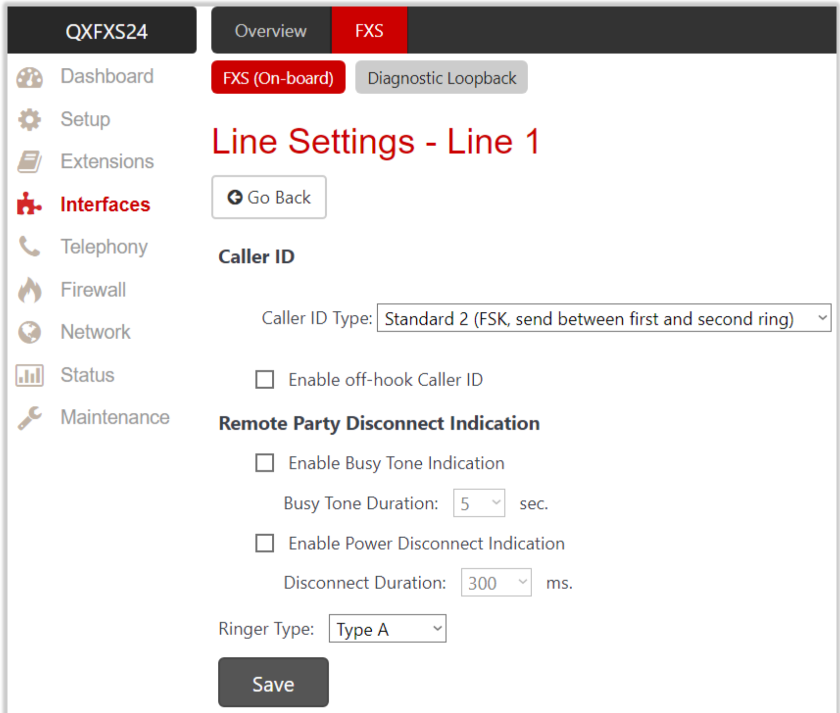


Figure 34: Line Settings – Line# page

- 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 (in seconds) when a busy tone will be 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 (in milliseconds) when the FXS line power will be down.
- Ringer Type – is used to select the frequency of the ringer supported by the phone attached to the line. Information can be found on the phone enclosure or in the phone's manual. Problems with the ringer might occur if the ringer type selected here does not correspond to the one supported by the phone.
  TIP: The supported ringer type can be found on the bottom of the phone, in the Ren:x.xN value where N is the ringer type supported by the phone. For example, if N=A, the TypeA ringer type should be selected, if N=B, the TypeB&Z ringer type should be selected.

Information on the Caller ID system

Caller ID service is used to identify the caller (when performing 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 notification are available on QX: FSK and DTMF.

<u>FSK Standard</u>

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

<u>DTMF Standard</u>

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. TIP: 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.

7.1.2 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, any incoming calls to the corresponding line will automatically pick up on the first ring and any voice towards the line will automatically be sent back to the caller (the caller will hear themselves in the handset).

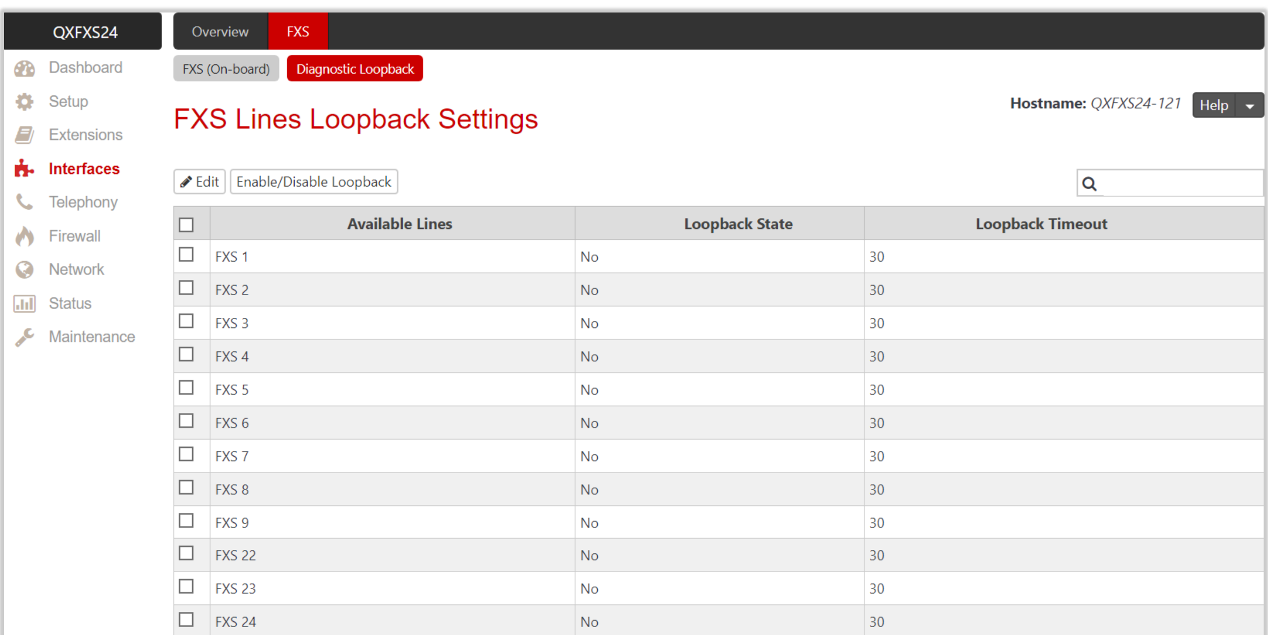


Figure 35: FXS Lines Diagnostic Loopback page

- **Edit** – leads to **FXS Lines Loopback Settings – Edit Entry** page to configure the **Loopback Timeout** (in seconds) for the selected FXS line(s).

- ➢ **Loopback Timeout** – is used to put a limit 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 loopback service on the selected FXS line(s).

7.2 IP Lines

The **IP Lines** page is available on the QXFXO4 and QXE1T1 GWs and used to configure the IP lines to connect IP phones to QX to support the Hosted PBX Survivability.

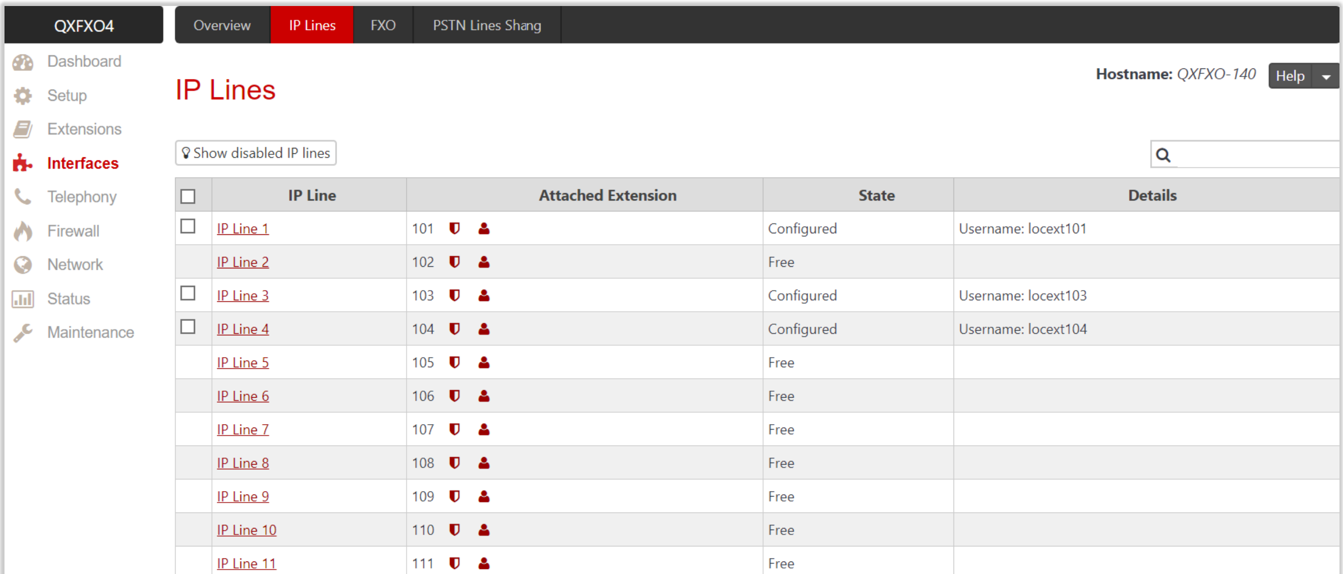


Figure 36: IP Lines page

The **IP Lines** table lists all IP lines available on QX with specific details for each:

- **Available IP Lines** – shows all IP lines available on the QX. Click an IP line to go the **IP Line Settings** page (**Error! Reference source not found.**).
- **Attached Extension** – shows the QX 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 the extension's admin settings.
  - ➢ Click the **User Settings** icon to go the extension's user settings.
- **State** – shows whether the IP line is **Disabled**, **Configured** or **Free**.
- **Details** – displays the settings for the IP phone configured on the corresponding line, such as the authorization credentials.

IP Line Settings – IP Line # page is used to configure the IP Line with a phone.

- 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:
  - Username and Password – define the authentication parameters to register the IP phone on the QX. TIP: Set the same Username and Password as SIP registrar, SIP proxy, SIP authentication values on the IP phone for successful registration.
  - Transport – 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 Session Timer – enable the SIP session timer for the corresponding 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.

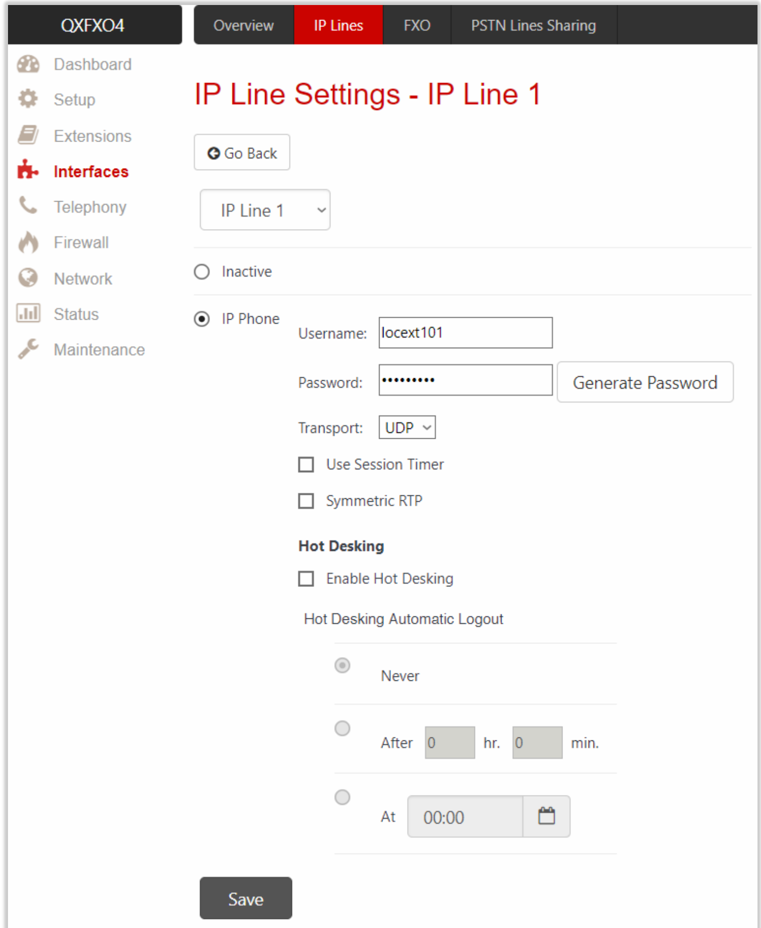


Figure 37: IP Line Settings – IP Line # page

The Hot Desking section is used to enable and configure the [Hot Desking] service on the IP Line as follows:

- Enable Hot Desking – enable the Hot Desking on the corresponding IP line.
- Hot Desking Automatic Logout – with this option enabled, QX will control the extension login timeout. Once the predefined expiration time arrives, the currently logged in extension will automatically log out and make available the public phone for other extensions. The following options are available:
  - Never – if selected, the Hot Desking will never expire for the extension.
  - After – if selected, extension will automatically log out from the public phone after the defined period.
  - At – if selected, extension will automatically log out from the public phone at the defined moment (hour and minute).

For information on how to configure and use Hot Desking service, please refer to the [Hot Desking Service on QX IP PBXs] guide.

7.2.1 Hosted PBX Survivability feature on QX

QXE1T1 and QXFXO4 gateways support the Hosted PBX Survivability (HS). This feature can be helpful in the scenario when using a Hosted PBX, but cannot make calls due to loss of the broadband connection. Using QXE1T1 and QXFXO4 gateways with HS allow IP phones to work, even when the broadband link or Hosted PBX are down. Users can also use the HS feature to provide access to remote phones in a branch office.

Generally, IP phones register on the Hosted PBX, where they make and receive calls, as a primary SIP proxy server. Additionally, IP phones register on the QX Gateway as a secondary SIP proxy server. When the broadband link or Hosted PBX fail, the QX Gateway takes control of the IP phone calls, connecting them to the PSTN. Transition from the Hosted PBX to the QX via the HS is transparent to users. This list of IP phones configured and tested to work properly with QXE1T1 and QXFXO4, supporting most of Epygi telephony features and HS, is provided in the table below.

Vendor	Model	SW/FW Version
Aastra	6757iCT(57iCT)	3.3.1.2256–SIP
Aastra	9480iCT(35iCT)	3.3.1.2256–SIP
Grandstream	GXP1100	1.0.8.6
Grandstream	GXP1105	1.0.8.6
Grandstream	GXP1160	1.0.8.6
Grandstream	GXP1165	1.0.8.6
Grandstream	GXP1400	1.0.8.6
Grandstream	GXP1405	1.0.8.6
Grandstream	GXP1450	1.0.8.6
Grandstream	GXP1610	1.0.2.27
Grandstream	GXP1620/GXP1625	1.0.2.27
Grandstream	GXP2100	1.0.8.6
Grandstream	GXP2110	1.0.8.6
Grandstream	GXP2120	1.0.8.6
Grandstream	GXP2124	1.0.8.6
Grandstream	GXP2130	1.0.7.99
Grandstream	GXP2140	1.0.7.99
Grandstream	GXP2160	1.0.7.99
Grandstream	GXP2200	1.0.3.27
Grandstream	GXV3140	1.0.7.80
Grandstream	GXV3175	1.0.3.76
Grandstream	GXV3240	1.0.3.62
Grandstream	GXV3275	1.0.3.62
Mitel (Aastra)	6730	3.3.1.4305-SIP
Mitel (Aastra)	6731	3.3.1.4305-SIP
Mitel (Aastra)	6735	3.3.1.8140-SIP
Mitel (Aastra)	6737	3.3.1.8140-SIP
Mitel (Aastra)	6739	3.3.1.4305-SIP
Mitel (Aastra)	6753	3.3.1.4305-SIP
Mitel (Aastra)	6755	3.3.1.4305-SIP
Mitel (Aastra)	6757	3.3.1.4305-SIP
Mitel (Aastra)	9143	3.3.1.4305-SIP
Mitel (Aastra)	9480	3.3.1.4305-SIP
Mitel	6863	4.2.0.2023-SIP
Mitel	6865	4.2.0.2023-SIP
Mitel	6867	4.2.0.2023-SIP
Polycom	SoundPoint IP 330SIP	3.3.5.0247
Polycom	SoundPoint IP 331SIP	3.3.5.0247
Polycom	SoundPoint IP 335SIP	3.3.5.0247

Vendor	Model	SW/FW Version
Polycom	SoundPoint IP 450SIP	3.3.5.0247
Polycom	SoundPoint IP 550SIP	3.3.5.0247
Polycom	SoundPoint IP 650SIP	3.3.5.0247
Polycom	SoundPoint IP 670SIP	3.3.5.0247
Polycom	SoundStation IP 5000	3.3.5.0247
Polycom	SoundStation IP 6000	3.3.5.0247
Polycom	VVX 1500	3.3.5.0247
Polycom	VVX 300/310	4.1.7.1210
Polycom	VVX 400/410	4.1.7.1210
Polycom	VVX 500	4.1.7.1210
Polycom	VVX 600	4.1.7.1210
Yealink	CP860	37.80.0.30
Yealink	SIP-T19P	31.72.0.1
Yealink	SIP-T19P E2	53.80.0.130
Yealink	SIP-T20P	9.72.0.1
Yealink	SIP-T21P	34.72.0.1
Yealink	SIP-T21P E2	52.81.0.25
Yealink	SIP-T22P	7.72.0.1
Yealink	SIP-T23G(P)	44.81.0.25
Yealink	SIP-T26P	6.72.0.1
Yealink	SIP-T27G	69.81.0.25
Yealink	SIP-T27P	45.81.0.25
Yealink	SIP-T28P	2.72.0.1
Yealink	SIP-T29G	46.81.0.25
Yealink	SIP-T32G	32.70.0.130
Yealink	SIP-T38G	38.70.0.125
Yealink	SIP-T40P	54.81.0.25
Yealink	SIP-T41P	36.81.0.25
Yealink	SIP-T41S	66.81.0.25
Yealink	SIP-T42G	29.81.0.25
Yealink	SIP-T42S	66.81.0.25
Yealink	SIP-T46G	28.81.0.25
Yealink	SIP-T46S	66.81.0.25
Yealink	SIP-T48G	35.81.0.25
Yealink	SIP-T48S	66.81.0.25
Yealink	SIP VP-T49G	51.80.0.100
Yealink	VP-530	23.70.0.40
Yealink	W52P	25.30.0.20

Table 1: Tested IP Phones

7.3 FXO Settings

The **FXO Settings** is used to configure the QX's on-board FXO Lines to make PSTN calls through the on-board FXO ports. FXO ports are available on QXFXO4 (4 ports).

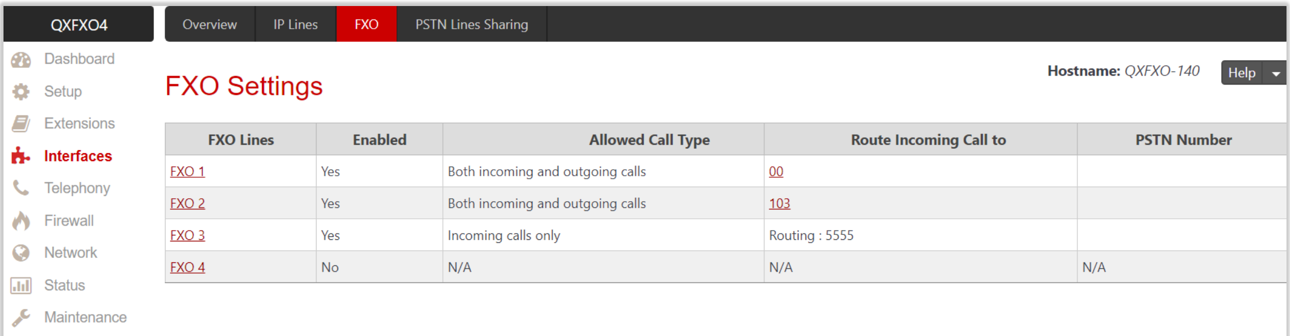


Figure 38: FXO Settings page

Click a hyperlinked FXO line to go to the **FXO Settings – FXO#** page to modify the settings of the selected line.

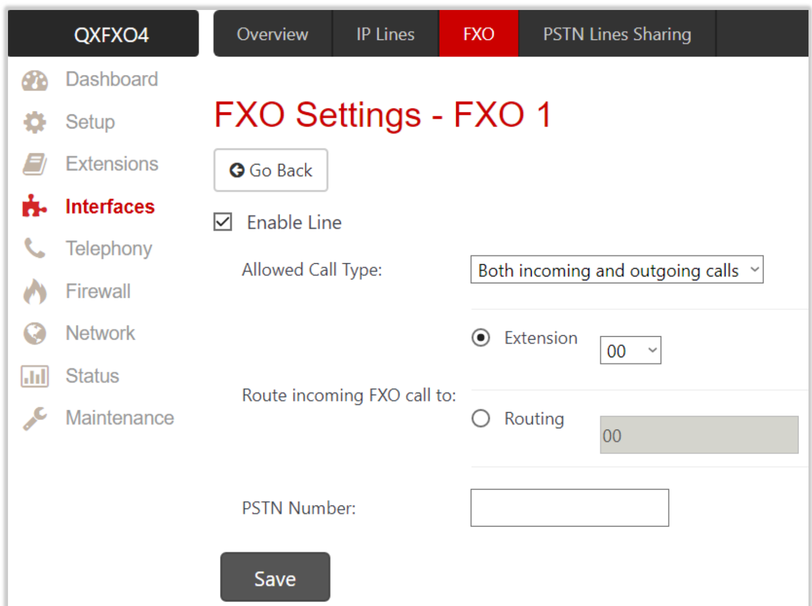


Figure 39: FXO Line Settings page

- **Enable Line** – activate the selected FXO line.
- **Allowed Call Type** – select the allowed call directions for the FXO line. The following options are available:
  - **Both incoming and outgoing calls** will be enabled for the selected FXO line.
  - **Incoming calls only** (prohibiting outgoing calls) will be enabled for the selected FXO line.
  - **Outgoing calls only** (prohibiting incoming calls) will be enabled for the selected FXO line.
- **Route incoming FXO Call to** – define the destination where the incoming calls will be forwarded to.
  - **Extension** – is used to forward the calls to either PBX user or auto attendant extension.
  - **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.
- Enter a **PSTN Number** for the current FXO line if needed for information.

7.4 E1/T1 Trunk Settings

The **E1/T1 Trunk Settings** allows QXE1T1 to be connected to the legacy PBX or to the CO (Central Office) via E1/T1 trunk, using CAS or CCS signaling. If connected to the PBX, the QX should be configured in the **Network** mode. If connected to the CO, the QX should be configured in the **User** mode. The QXE1T1 has one E1/T1 trunk available.

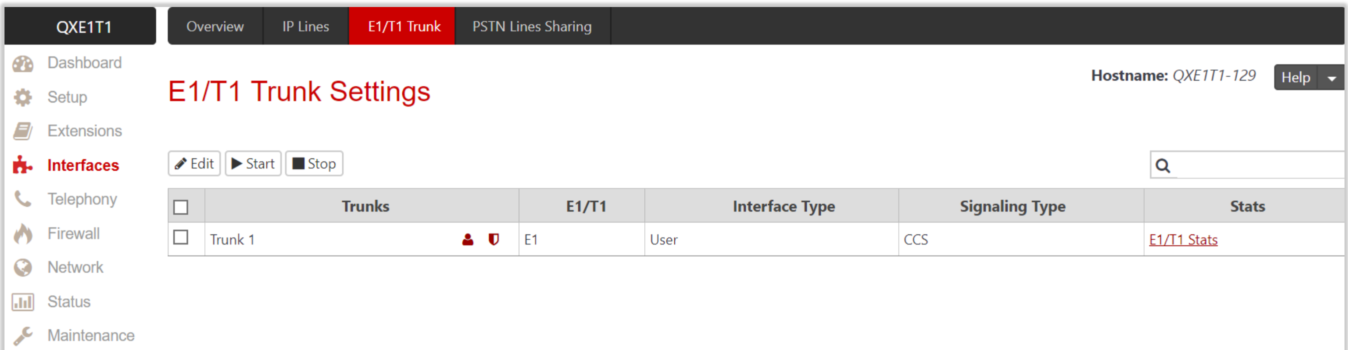


Figure 40: E1/T1 Trunk Settings page

The **E1/T1 Trunk Settings** table lists the available E1/T1 trunks on the QX and their settings (Trunk name, E1/T1 mode, interface, signaling types).

The following buttons are available:

- **Start** and **Stop** are used to start/shutdown the E1/T1 trunk. TIP: When E1/T1 trunk is in a shutdown state, no E1/T1 calls could be placed and received.
- **E1/T1 Stats** link leads to the E1T1 Status page, where E1/T1 trunk and traffic statistics can be viewed.
- Click the **Modify Trunk Settings** icon to select the trunk type (E1 or T1) and signaling (CAS or CCS) and other trunk specific settings.
- Click the **Modify Signaling Settings** icon to configure the signaling settings. TIP: Depending on the selected signaling type, you will be forwarded either to the Trunk CAS Signaling Settings or Trunk CCS Signaling Settings pages respectively.

Trunk - 1 - Edit Entry page

The **Trunk – 1 – Edit Entry** page consists of the following components:

- **Interface Type** – is used to select the interface configuration (**User** or **Network**).
- **Signaling Type** – is used to select the signaling type for the trunk. The **CAS** (Channel Associated Signaling) and **CCS** (Common Channel Signaling) signaling types are available.
  - Up to **30** timeslots will be available for placing **E1** calls regardless the trunk signaling type. The timeslot TS0 is reserved for framing and the timeslot TS16 for signaling purposes.
  - Up to **23** timeslots will be available for placing **T1** calls if the trunk signaling type is **CCS**. The timeslot TS24 is reserved for signaling purposes.
  - Up to **24** timeslots will be available for placing **T1** calls if the trunk signaling type is **CAS**. Each timeslot is used both for voice and signaling purposes.
- The **E1** and **T1** radio buttons are used to select the mode for the trunks. Both selections allow to configure the **Line Code**, **Frame mode**, **Line Build Out**, **Coding Type**, **LoopBackMode** and **Clock Mode** settings to match the E1/T1 settings for ITSP's.

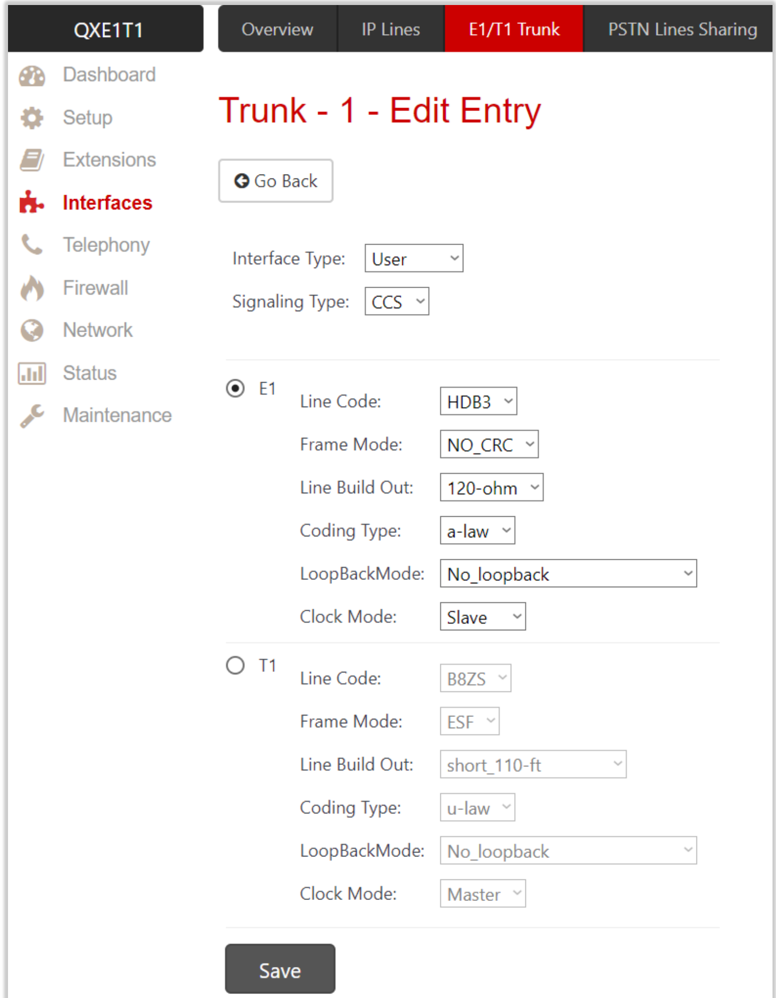


Figure 41: Trunk-1 – Edit Entry page

Click the Modify Signaling Settings icon to open the Trunk 1 – Signaling Type page. Different settings and options are available for configuration depending on the selected signaling type (CAS or CCS).

7.4.2 Signaling Type – CCS

The Trunk CCS Signaling Settings page allows configuring CCS signaling settings and gives a possibility to select timeslots for signaling data transfer/receive and voice transfer. The following sections are available:

Call Handling

- Route Incoming Call to – is used to define the destination where the incoming calls 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. It will automatically use the initially dialed number to connect the destination without any additional dialing.
- Incoming Called Digits Size – indicates the number of received digits required to establish the call. When field has 0 value, system uses either timeout defined in the T302 field or the Sending Complete Information element messages to establish the call. Independent on the value in this field, Sending Complete Information element and pound sign accelerate the call establishment.

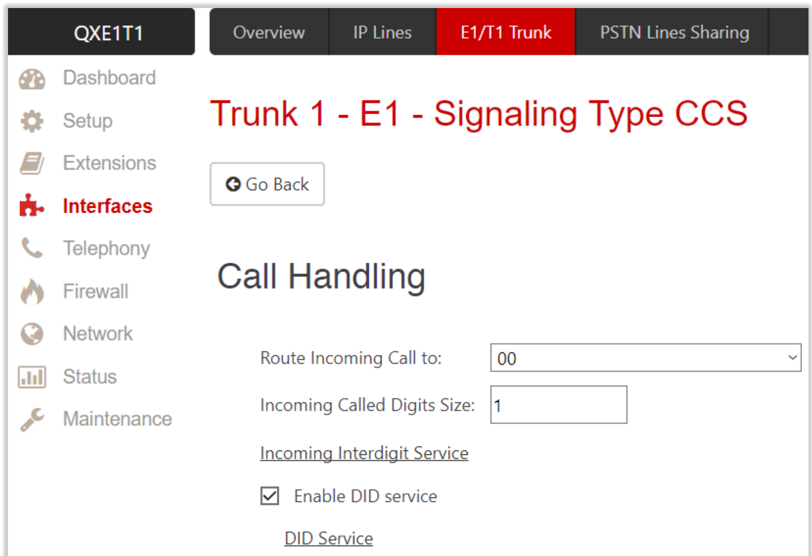


Figure 42: Call Handling section

- Incoming Interdigit Service – link leads to the page where the dial plan for incoming E1/T1 calls from CO or PBX to the QX can be configured.
- Enable DID Service – is used to enable DID service. TIP: DID service is available for User interface only.
  - DID Service link leads to the CCS DID Service page to configure the DID number(s).

ISDN L3 Settings

- B Channels link leads to the Signaling Type CCS – B Channel Settings page where available timeslots can be enabled/disabled for the voice transfer and echo cancellation feature can be configured.
- Switch Type – this configuration parameter depends on the CO when acting in the User mode and the legacy PBX capabilities when acting in the Network mode.
- Bearer Establishment Procedure – allows to select the session initiation method on the B channels. One of the following possibilities of the transmission path completion prior to receipt of a call acceptance indication can be selected:
  - on channel negotiation at the destination interface
  - on progress indication with in-band information
  - on call acceptance
- 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:
  - None – configures the system to send ALERT messages without the Progress Indicator Information Element.
  - Unconditional – configures 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 – configures the system to send ALERT/PROGRESS messages with Progress Indicator IE. With this option, the system will send its own progress tone only if there is no early media (180/183 with SDP) from the called party.
- T302 Timer – indicates the time frame system will wait for digit to be dialed and when timer expires, it initiates the call. TIP: Timer is not applicable for DMS-100 switch types.
- T309 Timer – this option is responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is 0, T309 timer will be disabled.
- T310 Timer – this option is responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) is not yet arrived.

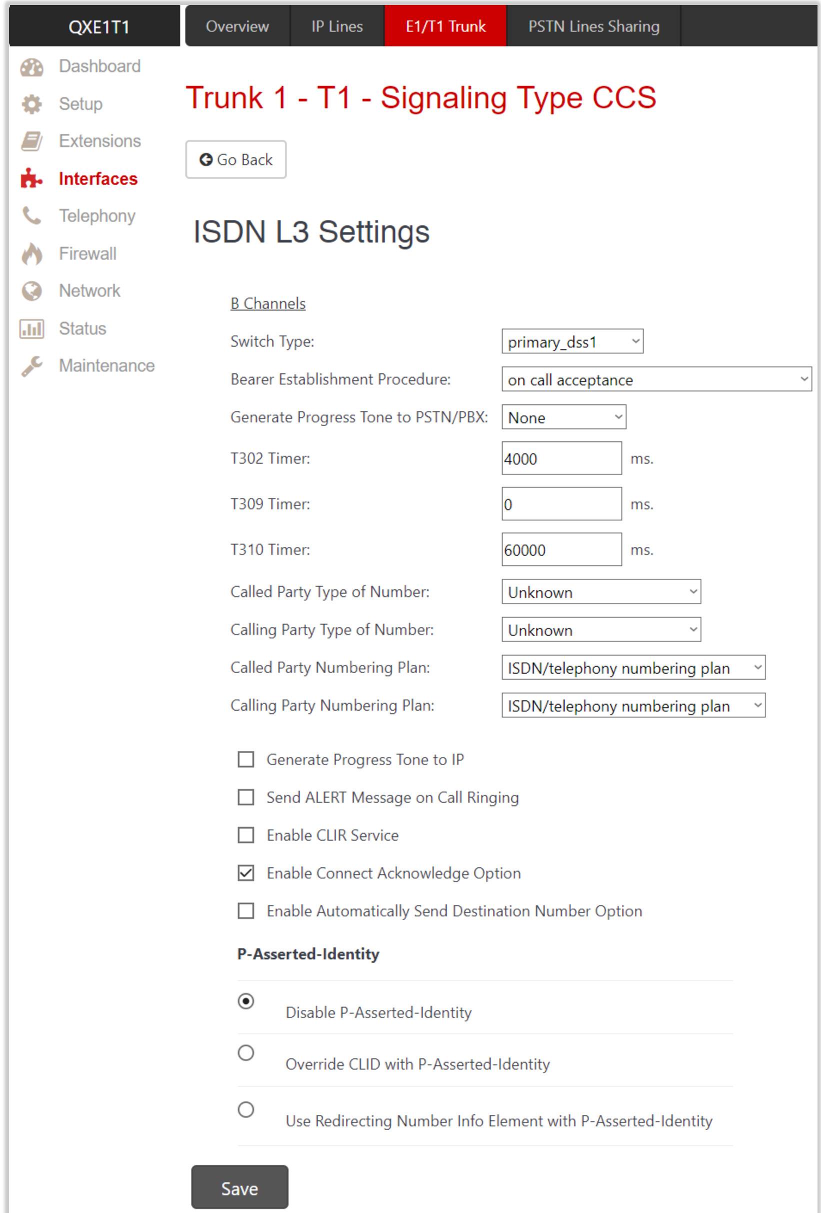


Figure 43: Signaling Type CCS – ISDN L3 Settings section

- No Answer Disconnect Timer – this option is used in certain types of legacy PBXs. The value 0 indicates that the timer is disabled. When time expires, QX will play a busy tone towards the legacy PBX if the call has been disconnected by the peer. TIP: This option is available only in Network mode.
- 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 call.
- Called Party Numbering Plan and Calling Party Numbering Plan – indicate correspondingly the numbering plan of the called party and calling party.
- Generate Progress tone on IP – if selected, the progress tone to IP (SIP) will be generated.
- Send ALERT Message on Call Ringing – if selected, the system will send ALERT messages to callers from the PSTN/PBX on call ringing, otherwise the system will send a PROGRESS message on receiving early media from the called party if the Unconditional or Conditional options are selected for Generate Progress Tone to PSTN/PBX.
- Enable CLIR Service – if selected, the 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.
- Enable Connect Acknowledge Option – if selected, QX will stop the T303 and T310 timers upon receiving the CONNECT message, will send a CONNECT ACKNOWLEDGE message to the remote side and enter the active state, otherwise QX will stop the T303 and T310 timers upon receiving the CONNECT message and will enter the active state without sending the CONNECT ACKNOWLEDGE message to the remote side.
- P-Asserted-Identity – is used to configure P-Asserted-Identity for the calls from SIP to E1/T1 and vice-versa.
  - Disable P-Asserted-Identity – disables 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 E1/T1 if the Invite SIP message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on E1/T1 is sent with the original Caller ID which comes from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field. For the calls from E1/T1 to SIP with restricted Caller ID, the SIP Invite message contains P-Asserted-Identity field with the value from the Caller ID on E1/T1. The "SIP From" field contains anonymous.
  - Use Redirecting Number Info Element with P-Asserted-Identity – enables full support of the SIP P-Asserted-Identity. For the calls from SIP to E1/T1, if the SIP Invite message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on E1/T1 contains the number from the user name field and the Redirecting Number IE contains the original number from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field. For the calls from E1/T1 to SIP with Caller ID, the SIP Invite message contains P-Asserted-Identity field with the original number value from the Redirecting Number IE on E1/T1. The "SIP From" field contains the value from the user name.

Signaling Type CCS - B Channels

The Signaling Type CCS – B Channels table lists the available timeslots of the trunk and their settings.

- Channel Selection – is used to select B channel selection method. For Preferred channel selection, the CO answers to the call request by the first available timeslot, while for Exclusive channel selection CO should feedback only by the timeslot used for the call request.
- Channel Selection Ordering – is used to choose the B channels selection order.
- Force Update – is used to apply immediately the new settings on the selected timeslot(s). This will force the selected timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.

- Restart – is used to bring timeslot(s) to the initial idle state on the both sides. TIP: When applying one of these options (Force Update or Restart), any active traffic on the timeslot(s) will be terminated.
- Edit – leads to the Signaling Type CCS – B Channels – Edit Entry page where the key parameters specific to the selected timeslot(s) can be configured. The following options are available:
  - Enable Timeslot – enables/disables the selected timeslot(s).
  - Force Update Timeslot – applies new settings immediately by restarting the selected timeslot(s).
  - Enable Echo Cancellation – enables/disables the echo cancellation on the selected timeslot(s).

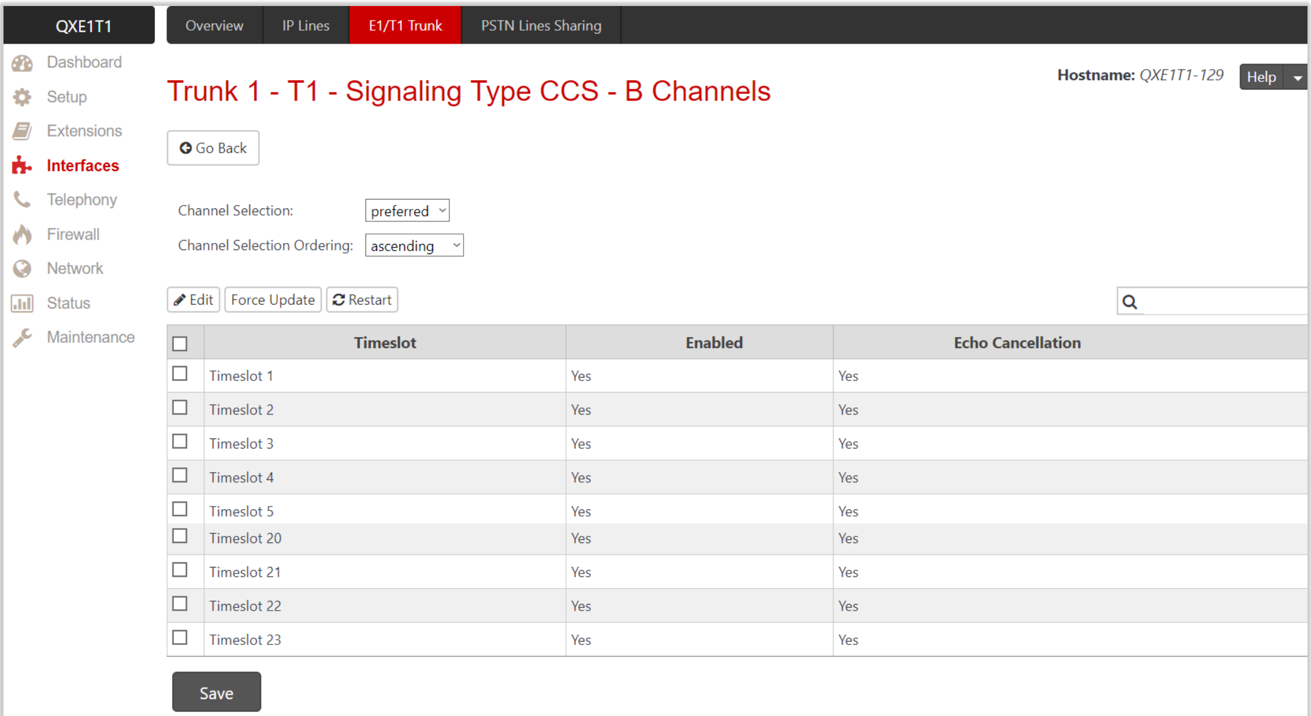


Figure 44: Signaling Type CCS – B Channels page

Note: A timeslot can be used either for voice or data transfer. The timeslot reserved for the D Channel receive/transmit is missing from the list of B channels.

ISDN L2 Settings

- Non Automat – if selected, the non-automatic Terminal Endpoint Identifier (TEI) searching will be activated.
  - TEI Address – enter the TEI number for connection establishment between CO and E1/T1 client. In automatic mode, an E1/T1 connection will be established on the first available TEI, while in non-automatic mode a specific TEI may be reserved for the connection. In this case, both call partners need to specify the same TEI in their settings.
  - SAPI Value – enter the additional Service Access Point Identifier (SAPI) value that is used to support additional interface between ISDN Layer 2 and Layer 3. Leaving this field empty (default value), only Call Control and Layer 2 management procedures will be activated.
- Alternative Disconnection Mode – if not selected, QX will disconnect the call as soon as disconnect message has been received from the peer, otherwise, QX's user may hear a busy tone when peer has been disconnected.
- Excessive Ack. Delay T200 – is used to configure the period between the transmitted signaling packet and its acknowledgement received.

- Idle Timer T203 – is used to configure the period for E1/T1 client idle timeout.
- D Channel Timeslot for Transmit/Receive – is used to reserve the timeslot for transmitting/receiving signaling data.

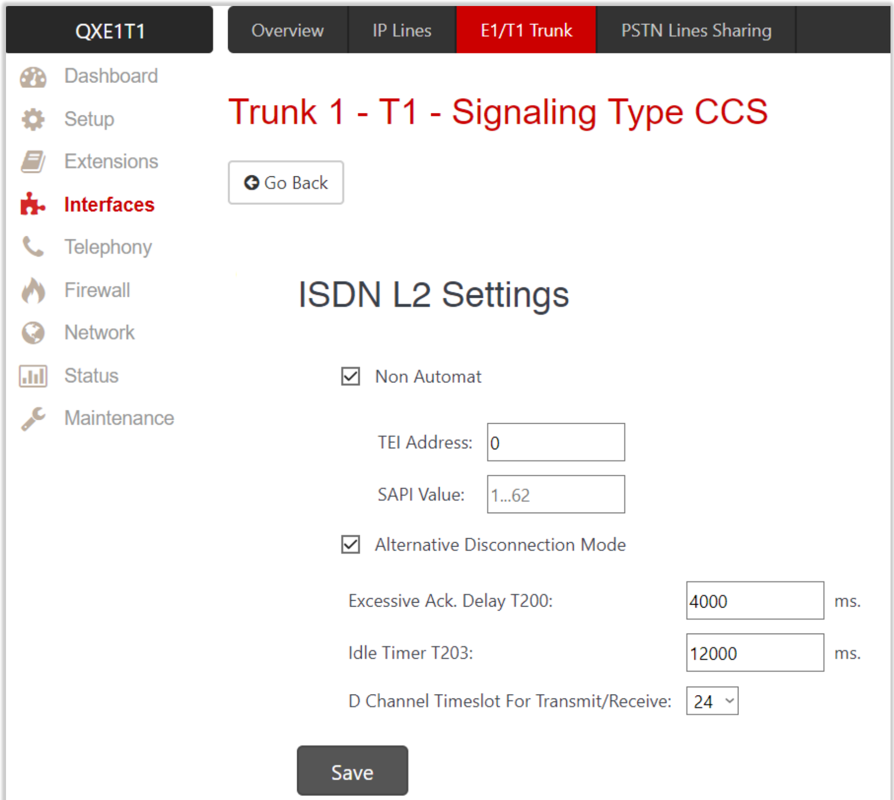


Figure 45: Signaling Type CCS – ISDN L2 Settings part

Note:

- In the Network Mode (PBX connected):
  - If Non Automat mode is selected, the same TEI address should be specified on both sides (QX and legacy PBX).
  - If Automat mode is selected, the user on PBX side will have the opportunity to set any mode related to TEI assignment in PBX configuration. This will allow PBX connection to the QX without providing the TEI address from QX.
- In the User Mode (CO connected) the TEI assignment is dependent on CO settings:
  - Select Non Automat mode and enter the same TEI address provided by CO.
  - Select any mode related to TEI assignment if automat TEI searching mode is selected on CO side.

7.4.3 Signaling Type – CAS

The following settings are available when the signaling type for the trunk is selected as CAS:

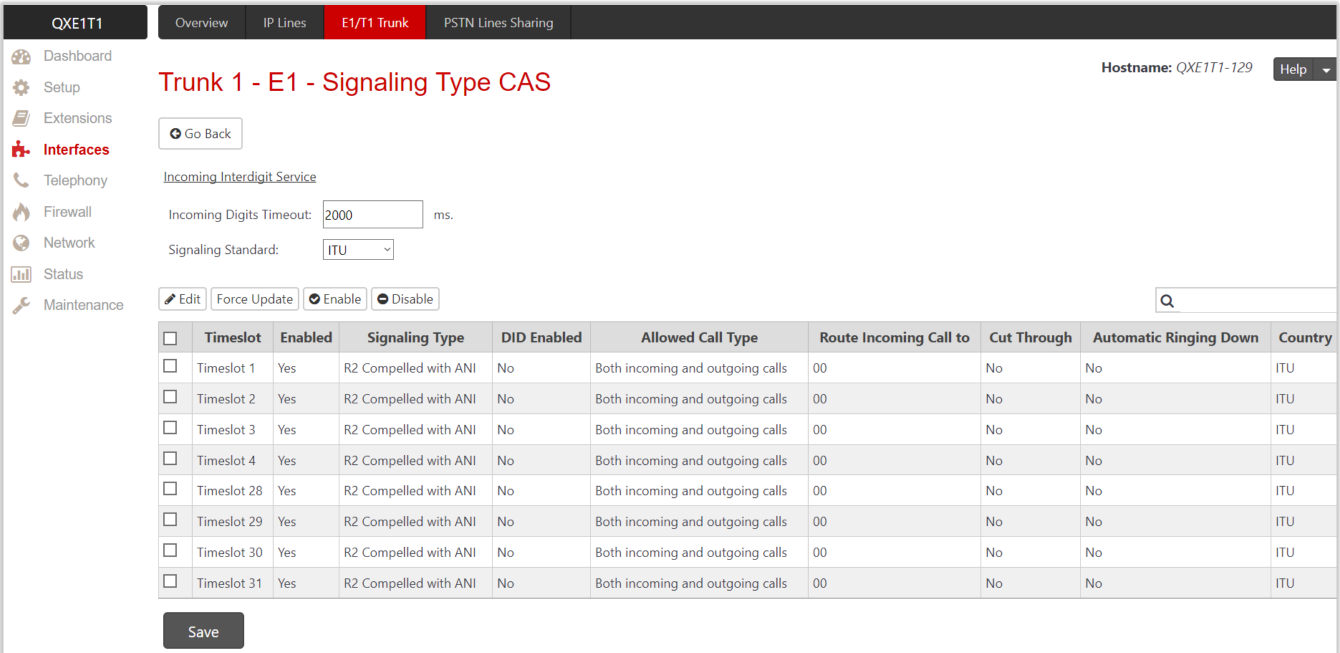


Figure 46: Trunk 1 CAS Signaling Settings page

- Incoming Interdigit Service – leads to the page to configure the dial plan for incoming E1/T1 calls from CO/PBX to the QX can be configured.
- Incoming Digits Timeout – is used to define the timeout during which incoming digits from the destination party will be collected before being applied as an incoming called number.
- Signaling Standard – is used to select the signaling standard for connection (N/A for T1 interface).

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

- Force Update – is used to apply immediately the new settings on the selected timeslot(s). This will force the timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.
- Edit – leads to the CAS Signaling Wizard where the key configuration parameters specific to the selected timeslot(s) can be configured.

The CAS Signaling Wizard consists of the following sections:

Signaling Type Settings

This section is used to configure the signaling type settings. The following options are available:

- Trunk – shows the trunk number.
- Selected Timeslots – shows the selected timeslots.
- Allowed Call Type – is used to select the call directions: incoming, outgoing or both.
- Signaling Type – is used to select the CAS signaling type. R2 signaling (compelled and non-compelled) can be used with an E1 interface both in User and Network modes. QX with E1 interface in the CAS mode detects the busy tone only in case of R2 compelled and non-compelled (both with and without ANI) signaling types. QX does not support the Forward Digit selected on the CO when acting in the User mode with Loop Start signaling type.

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

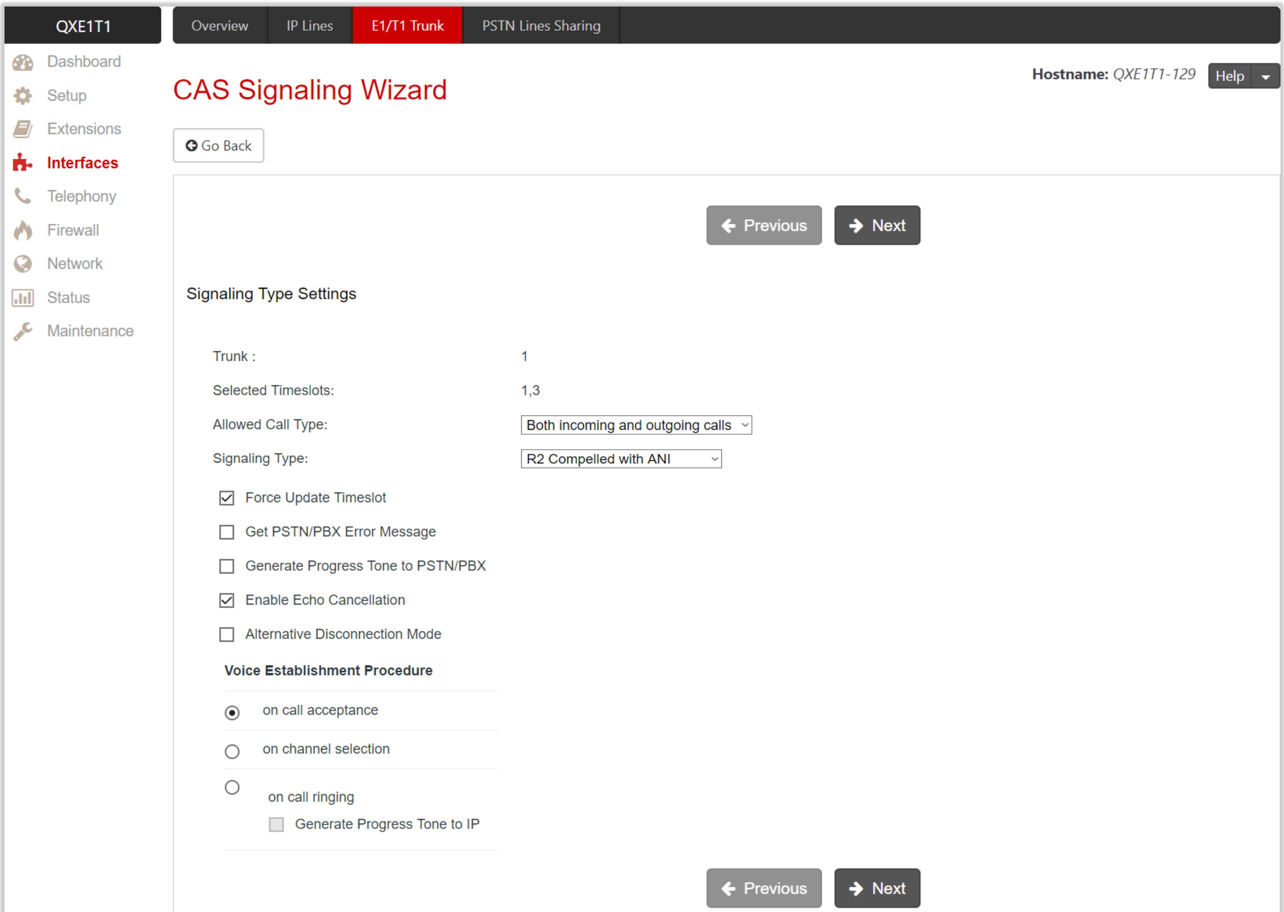


Figure 47: Signaling Type Settings section

- Get PSTN/PBX Error Message – if selected, a notification message will be played when the outgoing call is not established (destination unreachable, incorrect or non-existent number), otherwise the call will be disconnected.
- Generate Progress Tone to PSTN/PBX – if selected, QX generates ring tones to incoming callers during E1/T1 call dialing. This feature is mainly applicable to 2-stage dialing mode.
- Enable Echo Cancellation – enables the echo cancellation mechanism on the selected timeslot(s).
- Alternative Disconnection Mode – if selected, the QX will play a busy tone towards the PBX/CO when the call is failed. After 60 second timeout, the QX will stop playing the busy tone and the call will be disconnected.
- Voice Establishment Procedure – is used to select a method of voice establishment on the trunk:
  - on call acceptance – if selected, the voice will be established after call is being accepted.
  - on channel selection – the call will be accepted during channel selection. TIP: This selection is not allowed for R2 signaling.
  - on call ringing – the voice will be established after call is being ringing. The Generate Progress Tone checkbox which is used to enable the progress tone generation upon voice establishment.

DID Service Settings

This section becomes available only if the Signaling Type is set to any of the E&M types or to R2 DTMF in Signaling Type Settings section.

- Enable DID Service – is used to enable DID (Direct Inward Dialing) service for the selected timeslot(s).

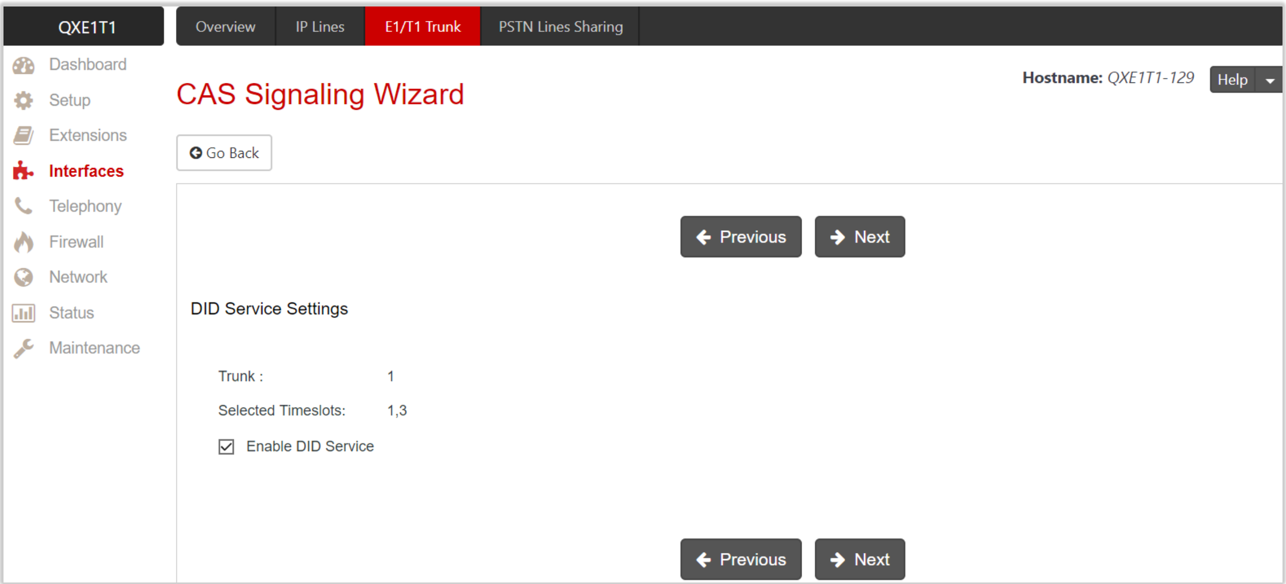


Figure 48: DID Service Settings section

Routing Settings

This section is used to set the destination for incoming calls to be routed to and to enable Cut Through and Automat Ringing Down services for signaling different from R2 (all types). The following options are available:

- Trunk – shows the trunk number.
- Selected Timeslots – shows the selected timeslots.
- Route Incoming Call to – is used to define the destination where the incoming calls 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. It will automatically use the initially dialed number to connect the destination without any additional dialing.
- Cut Through – is used to reconnect the call (terminated by some reason, e.g. user error, network problems, etc.) by going on-hook and off-hook again even if the call partner is off-hook and not involved in the call. TIP: This option is available when the Enable DID Service checkbox not selected from the previous section.
- Automat Ringing Down – allows an E1/T1 device connected to the QX to establish a hot-line call (automatic call without any digits dialed). TIP: This option is available when the Enable DID Service checkbox not selected from the previous section.
- Pass Through Pound Sign # – if selected, the # detected in the dialed number will be passed through and will be considered as a part of the dialed number. When this checkbox is not selected, the detected # will be considered as a call acceleration digit. TIP: This option is not available when selected Signaling Type on the Signaling Type Settings section is R2 Compelled, R2 Non-Compelled, R2 Compelled with ANI or R2 Non-Compelled with ANI.

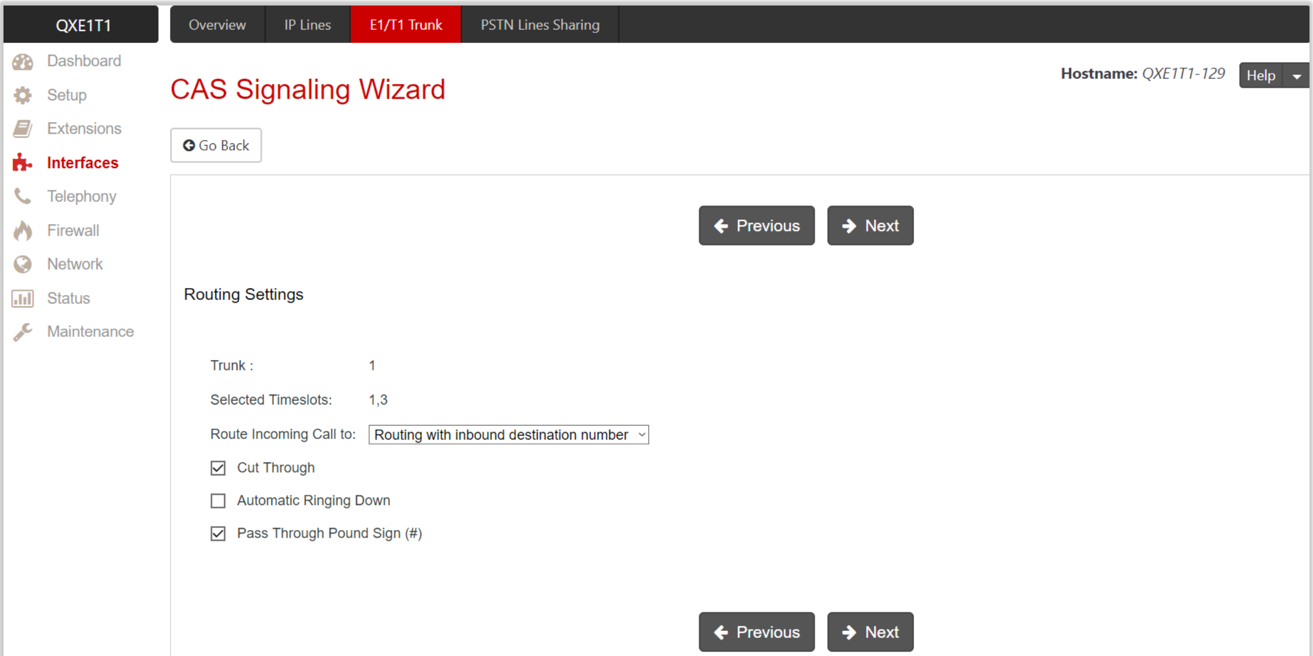


Figure 49: Routing Settings section

Country Settings

This section becomes available only for E1 interface and the Signaling Type is set to any of the R2 signaling types in Signaling Type Settings section. The following options are available:

- Trunk – shows the selected trunk number.
- Selected Timeslots – shows the selected timeslots.
- Country – is used to select the location where QX is located to support the correct functionality of R2 signaling. For the locations missing in the list, use the ITU option.
- Use Default Country Settings – is used to restore default advanced settings for the selected location. You can manually configure Country Settings in the next section if the checkbox is not selected.

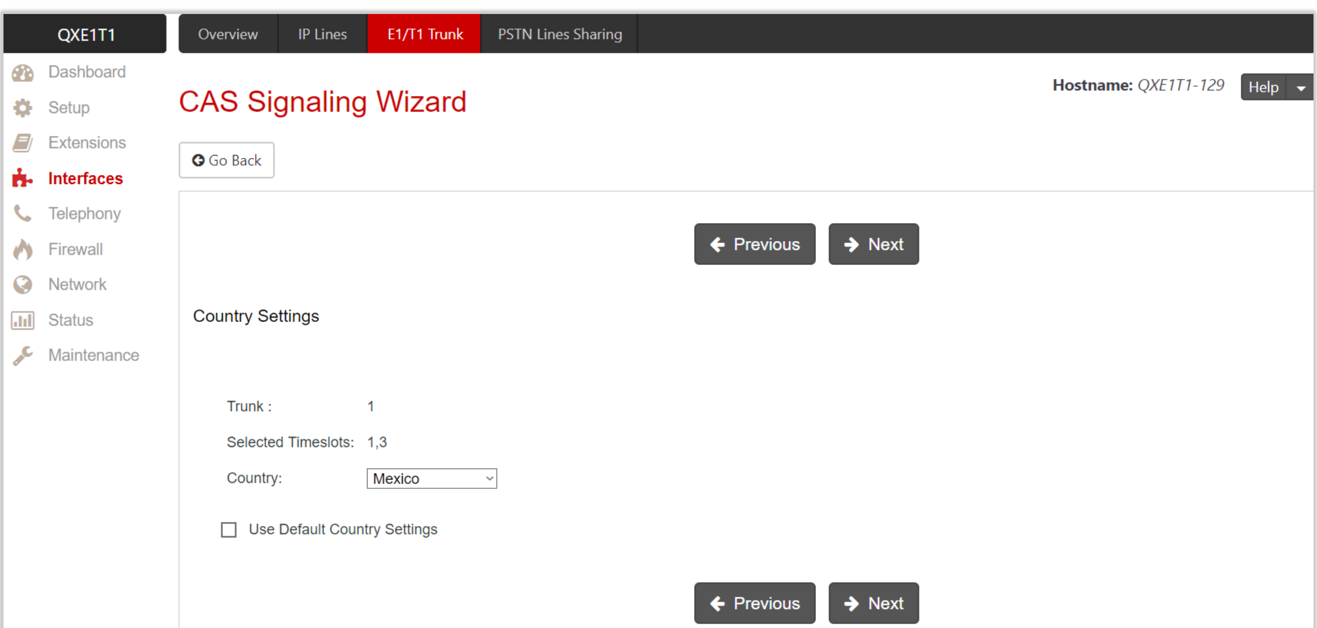


Figure 50:Country Settings section

Advanced Country Settings

This section becomes available only if the Use Default Country Settings checkbox is not selected in Country Settings section.

- Trunk – shows the selected trunk number.
- Selected Timeslots – shows the selected timeslots.
- Country – shows the selected country.
- ANI Category – is used to select the calling party priority depending on the call originator's location specifics (N/A for R2 DTMF signaling).
- ANI Request Transmit and ANI Request Receive – is used to select the Caller ID request R2 tones for transmit and receive.
- Seize Acknowledge Timeout – is used to define a timeout between incoming seize signal and the corresponding feedback.
- Answer Guard Timeout – is used to define a wait timeout Group-B Answer Signal and Line Answer.
- Release Guard Timeout – is used to define an idle timeout between the disconnect signal receipt and call disconnection.
- Dialing Delay Timeout – is used to define a timeout before injecting dialed digits. TIP: Timeout specially refers to R2 DTMF signaling.
- Incoming DNIS Size – indicates the number of received digits required to establish a call. When field has 0 value, system uses either timeout defined in the Incoming digits timeout field or the End of Address messages to establish a call. Independent on the value in this field, the message End of Address always causes the call establishment.
- Unused A:B:C:D – is used to configure unused C and D bits of E1/T1 CAS signaling (A and B bits are predefined). Fields may have either 0 or 1 values.
- Invert A:B:C:D – is used to invert the ABCD status bits in timeslot 16 before TX and after RX. If bit is set to 1, the router inverts it before transmission and after the receipt.
- End of DNIS (I-15) – is used to enable End of DNIS service.
- Collect Call – if selected, then in case of incoming calls, always the called destination will pay for the call (applicable only for Brazil). Option is particularly applicable when calling from the mobile phone. It should be selected when the appropriate feature is enabled on the legacy PBX.
- Allow Timeslot Blocking – indicates whether the system should use blocked timeslots to make outgoing PSTN calls. If this checkbox is selected, the system will NOT use timeslots blocked by the carrier, otherwise the system will try to unblock the timeslots and will make outgoing calls if succeeded.
- Override CLID with P-Asserted-Identity – enables the SIP P-Asserted-Identity support. For the calls from SIP to E1/T1 if the Invite SIP message contains a P-Asserted-Identity or a P-Preferred-Identity or a Remote-Party-ID, then the CallerID on E1/T1 is sent with the original Caller ID which comes from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field. For the calls from E1/T1 to SIP with restricted Caller ID, the SIP Invite message contains P-Asserted-Identity field with the value from the Caller ID on E1/T1. The "SIP From" field contains anonymous.

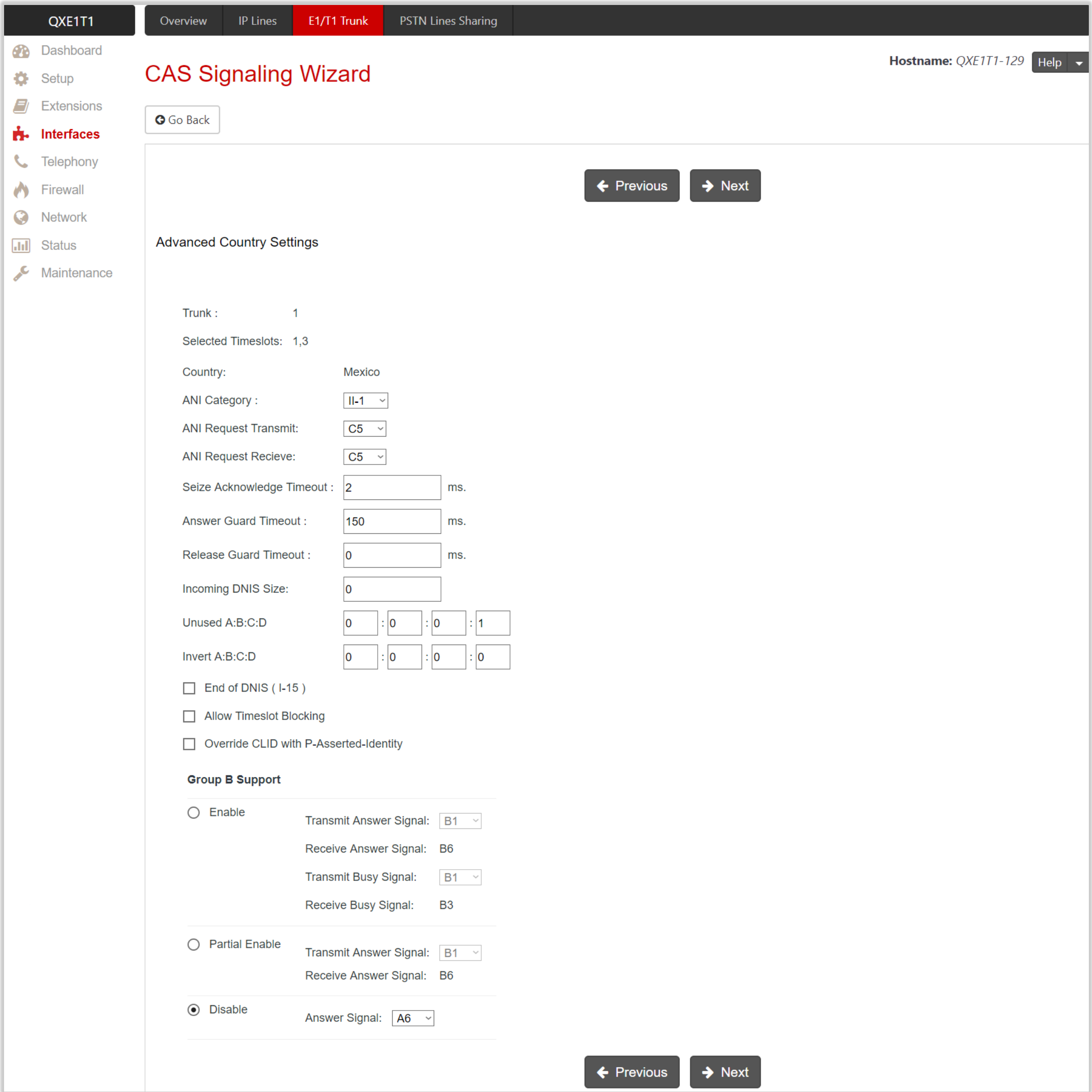


Figure 51:Advanced Country Settings section

- Group B Support – enables/disables the Group B Support. This section becomes available only for E1 interface and the Signaling Type is set to any of the R2 types (except R2 DTMF) in Signaling Type Settings section. The following selections are available:
  - Enable – this selection enables Group B Support both for answer and busy recognitions of transmit and receive signals. This selection requires you to define transmit and receive signals. The Transmit Answer Signal and Transmit Busy Signal parameters are defined from the drop-down lists on this section.
  - Partial Enable – selection partially enables Group B Support with for answer recognition only. This selection requires you to define transmit and receive signals. The Transmit Answer Signal parameter is defined from the drop-down list on this section. When the "transmit" signal is selected, click Next to access the R2 Receive Signal Settings section where Receive Answer Signal should be defined. Use the checkboxes to select the Receive Answer Signal value. Multiple values are allowed for each signal.
  - Disable – selection disables Group B Support and requires defining the Answer Signal parameter.

R2 Receive Signal Settings

This section is used to select Receive Answer Signal and Receive Busy Signal. Use the checkboxes to select the Receive Answer Signal and Receive Busy Signal values. Multiple values are allowed for each signal.

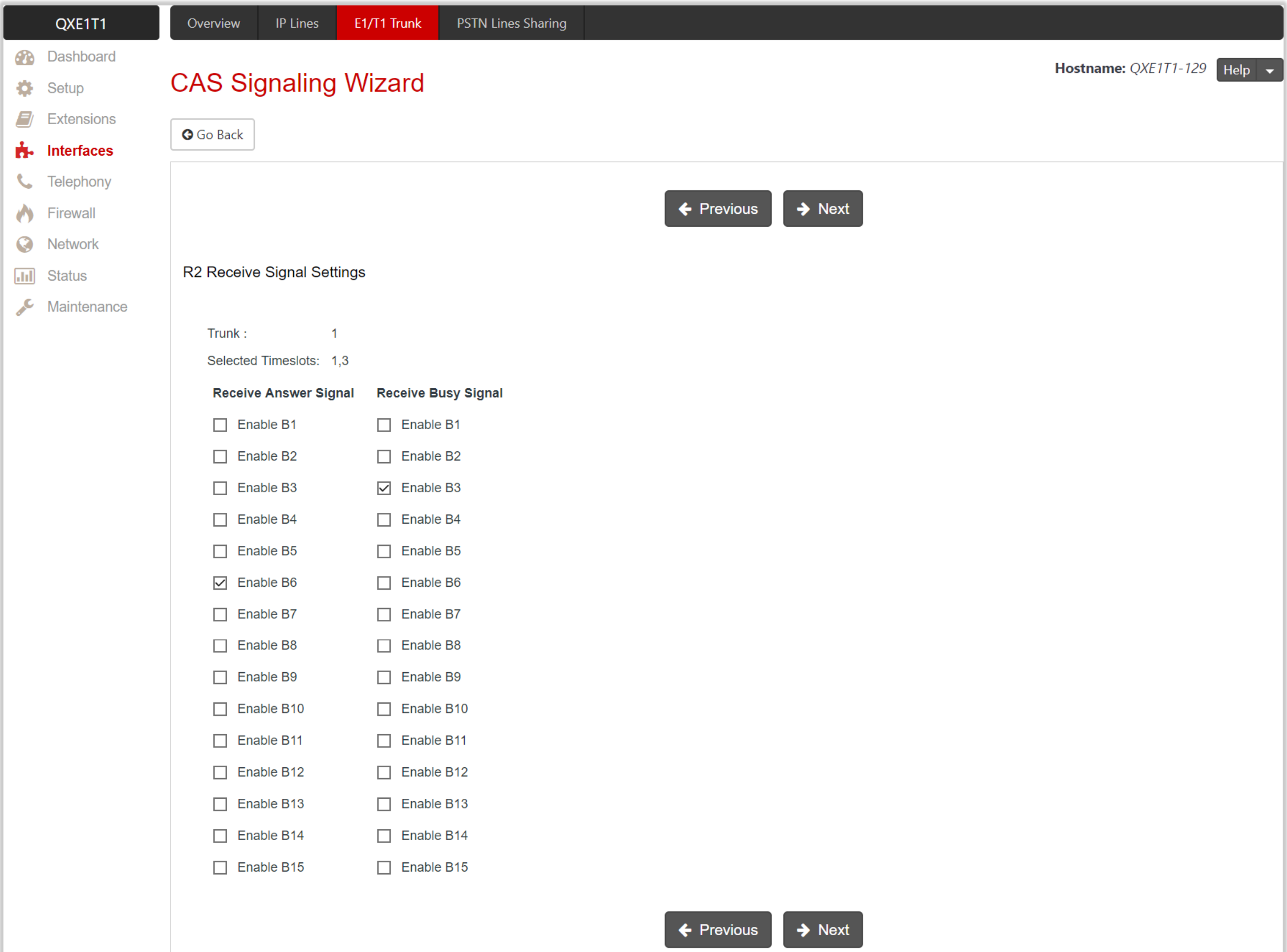


Figure 52: R2 Receive Signal Settings section

Summary results of CAS Settings

This section is used to show all configured settings for the selected timeslot(s).

7.4.4 CCS – DID Service

The Trunk 1 - CCS - DID Service page is used for mapping a group of DID numbers to the certain destinations on the QX.

The **Use Default outgoing Caller ID** is used to overwrite the source caller information with the one specified in the Default outgoing Caller ID field when placing outgoing calls toward the CO, if the default Caller ID does not match one(s) listed in the **Route Incoming Call to** field. Click **Save** to apply changes.

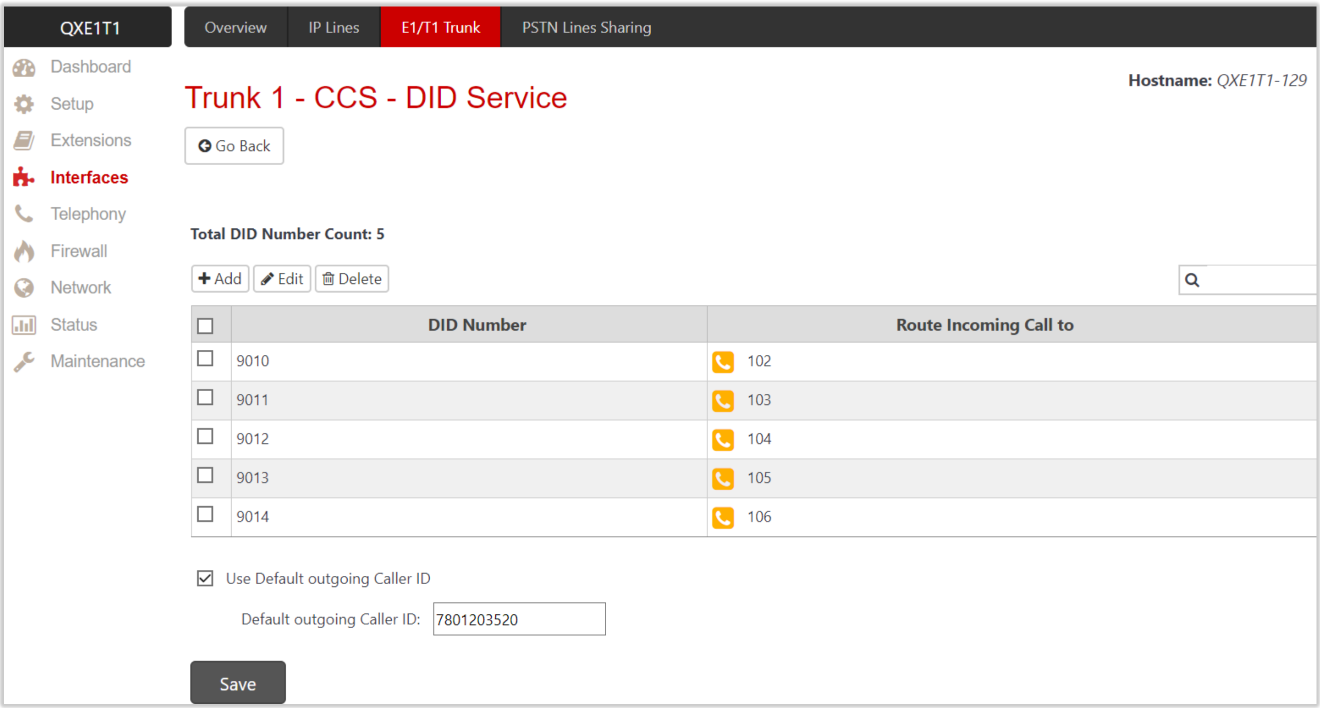


Figure 53: CCS - DID Service page

To add a new DID number:

1. Click **Add** and enter the following information:
   - **Start DID Number** – enter the number for the first DID. TIP: A maximum DID number length is 20 digits.
   - **Quantity** – specify the amount of DID numbers. TIP: Up to 500 DID numbers can be specified.
   - **Route Incoming Call to** – is used to define the destination where the incoming calls 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**. It will automatically use the initially dialed number to connect the destination without any additional dialing.
   - **Generate from selected Extension Number** – if selected the system will automatically assign DID numbers to consecutive extensions starting from the selected extension. TIP: If the ordinal extension is missing the DID number will be assigned to 00 Auto Attendant.
2. Click **Save**, the new entry(ies) will be added to the CCS - DID Service table.

7.4.5 Incoming Interdigit Service

The **Incoming Interdigit Service** allows to speed up the call procedure by detecting the prefix according to the time set in the **Incoming Digits Timeout** field. When the system detects incoming dialed number starting with any of the prefixes listed in the **Incoming Interdigit Service** table, it will wait for the rest of the digits, as specified for the corresponding prefix in the **Incoming DNIS Size**. Once all digits are received, the system will immediately route the call to the destination.

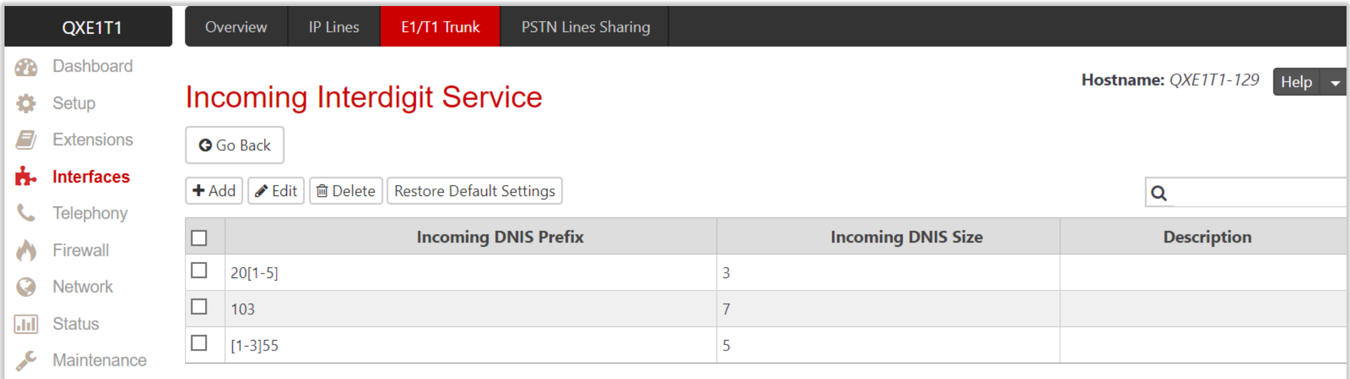


Figure 54: Incoming Interdigit Service page

The **Incoming Interdigit Service** table lists existing dial plan entries and allows you to manage them. By default, the table lists the local specific (selected from the **System Configuration Wizard**) dial plan settings. TIP: For some countries, this table may however be empty.

To add a new Incoming DNIS Prefix:

1. Click **Add** and enter the following information:
   - **Incoming DNIS Prefix** – enter the prefix of the incoming dialed number. The **Incoming DNIS Prefix** may contain wildcards.
   - **Incoming DNIS Size** – enter the total length of the dialed number, including the prefix digits. The number defined here should be greater than the longest prefix defined in the **Incoming DNIS Prefix**.
   - Enter any **Description**, if needed.
2. Click **Save**, the new entry will be added to the Incoming Interdigit Service table.
3. Click **Restore Default Settings** to restore the locale specific dial plan entries.

7.4.6 E1T1 Status page

The E1/T1 Trunk Status page shows information about the trunk and link state, transfer and error statistics. The following sections are available:

<u>General Information</u>

This section contains the following components:

- Active Calls – currently active calls.
- Outgoing Calls – total amount of outgoing calls (historical data).
- Incoming Calls – total amount of incoming calls (historical data).
- Last Time Cleared shows the date and time when the E1/T1 Stats has been manually cleared last time. TIP: Click the Clear Statistics button, to reset the statistics counters.

<u>Layer 1 - Trunk Settings and Link Status</u>

This section contains the following components:

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

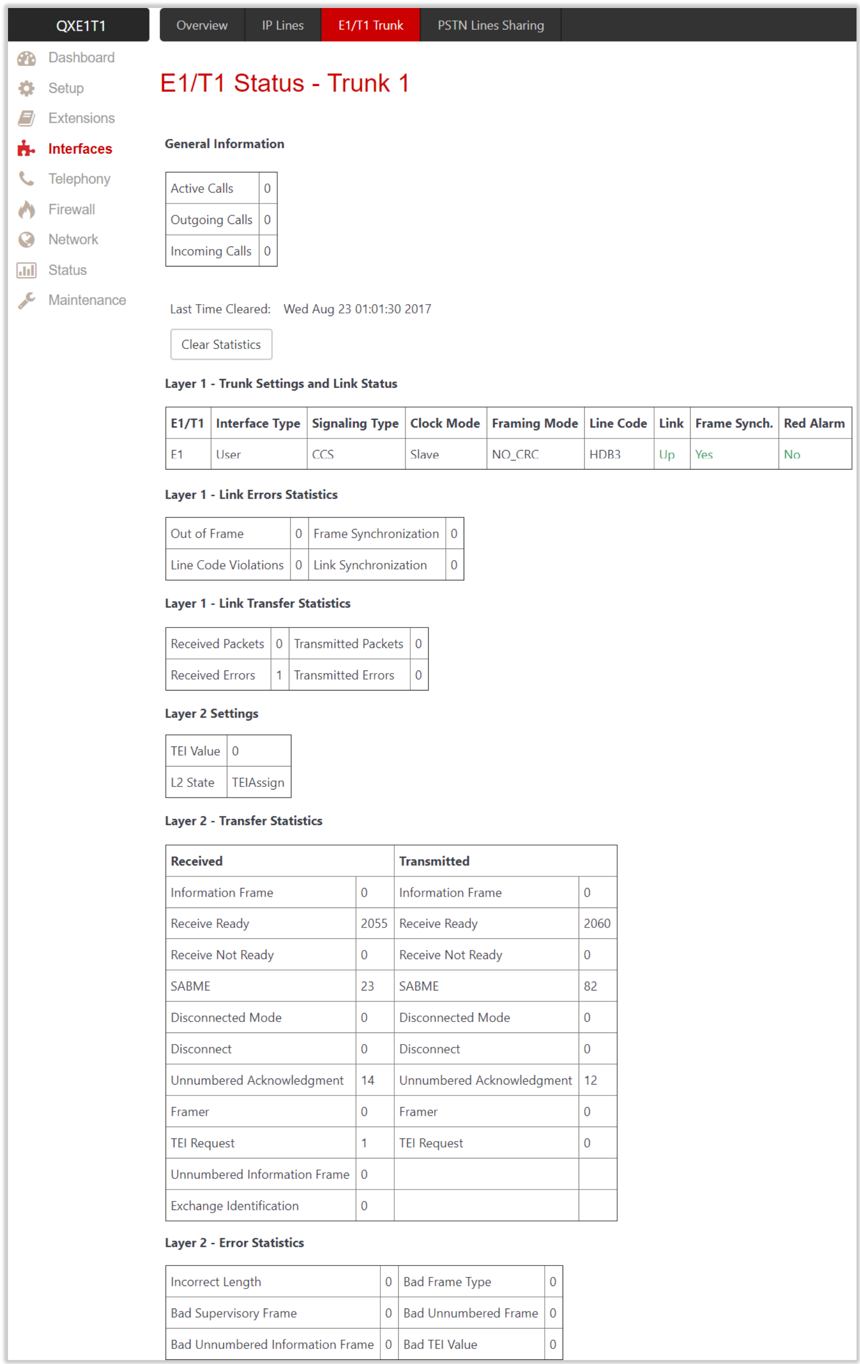


Figure 55: E1/T1 Status page

Layer 1 - Link Error Statistics

This section contains the following components:

- Out of Frame – shows the number of Out of Frame errors.
- Line Code Violation – shows the number of Line Code Violation errors.
- Frame Synchronization – shows the number of Frame Synchronization errors.
- Link Synchronization – shows the number of Link Synchronization errors.

Note: The below-listed sections are available only if CCS Signaling is selected.

Layer 1 - Link Transfer Statistics

This section contains the following components:

- Received Packets – shows the number of received packets.
- Received Errors – shows the number of received defective packets.
- Transmitted Packets – shows the number of transmitted packets.
- Transmitted Errors – shows the number of transmitted defective packets.

Layer 2 Settings

This section contains the following components:

- TEI Value – shows the actual TEI assigned value.
- L2 State – shows the state of the TEI assignment.

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 E1/T1 link is up.
- Receive Not Ready – shows the control packets when unable to accept calls by destination.
- SABME – shows the packets during connection establishment.
- Disconnected Mode – shows the packets when connection is being terminated.
- Disconnect – shows the packets during connection termination.
- Unnumbered Acknowledgement – shows the packets during accepting connection establishment/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.
- Bad TEI Value – shows the packets with bad TEI value.

Note: The Blocked Timeslots section lists the timeslots blocked by the carrier.

7.5 ISDN Trunk Settings

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

The ISDN service allows QXISDN4 gateway act in the following modes:

- network – if connected to a private PBX
- user – if connected to the ISDN trunk from the CO (Central Office). The QXISDN4 supports the MSN (Multiple Subscriber Number) 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. There are 4 ISDN trunks available on the QXISDN4 gateway. The Trunk Settings table lists the available ISDN trunks and their settings (trunk name and interface types).

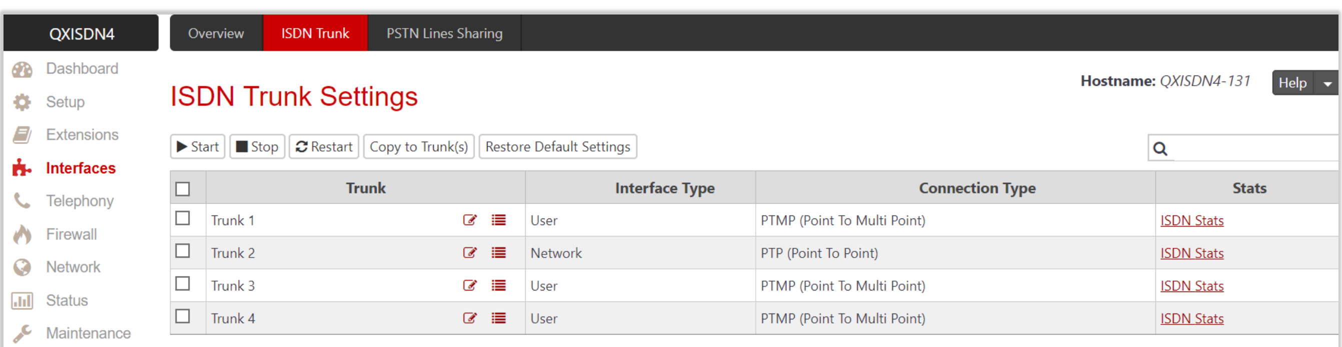


Figure 56: ISDN Trunk Settings page

The 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 – restores the default settings of the selected ISDN trunk(s).
- Click the Incoming Interdigit Service to configure dial plan for incoming ISDN calls from CO/PBX to the QX.
- Click the Modify ISDN Trunk icon to configure the ISDN trunk settings.

ISDN Wizard

The **ISDN Wizard** consists of the following sections:

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

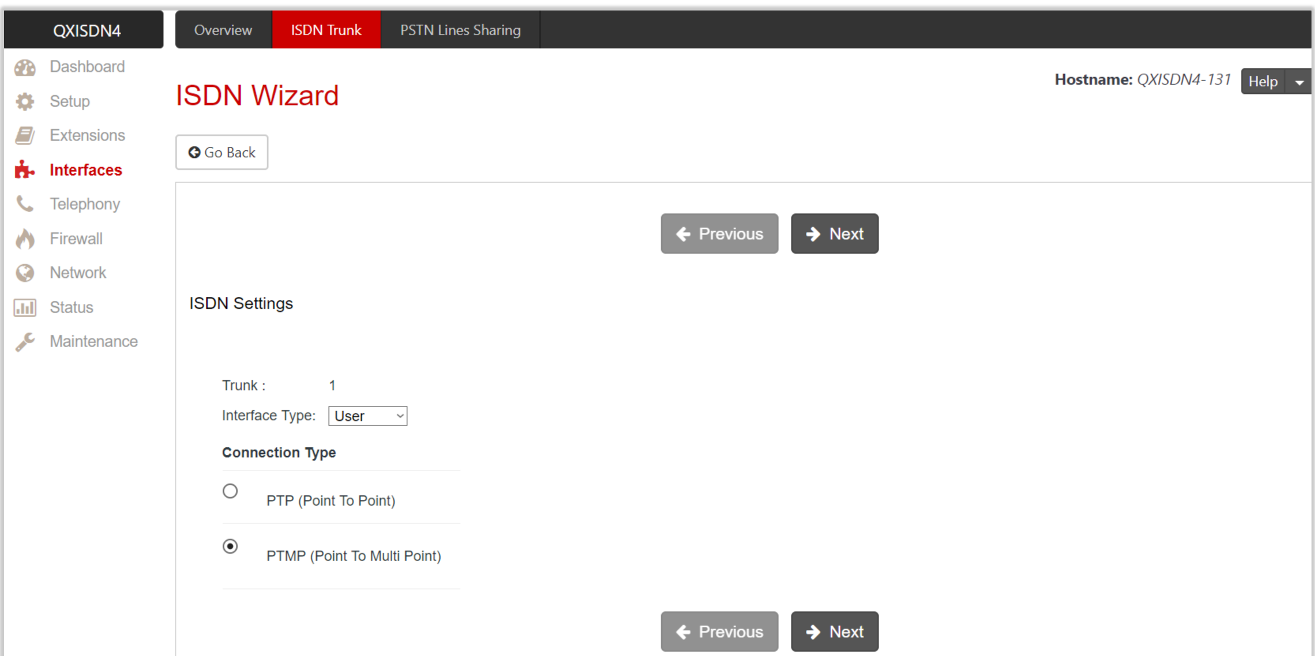


Figure 57: ISDN Settings section

➢ **PTMP** (Point to Multi Point) – in case of connection to the CO (**User** interface type is selected) choose this option if there can be other devices connected to the same ISDN trunk from CO except the QX. In case of connection to legacy PBX (**Network** interface type is selected) choose this option if there can be other devices connected to the same ISDN trunk except for the legacy PBX. 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. This section becomes available only if the interface type is **User**. It is recommended to enable the MSN when there are multiple ISDN devices connected to the same ISDN bus. If the MSN is enabled the next section will require the MSN table configuration.

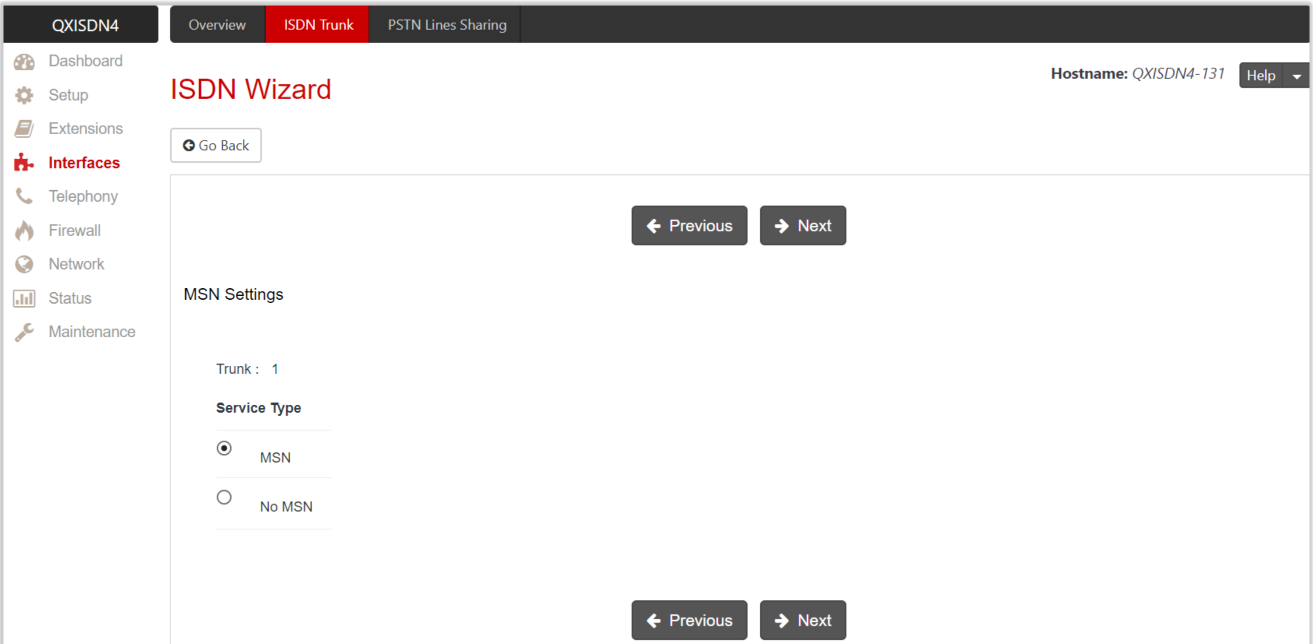


Figure 58: MSN Settings section

Routing Settings

This section content is dependent 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 the QX.
  - The fields in the **MSN Number** column require the MSN numbers allocated to the 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. 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 selected interface type is **Network**, this section contains only one **Route Incoming Call to** option.
- **Use Default outgoing Caller ID** – is used to overwrite the source caller information with the one specified in the Default outgoing Caller ID field when placing outgoing calls toward the CO, if the default Caller ID does not match one(s) listed in the **Route Incoming Call to** field.
- **Advanced Settings** – select this if you want to adjust trunk's L2 and L3 Settings manually in the next section, otherwise leave it unselected to use the system default values.

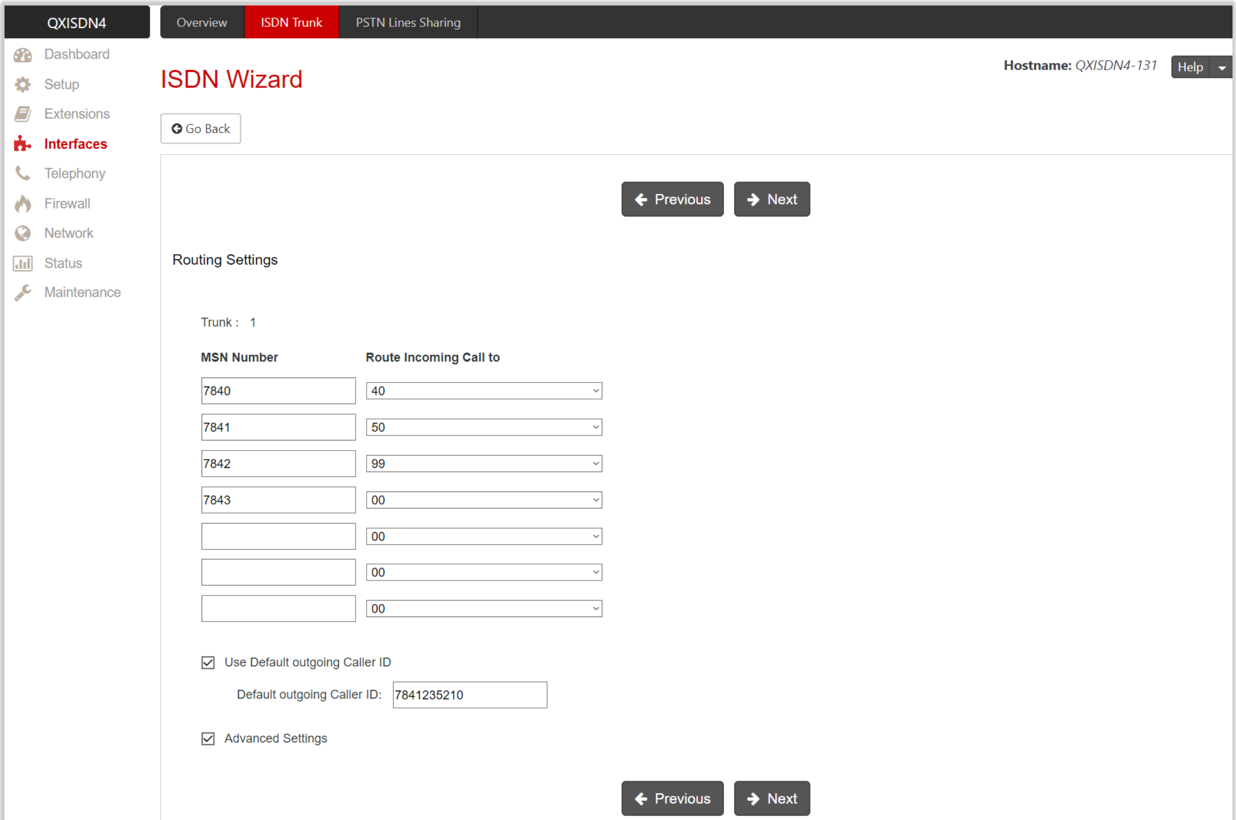


Figure 59: Routing Settings section

ISDN Low Level Settings

This section is used to enable **Power Source** option. This section becomes available only if the selected interface type is **Network**.

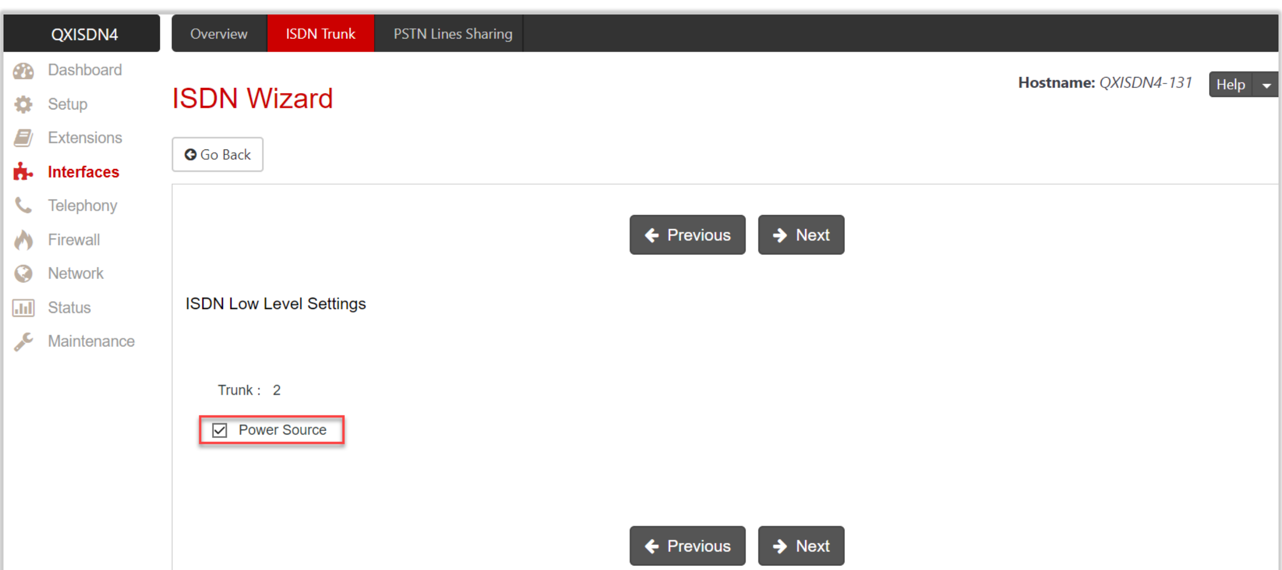


Figure 60: ISDN Low Level Settings section

- **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 connected to the QX.

L2 & L3 Settings

This section is used for advanced configuration of L2 and L3 settings. This section becomes available only if the Advanced Settings checkbox is selected 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 and when timer expires, it initiates the call.
- T309 Timer – this option is responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is 0, T309 timer will be disabled.
- T310 Timer – this option is responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) is not yet arrived.
- Alert Guard Timeout – enter the value for the Alert Guard Timer between CALL PROC and ALERT messages. Alert Guard Timer is used when QX is connected to a slow 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 the B channels. One of the following possibilities of the transmission path completion prior to receipt of a call acceptance indication can be selected:
  - on channel negotiation at the destination interface
  - on progress indication with in-band information
  - on call acceptance

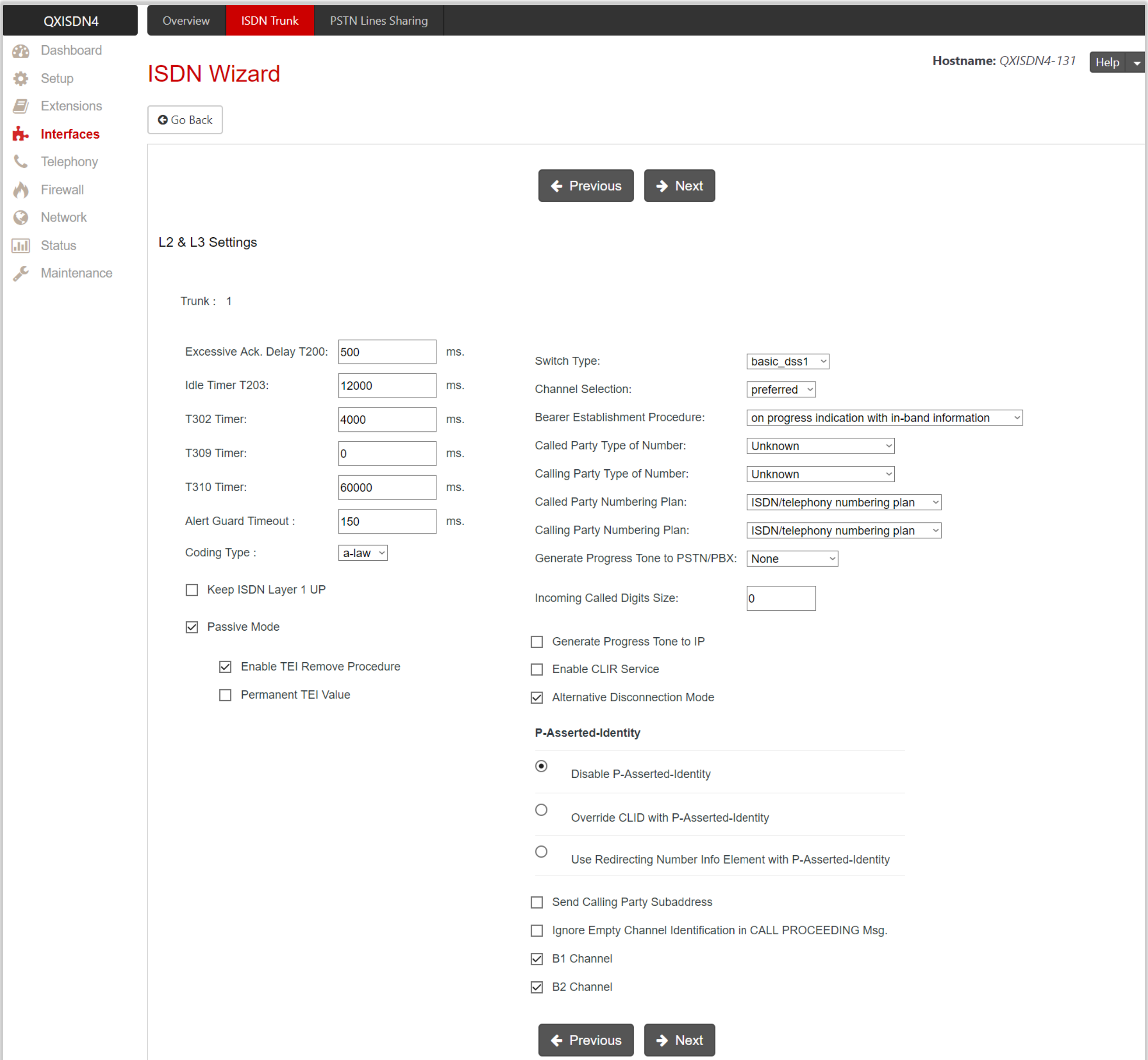


Figure 61: ISDN Low Level Settings section

- **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 call.
- **Called Party Numbering Plan** and **Calling Party Numbering Plan** – indicate correspondingly the numbering plan of the called party and calling party.
- **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** – configures the system to send **ALERT** messages without the **Progress Indicator Information Element**.
  - ➢ **Unconditional** – configures 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** – configures 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, QX's 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 – disables 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 which comes from the identity field. SIP user agent should check for the existence of the P-Asserted-Identity, then the P-Preferred-Identity, then the Remote-Party-ID to fill the identity field. For the calls from ISDN to SIP with restricted Caller ID, the SIP Invite message contains P-Asserted-Identity field with the value from the Caller ID on ISDN. The "SIP From" field contains anonymous.
  - 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 response 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 for the ISDN trunk.

ISDN Status page

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

General Information

This section contains the following components:

- Active Calls – currently active calls.
- Outgoing Calls – total amount of outgoing calls (historical data).
- Incoming Calls – 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 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.

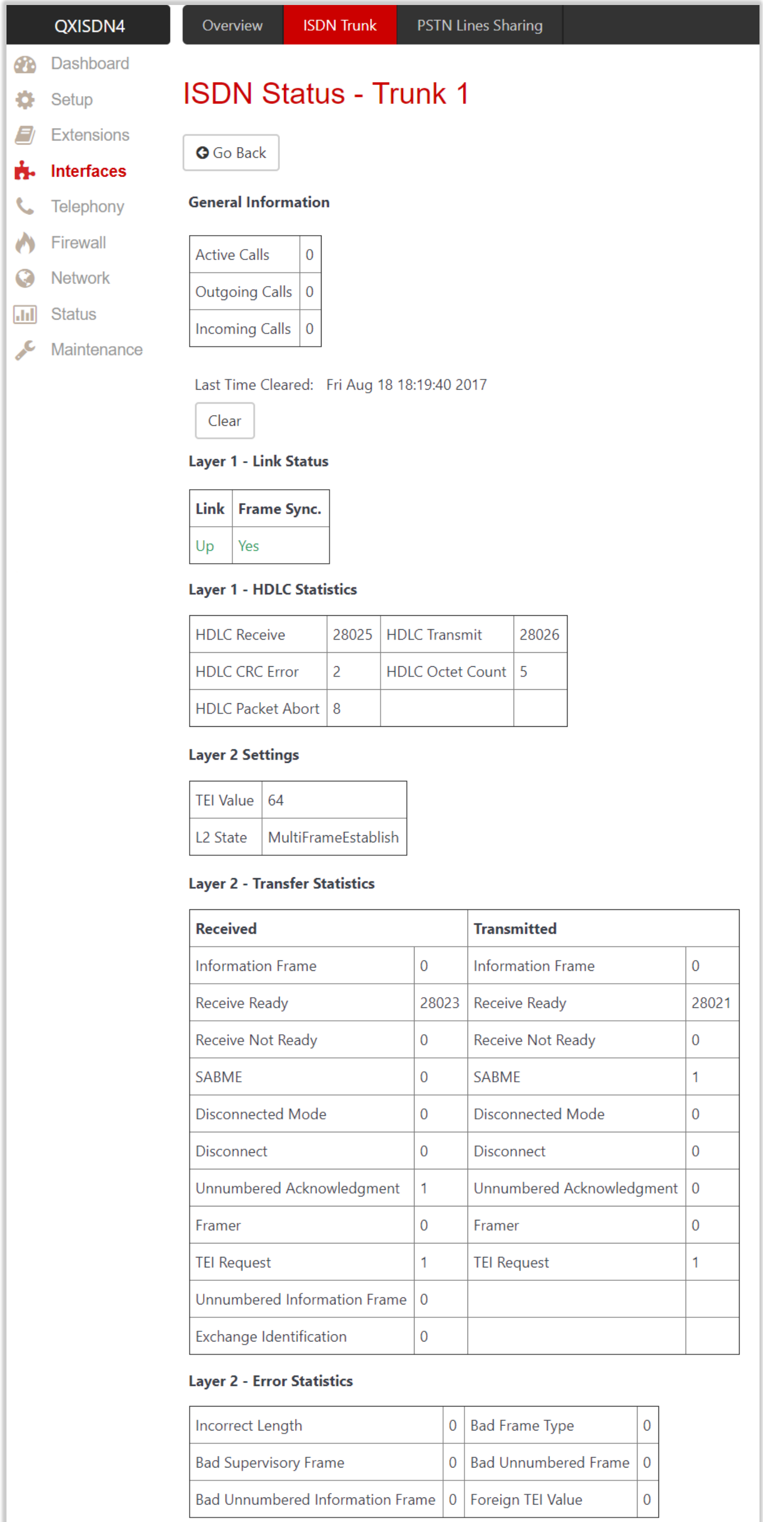


Figure 62: ISDN Status page

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 by destination.
- SABME – shows the packets during connection establishment.
- Disconnected Mode – shows the packets when connection is being terminated.
- Disconnect – shows the packets during connection termination.
- Unnumbered Acknowledgement – shows the packets during accepting connection establishment/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.

7.6 PSTN Gateway Operation Mode

The **PSTN Gateway Operation** page is used to select the PSTN Gateway operational mode.

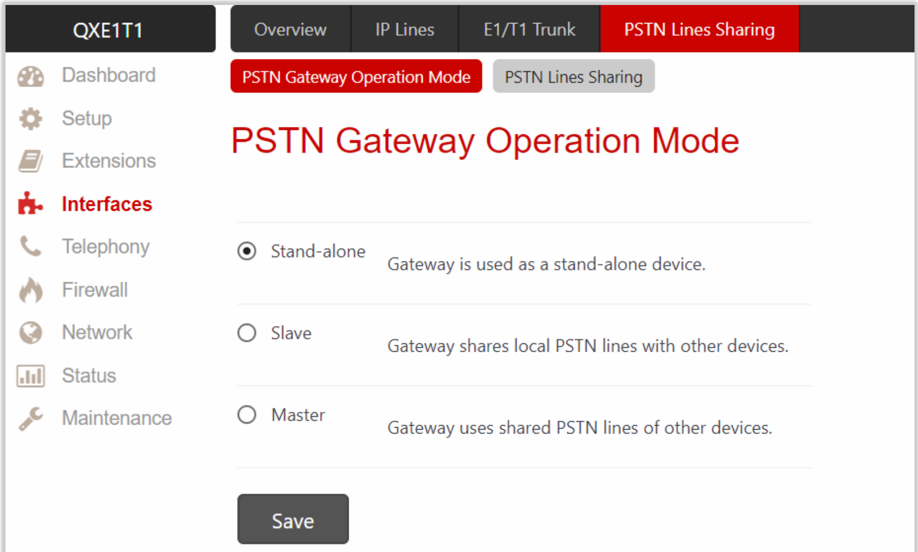


Figure 63: PSTN Gateway Operation Mode page

The following modes are available:

- **Stand-alone** – is used to configure and run the QX as a stand-alone device.
- **Slave** – is used to configure the QX to share local PSTN lines with other device (QX IP PBX or QX Gateway) running un the **Master** mode.
- **Master** – is used to configure the QX to use PSTN lines of the other PSTN Gateways running in the **Slave** mode.

For more information on how to configure and use **QX Gateways** with **QX IP PBXs** in **Share mode**, please refer to the Configuring QX Gateways with QX IP PBXs in Sharing Mode guide.

For more information on how to configure and use QXE1T1 Gateways in Share mode, please refer to the PSTN Lines Sharing Configuration on QXE1T1 Gateways guide.

7.7 PSTN Lines Sharing

The **PSTN Lines Sharing** page is used to allow the QX Gateway either share its PSTN lines (FXO lines, E1T1 and/or ISDN trunks) with another QX Gateway or QX IP PBX. Depending on the selected operation mode, different configuration parameters will appear on this page.

Slave mode

The **PSTN Lines Sharing** page is used to configure the slave QX Gateway with the master QX device. The master QX device (IP PBX or Gateway) will be allowed to make PSTN calls through shared FXO lines, E1T1 or ISDN trunks.

To run the device in slave mode and connect it to the master:

1. Go to the **Interfaces→PSTN Line Sharing→PSTN Gateway Operation Mode** page.
2. Select the **Slave** option and click **Save** to apply changes.
3. Go to the **Interfaces→PSTN Line Sharing→PSTN Line Sharing** page. Enter the following information:

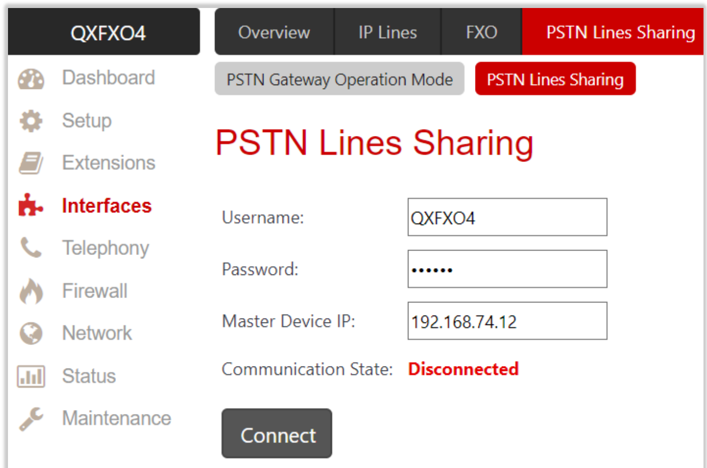


Figure 64: PSTN Lines Sharing (Slave mode) page

- **Username** and **Password** – are used to define the authentication parameters. TIP: The **Username** and **Password** should match on both master and slave devices for the successful PSTN Lines sharing.
- **Master Device IP** – is used to define the IP address of the master device.

4. Click **Connect** to connect the device with the master and start sharing the onboard lines(trunks) with master device. After the slave-master connection successfully established, appropriate routing rules will be created on the **Call Routing Table** for both devices (slave and master) to support PSTN line sharing.
5. Click **Disconnect** to disconnect the device from the master. The corresponding routing rules will be removed, but the device will continue to run in slave mode. Note: To switch off the slave mode completely, navigate to the **Interfaces→PSTN Line Sharing→PSTN Gateway Operation Mode** page and select the **Stand-alone** or **Master**.

Master mode

The PSTN Lines Sharing page is used to create accounts for the slave QX Gateway(s) to connect it to the master QX Gateway for PSTN lines (FXO lines, E1/T1 and/or ISDN trunks) sharing.

Attention: Master gateway can be configured in sharing mode only with the same model of slave gateway(s).

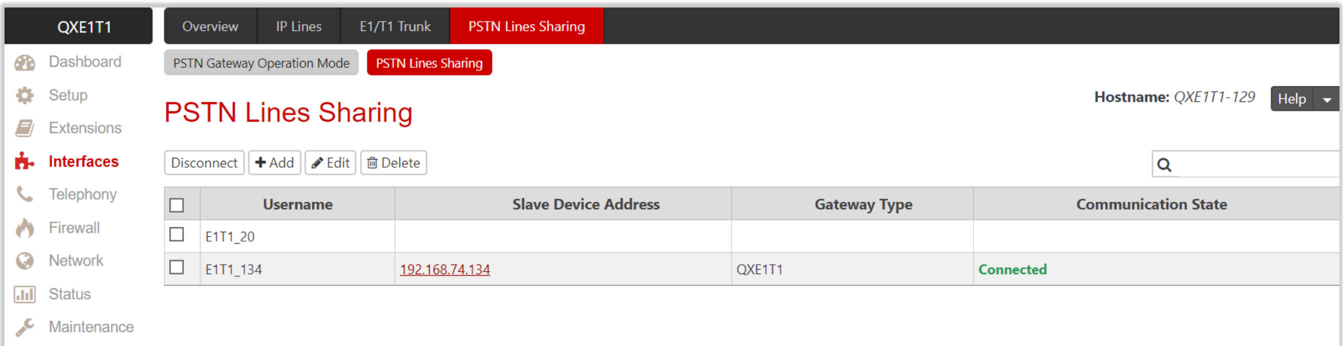


Figure 65: PSTN Lines Sharing (Master mode) page

To run the device in master mode and connect it with slave:

1. Go to the **Interfaces→PSTN Line Sharing→PSTN Gateway Operation Mode** page.
2. Select the **Master** option and click **Save** to apply changes.
3. Go to the **Interfaces→PSTN Line Sharing→PSTN Line Sharing** page.
4. Click **Add** and enter the following information:
   - **Username** and **Password** – are used to define the authentication parameters. TIP: The **Username** and **Password** should match on both master and slave for the successful PSTN Lines sharing.
   - Click **Save**. The new entry will be added to the PSTN Lines Sharing table.
5. The master device will start listening connection requests from slave device. After the slave-master connection successfully established, appropriate routing rules will be created on the **Call Routing Table** for both devices (slave and master) to support PSTN line sharing.
6. Click **Disconnect** to disconnect the slave device from the master. Note: The slave device will not be reconnected automatically. You need to manually reconnect the slave device to master from slave's WEB GUI.

8 Telephony Menu

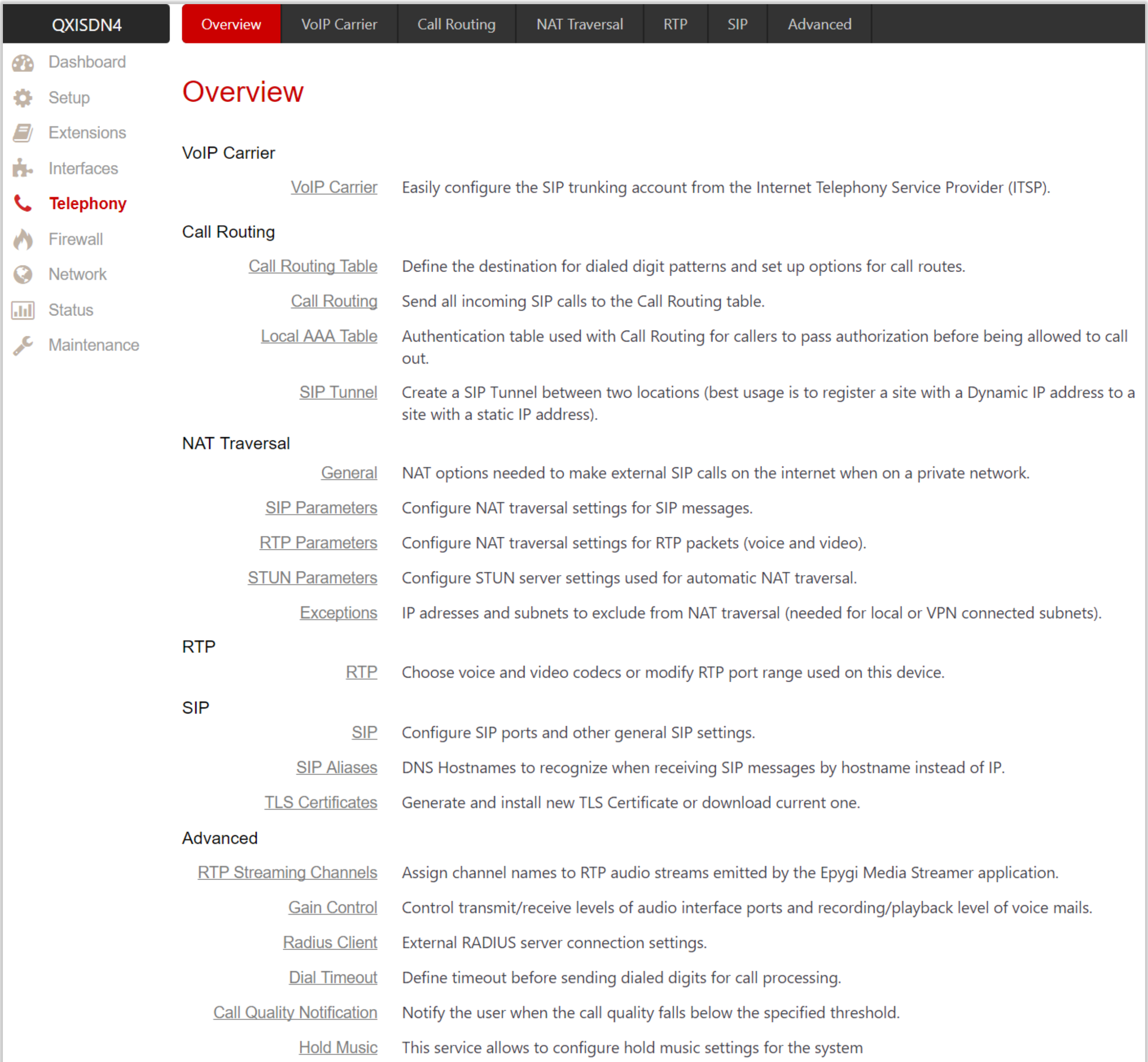


Figure 66: Telephony Menu overview

8.1 VoIP Carrier Wizard

The VoIP Carrier Wizard simplifies the configuration of the QXs with different VoIP SIP trunking services. The wizard is for collecting the data and generating the configuration for each specific VoIP SIP trunking service on the QX. After finishing the wizard, the extensions on the QX will be able to receive calls from the VoIP carrier SIP trunks, as well as to place calls to the PSTN using the carrier SIP trunks.

For each configured VoIP SIP trunking service, the wizard creates a specific IP-PSTN type routing rule in the QX's Call Routing Table. By default, only PBX users can make calls through the corresponding VoIP carrier. Additionally, a virtual extension will be automatically generated in the Extensions Management table and registered on the VoIP Carrier's SIP server. The settings of that extension will be used to make calls towards the created VoIP Carrier SIP Trunks.

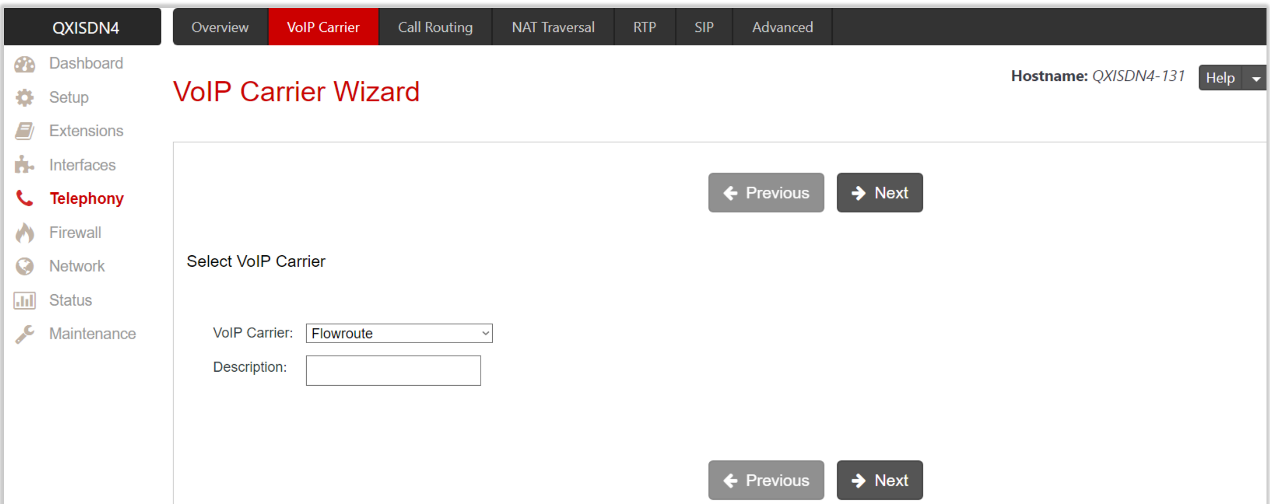


Figure 67: Select VoIP Carrier section

The wizard composed of the following sections:

- Select VoIP Carrier section is used to select a carrier from the VoIP Carrier list. Once a carrier is found and selected, the carrier's 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 section is used to define and configure the account from provider.
  - Authentication by IP Address – if selected, deactivates the Account Name and Password fields, thus allow skipping the IP address authentication settings. This option is intended for VoIP carriers requiring IP address authentication instead of account authentication and will be available if Manual has been selected in the previous section.
  - Account Name – enter the username for authentication on the carrier's SIP server.
  - Password – enter the password for authentication on the carrier's SIP server and confirm it in the Confirm Password field.
  - SIP Server – enter the IP address or hostname for the carrier's SIP server.
  - SIP Server Port – enter the SIP server port for the carrier's SIP server.
  - Use RTP Proxy – if selected, the RTP 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 VoIP Carrier from a peer located outside the QX.

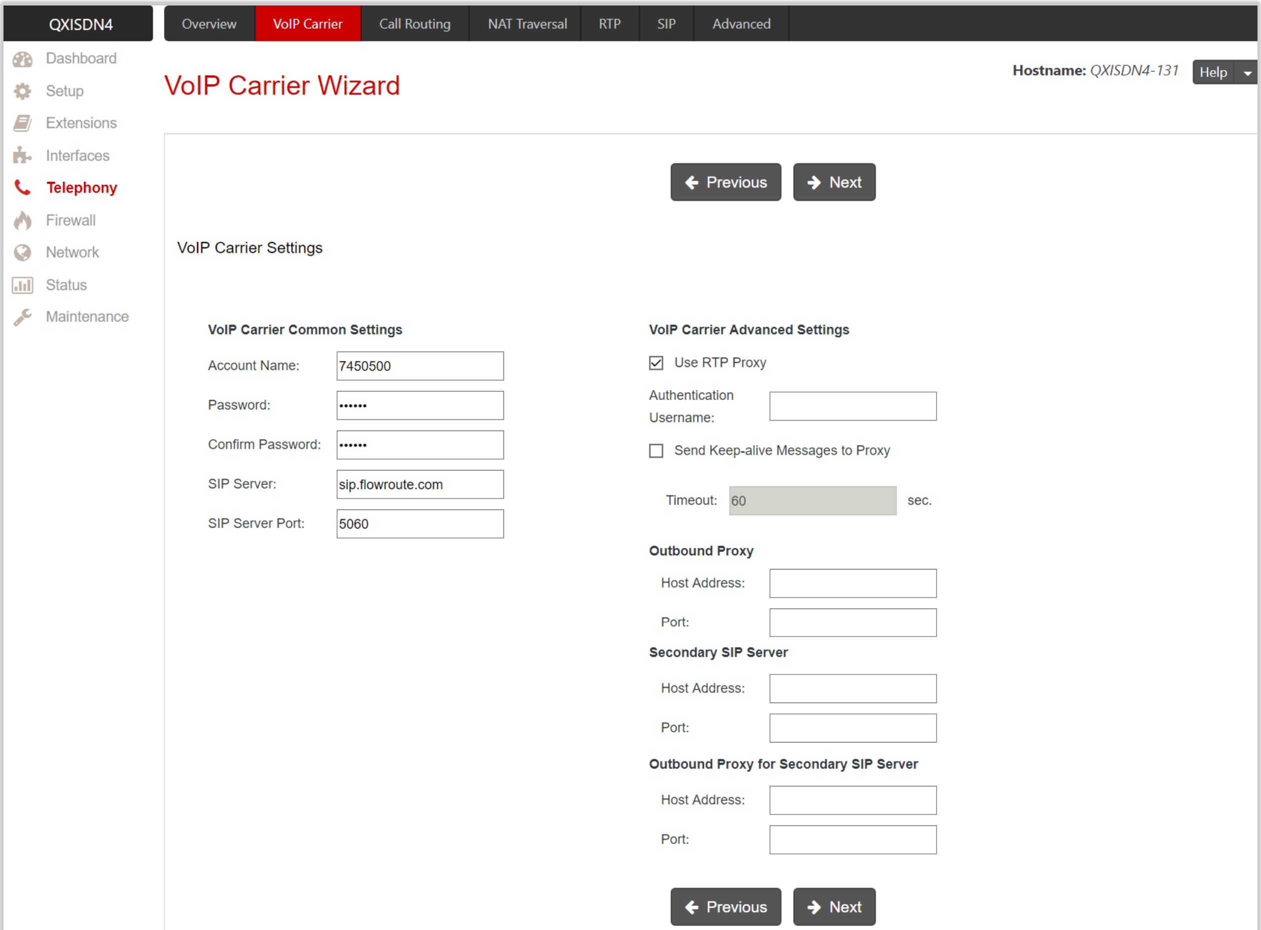


Figure 68: VoIP Carrier Settings section

- Authentication Username – enter an identification parameter to reach the SIP server. It should be provided by the SIP trunking service provider and can be requested only for certain SIP servers. For others, the field should be left empty.
- Send Keep-alive Messages to Proxy – enables the SIP registration server accessibility to the verification mechanism. The Timeout field is used to define the timeout between two attempts of SIP registration server accessibility verification. If a reply is not received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will continue to be sent to the server.
- 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 provider and are used by the QX to reach to the selected SIP servers.

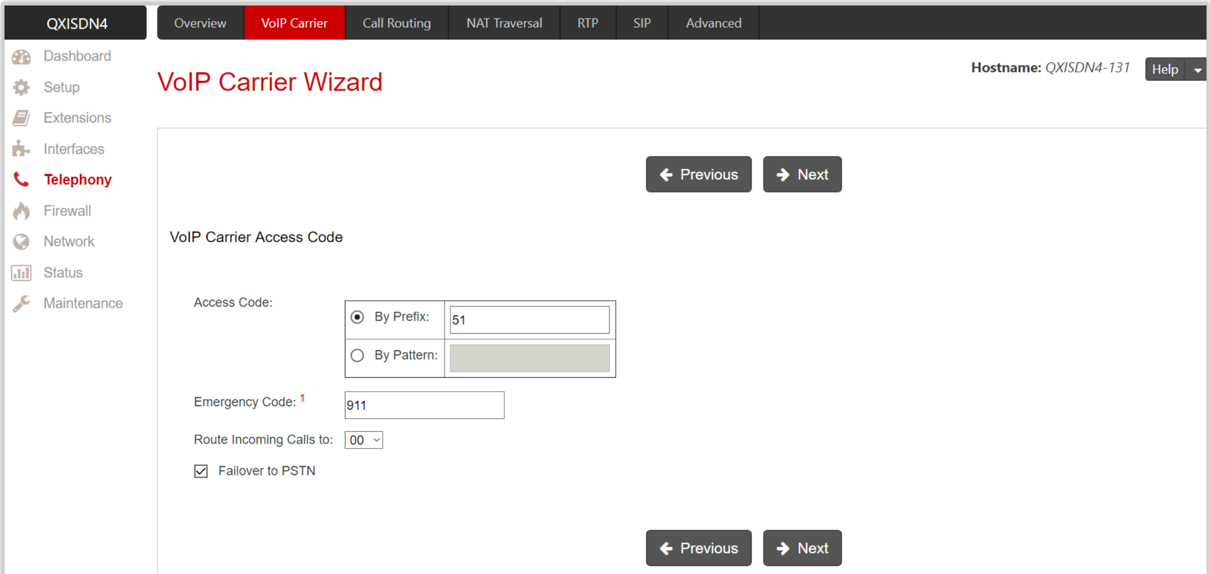
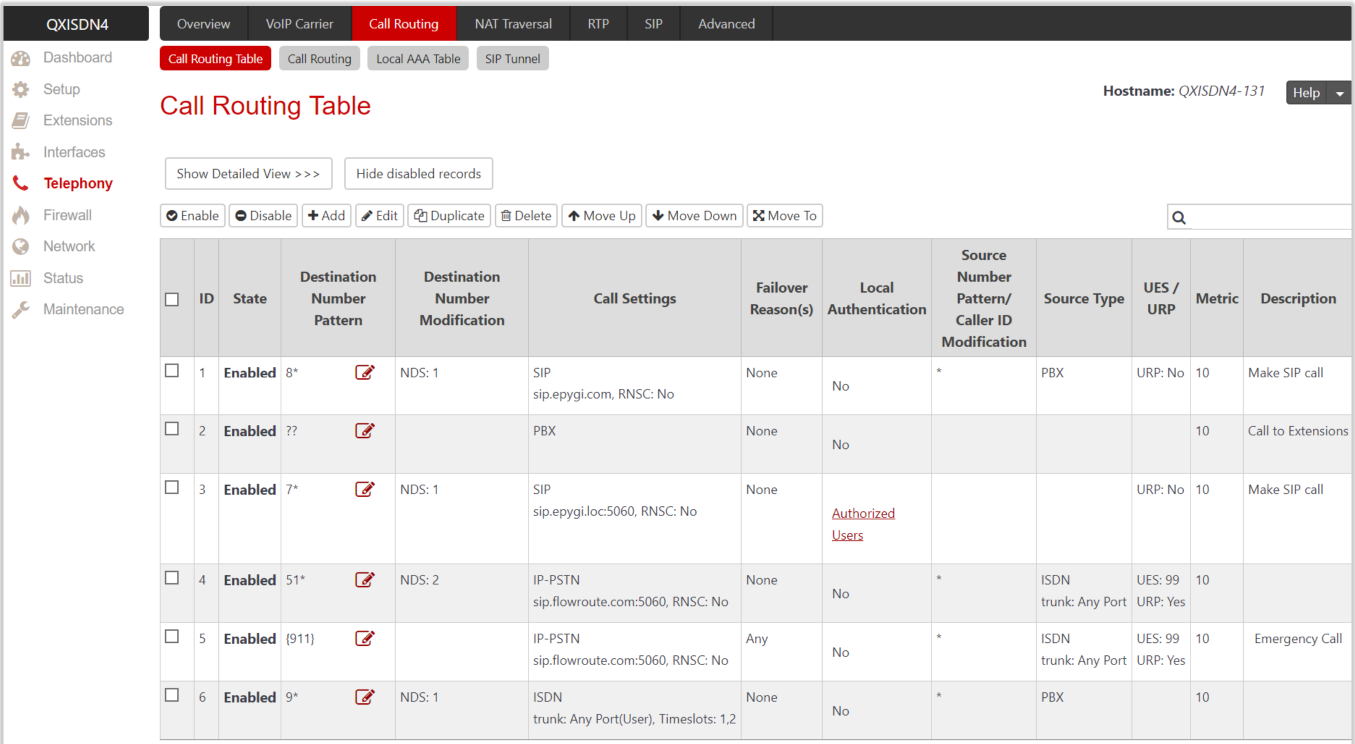


Figure 69: VoIP Carrier Access Code section

- VoIP Carrier Access Code section is used to define the routing rules for outbound/inbound calls through VoIP carrier SIP trunks.
  - Access Code – defines the routing rule for outbound calls.
    - By Prefix – is used for entering the numeric prefix that should be dialed to route call through carriers SIP trunks. The system will route all digits matching this prefix to the carriers SIP trunks.
    - By Pattern – is used to specify the pattern that should be applied to dialed digits. If an outbound call has a destination number that matches the specified pattern, it will be completed according to the current rule. A routing pattern may contain wildcards.
  - Emergency Code – enter the emergency code supported by the specified VoIP provider. 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 – select an extension (user extension or Auto Attendant) on the QX where the incoming calls from the configured VoIP Carrier should be routed to. There will be an unconditional forwarding set up automatically which will care for incoming calls forwarding 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 VoIP Carrier SIP trunks are not available.

8.2 Call Routing Table

The **Call Routing Table** lists the settings of all call routing records (rules) either generated by default, or added automatically with one of the QX's system wizards: **Call Routing Wizard** and **VoIP Carrier Wizard**.



	ID	State	Destination Number Pattern	Destination Number Modification	Call Settings	Failover Reason(s)	Local Authentication	Source Number Pattern/ Caller ID Modification	Source Type	UES / URP	Metric	Description
☐	1	Enabled	8*	NDS: 1	SIP sip.epygi.com, RNSC: No	None	No	*	PBX	URP: No	10	Make SIP call
☐	2	Enabled	??		PBX	None	No				10	Call to Extensions
☐	3	Enabled	7*	NDS: 1	SIP sip.epygi.loc:5060, RNSC: No	None	Authorized Users			URP: No	10	Make SIP call
☐	4	Enabled	51*	NDS: 2	IP-PSTN sip.flowroute.com:5060, RNSC: No	None	No	*	ISDN trunk: Any Port	UES: 99 URP: Yes	10	
☐	5	Enabled	{911}		IP-PSTN sip.flowroute.com:5060, RNSC: No	Any	No	*	ISDN trunk: Any Port	UES: 99 URP: Yes	10	Emergency Call
☐	6	Enabled	9*	NDS: 1	ISDN trunk: Any Port(User), Timeslots: 1,2	None	No	*	PBX		10	

Figure 70: Call Routing Table (brief view)

The following components are available:

- **Show Brief View** – if pressed, displays the most important settings of the entries in the **Call Routing Table.**
- **Show Detailed View** – if pressed, displays all settings of the entries in the **Call Routing Table.**
- **Hide disabled records/Show all records** – are used to hide/show disabled records respectively.
- **Enable** – enables (activate) the selected route(s).
- **Disable** – disables (deactivate) the selected route(s).
- **Add** – leads to the **Call Routing Wizard – Add Entry** page to configure a new routing pattern.
- **Duplicate** – creates a routing pattern with the settings duplicated from the selected one.
- **Move Up/Move Down** – moves the selected call routing record one position up/down.
- **Move To** – moves the selected record to specified position.
- **Local Authentication** – if selected, displays Authorized Users link for the selected routing rule.

For more information on how to configure and use routing rules , please refer to the Call Routing on QX IP PBXs guide.

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.

1. If the dialed number matches only with a single pattern, then the record with respective pattern will be used to set up the call.
2. If multiple patterns have been found to match the dialed number, the QX uses the Best Matching Algorithm to prioritize the matching patterns.
3. Once the patterns are prioritized, the record having pattern of the highest priority will be used as a preferred route for call setup.

The **Add** button starts the **Call Routing Wizard** for configuring a new call routing record. In general, the Wizard passes through the following sections:

- Destination Call Type
- Call Settings
- Filter on Source / Modify Caller ID
- Date / Time Settings
- Overall Calls Duration Limit
- Tracing / Debug Options
- Summary

Destination Call Type

This section contains the following components:

- **Enable Record** – this checkbox disables/enables the routing record. By default, the record is enabled.
- **Destination Number Pattern** – specifies a template for filtering out the calls that can be routed via respective call routing record. If destination number of the call matches with specified pattern, then the call can be completed via respective call routing record. The **Destination Number Pattern** may contain wildcards.
- **Number of Discarded Symbols** – specifies the number of symbols/digits/characters that shall be removed from the beginning of the destination number after matching it against the destination number pattern. The field should be empty if no symbols need to be discarded.
- **Prefix** – specifies the symbols/digits/characters that will be added in front of the destination number after discarding the 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 3rd digit and up to the end will be assigned to prefix.
  - **<dialednum: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 3rd 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/T1destination types.
- **Suffix** – specifies the characters that will be added to destination number from the end after discarding the 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 (N/A for QXFXS24) – local call to QX's extension.

- SIP – calls through a SIP server.
- SIP_Tunnel – calls through an established SIP tunnel.
- IP-PSTN (N/A for QXFXS24) – calls through the IP-PSTN provider to the global PSTN network.
- FXO – calls to the PSTN network through on-board FXO lines (available only for QXFXO4).
- ISDN – calls to the PSTN network through ISDN trunks (available only for QXISDN4).
- E1/T1 – calls to the PSTN network through E1/T1trunk(s) (available only for QXE1T1).

- Metric – is used to enter a rating for the selected route in a range from 0 to 20. If no value is entered into this field, 10 will be used as the default. If two route entries match a user's dial string, the route with the lower metric will be chosen.
- Enabler Key and Disabler Key (N/A for QXFXS24)– is a digital code which should be dialed from handset or the 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 routing rule, and as disabler for another one) – this will allow managing several routing rules with the single key.
  - Require Authorization for Enabling/Disabling – is used to enable administrator's password (Phone Access Password) authentication when enabler/disabler keys are configured for a certain routing rule. The service can be used locally from the handset or remotely on the Auto Attendant. When this checkbox is selected, the password will be requested to enable/disable the certain routing rule(s). TIP: If the password has been entered incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.

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 define a validity period(s) for the routing pattern by setting date/time rules.
- Overall Call Duration Limit – allows to control and limit the total calls duration for the routing pattern.
- Tracing / Debug Options – allows to enable/disable generating event notifications on the result of using the routing rule.

Call Settings

The content of this section strictly depends on the Call Type selected on the previous section.

Call Type – PBX

- Local Authentication – if selected, the caller(s) will need to pass an authorization to make PBX calls.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching pattern(s) regardless of the failover.
  - Busy – the system will use next matching pattern(s) if the dialed destination is busy.
  - Wrong Number – the system will use next matching pattern(s) if the dialed number is wrong.
  - Any – the system will use next matching pattern(s) regardless the failover reason.

Call Type – SIP

- Use Extension Settings – is used to select the extension (also Auto Attendant) on behalf of which the call will be placed. The SIP settings of the selected extension will be used as the 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's 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 renamed to Modified Destination Host if the Destination Number Pattern field (in the wizard's first page) contains "@" symbol.
- Destination Port – is the port number of the destination or the SIP server. TIP: This field renamed Modified Destination Port if the Destination Number Pattern field (in the wizard's first page) contains "@" symbol.
- Username and Password – is used to define 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 define the number of simultaneous calls.
- Use RTP Proxy – if selected, the RTP streams between peers will be routed through the QX. This is applicable when the peers are both located outside the QX. If not selected, the RTP streams will move directly between peers. Voice Transcoding is used to convert the RTP stream to different codec before transmitting to the destination.
- Single Call Duration Limit – is used to limit the duration of the call placed through the routing rule. The single call duration will be unlimited If the checkbox is not selected. Maximum Duration is used to define the maximum duration of the call (in seconds). 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 an authorization to make SIP calls.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching pattern(s) regardless of the failover.
  - Busy – the system will use next matching pattern(s) if the dialed destination is busy.
  - Wrong Number – the system will use next matching pattern(s) if the dialed number is wrong.
  - Network Failure – the system will use next matching pattern(s) when system overload, network failure or timeout expiration occurred.
  - System Failure – the system will use next matching pattern(s) if indicates one of cases in the Network Failure or Other fail reason groups.
  - Other – the system will use next matching pattern(s) if indicates cases when authorization, negotiation, not supported, request rejected or other unknown errors occur.
  - Any – stands for all failure reasons mentioned in the Failover Reason(s) group.
- Enable Failover Timeout – is used to define the period after which the call could be considered as failed (SIP response message isn't received). The Failover Timeout is used to define the timeout duration (in the range from 1 to 180 seconds). The call will be established through next matching pattern(s) after the timeout expired if the failover reason is enabled for the 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 for the corresponding route. Selection enables a group of checkboxes to choose the key headers to be fully or partly hidden or replaced. Require Privacy checkbox 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 the destination.
- Transport Protocol for SIP messages – is used to select the transport protocol (UDP, TCP or TLS) for transmitting the SIP messages.

<u>Call Type – SIP Tunnel</u>

- Use Extension Settings – is used to select the extension (also Auto Attendant) on behalf of which the call will be placed. The SIP settings of the selected extension will be used as the caller information. If an entry is not selected from this list, the original caller information will be kept.
- Keep Original Caller ID – if selected, the called destination will receive the original caller's information.
- Add Remote Party ID – if selected, the Remote Party ID parameter will be added in the outgoing Invite message.
- SIP Tunnel – is used to select the previously configured SIP tunnel to route the calls through tunnel to the remote QX device (QX IP PBXs and QX Gateways).
- Use RTP Proxy – is applicable when a route is used for calls through QX between peers that are both located outside the QX. RTP streams between the peers will be routed through QX if the checkbox selected, otherwise the RTP packets will move directly between peers. Voice Transcoding is used to convert the RTP stream to different codec before transmitting to the destination.
- Single Call Duration Limit – is used to limit the duration of the call placed through the routing rule. The single call duration will be unlimited if the checkbox is not selected. Maximum Duration is used to define the maximum duration of the call (in seconds). The call will be disconnected without prior notice if the maximum duration is reached.
- Local Authentication – if the checkbox selected, the caller(s) will need to pass authorization to make SIP call through the tunnel.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching pattern(s) regardless of the failover.
  - Busy – the system will use next matching pattern(s) if the dialed destination is busy.
  - Wrong Number – the system will use next matching pattern(s) if the dialed number is wrong.
  - Network Failure – the system will use next matching pattern(s) if the system overload, network failure or timeout expiration occurred.
  - System Failure – the system will use next matching pattern(s) if indicates one of cases in the Network Failure or Other fail reason groups.

- Other – the system will use next matching pattern(s) if the authorization request rejected or other unknown errors occur.
- Any – the system will use next matching pattern(s) regardless the failover reason.

- Enable Failover Timeout – is used to define the period after which the call could be considered as failed (SIP response message isn't received). The Failover Timeout is used to define the timeout duration (in the range from 1 to 180 seconds). The call will be established through next matching pattern(s) after the timeout expired if the failover reason is enabled for the 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.
  - Default Privacy – if selected, QX specific SIP privacy will not be applied and all privacy will rely on the configuration of the SIP Server.
  - Disable Privacy – if selected, SIP call security will be disabled and all headers of the SIP message will be transparently visible to the destination.
  - Enable Privacy – if selected, QX specific SIP privacy will be specified for the corresponding route. Selection enables a group of checkboxes to choose the key headers to be fully or partly hidden or replaced. Require Privacy 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 the destination.
- Transport Protocol for SIP messages – is used to select the transport protocol (UDP, TCP or TLS) for transmitting the SIP messages.

Call Type – IP-PSTN

- Use Extension Settings – is used to select the extension (or Auto Attendant) on behalf of which the call will be placed. The SIP settings of the selected extension will be used as the caller information. If an entry is not selected from this list, the original caller information will be kept.
- Keep Original Caller ID – if selected, the called destination will receive the original caller's 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 the hostname of the destination (for a direct call) or the SIP server (for calls through the SIP server). TIP: This field renamed to Modified Destination Host if the Destination Number Pattern field (in the wizard's first page) contains "@" symbol.
- Destination Port – is the port number of the destination or the SIP server. TIP: This field renamed Modified Destination Port if the Destination Number Pattern field (in the wizard's first page) contains "@" symbol.
- Username and Password – is used to define the authentication parameters for 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 define the number of simultaneous calls.
- Enable Failover Timeout – is used to define the period after which the call could be considered as failed (SIP response message isn't received). Failover Timeout is used to define the timeout duration (in the range from 1 to 180 seconds). The call will be established through next matching pattern(s) after the timeout expired if the failover reason is enabled for the routing rule.
- Use RTP Proxy – if selected, the RTP streams between peers will be routed through the QX. This is applicable when the peers are both located outside the QX. If not selected, the RTP streams will move directly between peers. Voice Transcoding is used to convert the RTP stream to different codec before transmitting to the destination.
- Single Call Duration Limit – is used to limit the duration of the call placed through the routing rule. The single call duration will be unlimited If the checkbox is not selected. Maximum Duration is used to define

the maximum duration of the call (in seconds). 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 an authorization to make calls.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching pattern(s) regardless of the failover.
  - Busy – the system will use next matching pattern(s) if the dialed destination is busy.
  - Wrong Number – the system will use next matching pattern(s) if the dialed number is wrong.
  - Network Failure – the system will use next matching pattern(s) if the system overload, network failure or timeout expiration occurred.
  - System Failure – the system will use next matching pattern(s) if indicates one of cases in the Network Failure or Other fail reason groups.
  - Other – the system will use next matching pattern(s) if the authorization request rejected or other unknown errors occur.
  - Any – the system will use next matching pattern(s) regardless the failover reason.
- 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.
  - Default Privacy – if selected, QX specific SIP privacy will not be applied and all privacy will rely on the configuration of the SIP Server.
  - Disable Privacy – if selected, SIP call security will be disabled and all headers of the SIP message will be transparently visible to the destination.
  - Enable Privacy – if selected, QX specific SIP privacy will be specified for the corresponding route. Selection enables a group of checkboxes to choose the key headers to be fully or partly hidden or replaced. Require Privacy checkbox 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 the destination.
- Transport Protocol for SIP messages – is used to select the transport protocol (UDP, TCP or TLS) for transmitting the SIP messages.

Call Type – FXO

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

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

  - Any Available Line – the call will be established through the first available on-board FXO lines 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 the selected shared FXO line.
- FXO Lines Load Balancing – is used to enable load balancing mechanism on the 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 the 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).

- Local Authentication – if selected, caller(s) will need to pass an authorization to make FXO calls.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching 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 pattern(s) regardless the failover reason.

Call Type – ISDN

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

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

  - Any Trunk(User)@Any – the 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 – the 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#@ – the calls will be established through the selected shared ISDN trunk.
  - Any Trunk(User)@ – the calls will be established through the first available shared ISDN trunks running in User mode.
  - Any Trunk(Network)@ – the calls will be established through the first available shared ISDN trunks 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's.
- Local Authentication – if selected, the caller(s) will need to pass an authorization to make ISDN calls.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - None – the system will not use next matching 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 pattern(s) regardless the failover reason.

Attention: 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

- Keep Original Caller ID – if selected, the called party will receive the original caller's information (mobile number, PSTN/SIP number, etc.) instead of extension's information when the call(s) are forwarded.
- E1/T1 Trunks to Use – is used to select a specific shared E1/T1 trunk to route the call(s). The following option is available:
  - ➢ E1/T1 Trunk1 – the calls will be established through the on-board E1/T1 trunk.

If another QXE1T1 gateway is connected to the QX in share mode, the following option will be available:

- ➢ E1/T1 Trunk1@ – the call will be established through the selected shared 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's.
- Single Call Duration Limit – if selected, puts a limit on the duration of the call placed through the routing rule, otherwise the call duration will be unlimited. Maximum Duration is used to define the maximum duration of the call (in seconds).
- Local Authentication – if selected, the caller(s) will need to pass authorization to make E1/T1 call.
- Client Code Identification – if selected, the code identification service will be activated: a caller, after dialing the destination phone number, may optionally enter * and then an 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 (Call Detail Reports) and might be used by a billing program for grouping the calls having the same Identity Code.
- Failover Reason(s) – the system will use next matching pattern(s) to establish the call if the call setup fails due to below presented failover reasons:
  - ➢ None – the system will not use next matching 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 pattern(s) regardless the failover reason.

Attention: 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 the trunk signaling type.
  - ➢ 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

RADIUS Authentication and Authorization options are available for the routing pattern regardless destination call type if a RADIUS client is enabled.

- RADIUS Authentication and Authorization – is used to make the caller(s) pass the authorization through the RADIUS server to make calls.
- RADIUS Accounting – if selected, no authentication will take place, except for CDRs (call detail reports) of the calls made through this routing record will be sent to the RADIUS server. This checkbox selection enables the Client Code Identification checkbox. If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and password.

Filter on Source / Modify Caller ID

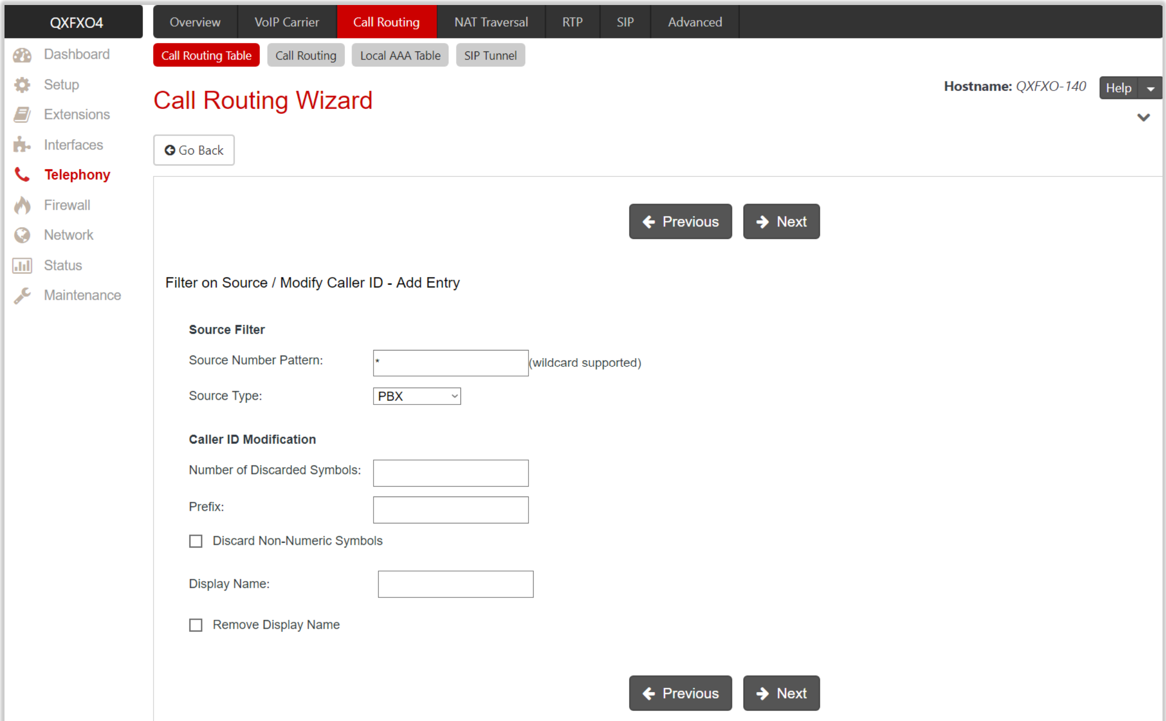


Figure 71: Filter on Source / Modify Caller ID section

The following components are available:

- Source Filter – is used to limit the routing pattern availability for selected caller(s).
  - Source Number Pattern – enter the caller address for which the routing pattern will be available. The Source Number Pattern may contain wildcards.
  - 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 caller source type.
    - PBX – only PBX extension(s) will be able to make calls.
    - SIP – only inbound SIP caller(s) will be able to make calls. To configure Source Host address (IP address or hostname) for SIP call type, an additional wizard page will be available.
    - SIP_Tunnel – only inbound callers from the selected SIP_Tunnel will be able to make calls. To select Inbound SIP Tunnel, an additional wizard page will be available.
    - FXO – only inbound FXO caller(s) will be able to make calls. To select Port ID for FXO call type, an additional wizard page will be available.
    - ISDN – only inbound ISDN caller(s) will be able to make calls. To select Port ID for ISDN call type, an additional wizard page will be available.
    - E1/T1 – only inbound E1/T1 caller(s) will be able to make calls. To select Port ID for E1/T1 call type, an additional wizard page will be available.
- Caller ID Modification – is used to modify the Caller ID before sending them to remote party.
  - Number of Discarded Symbols – enter the number of digits that should be discarded from the beginning of the Source Number Pattern. Left the field empty if no need to discard the digits.
  - Prefix – enter the symbols that will be placed in front of the Source Number Pattern. The Prefix may contain wildcards.
  - Discard Non-Numeric Symbols – is used to discard any non-numeric symbols from the Source Number Pattern.
  - Display Name – is used to replace an original caller's ID with the custom display name.
  - Remove Display Name – is used to remove caller IDs.

Date / Time Settings

The section is used to define a validity period(s) for the routing pattern:

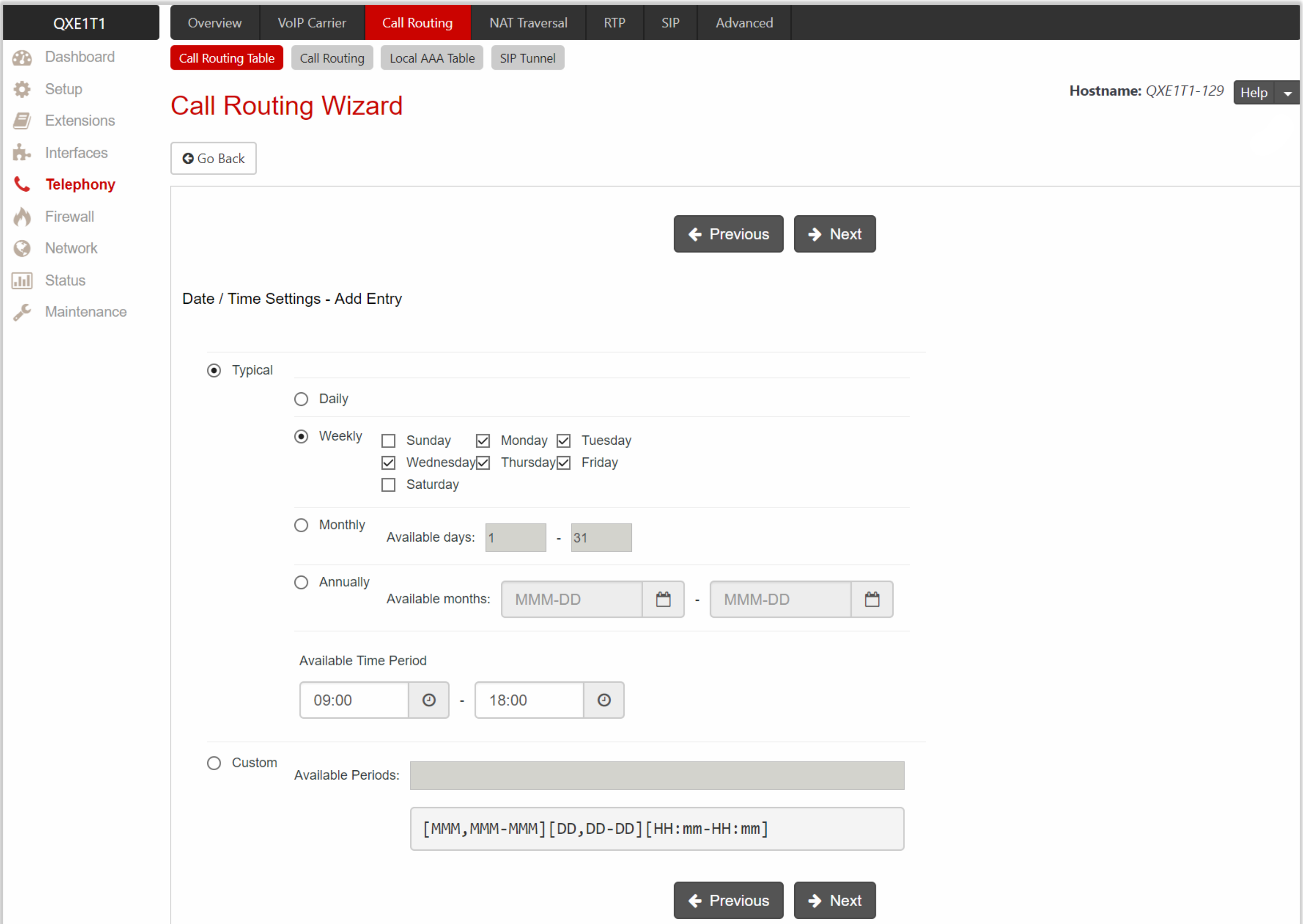


Figure 72: Date / Time Setting section

- 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 define the validation time range for the routing pattern. The defined time here will be checked against QX's time.
- Custom – is used to manually define the validity period(s). TIP: The entered values needs to be in the following format [MMM,MMM-MMM][DD,DD-DD][HH:mm-HH:mm].

Overall Calls Duration Limit

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

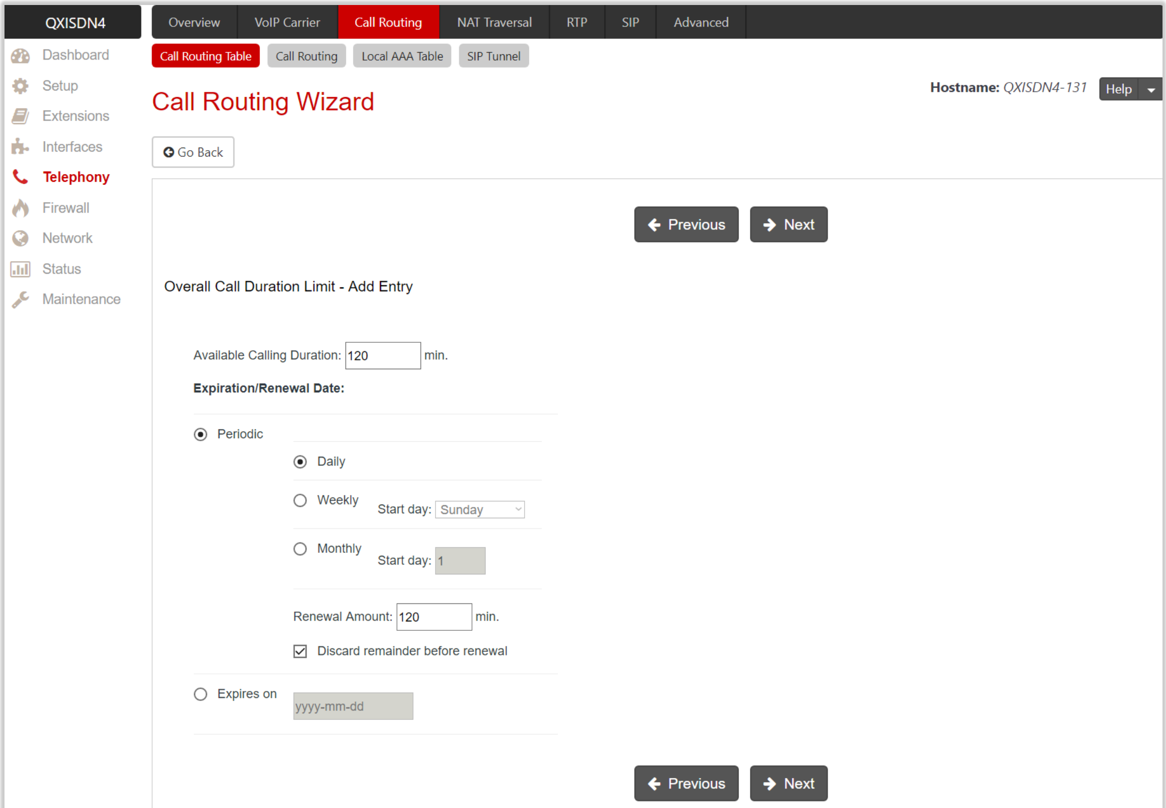


Figure 73: Overall Call Duration Limit section

- Available Calling Duration – define the total duration for the calls (in minutes) through the selected routing rule. Once the Available Calling Duration expires, the current call will be disconnected without prior notice. Placing new calls through this rule is not possible until the Available Calling Duration is not 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 Calling Duration will be renewed every day.
  - Weekly – the defined Available Calling Duration will be renewed every week on the specified weekday.
  - Monthly – the defined Available Calling Duration will be renewed every month on the specified day.
  - Renewal Amount – enter the renewal amount (in minutes) to be added to the available calling duration when the expiration date of the Available Calling Duration is reached. Leave the field empty, if you don't need to renew the Available Calling Duration.
  - Discard remainder before renewal – is used to discard the remainder of Available Calling Duration before renewal and set the Renewal Amount as the new Available Calling Duration.
- Expires on – is used to define the expiration date for the Available Calling Duration. After the Expiration Date, the routing rule becomes unavailable automatically and no new call will be possible until this field is updated.

Note: The Overall Call Duration Limit is not applicable for PBX call type.

Tracing / Debug Options

These options are used to generate event notifications on the certain execution result for the routing rule. The events will be generated and displayed in the **System Events** for the following cases:

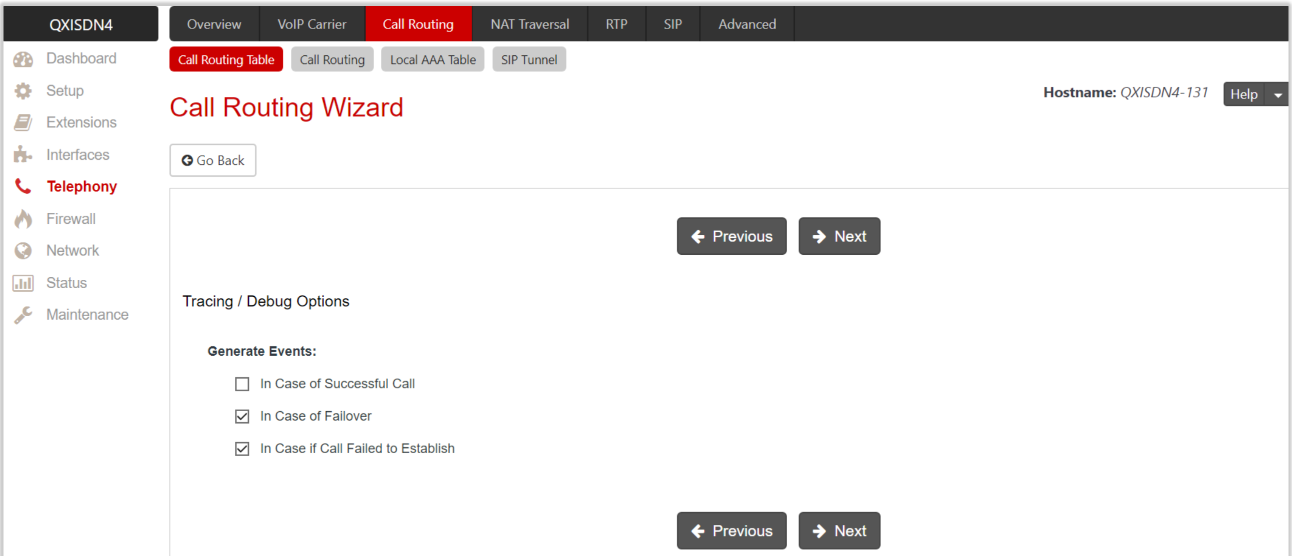


Figure 74: Tracing / Debug Options section

- **In Case of Successful Call** – when a call was successful established with the routing rule.
- **In Case of Failover** – when the call ends up due to one of the selected failover reasons.
- **In Case if Call Failed to Establish** – when the call executed through the routing rule failed.

Summary

The **Summary** section displays all configured settings for the routing pattern before applying them.

8.3 Call Routing

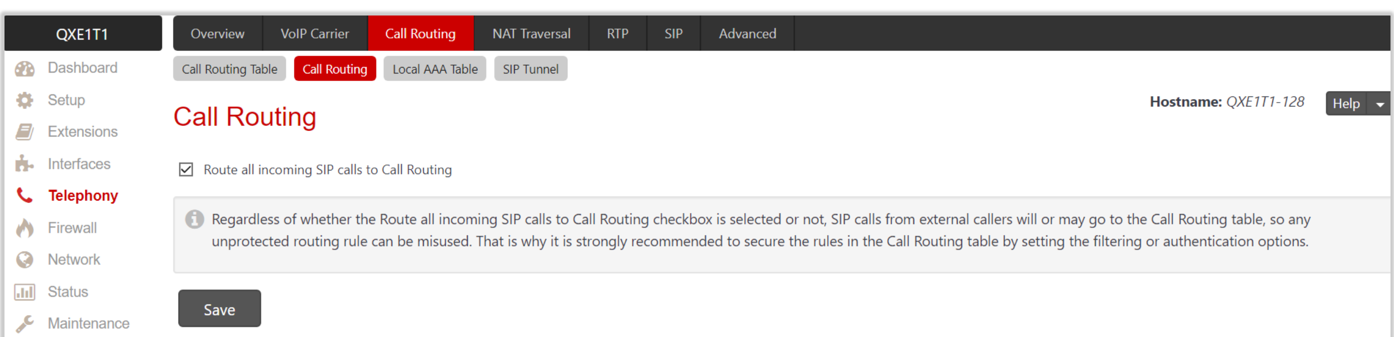


Figure 75: Call Routing page

Route all incoming SIP calls to Call Routing – if not selected, the system will first search the incoming SIP address (Username or DID Number) in the Extensions Management table. If matching occurred, the incoming SIP call will ring on the corresponding extension, otherwise the system will look for a matching routing rule in the **Call Routing Table**. If this option is selected, the system will directly look for a matching routing rule in the Call Routing Table and ignore the possible matches in the **Extensions Management** 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 routing rule can be misused. That is why it is strongly recommended to secure the rules in the Call Routing Table by setting the filtering or authentication options.

8.4 Local AAA Table

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

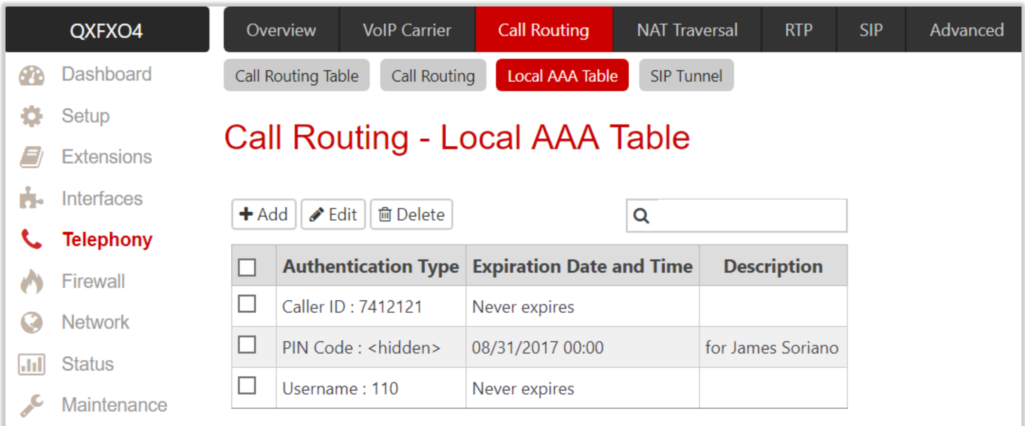


Figure 76: Call Routing – Local AAA Table page

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 – set the authentication based on the caller's phone number or SIP username (which is considered to be automatically detected).
   - Authentication by Login – set the authentication based on the Username and Password provided by the user upon login.
   - Authentication by PIN – 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 – select to enable the Expiration Date and Time option and define the expiration date for the configured local AAA entry.
4. Enter any Description, if needed.
5. Click Save, the new AAA entry will be added to the Local AAA table.

Authorized Users

Caller(s) have to pass an authorization if the AAA option is enabled on the routing pattern. The caller will automatically pass the authorization if the caller's phone number or SIP username is enabled in the Authorized Users table, otherwise will be asked to login (enter username and password) or enter the PIN Code.

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

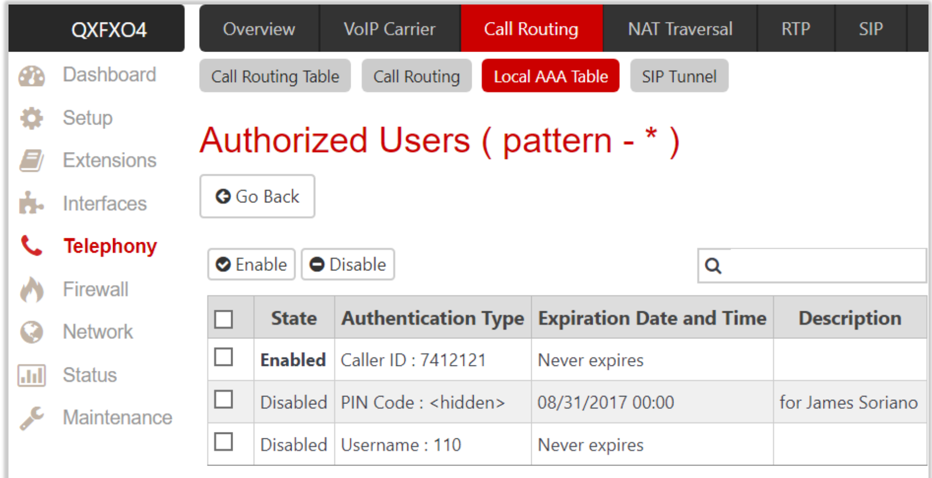


Figure 77: Authorized Users page

Allowed Characters and Wildcards

The following is the complete list of the characters and wildcards supported in the QX system. Not all characters and wildcards are supported for all QX 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
- 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. 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. 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. 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. 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.

Best Matching Algorithm

Each call through and within a QX are made according to call routing patterns that specify a destination based on a dialed number. When a user dials a number, the QX matches the dialed number against the existing routing patterns.

1. If the dialed number matches only to a single pattern, this pattern will be used to set up the call.
2. If multiple patterns have been found to match the number, the QX uses the Best Matching Algorithm to prioritize the matching patterns.
3. Once the patterns are prioritized, the pattern with the highest priority will be used as a preferred route for call setup.

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

Example: The 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 the 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.

Allowed SIP Addresses

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

Note: Wildcards are allowed for called party addresses. Exceptions are addresses in the Supplementary Addresses table that are used by Outgoing Call Blocking service.

8.5 SIP Tunnel

The SIP Tunneling feature provides means for building network on Epygi QX IP PBXs (herein QX). This network 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 information on how to configure and use SIP Tunnels, please refer to the SIP Tunneling Feature on QX IP PBXs guide.

8.6 NAT Traversal

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

8.6.1 General Settings

The **General Settings** page is used to select the mode NAT Traversal will be used for the SIP traffic.

- **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.

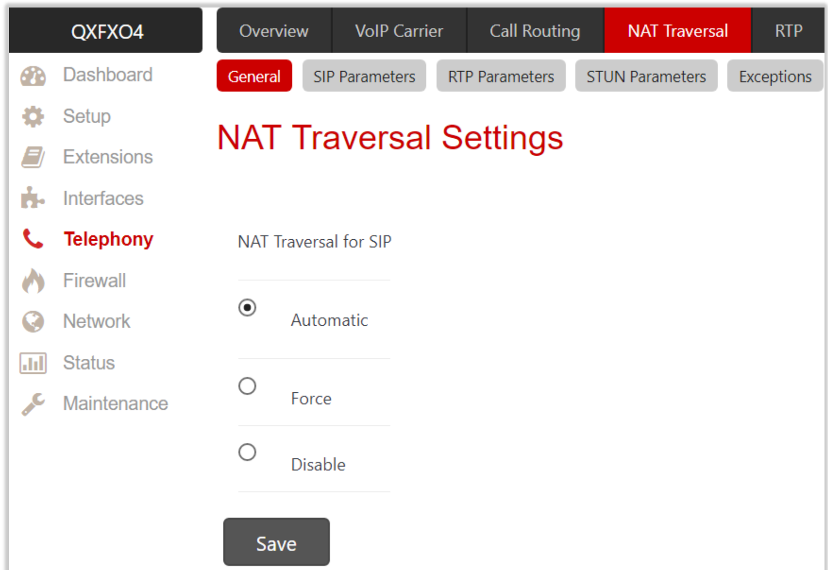


Figure 78: NAT Traversal Settings page

8.6.2 SIP Parameters

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

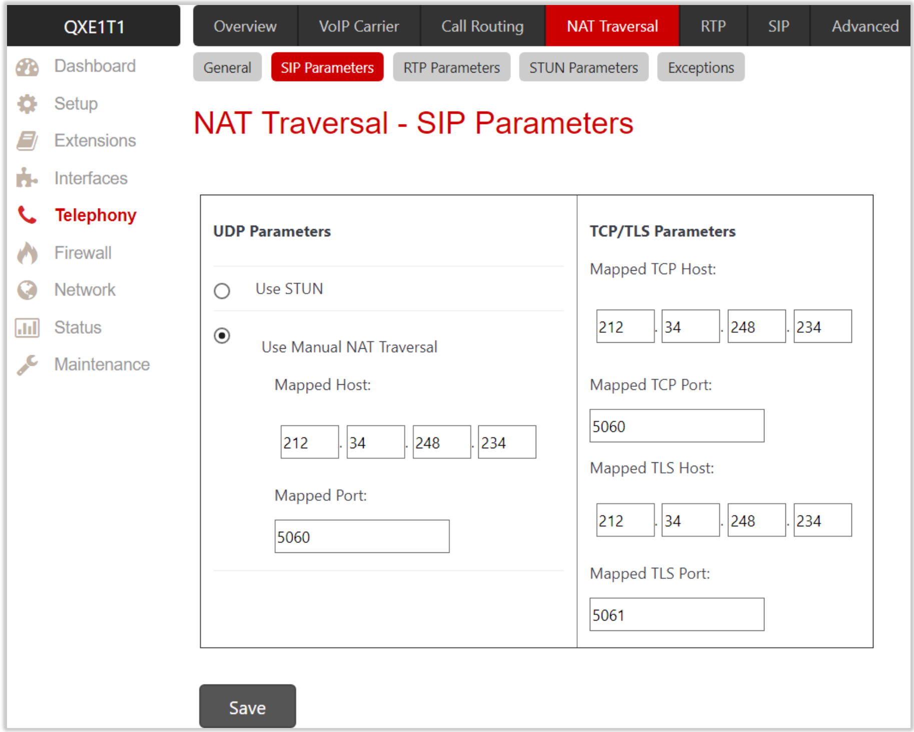


Figure 79: NAT Traversal – SIP Parameters page

- **Mapped TCP Host** – enter the IP address of the mapped host for SIP TCP traffic over NAT.
- **Mapped TCP Port** – enter the port number on the mapped host for the SIP TCP traffic over NAT.
- **Mapped TLS Host** – enter the IP address of the mapped host for SIP TLS traffic over NAT.
- **Mapped TLS Port** – enter the port number on the mapped host for the SIP TLS traffic over NAT.

8.6.3 RTP Parameters

The **RTP Parameters** page is used to select between the STUN and Manual NAT traversal connection for the RTP traffic and define 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 define the mapped host IP address for RTP traffic over NAT.
  - **Min** and **Max** – enter the port numbers on the mapped host for RTP and RTSP traffic. TIP: RTP/RTCP Mapped Port ranges should be greater than or equal to the RTP/RTCP port ranges defined on the RTP Settings page.

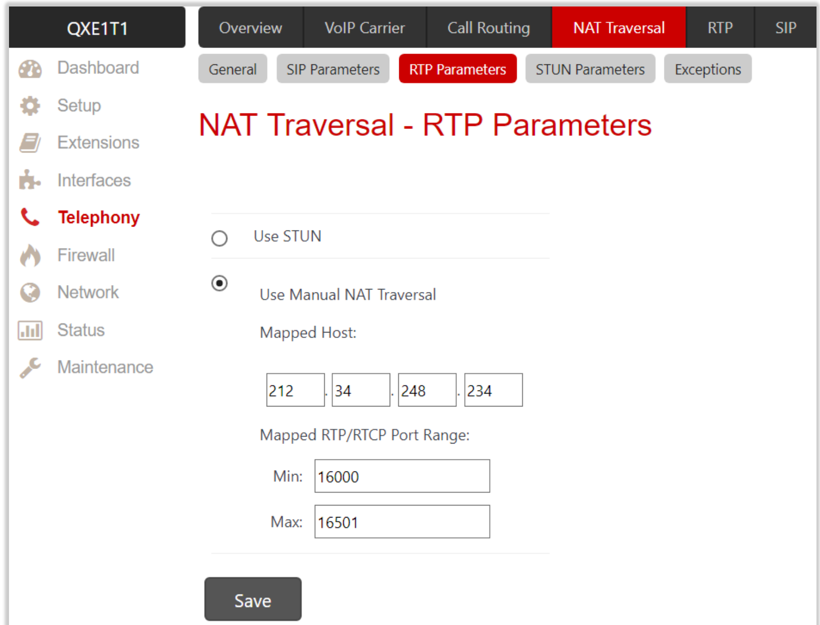


Figure 80: NAT Traversal – RTP Parameters page

8.6.4 STUN Parameters

The **STUN Parameters** page is used to enable automatic NAT configuration through the STUN server and is used to configure the STUN (Simple Traversal of UDP over NAT) client on the QX as follows:

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

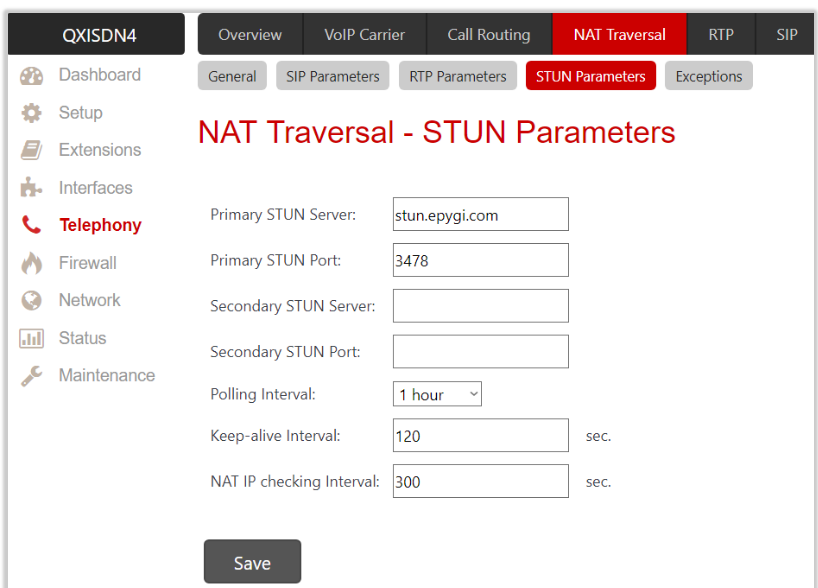


Figure 81: NAT Traversal – STUN Parameters page

8.6.5 Exceptions

The NAT Exclusion Table displays all possible IP ranges that are not included in the NAT process, but can be accessed directly. IP addresses that are not listed in the NAT Exclusion Table are accessed over NAT. For example, if a QX user needs to make SIP calls within the local network as well as outside of that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table. Otherwise, a malfunction may occur in SIP operations.

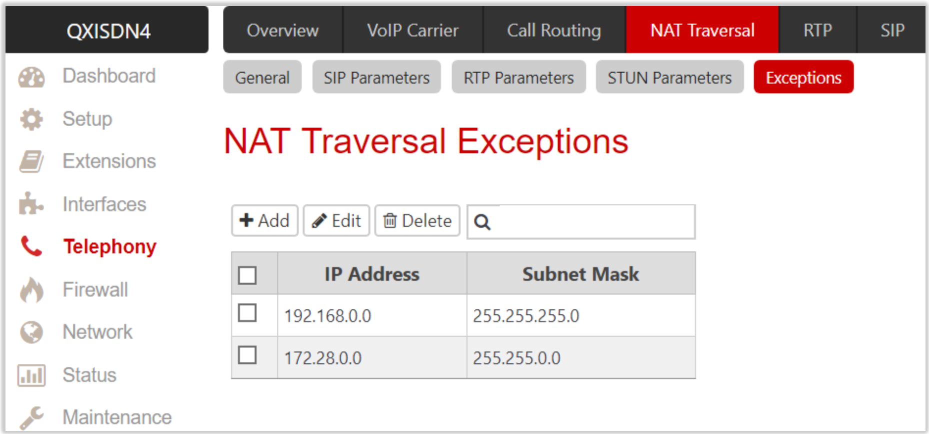


Figure 82: NAT Traversal Exceptions page

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, the new the exception entry will be added to the NAT Traversal Exceptions table.

8.7 RTP Settings

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 ranges and silence suppression associated to each.

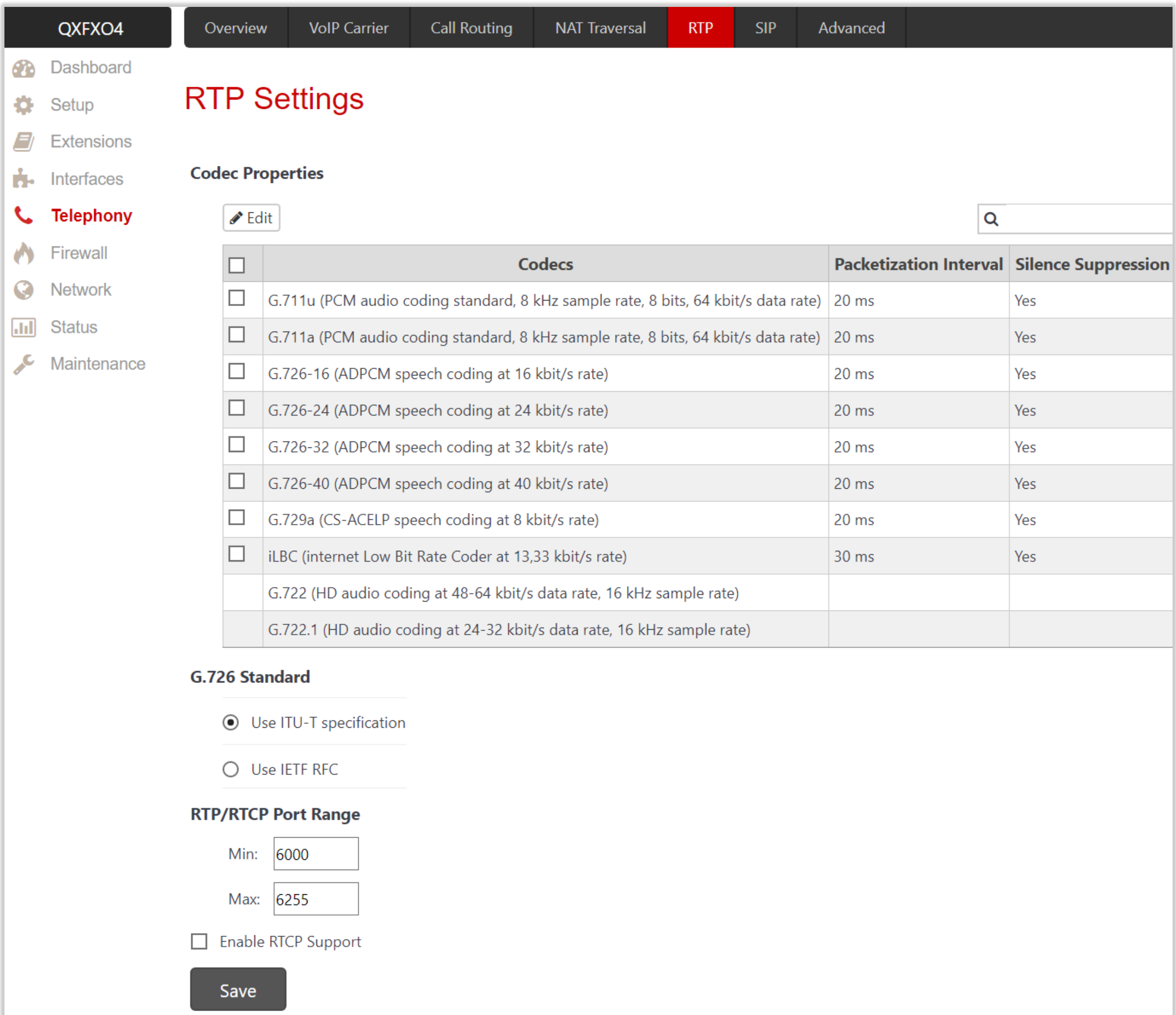


Figure 83: RTP Settings page

- Edit – leads to the RTP Settings – Edit Entry page to modify the selected codec settings.
  - ➢ Packetization Interval – is the time interval between two RTP packets of the same stream. If this interval is increased, the overhead is decreased, but the voice quality may deteriorate as a result. If the interval is decreased, the network load is increased and the delay is reduced.
  - ➢ 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 restarted immediately if any audio appears.
- G.726 Standard – is used to select between packaging method of the G.726 code words into octets. If you are experiencing problems with the voice quality when using G.726 with one of these options selected, try switching to the next one.
  - ➢ 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 starts 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 starts from the least significant positions in the octet.

- Min and Max – is used to enter the port numbers for RTP and RTSP traffic. TIP: RTP/RTCP Port ranges cannot include the defined SIP ports.
- Enable RTCP Support – enables Real Time Control Protocol support and allows the RTCP packets transmission. RTCP is used for monitoring the RTP streams and changing RTP characteristics depending on Network conditions.

8.8 SIP

8.8.1 SIP Settings

The SIP Settings page is used to select the SIP receive UDP and TCP ports, the DNS Server configurations for SIP and the SIP timers scheme.

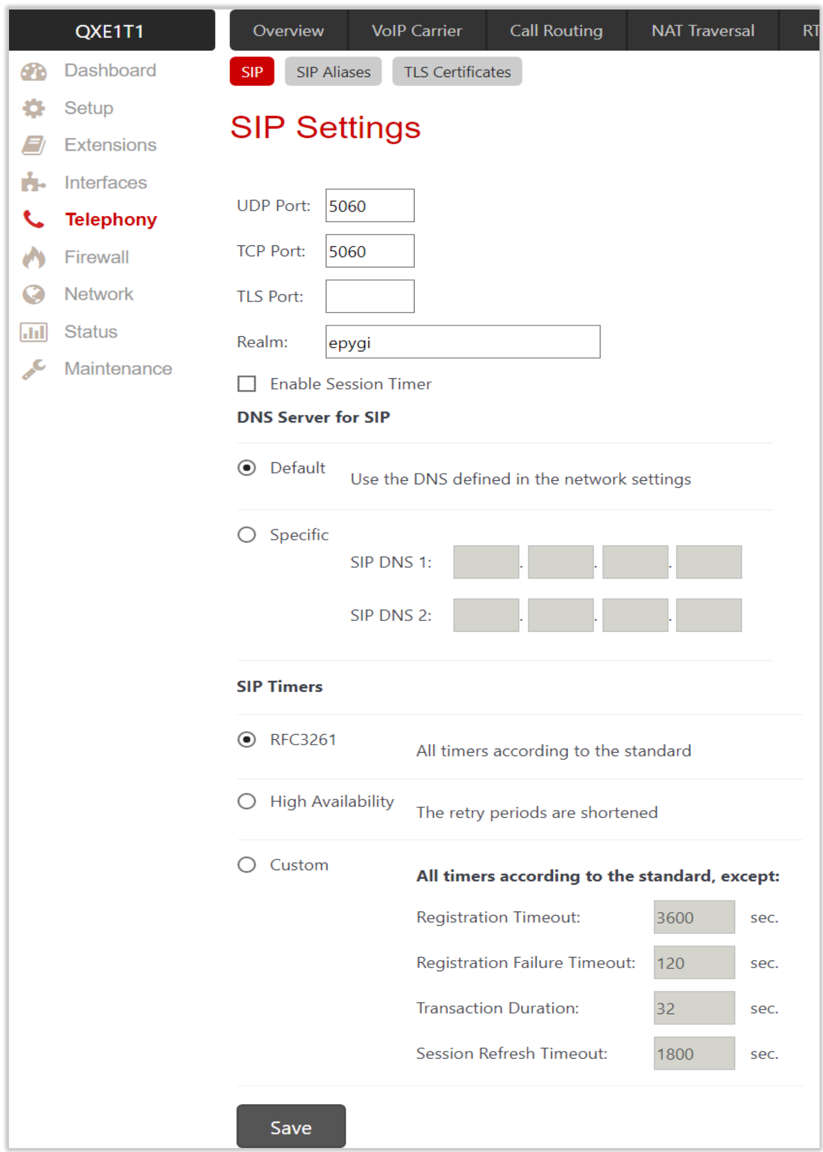


Figure 84: SIP Settings page

- UDP Port – indicates the SIP UDP receive port. By default, 5060 is selected and used. TIP: The SIP UDP port cannot be in the selected RTP/RTCP port range for FXS and IP lines.
- 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 field is left empty.
- TLS Port – indicates the SIP TLS receive port. By default, 5061 is selected and used. TLS port number should be different from the TCP Port number.
- Realm – is used to define the messaging level information to be included in SIP messages sent by the QX. This information might be used by remote side for authentication purposes.
- Enable Session Timer – enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.
- DNS Server for SIP allows to choose between regular DNS servers configured in the DNS Server Settings 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 define 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 the QX.
  - ➢ Custom – is used to manually define the Registration Timeout, Registration Failure Timeout, Transaction Duration and Session Refresh Timeout timers (in seconds).

8.8.2 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 the QX is registered with different names.

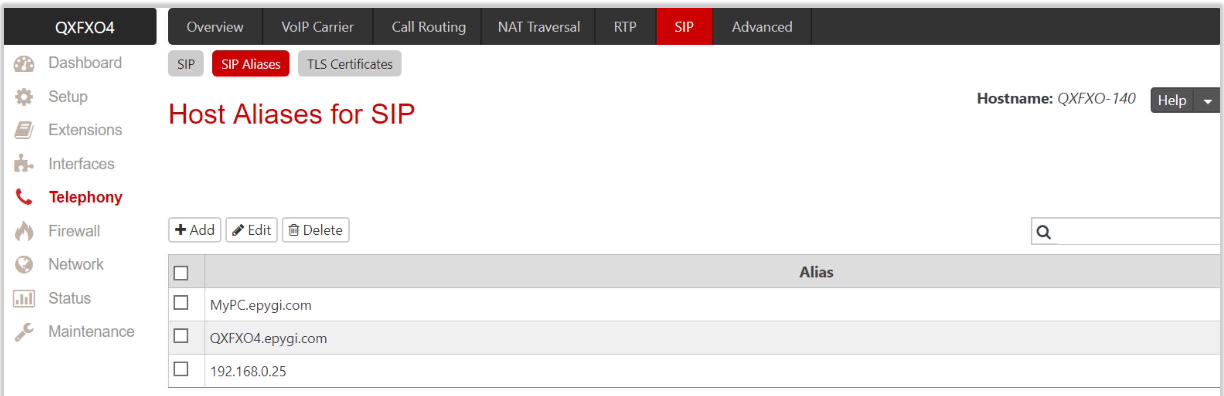


Figure 85: Host aliases for SIP page

8.8.3 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 root certificate specific information.

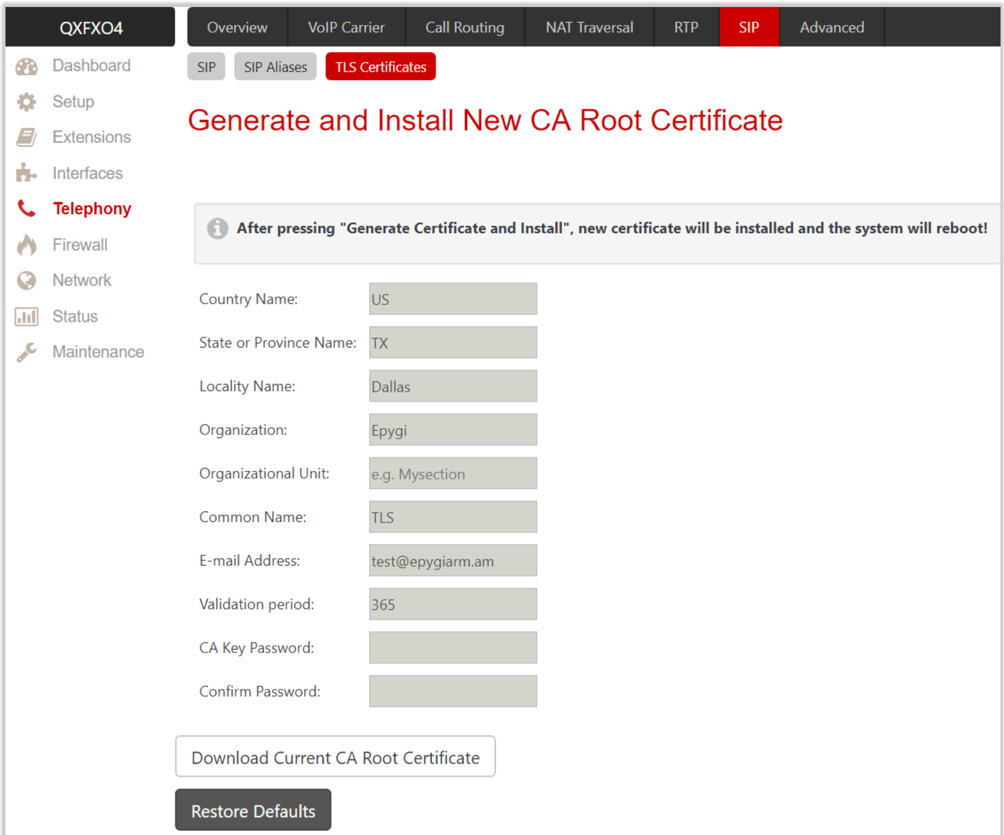


Figure 86: Generate and Install New CA Root Certificate page

- Generate Certificate and Install – generates a new CA root certificate based on the defined data and installs it on the QX. The 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 the (*.crt) format.

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

8.9 Advanced Settings

8.9.1 RTP Streaming Channels

The RTP Streaming Channels page (N/A for QXFXS24) is used to define the channels for the broadcast 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.

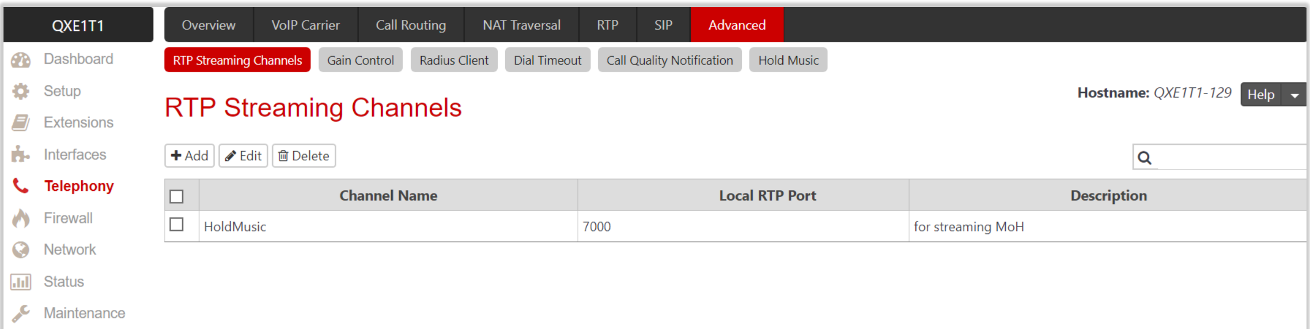


Figure 87: RTP Streaming Channel page

To add a new RTP channel:

1. Click Add and enter the following information:
   - RTP Channel Name – enter the name of the RTP channel.
   - Port Number – enter the broadcasting RTP port number.
   - Description – enter any descriptive information, if needed.
2. Click Save, the new RTP channel will be added to the RTP Streaming Channels table.

8.9.2 Gain Control

The Gain Control settings are used to define 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.

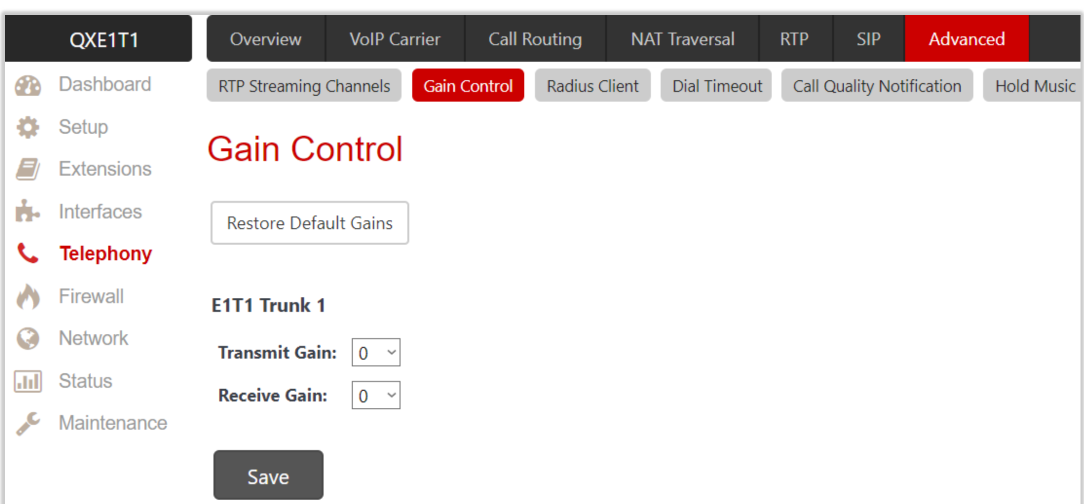


Figure 88: Gain Control page on QXE1T1

- Restore Default Gains – is used to restore the default values.
- For FXS lines (available for QXFXS24):

- Transmit Gain defines the phone speaker volume on the call.
- Receive Gain defines the volume of the phone microphone on the call.

- For FXO lines (available for QXFXO4):
  - Transmit Gain defines the level of voice transmitted from QX to the FXO network.
  - Receive Gain defines the volume of voice received by QX from the FXO network.
- For ISDN trunks (available for QXISDN4):
  - Transmit Gain defines the level of voice transmitted from QX to the ISDN network.
  - Receive Gain defines the volume of voice received by QX from the ISDN network.
- For E1/T1 trunks (available for QXE1T1):
  - Transmit Gain defines the level of voice transmitted from QX to the E1/T1 network.
  - Receive Gain defines the volume of voice received by QX from the E1/T1 network.

8.9.3 RADIUS Client Settings

Remote Authentication Dial in User Service (RADIUS) specifies the RADIUS protocol used for authentication, authorization and accounting, to differentiate, to secure and to account for the users. The RADIUS Server provides the option for a caller from/through QX to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the QX, and according to the configuration of AAA Required option, the RADIUS server will be used to authenticate user and/or to account for the call. This can be accomplished by automatic detection of the caller's number or a customized login prompt where the caller is expected to enter a username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, user passwords are encrypted when sent between the client and RADIUS server to eliminate the possibility of a party viewing an unsecured network where they could determine a user's password. If no response from the RADIUS Server is returned after the Receive Timeout expires, the request is resent numerous times as defined in the Retry Count list. The client can also forward requests to an alternate server(s) if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not recognize must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the QX Network.

- **Enable RADIUS Client** – is used to enable RADIUS client on the QX. TIP: The RADIUS Client cannot be disabled if there is at least one route with **RADIUS Authentication and Authorization** or **RADIUS Accounting** values configured in the **AAA Required** drop down list on the **Call Routing Table**. In order to disable the RADIUS Client on the QX, the configured routes should be removed first.
- **Primary Server** – enter the IP address of the primary Radius Server.
- **Secondary Server** – enter the IP address of the secondary Radius Server.
- **NAT Station IP** – enter the WAN IP address for the NAT station. If no NAT Station is specified here, QX's IP address will be sent to the RADIUS server.
- **Secret Key** – enter the secret key between the Radius client and server. Confirm the entered key in the **Confirm Secret Key** field.
- **Retry Count** – select the number of attempts authorized before canceling the registration.
- **Receive Timeout** – select the timeout (in seconds) between two attempts to register.

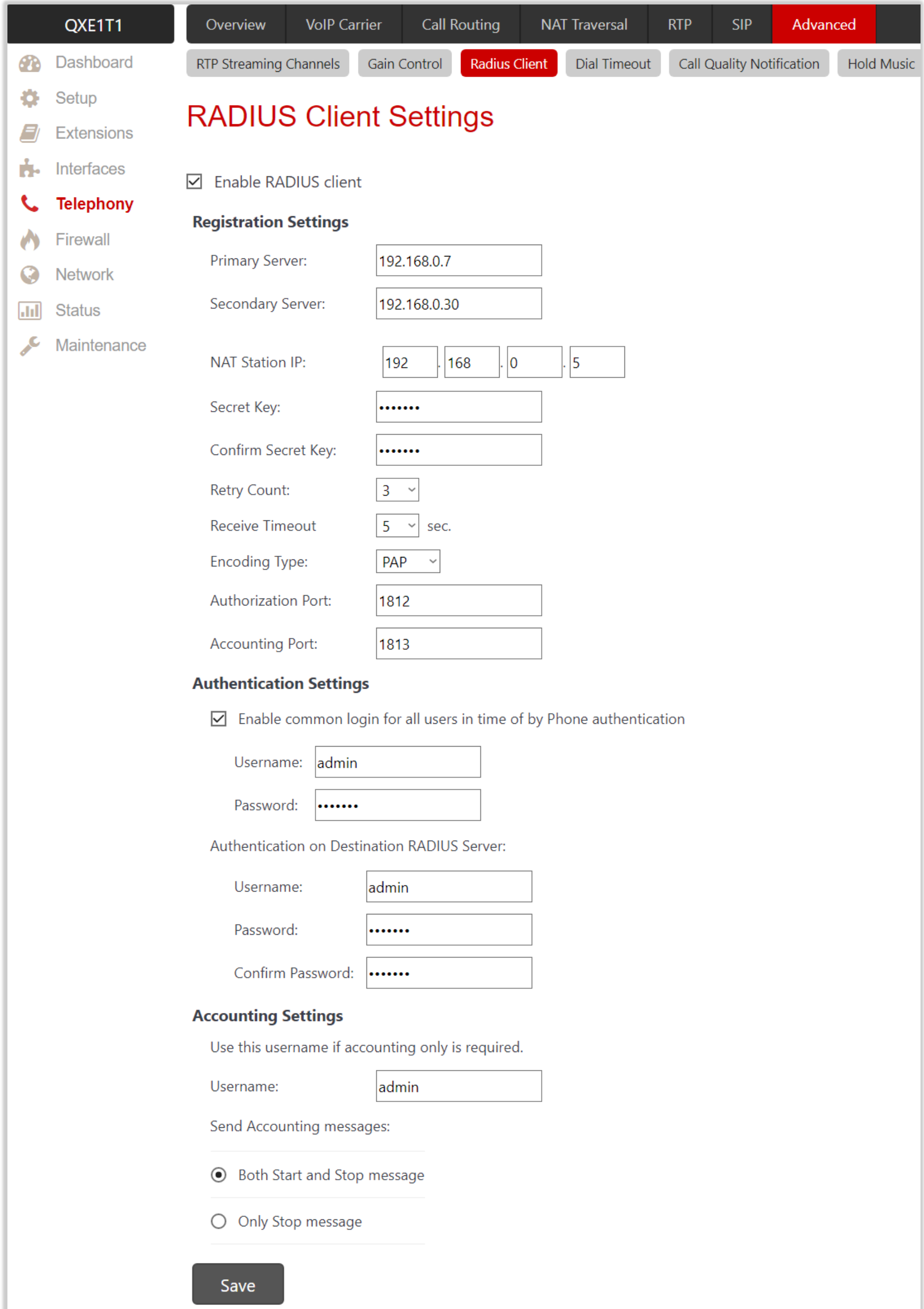


Figure 89: Radius Client Settings page

- **Encoding Type** – select the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type should also be requested from the Radius Server administrator.
- **Authorization Port** – enter the port number on the RADIUS server where QX is to send the authentication requests.
- **Accounting Port** – enter the port number on the RADIUS server where QX is to send the accounting messages.
- **Enable common login for all users in time of by Phone authentication** – enable custom settings for the callers who passed an authorization by phone on the QX. This checkbox enables **Username** and

Password fields to enter the custom settings that will stand instead of the source caller's settings when being delivered to the RADIUS server.

- Authentication on Destination RADIUS Server – enter Username and Password to pass authentication on the RADIUS Server of the destination QX. If these fields are left empty, the original authentication settings that users enter for authentication will be used.
- Username – enter an identification username for accounting purposes. When no username is specified in this field, the source username will be used for accounting. This field is dedicated for accounting services only.
- Send Accounting messages – select sending both Start and Stop accounting messages or only Stop accounting message.

8.9.4 Dial Timeout

The Dial Timeout Settings are used to adjust the timeout setting when dialing on the phone. The Routing Dial Timeout option is used to specify a period of time after the last dialed digit that the system identifies as a completion of dialing. If the user does not press any key within the specified timeout, the system assumes that the dialing is completed and starts processing the dialed number.

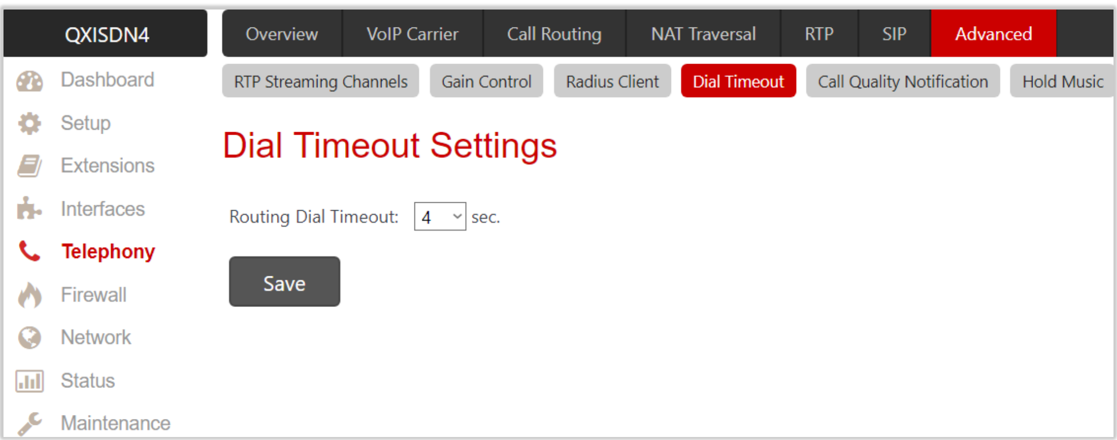


Figure 90: Dial Plan Settings page

8.9.5 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 allowed level.

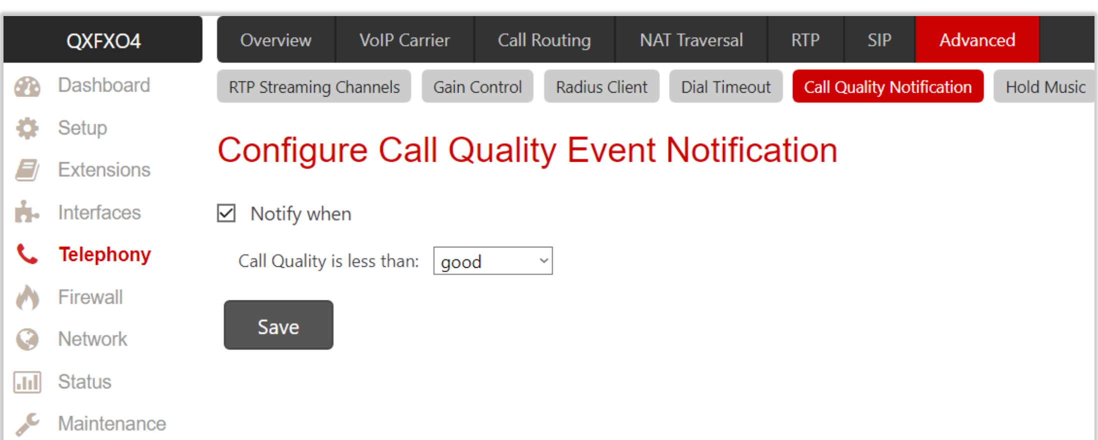


Figure 91: Configure Call Quality Event Notification page

- Notify when – is used to enable the call quality monitoring mechanism.
  - Call Quality is less than – is used to select the minimum satisfactory call quality. Notification will appear on the System Events about the call with lower quality.

8.9.6 Hold Music

The System Hold Music Settings allows you to define the hold music played to the PSTN party when it is held by the IP user. This page also allows you to define the percentage of system memory dedicated to the uploaded hold music file. The following options are available:

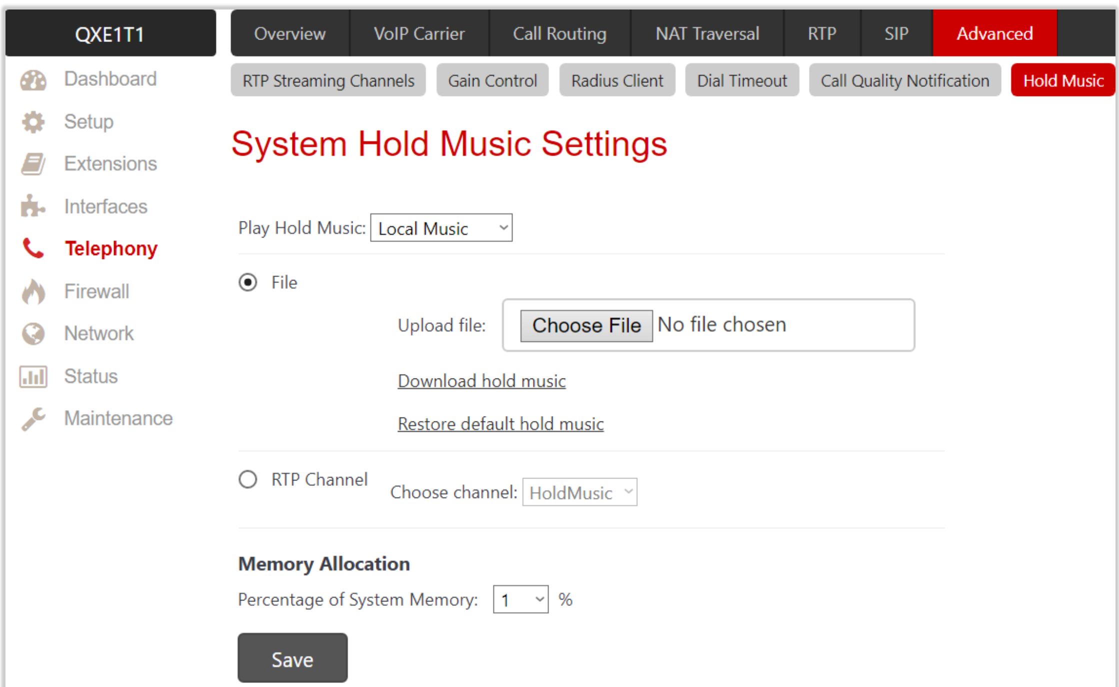


Figure 92: Hold Music Settings page

- Play Hold Music – is used to select the music played to the PSTN party when it is held by remote IP user. The following options are available:
  - Off – no music will be played.
  - Local Music –the music configured on the QX will be sent to the remote PSTN party while it is on hold.
  - Remote Music – the music sent by the IP party will be transparently passed to the PSTN user while it is held by the IP party.
- Percentage of System Memory – defines the memory space for system hold music.

You can select the way custom hold music will be provided: uploading/recording the music as a file or streaming the music through RTP Channel.

9 Firewall Menu

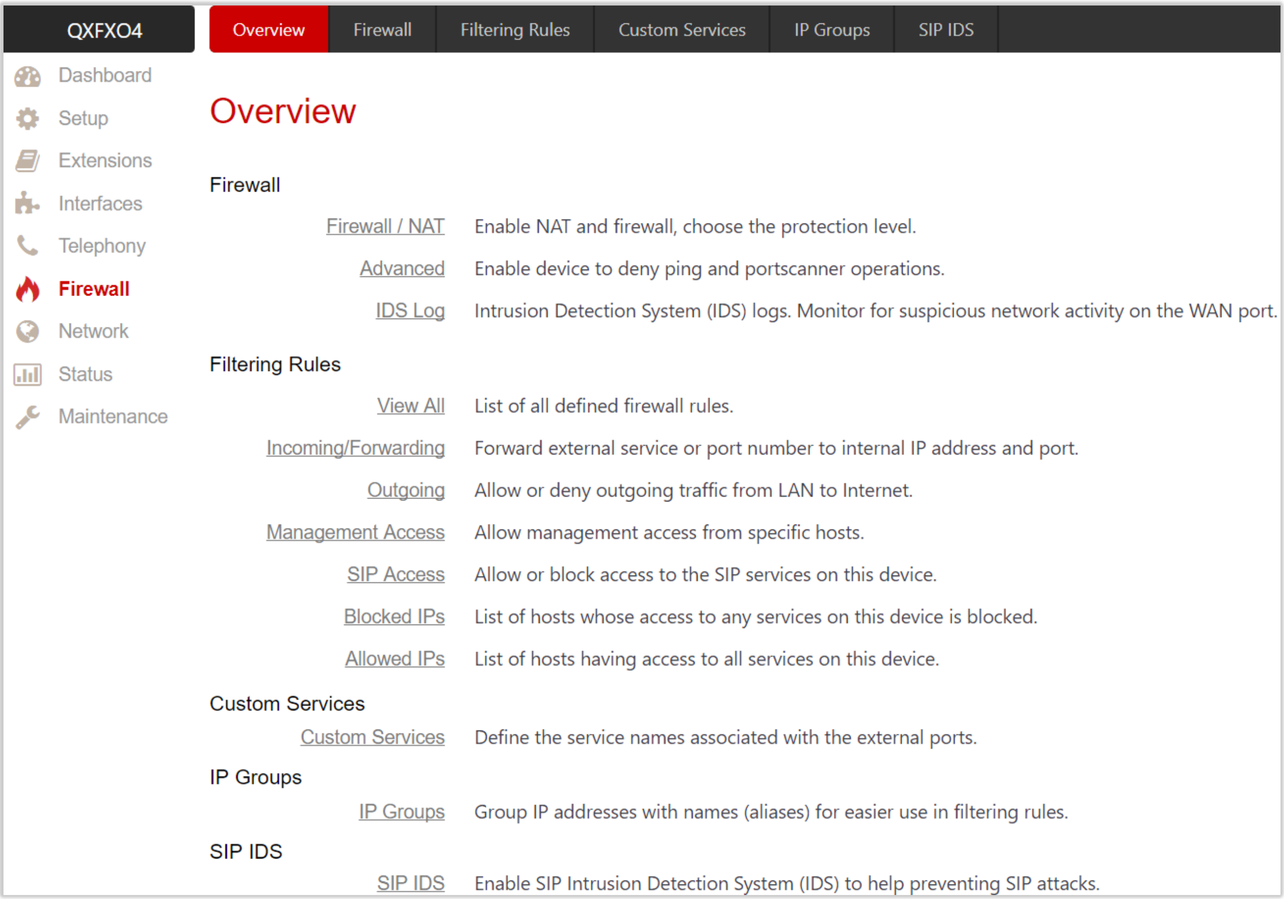


Figure 93: Firewall Menu overview

9.1 Firewall

The **Firewall Configuration** page allows setting up the Firewall, configuring the security level and enabling the **Network Address Translation** (NAT) and **Intrusion Detection System** (IDS) services on the QXs.

Firewall is a security service configurable through various criteria. It has three level of security policies: low, medium and high. The **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 members to the Internet using QX's WAN IP address. **NAT** also forwards incoming packets from the WAN to the PCs or devices in the QX's LAN. The **IDS** is a type of firewall. It 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 offers the following components:

- **Enable IDS** – enables the Intrusion Detection System.
- **Enable NAT** – enables the Network Address Translation.
- **Enable Firewall** – enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

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.

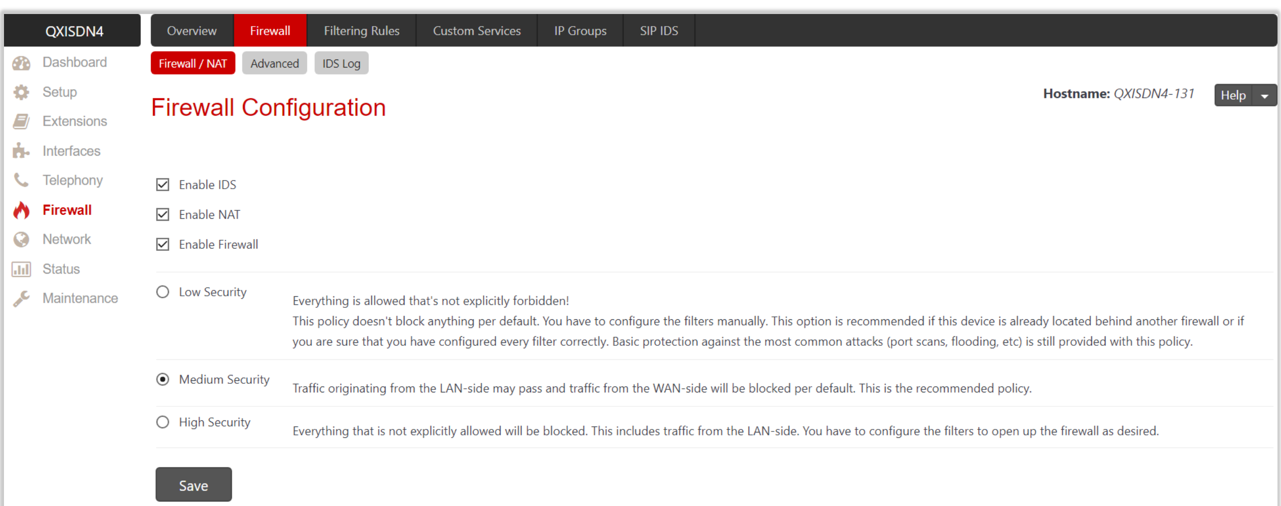


Figure 94: Firewall Configuration page

9.1.2 Advanced Firewall Configuration

The Advanced Firewall Settings are used to deny Ping and Portscanning operation addressed towards the device. The QX will answer with irritating message to the Ping and Portscanning operations. The Ping and Portscanning operations will be denied when the Firewall is enabled from the Firewall and NAT page.

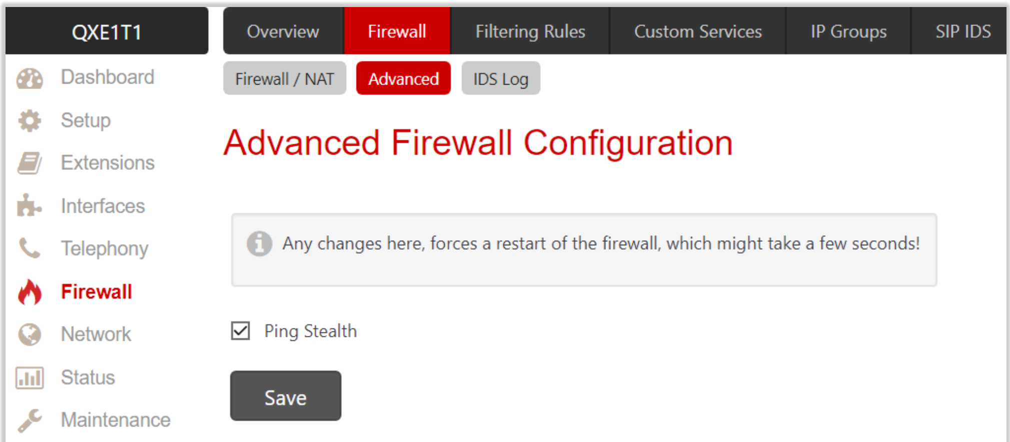


Figure 95: Advanced Firewall Settings page

9.1.3 IDS Log

The IDS log page (N/A for QXE1T1 gateway) contains information about 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. The 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 and NAT page. The IDS Logs table is a list of new or read IDS entries and descriptions referring to them.

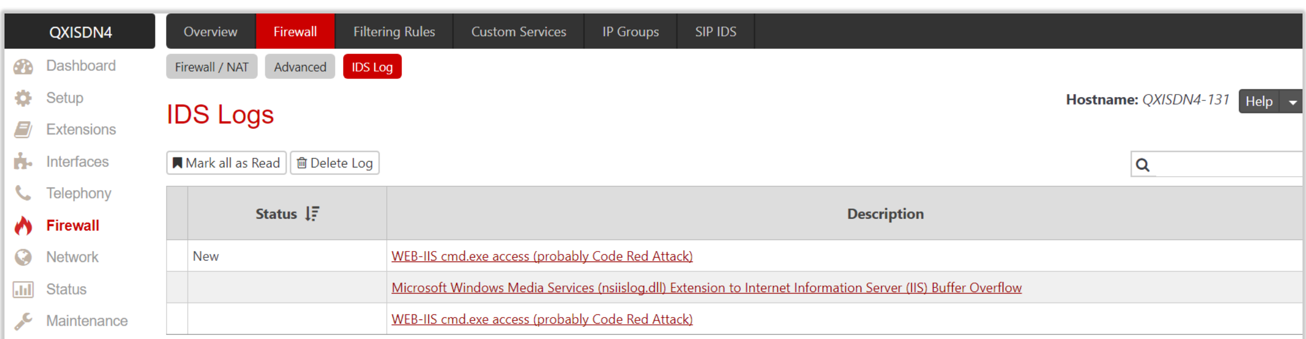


Figure 96: IDS Log page

Click on the desired entry to see it's detailed log in the IDS Detailed Logs table. The IDS Logs table is a detailed log that shows 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** page is 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 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) added into the Blocked IPs.

9.2.1 View All Filtering Rules

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

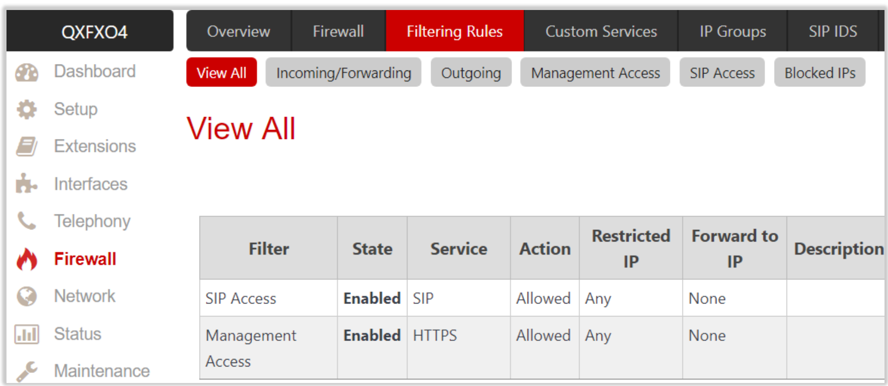


Figure 97: Filtering Rules page

9.2.2 Incoming Traffic / Port Forwarding

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

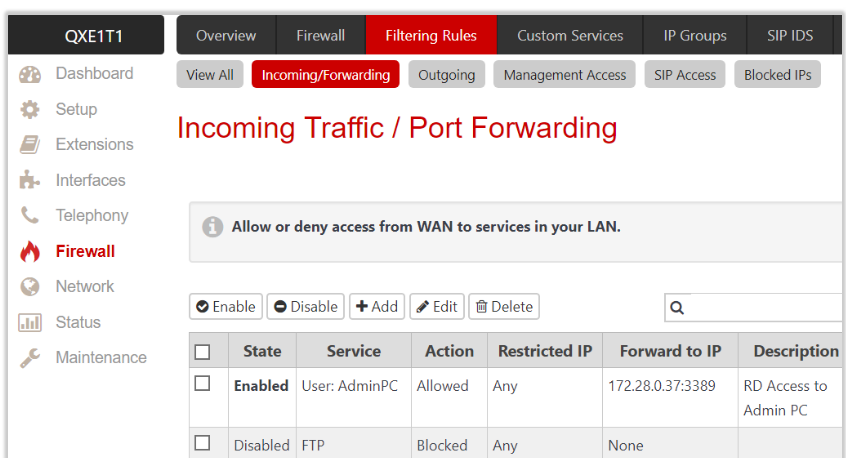


Figure 98: Incoming Traffic/Port Forwarding page

9.2.3 Outgoing Traffic

Outgoing Traffic filtering rules allow or deny access to the external services for QX's LAN users.

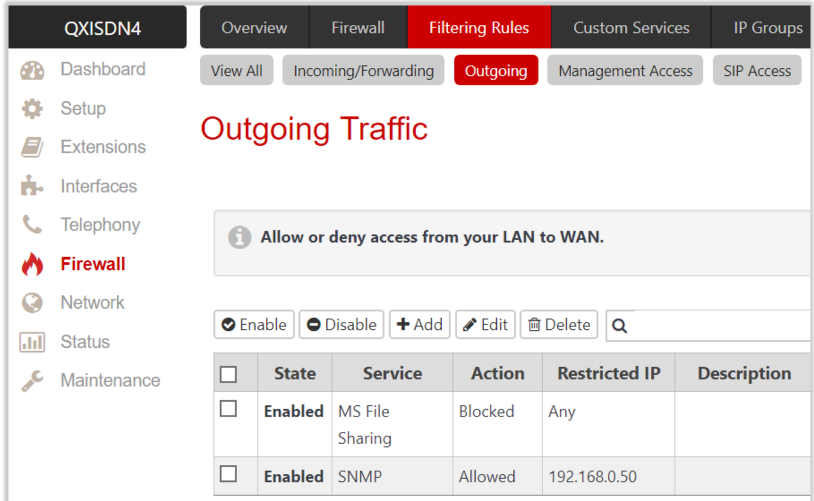


Figure 99: Outgoing Traffic page

9.2.4 Management Access

Management Access filtering rules are used to allow or deny hosts management access to the QX.

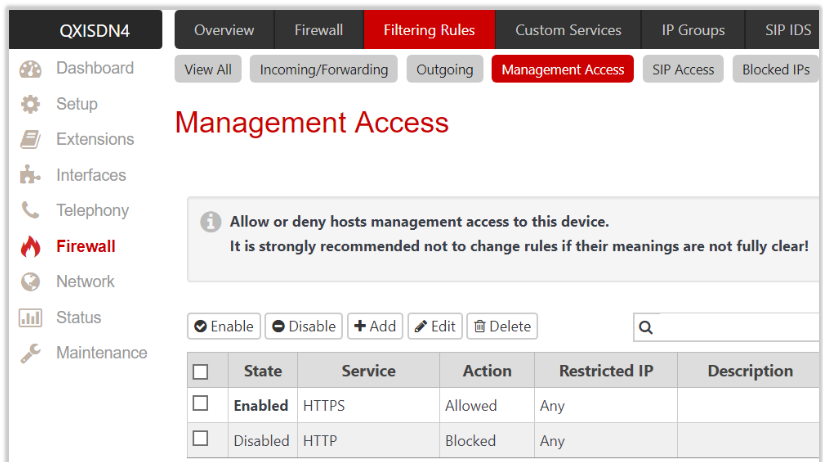


Figure 100: Management Access page

9.2.5 SIP Access

SIP Access filtering rules are used to allow or deny access to or from SIP servers and other SIP devices in the WAN. This filtering rule will prevent or allow incoming/outgoing SIP calls from/to specified SIP server(s) or host(s).

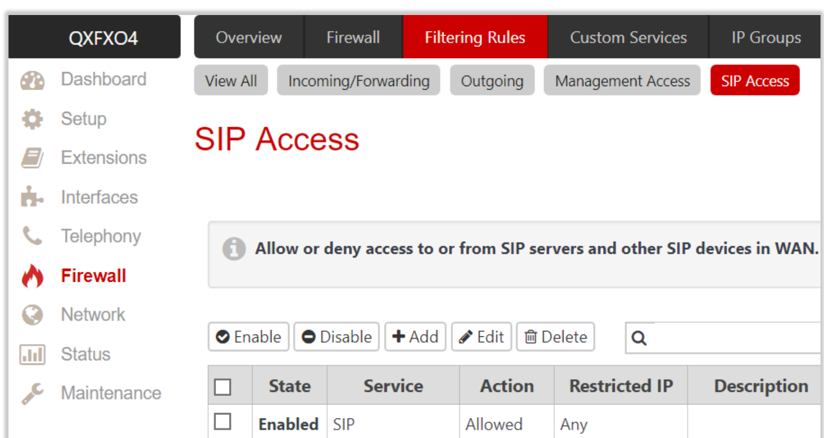


Figure 101: SIP Access page

9.2.6 Blocked IPs

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

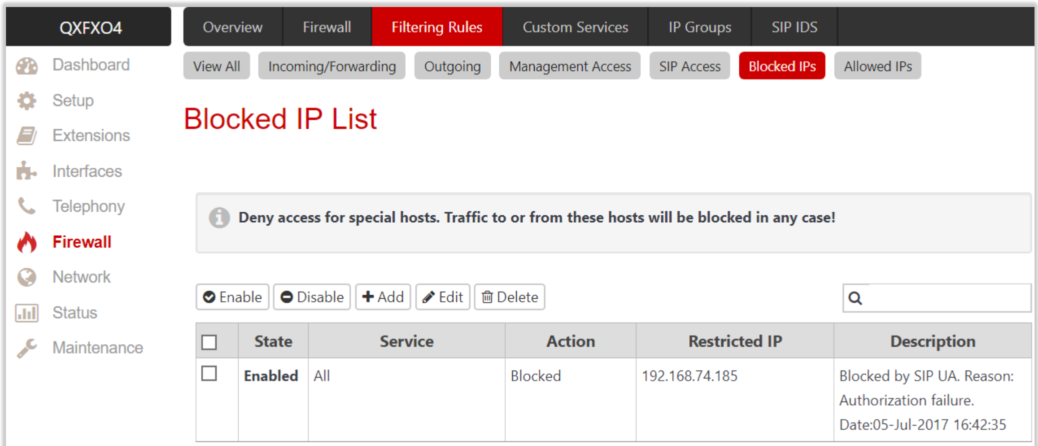


Figure 102: Blocked IP List page

9.2.7 Allowed IPs

Allowed IP List entries are used to allow trusted hosts to reach your network and vice versa. TIP: If a host also appears in the **Blocked IP List**, the **Blocked IP List** has a higher priority, and the traffic will be blocked.

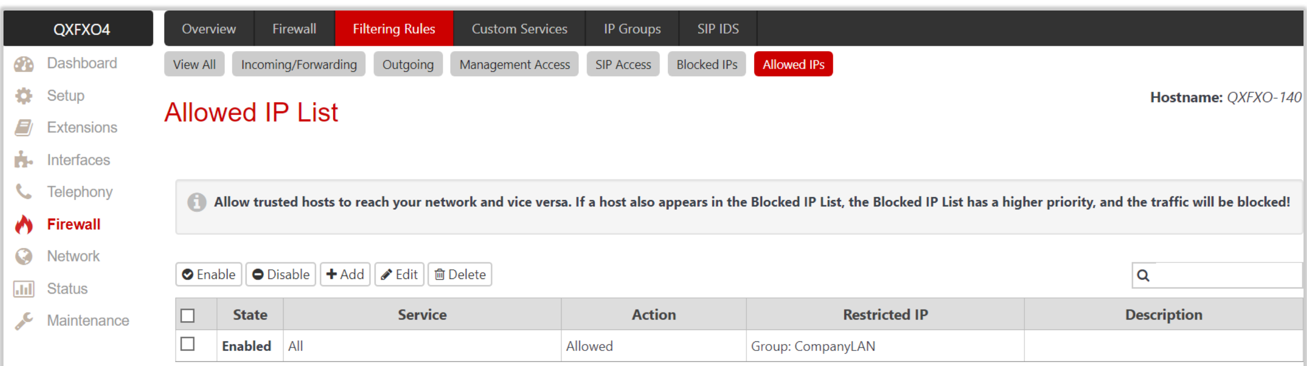


Figure 103: Allowed IP List page

To Add a Filtering Rule

1. Navigate to the **Filtering Rules** (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management 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**, the new filtering rule will be added in the corresponding **Filtering Rule** table and in the **View All** table.
4. Click **Enable** to activate the newly created filtering rule from the corresponding table.

9.3 Custom Services

9.3.1 Service Pool Configuration

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.
   - Define the Port Range.
2. Click Save, the new service will be added to the Service Pool Configuration table.

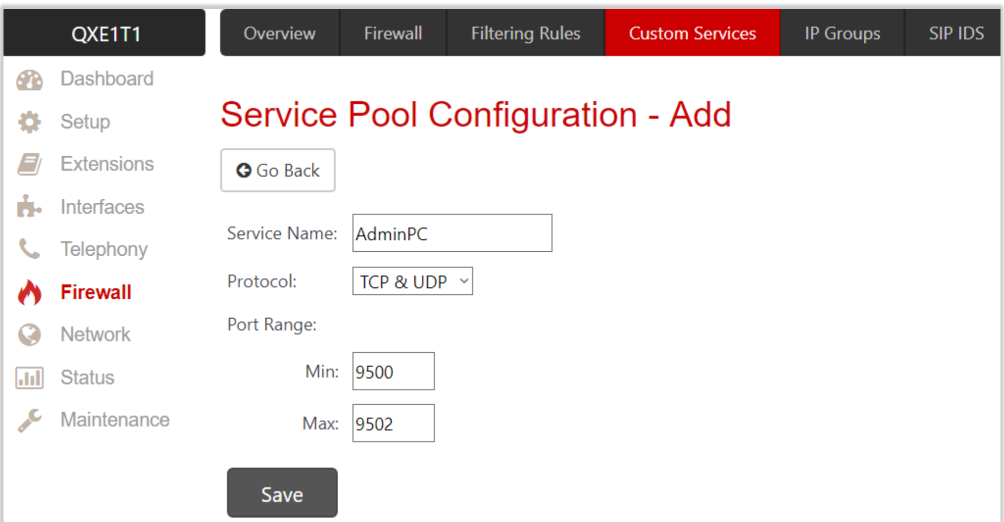


Figure 104: Service Pool Configuration – Add page

9.4 IP Groups

9.4.1 IP Pool Configuration

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 IP Pool Group Configuration page displays a list of all the added member IP addresses for the selected group as well as allows adding/modifying members.

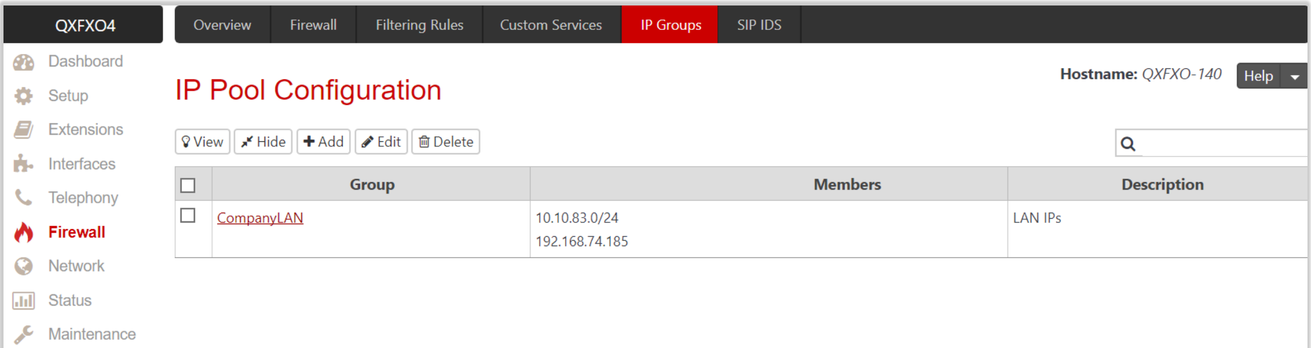


Figure 105: IP Pool Configuration page

Click **Group** name link to display an **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 **Description** (if needed).
3. Click **Save**, the new group will be added to the **IP Pool Configuration** table.
4. Open the **IP Pool Group Configuration** page by clicking the **group name** link.
5. Click **Add** on the **IP Pool Group Configuration** page.
   - 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**, the new member will be added to the **Current Group** table.

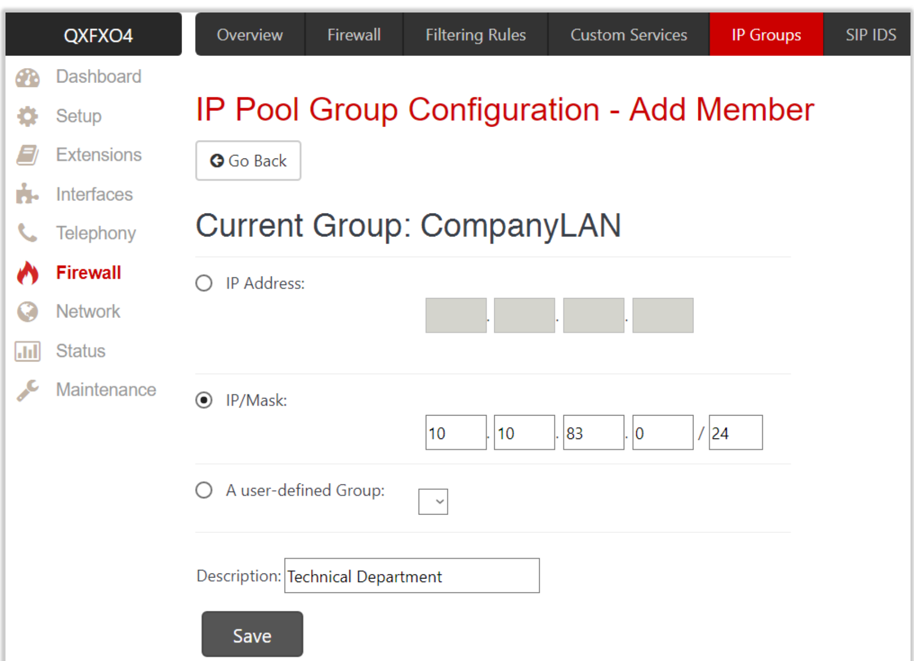


Figure 106: IP Pool Group Configuration – Add Member page

9.5 SIP IDS Settings

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

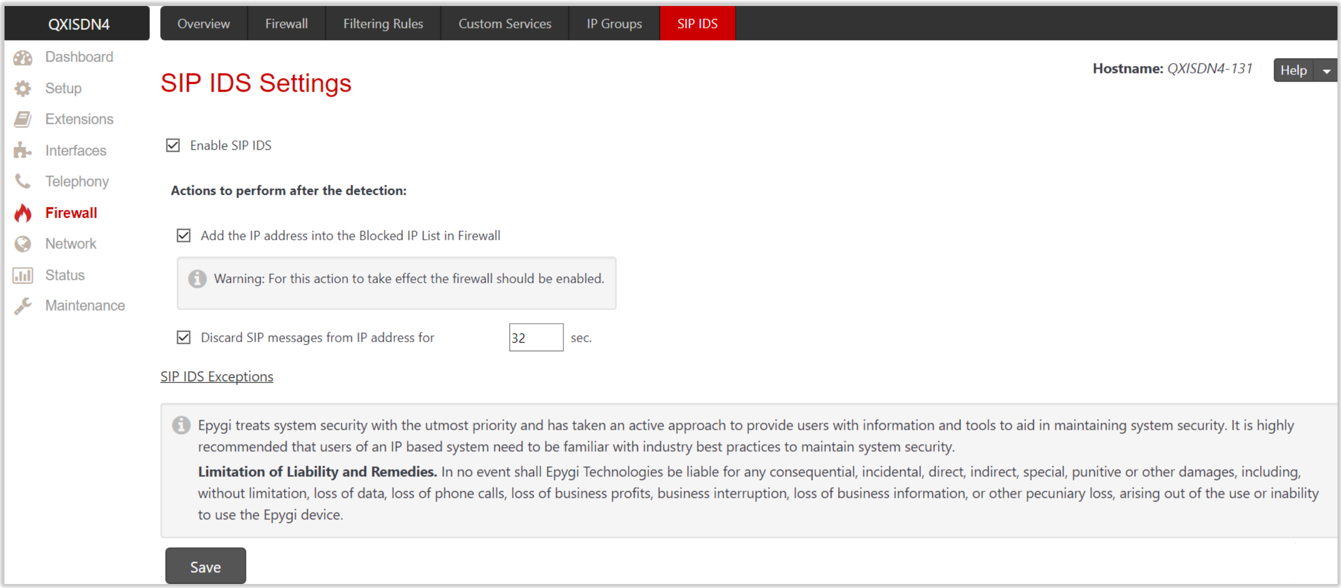


Figure 107: SIP IDS Settings page

- **Enable SIP IDS** – enables SIP attack prevention.
- **Add the IP address into the Blocked IP List in Firewall** – 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 **Firewall** is enabled on the QX.
- **Discard SIP messages from IP address for** – if selected, the system will ignore the SIP messages from attackers IP address for the specified time period after attack detection (default period is 32 seconds).
- **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.

To add a new SIP IDS exception:

1. Click the **SIP IDS Exceptions** link.
2. Click **Add** and enter the following information:
   - Enter the **IP Address**.
   - Enter the **Mask**. TIP: Enter **32** as a Mask to add only the IP address in exception list.
3. Click **Save**, the new exception entry will be added in the **SIP IDS Exceptions** table.

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.
- **2** messages causing **Non-self-Request-URI** from the same IP during **250** milliseconds.
- If there are **10** 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 **9** times and then successfully registered on the **10**th attempt, then it resets the counter to **0**. Next time the same IP can make another 9 unsuccessful attempts before being blocked.

10 Network Menu

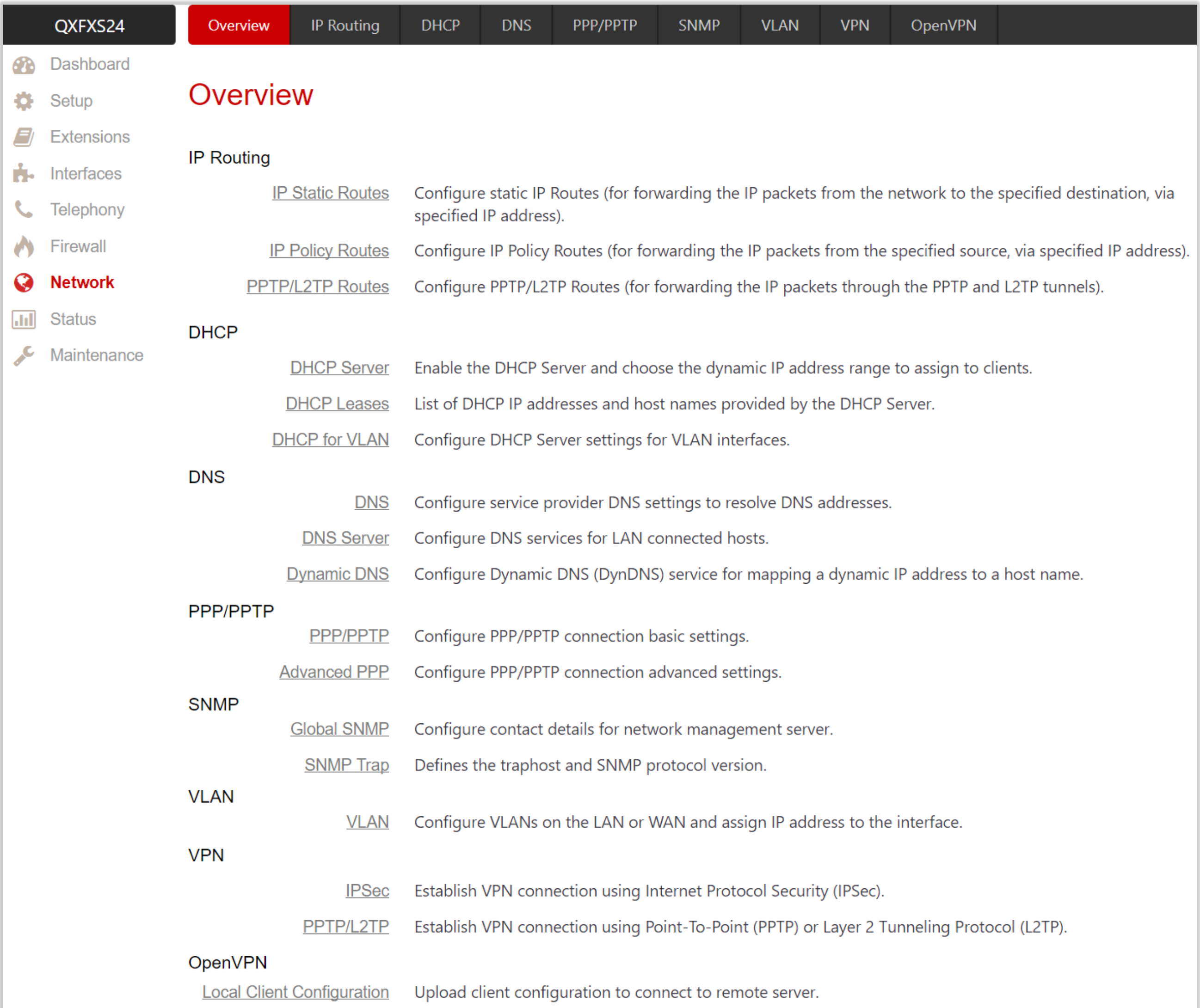


Figure 108: Network Menu overview

10.1 IP Routing

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

QX **IP Routing** service allows to route IP packets from one destination to another (or to a specified router) through the QX or QX's VPN. The **IP Routing** is used to make IP Static, IP Policy and PPTP/L2TP routes for IP packets routing. This page consists of three tables. Entries in the tables are color coded according to the state of the route. For example, yellow indicates disabled routes, green indicates successful routes and the red indicates routes with an error.

10.1.1 IP Static Routes

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

The **IP Static Routes** table displays all configured IP static routes with their parameters:

- **Target State** – state of the route (enabled or disabled)
- **Actual State** – state of the route connection (up, down or erroneous)
- **Route To** – subnet the incoming packets should be routed to
- **Via IP Address** – router IP address incoming packets should be routed through

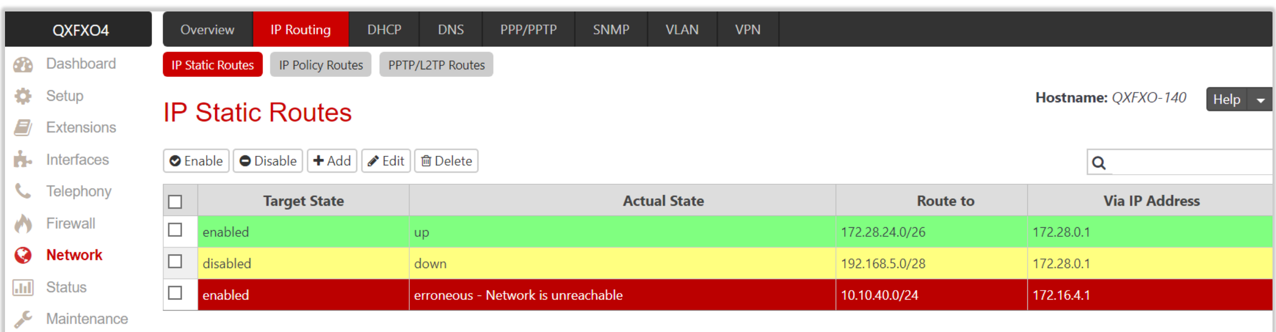


Figure 109: IP Static Routes page

To add a new IP Static Route:

1. Click **Add** and enter the following information:
   - **Route to** – enter the IP address and subnet mask of the destination the IP packet will be routed to.
   - **Via IP Address** – enter the IP address of the router that will forward the IP packet to the specified destination.
2. Click **Save**, the new route will be added 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.

10.1.2 IP Policy Routes

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

The IP Policy Routes table displays all specified IP policy routes with their parameters:

- Target State – state of the route (enabled or disabled)
- Actual State – state of the route connection (up, down or erroneous)
- Priority – route priority
- Route from – is where the subnet, routed packets come from
- Via IP Address – is where the router IP address incoming packets should be routed through

To add a new IP Policy Route:

1. Click Add and enter the following information:
   - Priority – define a 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 – enter the packet source IP address and subnet mask of the specified destination to match with the rule.
   - Via IP Address – enter the IP address of the subsequent router to forward the IP packet to.
2. Click Save, the new route will be added 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.

10.1.3 PPTP/L2TP Routes

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

The PPTP/L2TP Routes table displays all generated VPN routes with their parameters:

- Target State – state of the route (enabled or disabled)
- Actual State – state of the route connection (up, down or erroneous)
- Route to – subnet where the incoming packets should be routed
- Via Tunnel – VPN tunnel incoming packets should be routed through
- Tunnel State – actual state of the route tunnel (up or down)

To add a new PPTP/L2TP Route:

1. Click Add and enter the following information:
   - Route via – 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's LAN to the peer behind the PPTP/L2TP tunnel.
   - Route to – enter the IP address range of the possible peers behind the PPTP/L2TP tunnel the IP packets should be routed to.
2. Click Save, the new route will be added to the PPTP/L2TP Routes table.
3. Click Enable to activate the newly created route.

10.2 DHCP

The **DHCP Settings** are used to enable a DHCP server and controlling the QX user's LAN settings. Therefore, QX LAN users will automatically be provided with the following settings using the configured parameters:

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

10.2.1 DHCP Server

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

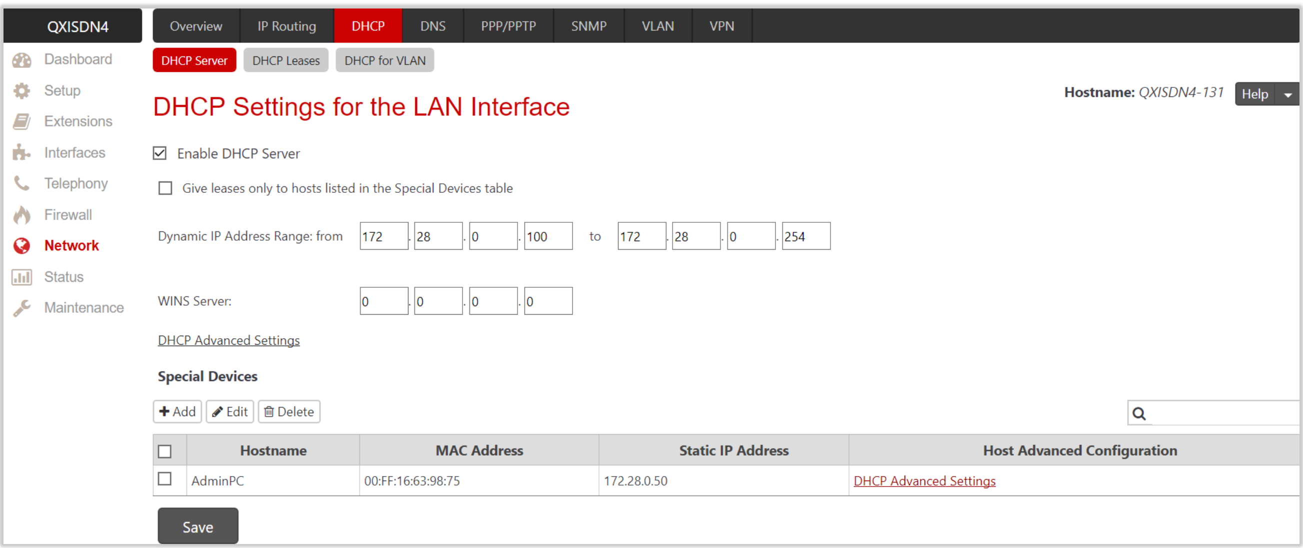


Figure 110: DHCP Settings page for the LAN interface page

- **Enable DHCP Server** – activates the DHCP server on the QX. If selected, QX will be able to assign dynamic IP addresses to its LAN devices.
- **Give leases only to hosts listed in the Special Devices table** – if selected, then the DHCP services will be provided only to the devices listed in the **Special Devices** table.
- **Dynamic IP Address Range (from to)** – defines a range of IP addresses that will be assigned to the QX LAN users.
- **WINS Server** – defines a WINS server IP address for the QX LAN users.
- **DHCP Advanced Settings** – leads to the DHCP Advanced Settings page to configure the advanced options of the QX's DHCP server.
- **Special Devices** – allows to set a static IP address binding on the MAC address of the device in the QX LAN. When this table is configured, the devices with defined hostnames and MAC addresses will always get the same LAN IP address from the DHCP server. Devices, not listed in this table, will get dynamic LAN IP addresses. This table is also displayed in the **System Configuration Wizard**.

To add a new host:

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

10.2.2 DHCP Advanced Settings

The **DHCP Advanced Settings** page is used to add new advanced options of the QX 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.

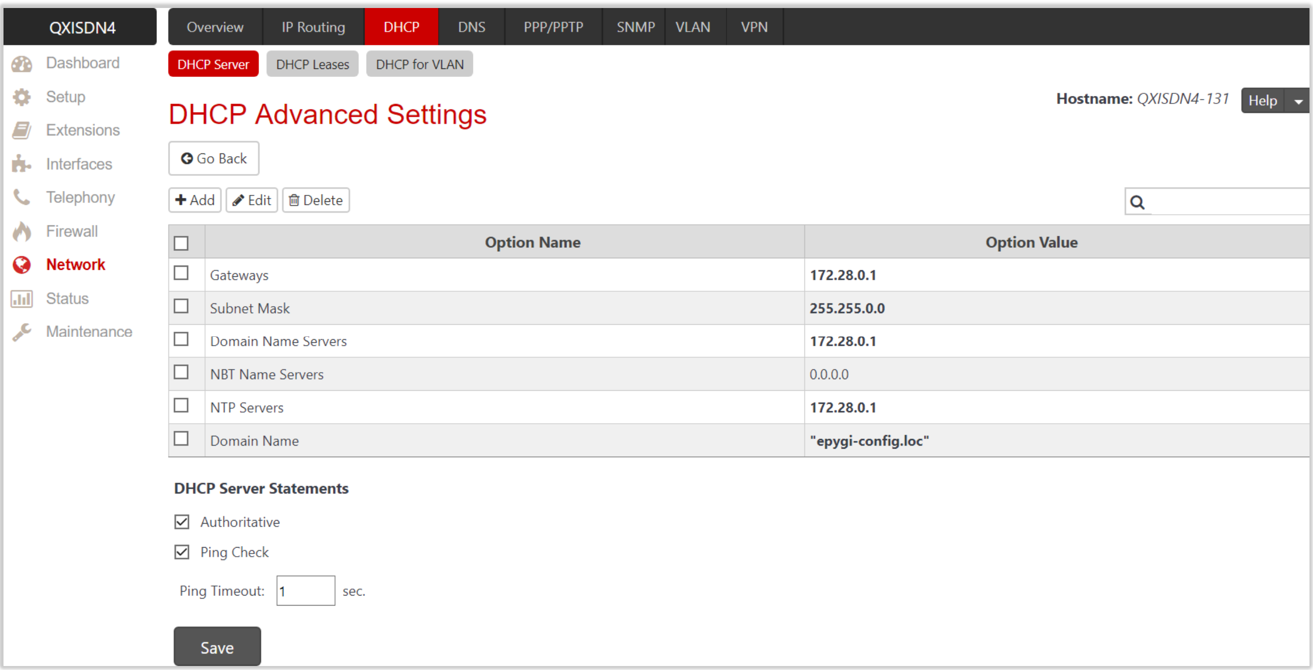


Figure 111: DHCP Advanced Settings page

To add a new DHCP option:

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

Note:

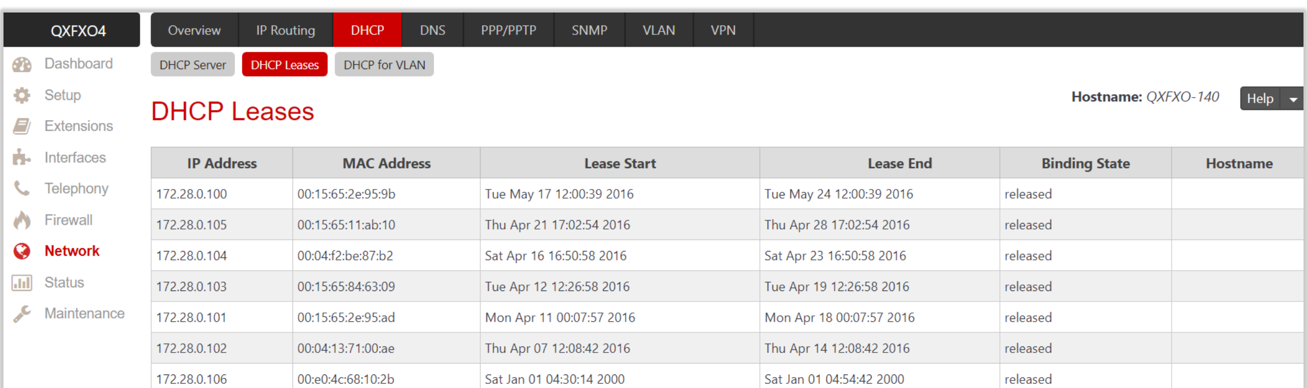
- If there are two or more values entered, they must be separated by commas.
- The changes made through the **System Configuration Wizard** regarding the DHCP server options will not immediately reflect on the **DHCP Advanced Settings** if DHCP sever option parameters are modified, so user will have 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** – enables/disables authoritative mode on the QX DHCP server. TIP: If several DHCP servers are used on the network and the QX has to provide network parameters to IP phones only then disable the **Authoritative** mode.
- **Ping Check** – if selected, verifies the availability of an IP address on the network before providing it to a client. The QX will first ping an 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** field (by default 1 sec), 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, the QX will provide an IP address immediately when requested.

10.2.3 DHCP Leases

The **DHCP Leases** page includes a list of the leased host addresses that are part of the QX LAN. For these hosts, QX acts as a server supplying them with a unique IP address. It displays a read–only table describing all the leased IP hosts and their parameters.



IP Address	MAC Address	Lease Start	Lease End	Binding State	Hostname
172.28.0.100	00:15:65:2e:95:9b	Tue May 17 12:00:39 2016	Tue May 24 12:00:39 2016	released	
172.28.0.105	00:15:65:11:ab:10	Thu Apr 21 17:02:54 2016	Thu Apr 28 17:02:54 2016	released	
172.28.0.104	00:04:f2:be:87:b2	Sat Apr 16 16:50:58 2016	Sat Apr 23 16:50:58 2016	released	
172.28.0.103	00:15:65:84:63:09	Tue Apr 12 12:26:58 2016	Tue Apr 19 12:26:58 2016	released	
172.28.0.101	00:15:65:2e:95:ad	Mon Apr 11 00:07:57 2016	Mon Apr 18 00:07:57 2016	released	
172.28.0.102	00:04:13:71:00:ae	Thu Apr 07 12:08:42 2016	Thu Apr 14 12:08:42 2016	released	
172.28.0.106	00:e0:4c:68:10:2b	Sat Jan 01 04:30:14 2000	Sat Jan 01 04:54:42 2000	released	

Figure 112: DHCP Leases page for LAN interface

- **IP Address** – host IP address, assigned by the QX.
- **MAC Address** – host MAC address, provided by the host itself.
- **Lease Start** – date and time when the leased IP address has been activated.
- **Lease End** – date and time when the leased IP address has been or will be deactivated.
- **Binding State** – indicates the state of the DHCP lease.
- **Hostname** – hostname, provided by the host itself.

10.2.4 DHCP Settings for the VLAN Interface

The **DHCP Settings for the VLAN Interface** page is used to establish virtual networks in the QX LAN or to integrate the QX into the corporate network's virtual LAN/WAN. DHCP service can be activated both on LAN or WAN interfaces. VLAN is useful in corporate companies to divide large networks into subgroups and to have devices like QXs and IP phones in each network separated (for example, to separate networks for data and voice transmission). Priorities may be assigned to the interfaces for packets prioritization.

With VLAN configuration, each virtual network will be characterized with a VLAN ID (tag). Packets addressed to that network will be checked towards the ID and if the ID number defined in the incoming packets matched the corresponding network's ID, the packets will be accepted. Otherwise, the packets will be dropped. In the same way, if the QX is integrated into the network that uses VLAN technology, outgoing packets should have the ID number of the corresponding virtual network, for the remote party to accept those packets.

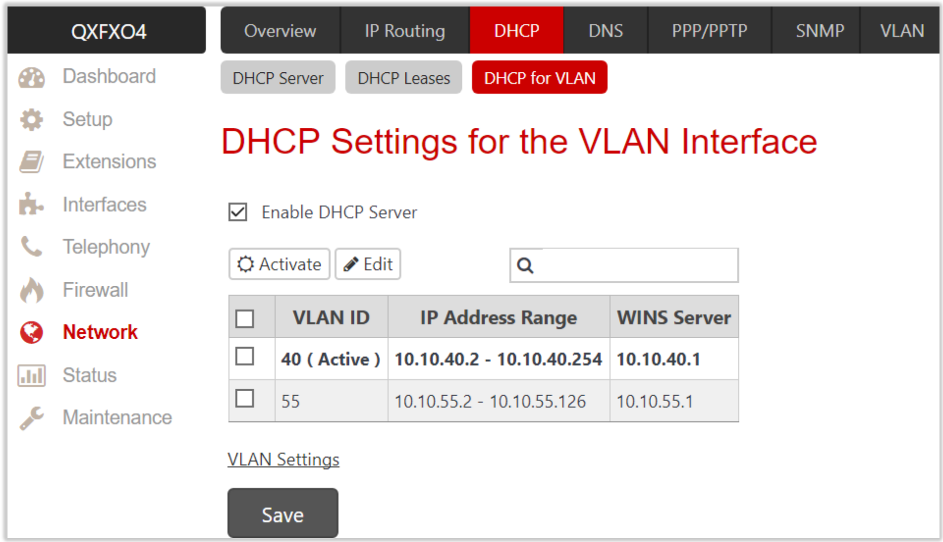


Figure 113: DHCP Settings page for VLAN interface

The **DHCP Settings for the VLAN Interface** table lists all enabled VLAN interfaces created in the **VLAN Settings** page and corresponding parameters (VLAN ID, IP Address Range and WINS Server).

- **Enable DHCP Server** – activates the DHCP server on QX for VLAN. If selected, the QX will be able to assign dynamic IP addresses to the devices in its VLAN.
- **Activate** – activates the DHCP service on one of the VLAN interfaces in the list. Only one VLAN interface can have DHCP service activated.
- **Edit** – is used to modify the selected VLAN interface. This page contains all the same components as the DHCP Server page.
- **VLAN Settings** – leads to the VLAN Settings page to create virtual LAN/WAN interfaces.

10.3 DNS Settings

The DNS Settings page provides the option of setting up a name server for the QX.

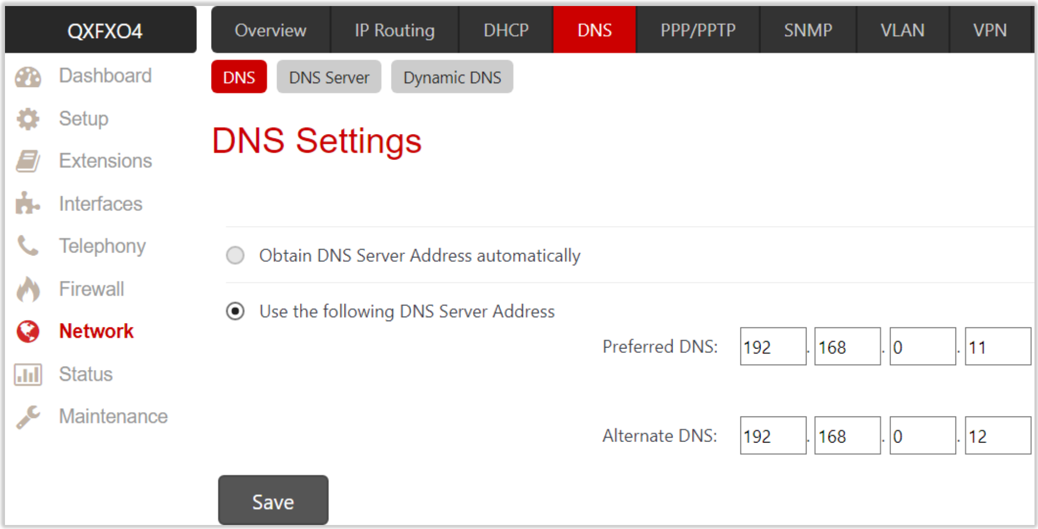


Figure 114: DNS Settings page

- Obtain DNS Server Address automatically – automatically configures the assignment of the name server address from the provider party.
- Use the following DNS Server Address – is used to manually assign a name server as follows:
  - Preferred DNS – enter the IP address of an external name server.
  - Alternate DNS – enter the IP address of the secondary name server that will be used if the main name server cannot be accessed.

10.3.1 DNS Server Settings

The DNS Server provides the services to the hosts in the QX LAN. With this service, QX returns the correct IP address to the requested domain name, so that any device in the LAN can be accessed by its hostname or alternative alias name. The DNS Server Settings page is used to configure DNS server settings on the QX and define a list of aliases for the devices in the QX's LAN.

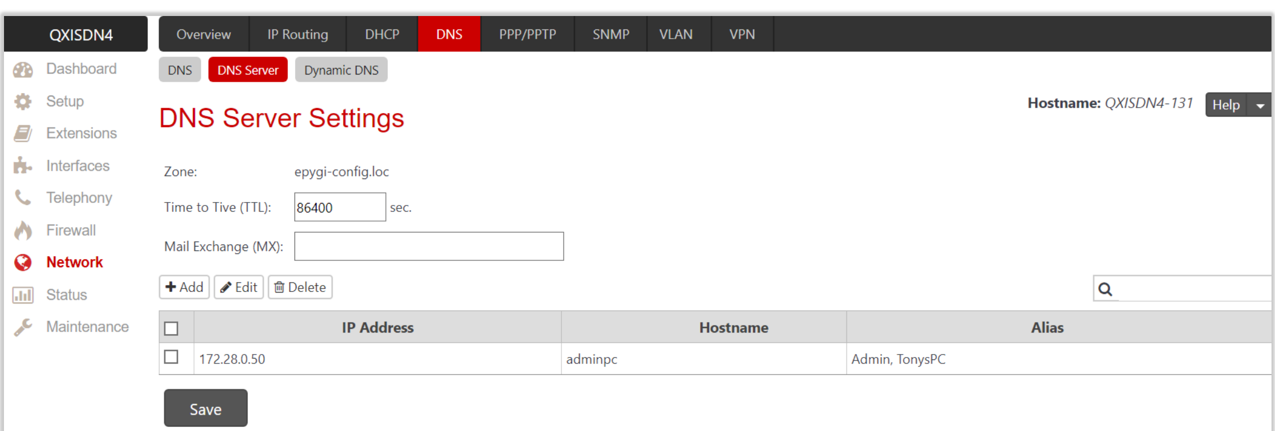


Figure 115: DNS Server Settings page

- Zone – shows the QX's domain name 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. When this 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 the external network. The value in this field will be used in the MX record in the DNS server on the QX.

The table on this page lists aliases for each of the device in the QX's LAN to be resolved through the DNS server.

To add a new host:

1. Click Add and enter the following information:
   - IP Address – enter the IP address of the host.
   - Hostname – enter the hostname of the device.
   - Alias – enter up to 5 alias names by which the device will be resolved.
2. Click Save, the new host will be added to the DNS Server Settings table.

10.3.2 Dynamic DNS Settings

The Dynamic DNS (DynDNS) service is used to map a dynamic IP address to a host name. This service is used if you are connected to the Internet with a dynamic IP address (and PPP, DHCP client) and want to allow access from the Internet to a device behind the firewall. For example, if you want to run your own WEB server.

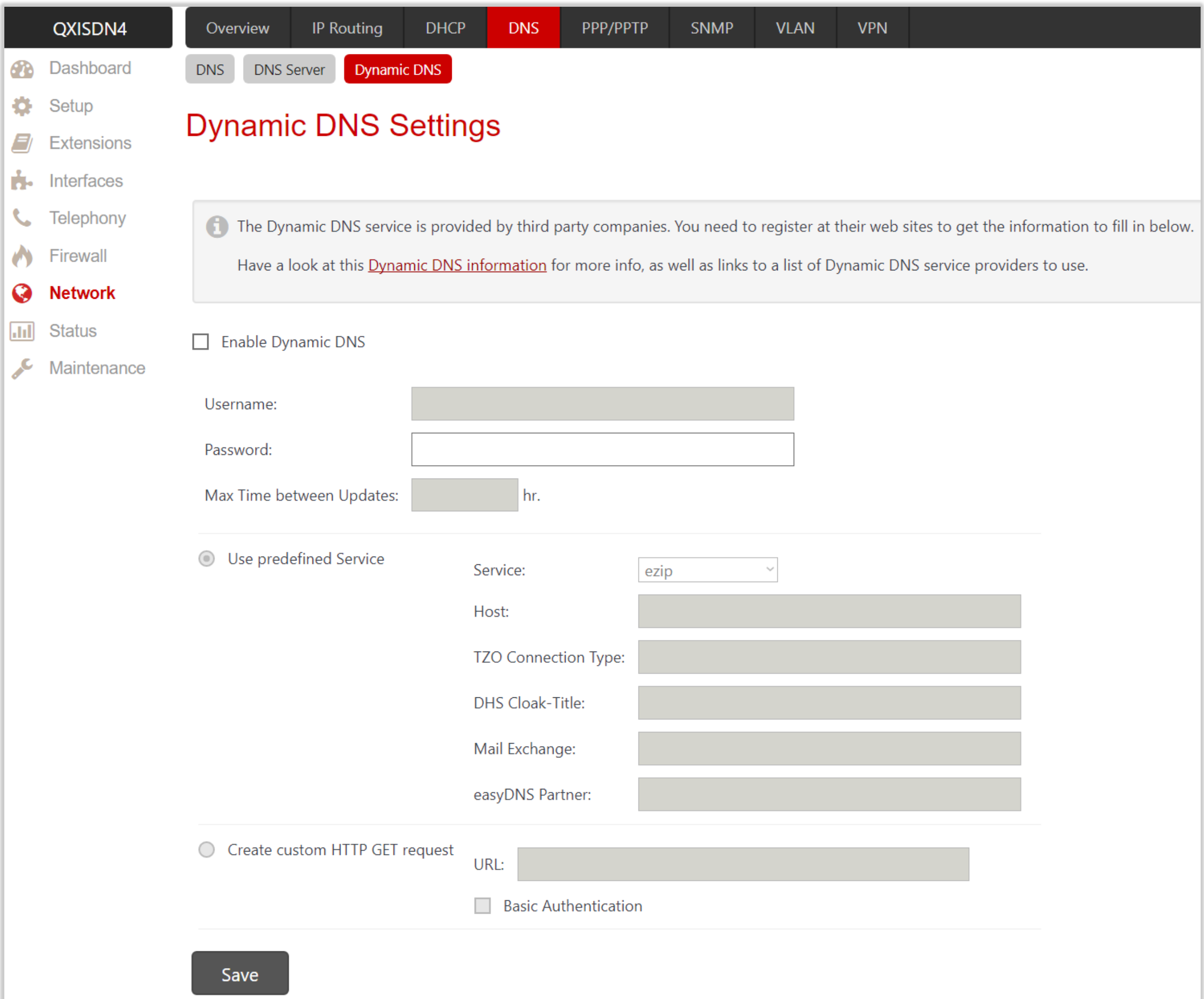


Figure 116: Dynamic DNS Settings page

- Enable Dynamic DNS – enables the dynamic DNS service. To enable the DynDNS service on QX gateway, you first have to choose a DynDNS provider and register at their website.
- Username and Password – is used to define the authentication parameters specified during the registration at the DynDNS provider.
- Max time between Updates – is used to define the period between two updates (in hours). 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 – select the provider to be subscribed to.
  - Host – enter the name of the host on the Internet.
  - TZO Connection Type – enter a special parameter required by the DynDNS provider TZO.
  - DHS Cloak-Title – enter a special parameter required by the DynDNS provider DHS.

- Mail Exchange – enter the address of the email server the DynDNS service provider will relay emails to. If this service is used, ensure that there is port forwarding configured for SMTP (port 25) to the internal email server.

- easyDNS Partner – 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, press Create Custom HTTP GET Request and enter the appropriate value into the URL text field.
  - URL – is used to define the complete request to be sent to the DynDNS server. The request modifies the nameserver 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 authentication settings.

Most of the DynDNS providers require an authentication for security. Authentication parameters can be provided in the URL text field to be used for the HTTP get request. The Basic Authentication checkbox can be selected if no authentication parameters to be provided.

10.4 PPP/ PPTP Settings

The PPP/PPTP Settings are used to establish a connection over the DSL link, or any other type of uplink, to the ISP. A connection is needed to set up and make or receive calls through PPP over Ethernet. The connection may be configured for manual setup or always up. Once a connection has been established between the QX and the provider, QX users will be able to make and receive calls at any time.

- PPTP Server – is used to define the IP address of the PPTP server.
- Encryption – is used to select the encryption for the traffic over the PPTP interface.
- Keep Connection Alive – keeps the connection alive by sending control packets dedicated to the link state verification.
- Authentication Settings – are used to enter the authentication parameters (Username and Password) to register on the ISP server.
  - Dial manually – if selected, a button will be displayed in the main management window that serves to switch the Internet connection on/off. When accessing the Internet, every station of the connected LAN has to connect to the QX first.
  - Always connected – if selected then the QX will always stay in the connected mode.

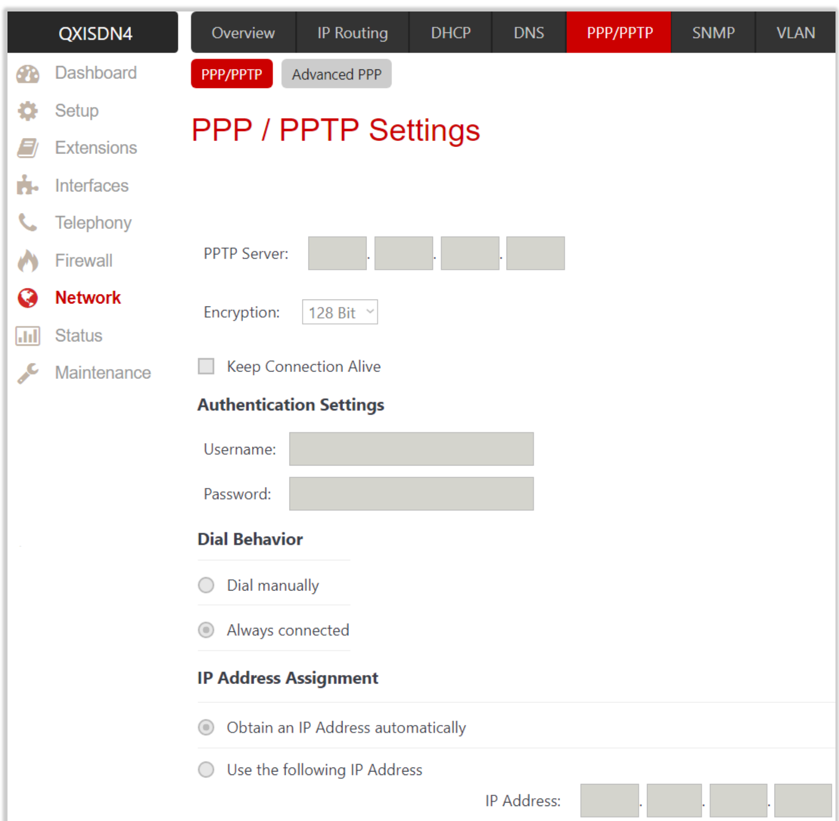


Figure 117: PPP/PPTP Settings page

- IP Address Assignment – is used to define the IP address assignment for the PPP interface with the following options:

- Obtain an IP Address automatically – with this option selected, QX will use DHCP to get an available IP address from your local network or ISP.
- Use the following IP Address – manually assign an IP address to the PPP interface.

10.4.1 Advanced PPP Settings

The Advanced PPP Settings are used to enable/disable certain parts of the negotiation process during connection establishment. These settings are available only if QX has a PPPoE WAN interface.
Note: It is strongly recommended to leave these switches unchanged if their meanings are not completely clear.

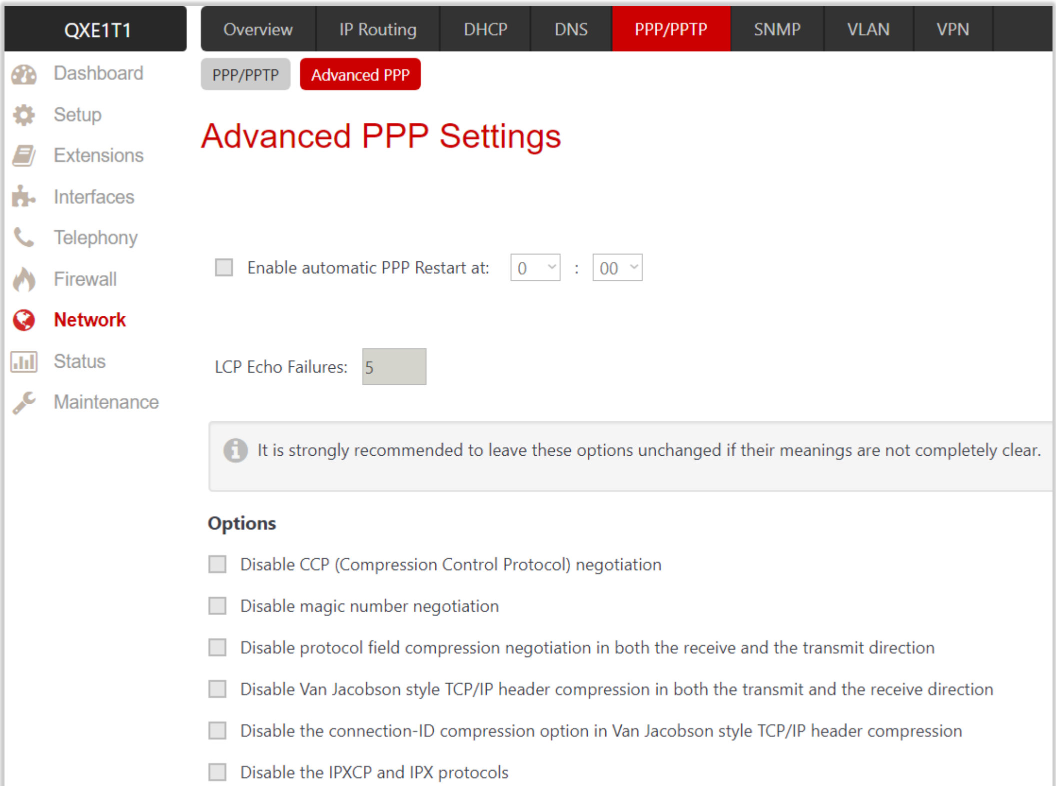


Figure 118: Advanced PPP Settings page

- Enable automatic PPP Restart – is used to select the time when the PPP connection will automatically be restarted.
- LCP Echo Failures – displays 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 – select if the peer system is not working properly. For example, if it is not accepting the requests from the PPPD (Point-to-Point Daemon) for CCP negotiation.
- Disable magic number negotiation – select if the peer system is not working properly. If selected, PPPD 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** – select if the peer is not working properly and cannot handle requests from PPPD for IPXCP negotiation.

10.5 SNMP Settings

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

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

For more information on how to configure and use **SNMP**, please refer to the Configuring SNMP Agent on QX IP PBXs guide.

10.6 VLAN Settings

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

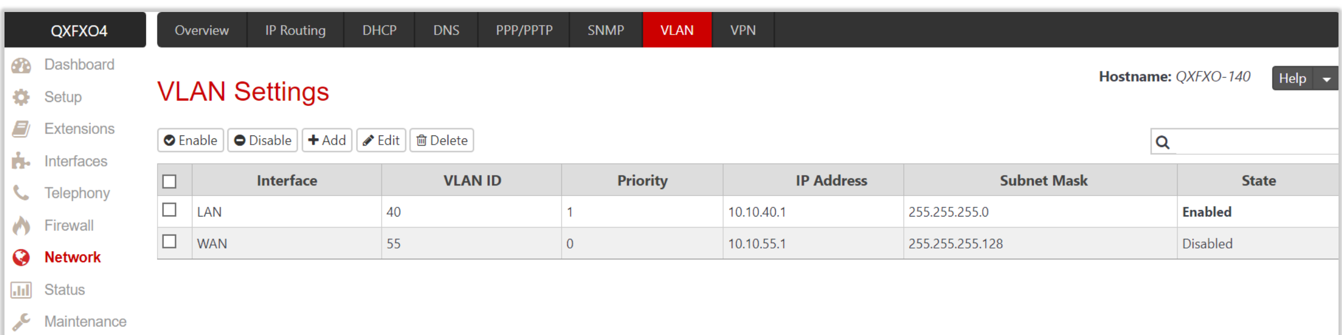


Figure 119: VLAN Settings page

To configure a new VLAN interface:

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

10.7 VPN Configuration

The Virtual Private Network (VPN) is established 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. Only authorized users may access the network and the data exchange cannot be intercepted.

In general, the VPN connection is similar to the Internet connection, both of them are based on the IP detection. The VPN gateway must authenticate the IP addresses of its partners' VPN gateways. Each time a specific VPN is to be established, usually the same IP addresses are expected. This will not create problems if both VPN partners have fixed WAN IP addresses. There may be circumstances reasons to prefer dynamically allocated IP addresses. To enable devices that use a variable IP address as part of a VPN, they are turned into "Road Warriors". For example, at this point they are able to reach their corporate network via authentication at the company's VPN gateway device. This VPN gateway device must have a fixed IP address for Internet access. Every VPN needs at least one VPN gateway with a fixed IP address.

The partner devices of a VPN must have different WAN IP addresses, and if they are connected to local area networks, these LAN's must have different IP addresses. As all QX 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.

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

10.7.1 IPSec Configuration

An IPSec connection includes authentication and encryption to protect data integrity and confidentiality. VPNs are "virtual" in the sense that individuals can use the public Internet as a means of securely accessing an internal network. Once the IPSec connection is established, users have access to the same network resources, addresses, and so forth as if they were connected locally. VPNs are "private" because the data is encrypted between two VPN gateways. Encryption makes it very difficult for anyone to intercept data and capture sensitive information such as passwords. The QX can be set up to act as a VPN router when connected to the Internet with a fixed IP address or as an IPSec connection Road Warrior when using dynamic IP addresses.

To establish an IPSec connection, it is required to have an operational VPN gateway on each side of the communication line. QXs, PCs and workstations can be equipped with VPN gateways. Home offices typically prefer dynamically allocated IP addresses. When the QX is connected to the Internet with a fixed IP address, it will be set up to act as a VPN gateway. QX is then prepared to establish an IPSec connection with another VPN gateway device, but also allows access to Road Warriors. A notebook /laptop used by a traveling employee could also be a Road Warrior. Access to their company's intranet via an IPSec connection can be obtained regardless of their location.

The QX can also be set up to act as a Road Warrior. If a home office is connected to the Internet via QX with Point to Point Protocol over Ethernet (PPPoE) and dynamic IP addressing, setting up the QX as a Road Warrior will allow an IPSec connection to the corporate network.

You need to use a key to encrypt and decrypt the data transmitted via the IPSec connection. RSA is an asymmetric key system used by the QX. It has to be available on both sides of the IPSec connection and will generate a different pair of keys on each side, a private key and a public key. During the connection establishment, some data is encrypted with the remote party's public key. They can be decrypting the data with their private key and the data encrypted there with QX's public key can be decrypted with QX's private key. Since the private key is never transmitted, it stays completely unknown to everyone, thus the system remains safe. Even if someone gets the public key, decryption cannot be possible without the private key. The QX generates such a pair of keys automatically when it is set up. The user cannot see the private key, but must know the public key because their IPSec connection partner will need it.

Note: A pair of keys will always be generated, a public one and a private one. The previously generated pair of keys will become invalid as well as all existing IPSec connections that use RSA keying.

The **IPSec Configuration** page consists of two sub-pages: **Connection** and **RSA Key Management**.

Connection

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

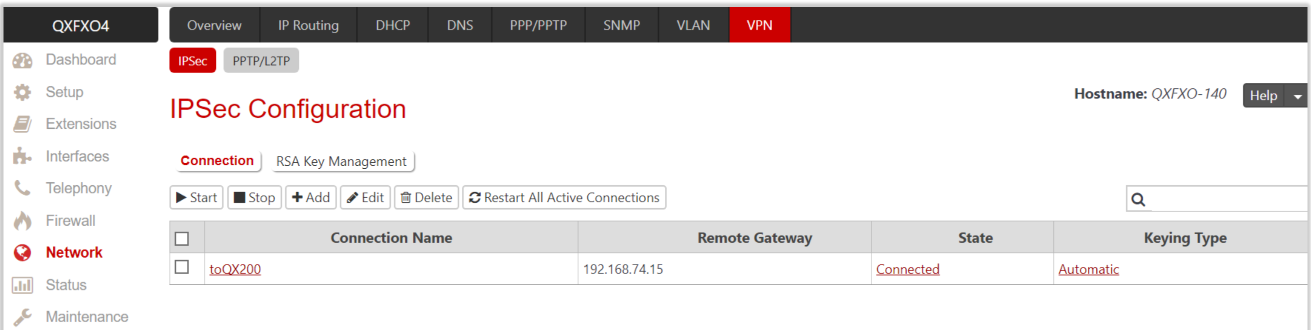


Figure 120: IPSec Configuration – Connection Settings page

The following buttons are available:

- **Start** – activates the selected IP Sec connection. The **State** will be changed to *Activated* or *Connected* depending on the IPSec connection type.
- **Stop** – disconnects the selected IPSec connection. The state of the IPSec connection will be changed to *Stopped*.
- **Edit** – leads to the **IPSec Configuration Wizard** to modify the parameters of the selected IPSec connection.
- **Delete** – removes the selected IPSec connection(s) from the table.
- **Restart All Active Connections** – restarts all active IPSec connections. The **State** of these IPSec connections will turn into **Connected** or **Activated** if the restart procedure has been successfully completed.
- **Add** – leads to the **Add IPSec Connection** wizard to define a new IPSec connection.

The **IPSec Configuration** wizard composed of the following sections:

- New IPSec Connection
- IPSec Keying Properties
- Automatic Keying
- IPSec Connection Properties
- Summary

New IPSec Connection

- **Connection Name** – enter the name of a new IPSec connection.
- **Peer Type** – select the remote machine type for the IPSec Connection to be established. If the list does not include the required type of machine, choose **Other**.

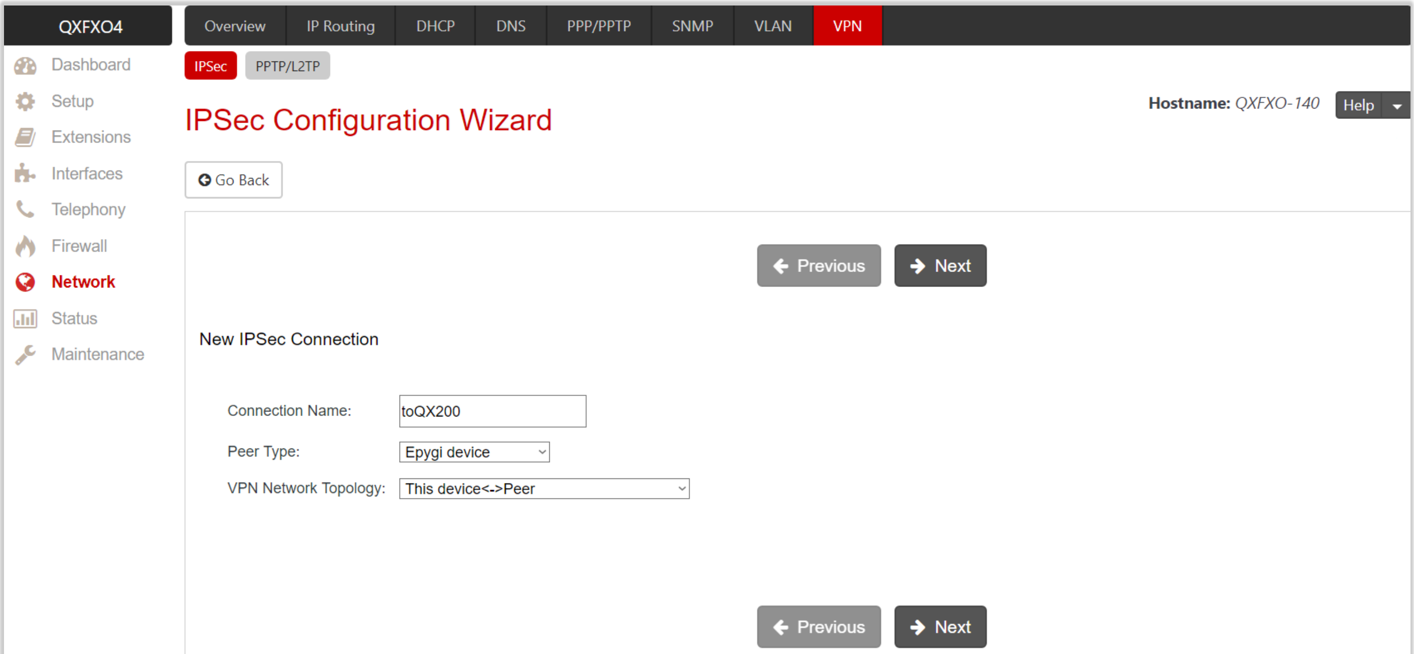


Figure 121: New IPSec Connection section

- VPN Network Topology – select the location of the peers participating to the VPN connection. The following options are available:
  - ➢ This device<>Peer – direct connection between the QX and peer.
  - ➢ This device<>[Internet]<>Peer – connection between the QX and peer over Internet.
  - ➢ This device<>NAT<>[Internet]<>Peer – connection between the QX and peer over Internet through QX provider's NAT.
  - ➢ This device<>[Internet]<>NAT<>Peer – connection between the 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 DES encryptions on a single data block with three different keys to achieve a higher security than is available from a single DES pass (block cipher algorithm with 64-bit blocks and a 56-bit key).
  - ➢ AES (128 bit) cryptography scheme is a symmetric block cipher, which encrypts and decrypts 128-bit blocks of data.
  - ➢ AES (192 bit) cryptography scheme is a symmetric block cipher, which encrypts and decrypts 192-bit blocks of data.
  - ➢ AES (256 bit) cryptography scheme is a symmetric block cipher, which encrypts and decrypts 256-bit blocks of data.

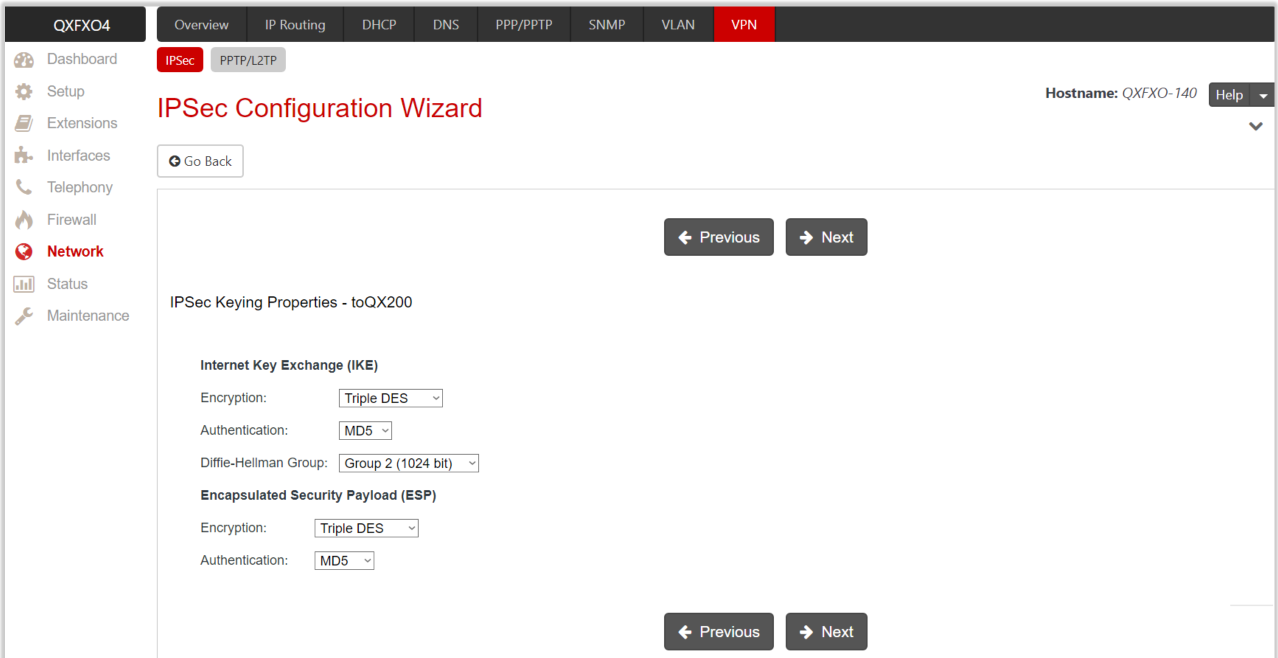


Figure 122: IPSec Keying Properties section

The ESP parameters group is used to provide origin authenticity, integrity and confidentiality protection of packets. The same IKE encryption and authentication parameters are used.

- Authentication – is used to select authentication type:
  - SHA/SHA1 (Secure Hash Algorithm) is a strong digest algorithm proposed by the US NIST (National Institute of Standards and Technology) agency as a standard digest algorithm and is used in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash. SHA and MD5 are the message digest algorithms available in IPSEC.
  - MD5 (Message Digest) is a hash algorithm that makes a checksum over the messages. The checksum is sent with the data and enables the receiver to notice whether the data has been altered.
- 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.

Automatic Keying

The Automatic Keying section is used to specify a Shared Secret password or RSA public key to secure the IPSec Connection.

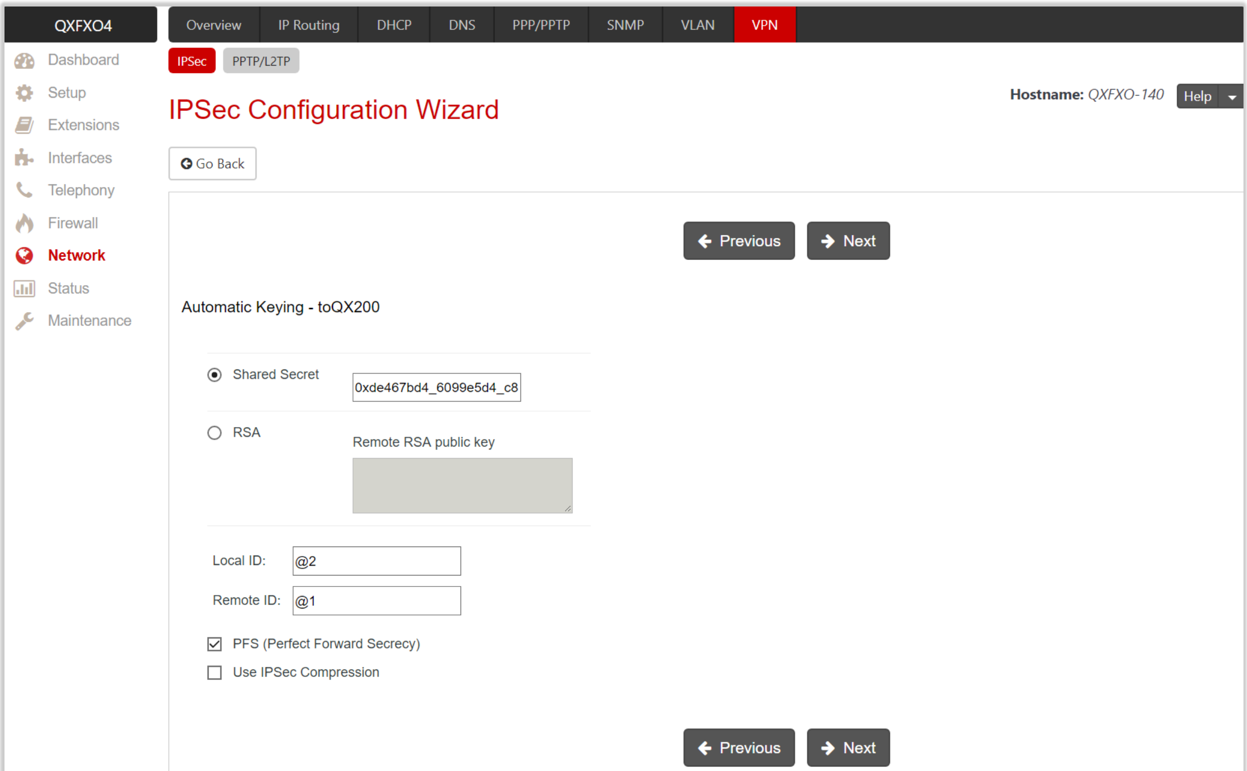


Figure 123: Automatic Keying Settings section

- 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 define the QX FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.
- Remote ID – is used to define the IPSec Connection partner's FQDN (Fully Qualified Domain Name) that is resolved to an IP address, or any @-ed string that is used in the same way.

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

- IP address – example: 10.1.19.32.
- Host name – example: vpn.epygi.com. This form requires additional resources to resolve the host name, therefore it is not recommended to use this format.
- @FQDN – example: @vpn.epygi.com. This form is considered as a string, and is not being resolved. It is recommended to use this form for most applications.
- user@FQDN – example: qx@vpn.epygi.com. This form is also considered as a string, and is not being resolved. It has no advantages over the previous form.

- PFS (Perfect Forward Secrecy) – is a procedure of system key exchange, which uses a long-term key and generates short-term keys as is required. Thus, an attacker who acquires the long-term key can neither read previous messages that they may have captured nor read future ones.
- Use IPSec Compression – enables IPSec data compression. This option is displayed only if the IPSec-VPN partner supports it.

Note:

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

IPSec Connection Properties

Dynamic IP/Road Warrior and Static IP/ Remote Gateway 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 options is used to configure IPSec connection:

- Dynamic IP/RoadWarrior – if selected, then the Remote Gateway IP Address field will automatically generate the value "any", to allow access independent from the sending IP address.
- Static IP/Remote Gateway – is used to enter the IP address or hostname of the remote QX (or another VPN gateway device) in the Remote Gateway field.
- This device<>Remote Gateway – allows 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 first page of the IPSec Connection Wizard.
- Local Subnet<>Remote Gateway – allows access from all stations connected to the local network to the remote VPN gateway device (local QX 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 first page of the IPSec Connection Wizard.
- This device<>Remote Subnet – allows 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 first page of the IPSec Connection Wizard.
- Local Subnet<>Remote Subnet – allows access from all stations of the local network to all stations of the remote LAN (VPN gateway devices are not included). In this case, the local and remote subnet IP addresses and subnet masks have to be entered in the corresponding fields Local Subnet IP and Remote Subnet IP.
- Stop connection if not successful – allows to stop the IPSec connection attempts if the partner remains unreachable after the timeout period. If not selected, then the system will continue to try to reach the IPSec connection partner.

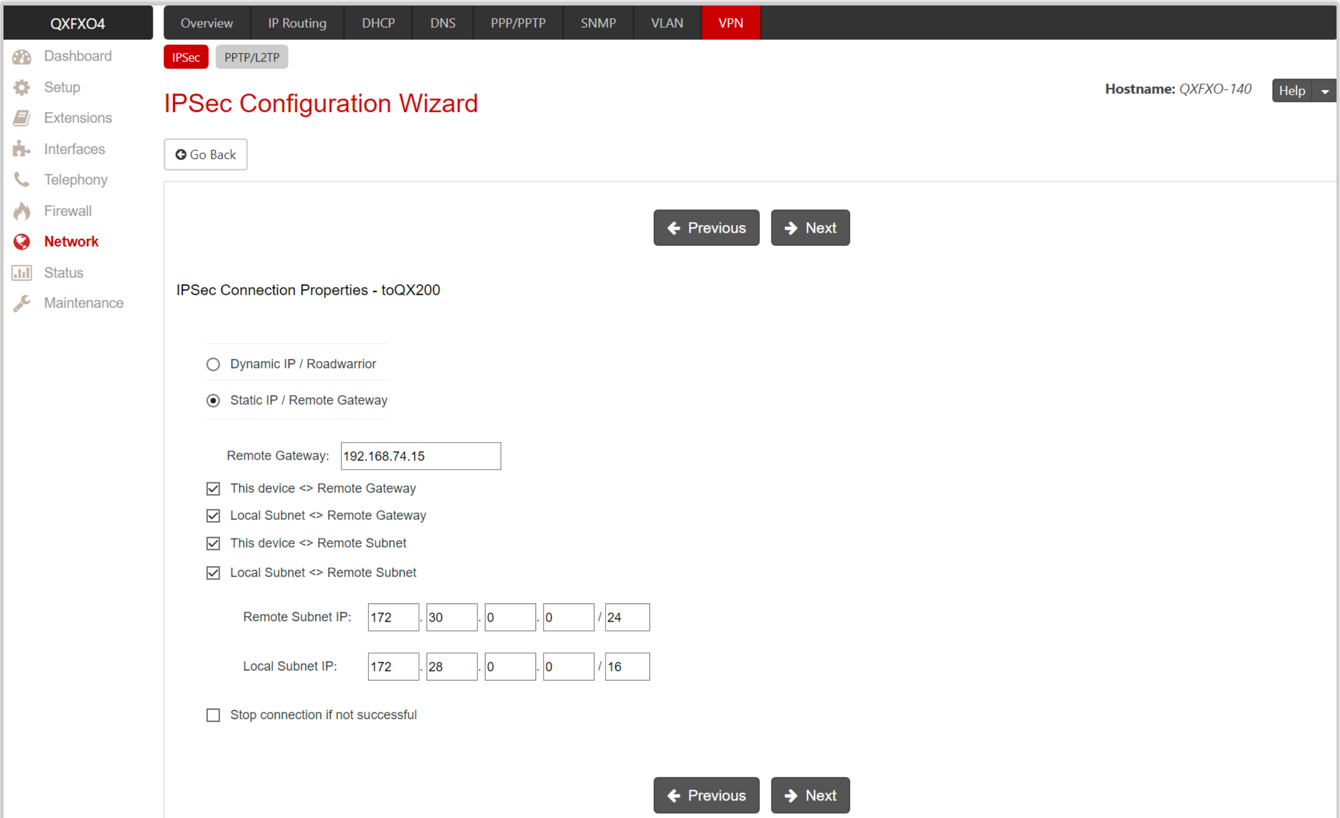


Figure 124: IPSec Connection Properties section

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

Summary

The **Summary** section displays all configured settings for the IPSec connection.

RSA Key Management

The **RSA Key Management** sub-page is used to generate a new RSA Key. Also, this page displays the current public RSA key and allows to send it to the IPSec connection partner.

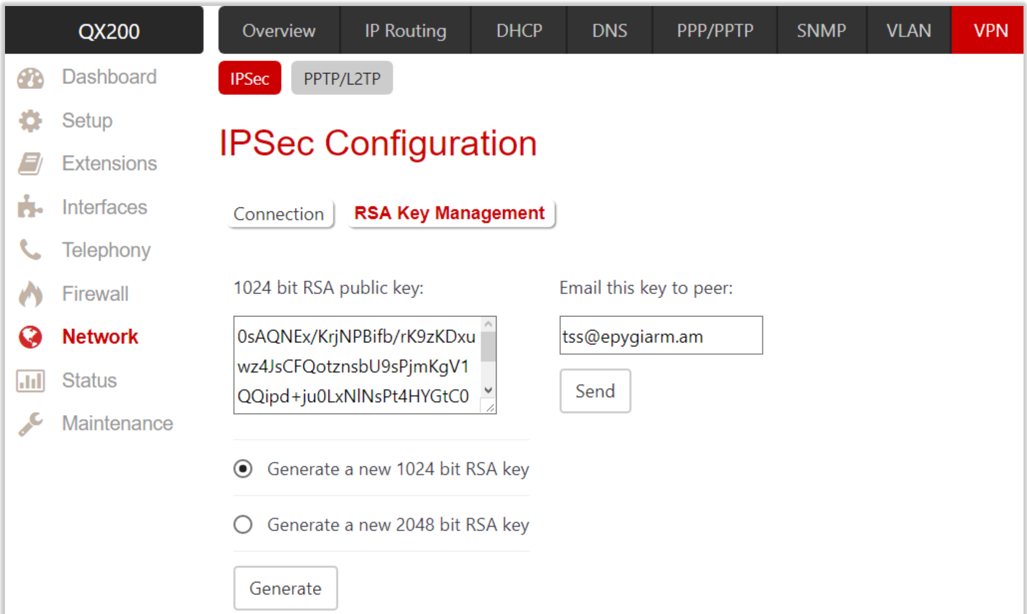


Figure 125: RSA Key Management page

To generate a new RSA key:

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

10.7.2 PPTP/L2TP Configuration

Point-to-Point Tunneling Protocol (**PPTP**) is used to establish a VPN over the Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers. PPTP encapsulates any type of network protocol (IP, IPX, etc.) and transports it over IP. Therefore, if IP is the original protocol, IP packets ride as encrypted messages inside PPTP packets running over the IP. PPTP is based on the Point-to-Point Protocol (**PPP**) and Generic Routing Encapsulation (**GRE**) protocol. Encryption is performed by Microsoft's Point-to-Point Encryption (**MPPE**), which is based on RC4.

Layer 2 Tunneling Protocol (**L2TP**) is a protocol from the IETF, which allows a PPP session to run over the Internet, ATM, or frame relay network. L2TP does not include encryption (as does PPTP), but defaults to using IPSec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN. Derived from Microsoft's Point-to-Point Tunneling Protocol (**MPPTP**) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP remote access concentrator (**LAC**). The LAC transmits the L2TP packets over the network to the L2TP network server (**LNS**) at the corporate side. Large carriers also may use L2TP to offer remote POPs to smaller ISPs. Users at the remote locations dial into the modem pool of an L2TP access concentrator, which forwards the L2TP traffic over the Internet or private network to the L2TP servers at the ISP side, which then sends them on to the Internet.

For **PPTP** and **L2TP** connections, two parties are required: **Client** and **Server**. The client is responsible for establishing the 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 Client hosts participating in a connection. Each side is specified by the **Host Name** and **Password**. The client should know the server's name and password (the QX server has no password) and the server should set the client's host name and a password. The client and server settings have to match on both sides for successful connection establishment.

Note:

- L2TP tunnels have no data encryption mechanism.
- Only one client can be connected to the server in the same network.

The **PPTP/L2TP Configuration** page consists of 3 sub-pages: **Connections**, **PPTP Server Configurations** and **L2TP Server Configurations**.

Connections

The **Connections** sub-page lists all existing connections characterized by their **Connection Name**, **Type** (PPTP or L2TP), **Client/Server** mode, **State**, **Remote Hostname IP** (IP address or hostname of the connection peer) and **Status**. The state of the PPTP and L2TP Connections, except for the "**Stopped**" state, is established as a link that refers to the page where login/logout information about the connection status is displayed. Logs can be useful to determine problems on PPTP or L2TP connections failure.

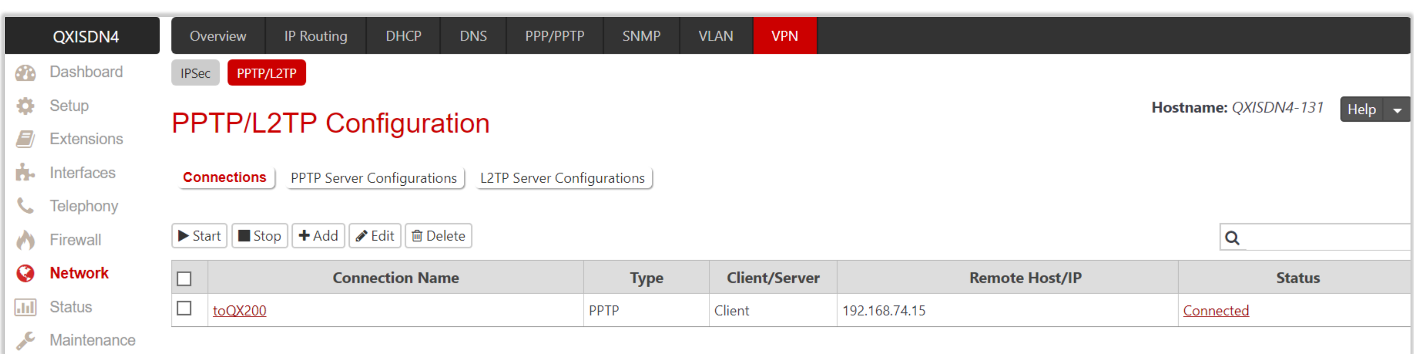


Figure 126: PPTP/L2TP Configuration – Connections page

- Start – initiates the selected connection(s). If it is a client connection, then this button initiates a client activity of reaching the server.
- Stop – stops the selected connection(s). Stopping the server connection will disconnect all connected clients and close the PPTP/L2TP tunnel.
- Add – leads to the PPTP/L2TP Connection Wizard to establish a new connection.

Note: 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.

The PPTP/L2TP Connection Wizard composed of the following sections:

- New PPTP/L2TP Connection
- PPTP Connection Properties
- Summary

New PPTP/L2TP Connection

- Connection Name – enter connection name. The name cannot start with a digit symbol; however, it can contain digits further in the name.
- Connection Type – select the type of the connection (PPTP or L2TP).

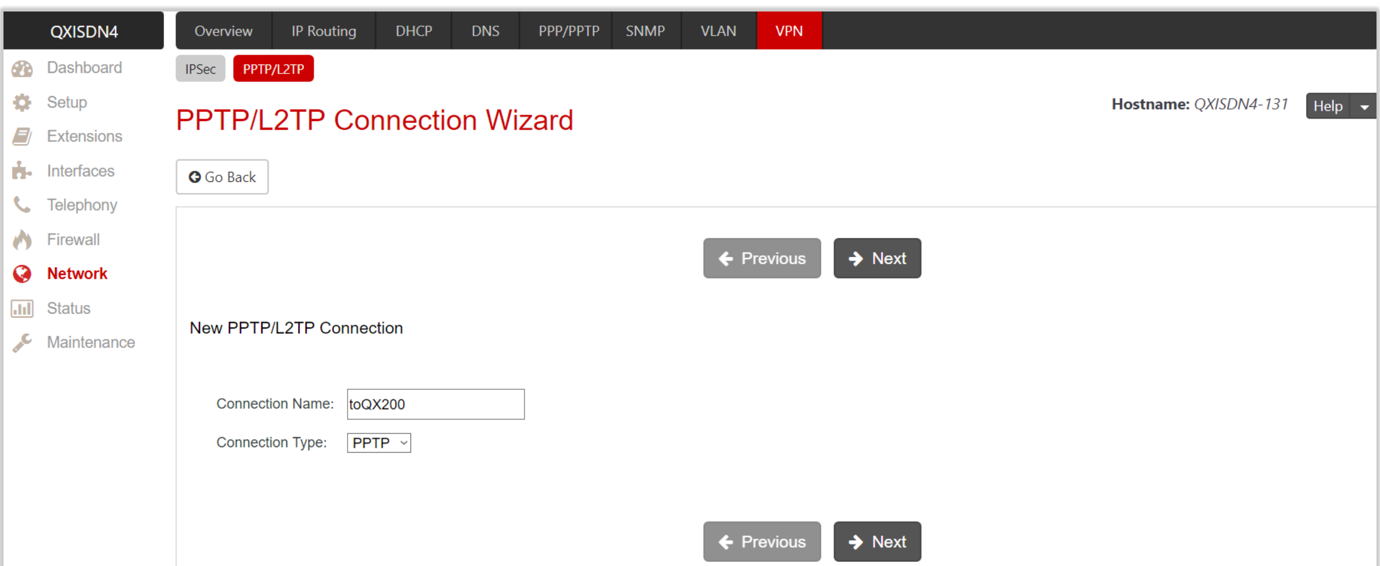


Figure 127: New PPTP/L2TP Connection section

PPTP Connection Properties

- Peer Name – 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 the QX's host name and Dial-in access exists on the server. When creating a connection with a Windows Client, ensure that the Peer Name specified on this page matches the Dial-in connection's username.

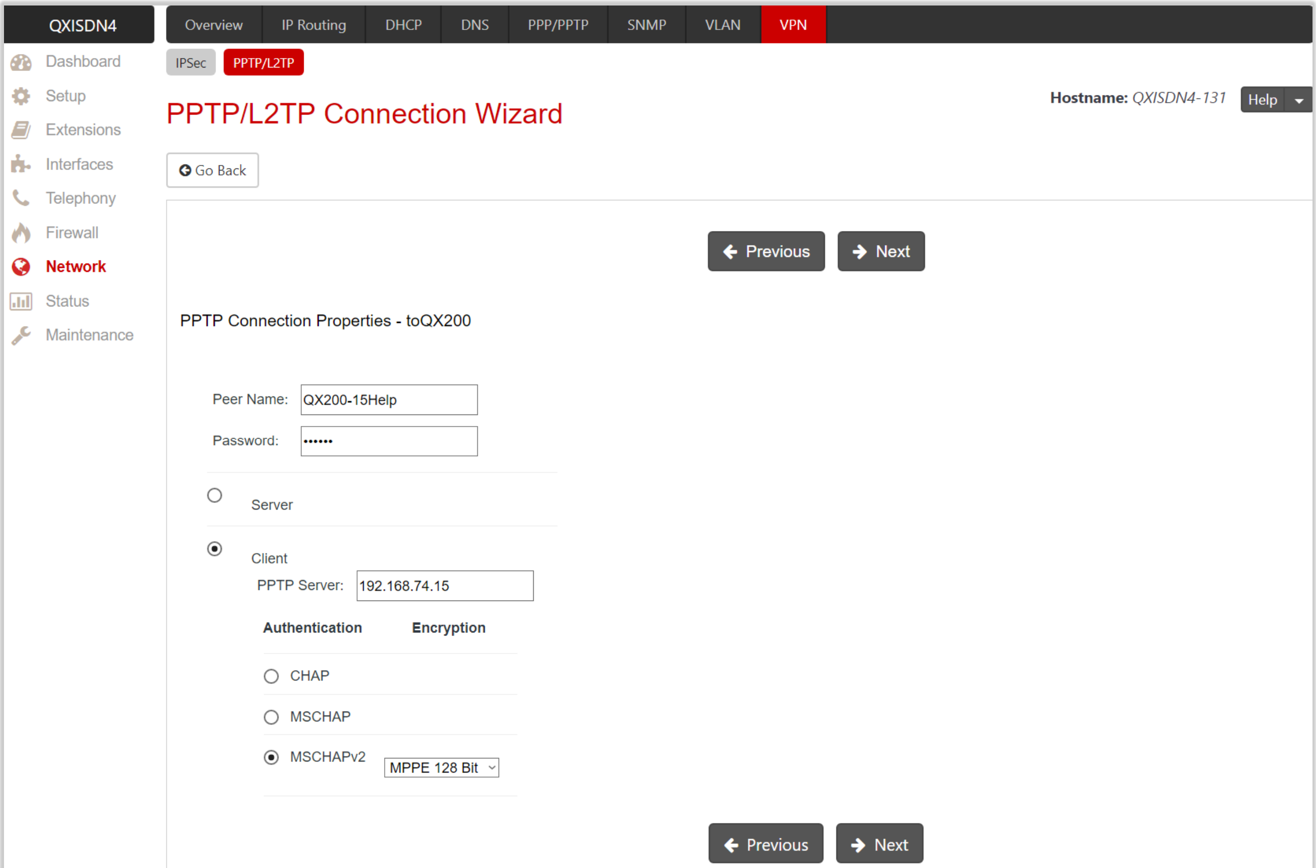


Figure 128: PPTP/L2TP Connection Wizard for PPTP connection

- Password – enter the password.
- Server/Client – select whether the new connection will be a server or client. For the Client radio button selection following information needs to be provided:
  - PPTP Server (if the PPTP connection type is selected) – enter an IP address or a host name of the PPTP server.
  - L2TP Server (if the L2TP connection type is selected) – enter an IP address of the L2TP server.
  - Authentication (N/A for PPTP connection) – select the authentication protocol through which the client will communicate with the server. 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 establishment.

Summary

The Summary section displays all configured settings for the PPTP/L2TP connection.

PPTP Server Configurations

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

- Subnet – is used to enter the IP address range for the PPTP server and clients within the PPTP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the PPTP connection. 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 corresponding 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.

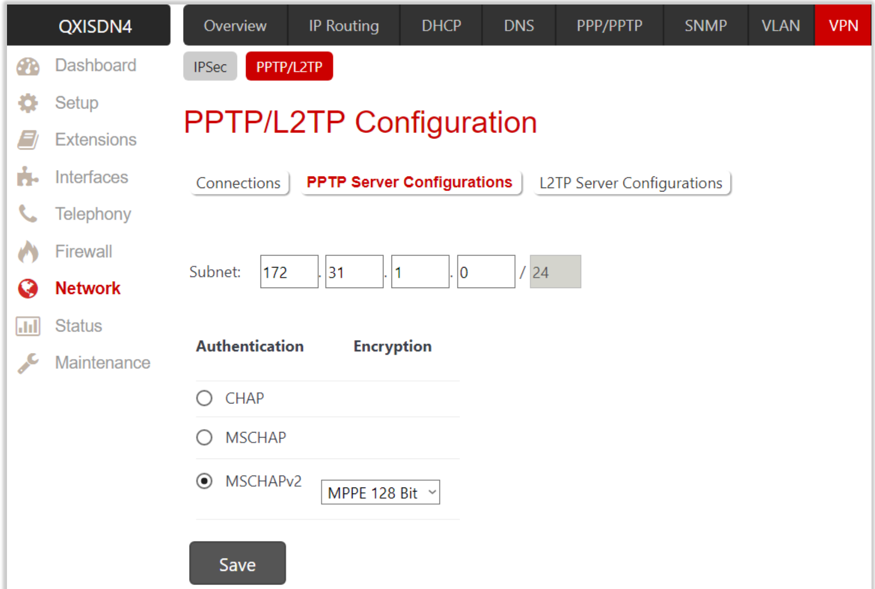


Figure 129: PPTP Server Configuration page

L2TP Server Configuration

The L2TP Subnet is used to enter the IP address range for the L2TP server and clients within the L2TP tunnel. The value specified for the subnet mask is fixed to 24 to restrict the possible number of clients for the L2TP connection. 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.

10.8 Local Client Configuration

The Local Client Configuration page (available only for QXFXS24) is used to upload the OpenVPN configuration file allowing to act QXFXS24 as an OpenVPN client. The OpenVPN configuration file should be uploaded on the QXFXS24 without any changes.

For information on how to configure and use OpenVPN, please refer to the OpenVPN Service on QX IP PBXs and Auto Configuration of Epygi Supported IP Phones using OpenVPN guides.

11 Status Menu

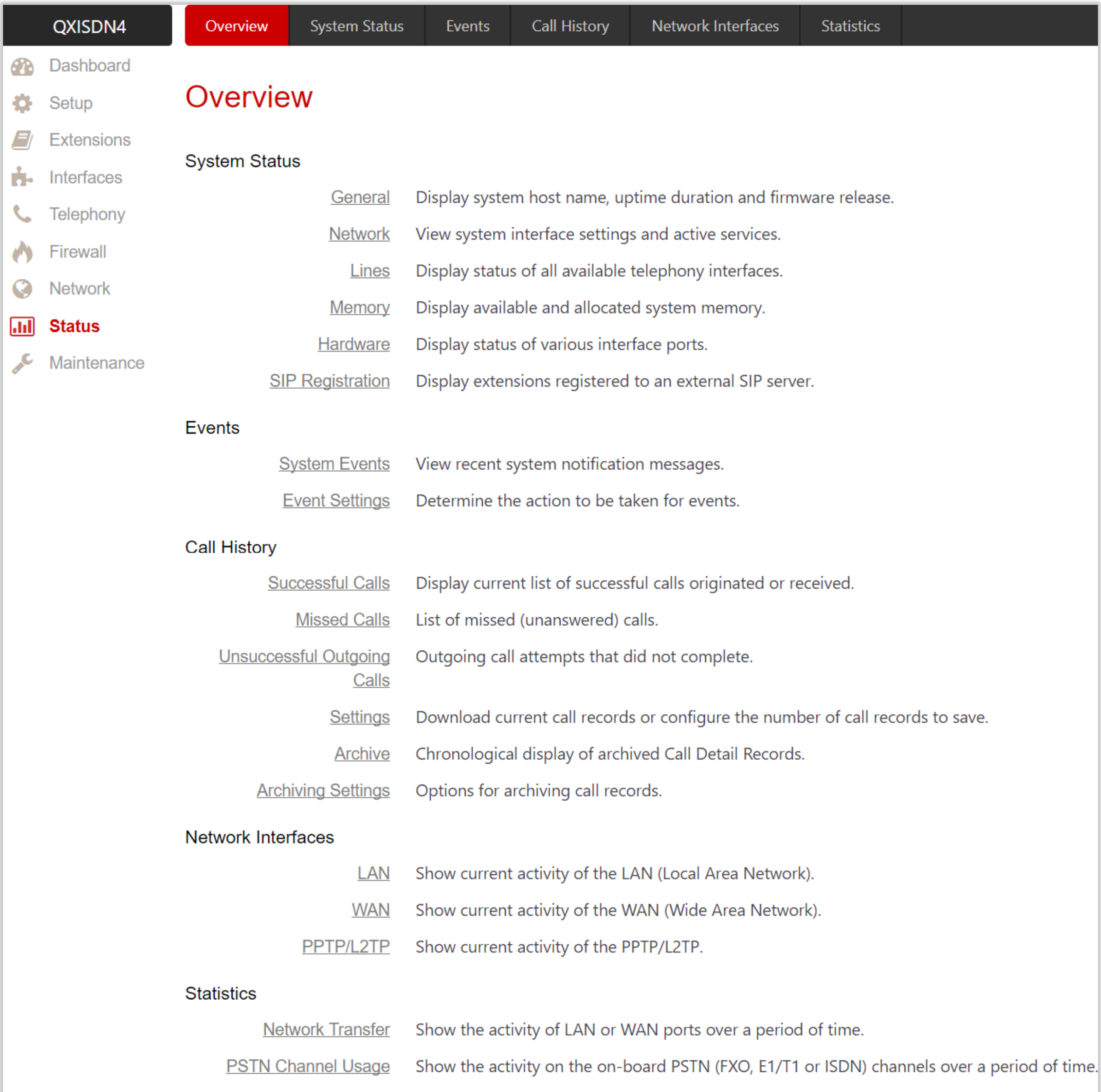


Figure 130: Status Menu overview

11.1 System Status

11.1.1 General Information

The General Information page provides the following information:

- Uptime Duration – time period the QX is running since last reboot.
- Device Hostname – displays the QX device host name.
- Firmware Version – the version of the QX's 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.

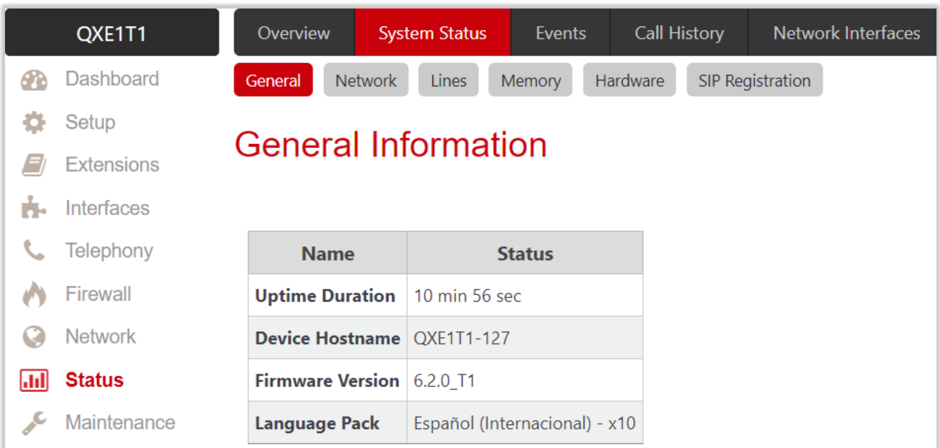


Figure 131: Status – General Information page

11.1.2 Network Status

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

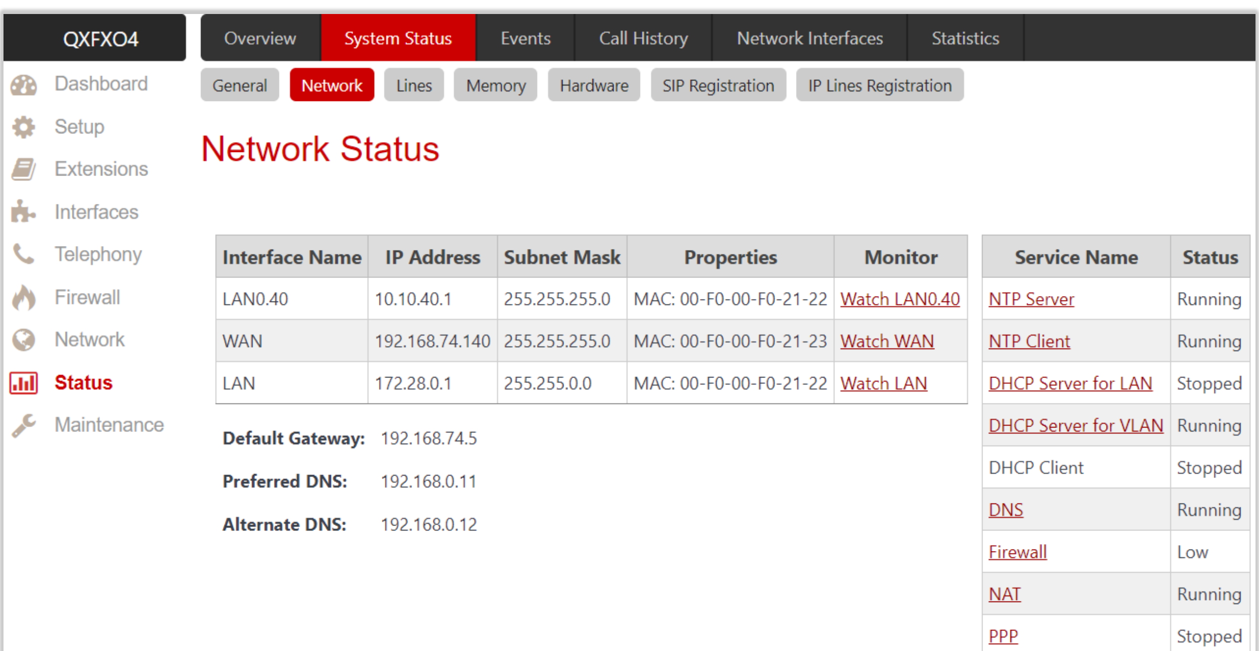


Figure 132: Status – Network Status page

The Network Status table displays the following information:

- Interface Name – network interfaces (LAN, WAN, VLAN and etc.) available and configured on the QX.
- IP Address – IP address for the network interface.
- Subnet Mask – subnet mask for the network interface.
- Properties – MAC address for the network interface or additional information about the interface.
- Monitor – allows to watch and monitor the interface.

The Preferred DNS, Alternate DNS and Default Gateway display the corresponding settings of QX, configured in the Internet Configuration Wizard.

The Services table displays the available services (NTP Server and Client, DHCP Server and Client, DNS, Firewall, NAT, PPP) with their current status.

11.1.3 Lines Status

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

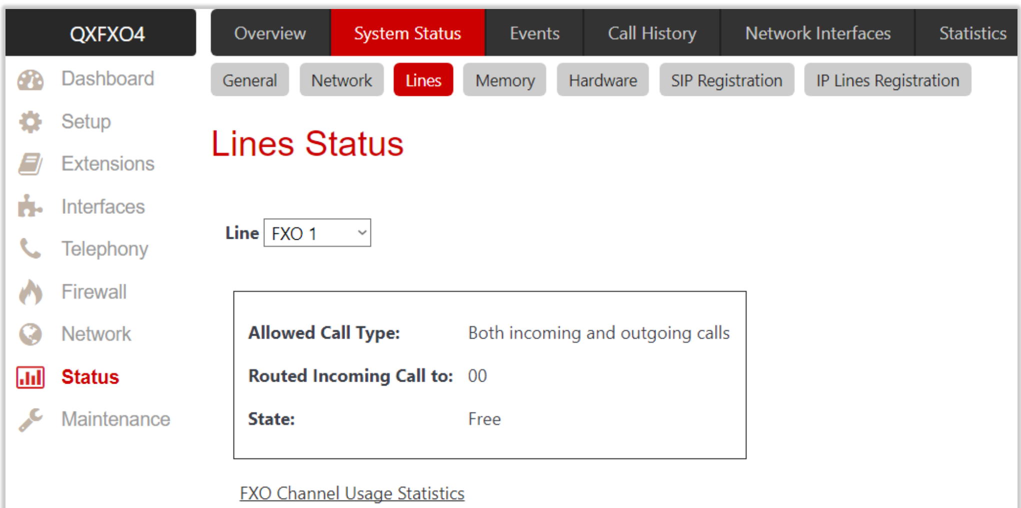


Figure 133: Status – Lines Status page

- FXS Line (available on QXFXS24) 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 (available on QXFXO4 and QXE1T1) 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 (available on QXFXO4) shows the Allowed Call Type, the destination for Incoming Calls (to Extension, Attendant or to Call Routing Table) and the state of the line (Free or Busy).
- ISDN Trunk (available on QXISDN4) 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.

- **E1T1 Trunk** (available on QXE1T1) shows the **Allowed Call Type**, the destination for **Incoming Calls** (to Extension, Attendant or to **Call Routing Table**) and the state of the timeslot (Free or Busy).

11.1.4 Memory Status

The **Memory Status** page (N/A on QXFXS24) displays information on available memory size and memory allocation among the applications and services on the QX.

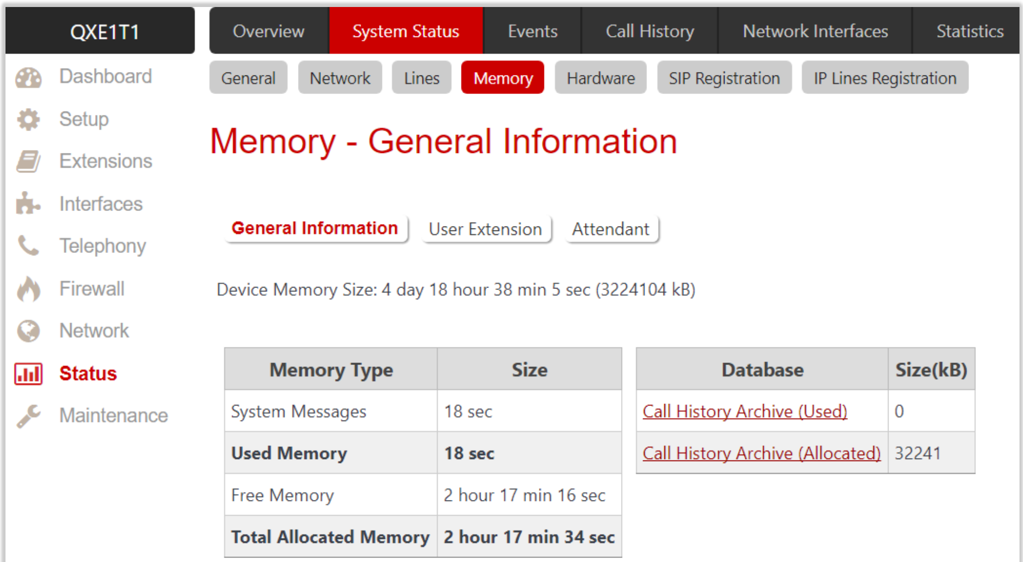


Figure 134: Status – Memory Status page

The **Memory Status** page consists of the following sub-pages:

- **General Information** – shows the memory size and current memory allocation(usage) for the system messages. The **Databases** table shows the memory size used by different QX services.
- **User Extension** – shows the memory size available and currently allocated(used) to recorded/uploaded system voice messages for each specific user extension. The **Universal Extension Recordings** shows the space used to define the system default voice messages common for all extensions.
- **Attendant** – shows the memory size available and currently allocated(used) to recorded/uploaded system voice messages for each Auto Attendant.

For information on **Memory Status**, please refer to the Memory Management on QX IP PBXs guide.

11.1.5 Hardware Status

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.

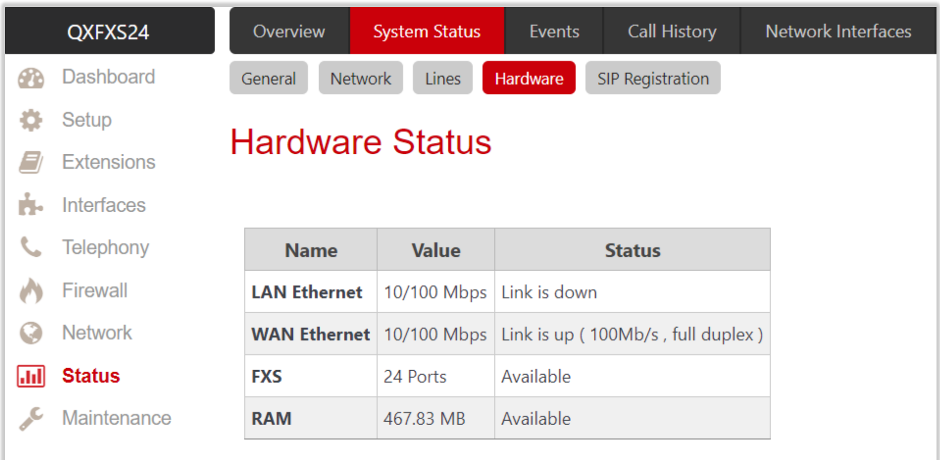


Figure 135: Status – Hardware Status page

11.1.6 SIP Registration Status

The SIP Registration Status page displays information about the QX extensions registration on SIP servers. Information about the configured SIP Tunnels between Epygi devices is displayed here as well.

The Registration on SIP Servers table shows the following information:

- Extension – shows the extension number. The hyperlinked Extension number leads to the Extensions Management – SIP Settings section where the SIP registration settings can be modified.
- Username/DID Number – is the registration username or the DID number on the server.
- SIP Server – indicates the address of the SIP server. It can be either an IP address or a host name.
- Registered – shows the registration status.
- Registration Time – shows the registration time.

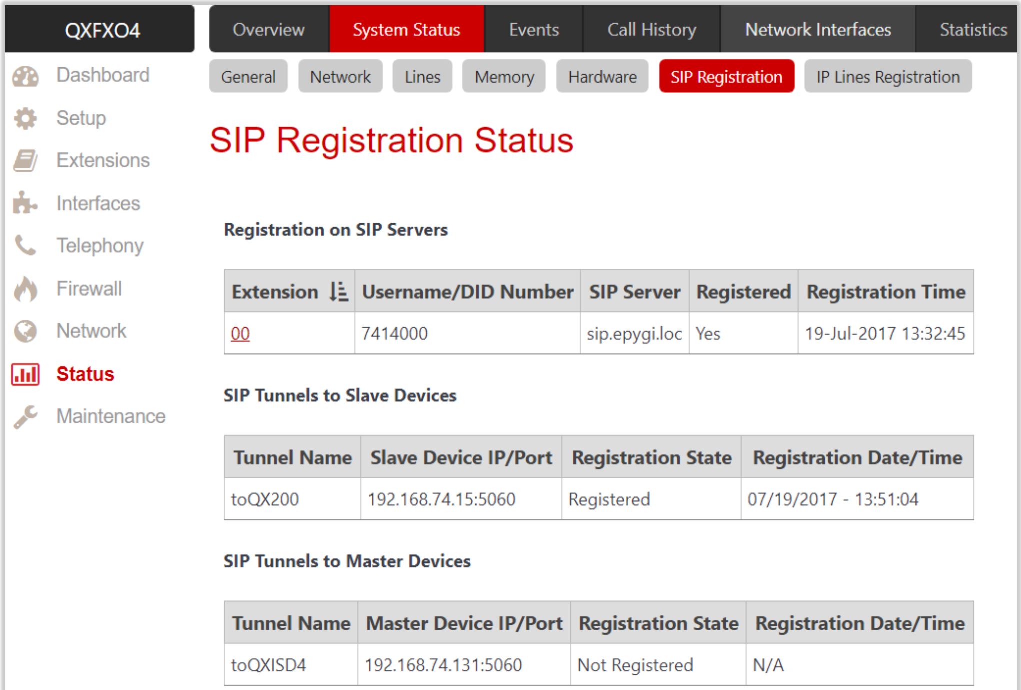


Figure 136: Status – SIP Registration Status page

The SIP Tunnels to Slave Devices and SIP Tunnels to Master Devices tables list the SIP tunnels between local and the remote Epygi devices. The SIP Tunnels to Slave Devices table lists those tunnels where local QX acts as a master. The SIP Tunnels to Master Devices table lists those tunnels where local QX acts as a slave.

11.1.7 IP Lines Registration

The IP Lines Registration Status (N/A for QXISDN4 and QXFXS24) page provides information on IP Lines registration on the QX.

The IP Lines Registration table lists the IP lines and remote extensions registered on the QX. The following information is available:

- IP Line – shows the number of IP line. The hyperlinked Line number leads to the IP Line Settings page where the IP Line settings can be modified.
- Extension – shows the extension number attached to the IP line.
- Username – indicates the registration username.
- Registered – shows the registration status.
- Binding IP Address – indicates the IP address of the registered device (IP phone, softphone or etc.).
- Registration Time – shows the registration time.
- Registration Expires in – shows when the registration will expire for the device.

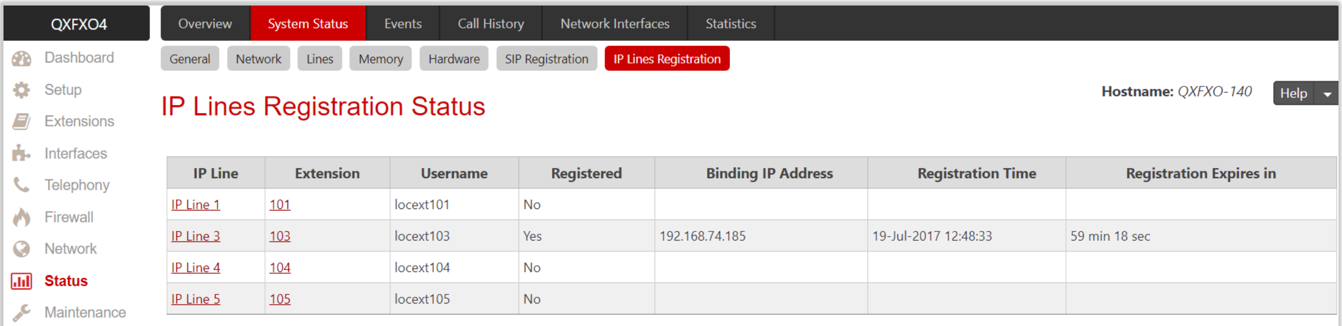


Figure 137: Status – IP Lines Registration Status page

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. Numerous circumstances may cause a certain application on the QX to flag an event. TIP: The warning link that leads directly to the **System Events** page will disappear from the management pages if the administrator has marked all new events as "**read**".

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

The table shows the **Status** of the event (new or read) as well as the name of the application the event refers to, event description, and the date when the event was received. For example, if the event was caused by the IDS service, the **Check IDS** link appears in the reference row that will lead to the **IDS Log** page, or if the event has occurred due to incorrect mail sending or SIP registration, the corresponding links will be seen in the **Reference** column of the table.

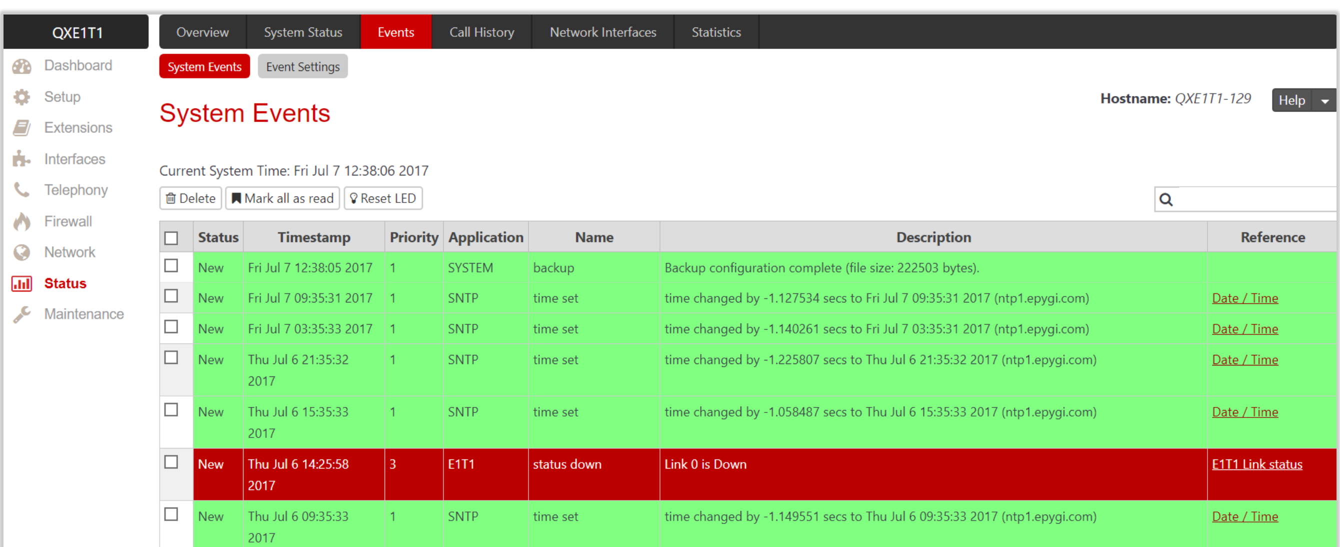
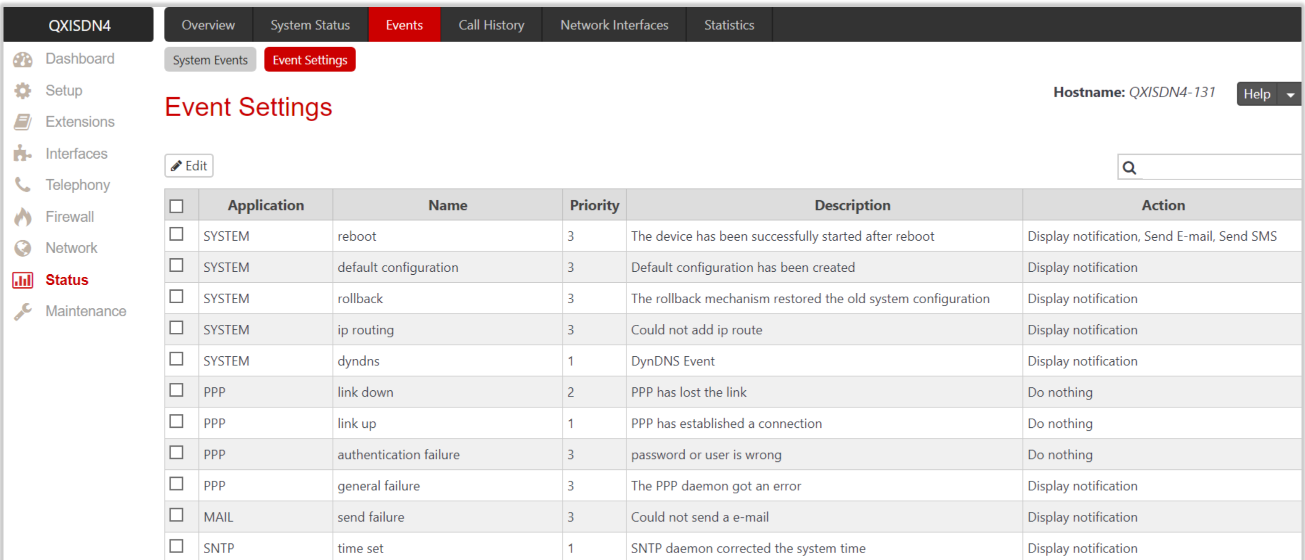


Figure 138:System Events page

- **Current System Time** – displays the local date and time on the QX.
- **Mark all as read** – marks newly occurred events as "**read**".
- **Reset LED** – switches off the flashing LED (if applicable) on the board. The **LED** notification may appear (depending on the notification type given) in the **Event Settings** page when a new event occurs.

11.2.2 Event Settings

The **Event Settings** page lists all possible events on the QX and allows controlling notification (action) when an event takes place. Each entry in the events' table has a checkbox assigned to each row. You can modify multiple events by selecting two or more events.



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

Figure 139: Event Settings page

- **Edit** – leads to the **Edit Event Settings** page to modify the event action.
  - ➢ **Application** – displays the application the event refers to. **Multiple** is shown here if more than one event has been selected for the action assignment.
  - ➢ **Name** – displays the name of the event. **Multiple** is shown here if more than one event has been selected for the action assignment.
  - ➢ **Description** – displays additional information about the event. **Multiple** is shown here if more than one event has been selected for the action assignment.
  - ➢ **Action** – is used to select event notification method:
    - ♦ **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** – an e-mail will be sent to the e-mail address specified in the E-mail (SMTP) page.
    - ♦ **Send SNMP Trap** – a trap will be sent to the traphost(s) listed in the **SNMP Trap Settings** table.
    - ♦ **Send SMS** (N/A for QXFXS24) – a SMS will be sent to the mobile number specified in the Short Text Messaging (SMS) page.

Note:

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

11.3 Call History

The **Call History** allows to track and report the call detail records (CDR) for calls originated and terminated on QX, as well as for calls passed through QX.

11.3.1 Successful, Missed and Unsuccessful Outgoing Calls

The **Successful Calls**, **Missed Calls** and **Unsuccessful Outgoing Calls** pages lists successful, missed and unsuccessful outgoing calls and their parameters. The following components are available:

- **Filter** – allows searching for call records based on at least one of the criteria: Call Start Time, Call Duration, 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 the (*.log) and (*.csv) formats respectively.

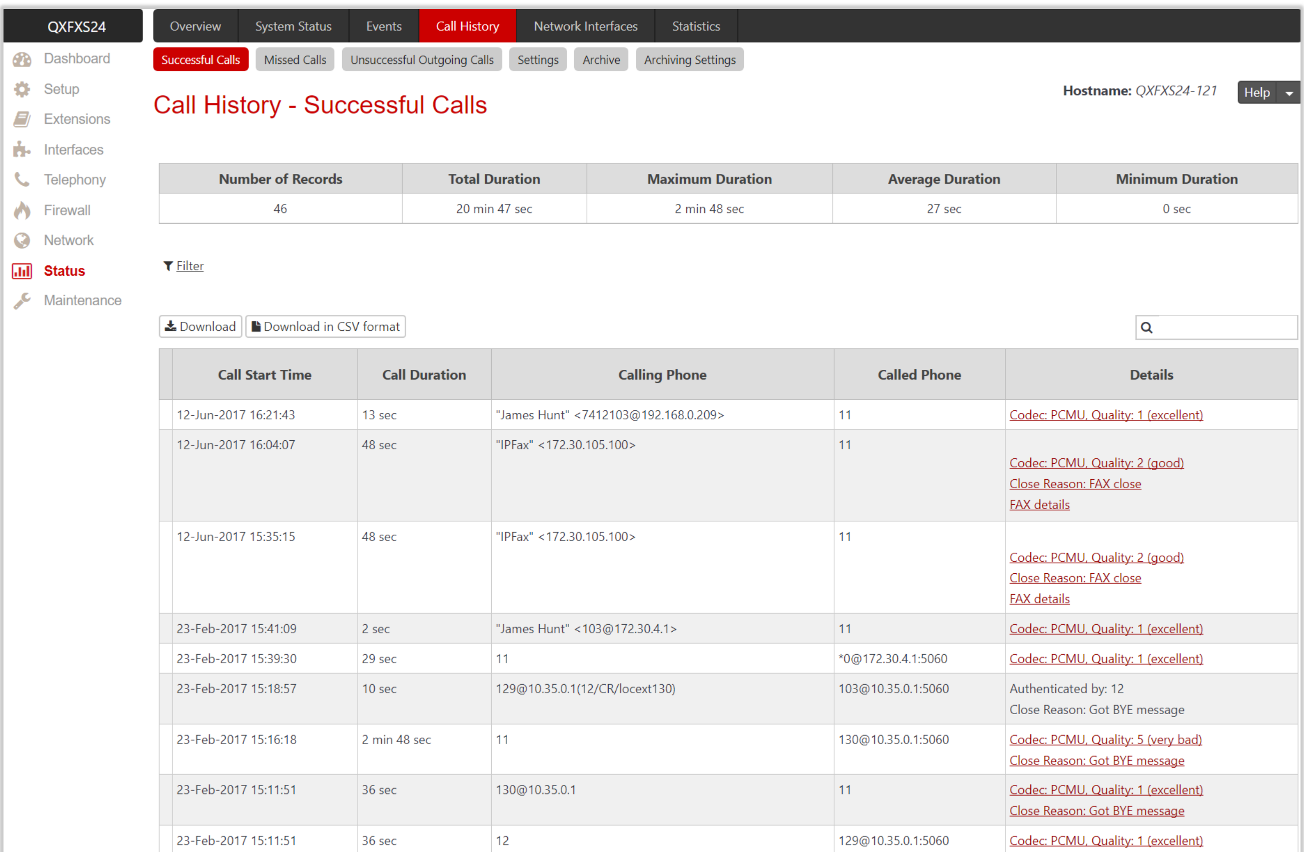


Figure 140: Call History – Successful Calls page

CDRs listed in the **Call History** tables are characterized by the following parameters:

- **Call Start Time** – shows the start date and time of the call.
- **Call Duration** – shows the duration of the call.
- **Calling Phone** – shows the caller's number and display name (if available).
- **Called Phone** – shows the callee's number and display name (if available).
- **Details** – provides the following additional information:
  - ➢ Details on the call quality, audio codec used to receive and transmit packets 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 Details information link leads to the RTP Statistics page where all RTP parameters of the call are shown.

- Authenticated By – shows the authentication parameters in the Local AAA Table, such as login or PIN code used to pass the authentication when making call. Information about FAX statistics for the calls that have a FAX transmission handled. It only appears when there was a FAX transmission during the call. The FAX link leads to the FAX Statistics page.

11.3.2 Settings

The Call History – Settings page is used to configure specific parameters for displaying Call History. The following options are available:

- Enable Call Reporting – enables/disables the CDR reporting and allows to select the maximal numbers of CDR entries to be displayed in the Call History tables respectively.
  - Maximum Number of Successful/Missed/Unsuccessful Call Records – these are used to select the maximum number of Successful, Missed and Unsuccessful Outgoing CDR entries to be displayed in the respective Call History tables. TIP: When the number of CDRs exceeds the numbers specified in the Call History – Settings page, the oldest entries are being automatically deleted. To keep the call history entries safe, configure and use the Archiving Settings service of the QX.
- The Download all CDRs and Download all CDRs in CSV format links are used to download the displayed Call History in the (*.log) and (*.csv) formats respectively.
- Clear all CDRs – is used to remove all CDRs.
- 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 call history files to make the CDR files more compact, thus more readable. For the detailed information about the CDR parameters listed in this page, please refer to the Call Detail Records on QX IP PBXs guide.

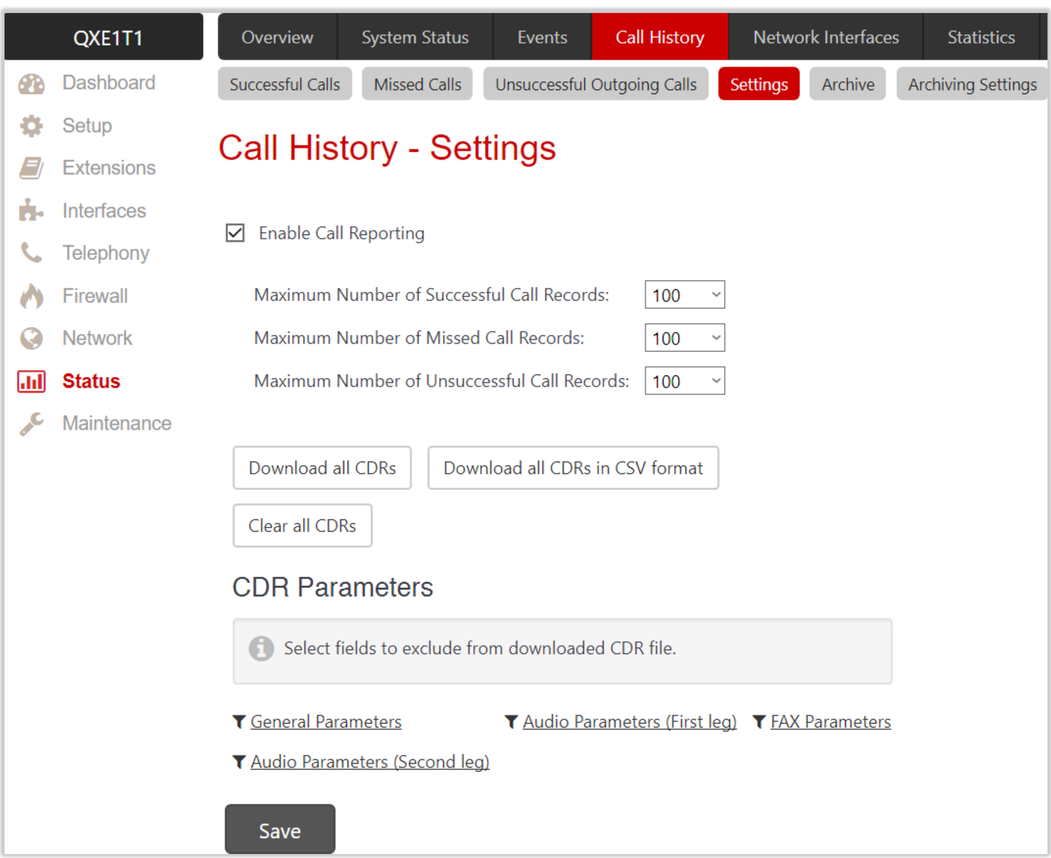


Figure 141: Call History – Settings page

11.3.3 Archive

The **Archive** page shows the **Call Details Record** (CDR) archived 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 the specific archived CDR records in the **Archive** table by the record's full name or some part of the name.
- **Delete** – removes the selected record(s) from in the **Archive**.
- **Clear all Records** – is used to remove all archived files.

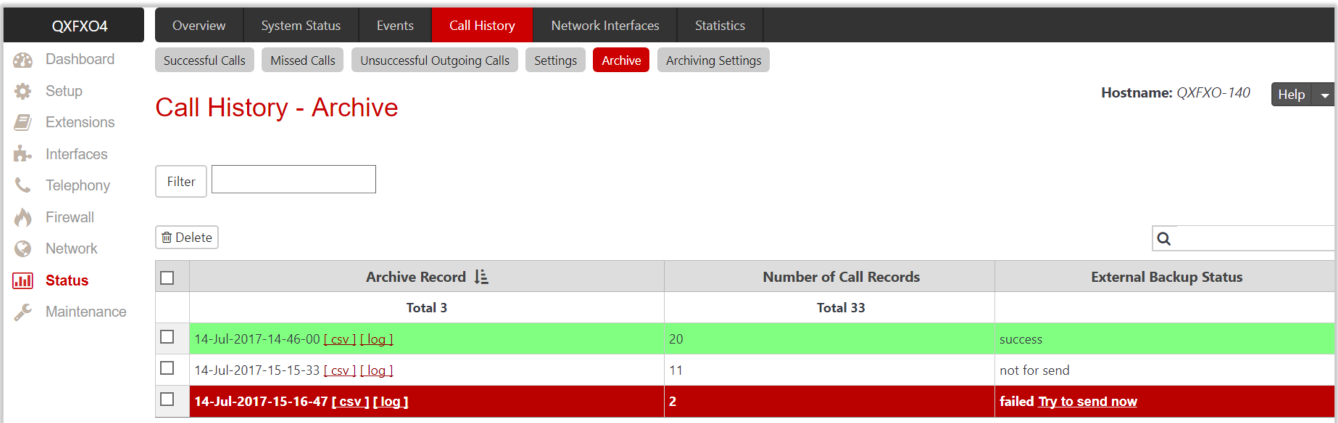


Figure 142: Call History – Archive page

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** – if the archived file has been successfully sent for backup (e-mail address, FTP or TFTP server).
  - **Failed** – if the archive file failed to be sent for backup (e-mail address, FTP or TFTP server). The **Try to send now** link will appear next to this status allowing to repeat the backup process.

11.3.4 Archiving Settings

The Call History Archiving feature is used to configure the automatic archiving of the Call History. The following options are available for archiving:

- **Percentage of Total Memory allocated for Archive** – defines the system memory allocated for call history archiving.
- **Enable Call History Archiving** – is used to enable the service.
- **File Format** – is used to select the archive file format as (*.log) and (*csv).

Archiving Mode

This section is used to select the archiving mode. The following modes are available:

- Archive by Record Count – file is being archived as soon as the number of records specified in the drop-down list is collected.
- Archive by Time Interval – file is being 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, archive file for that period will not be generated.

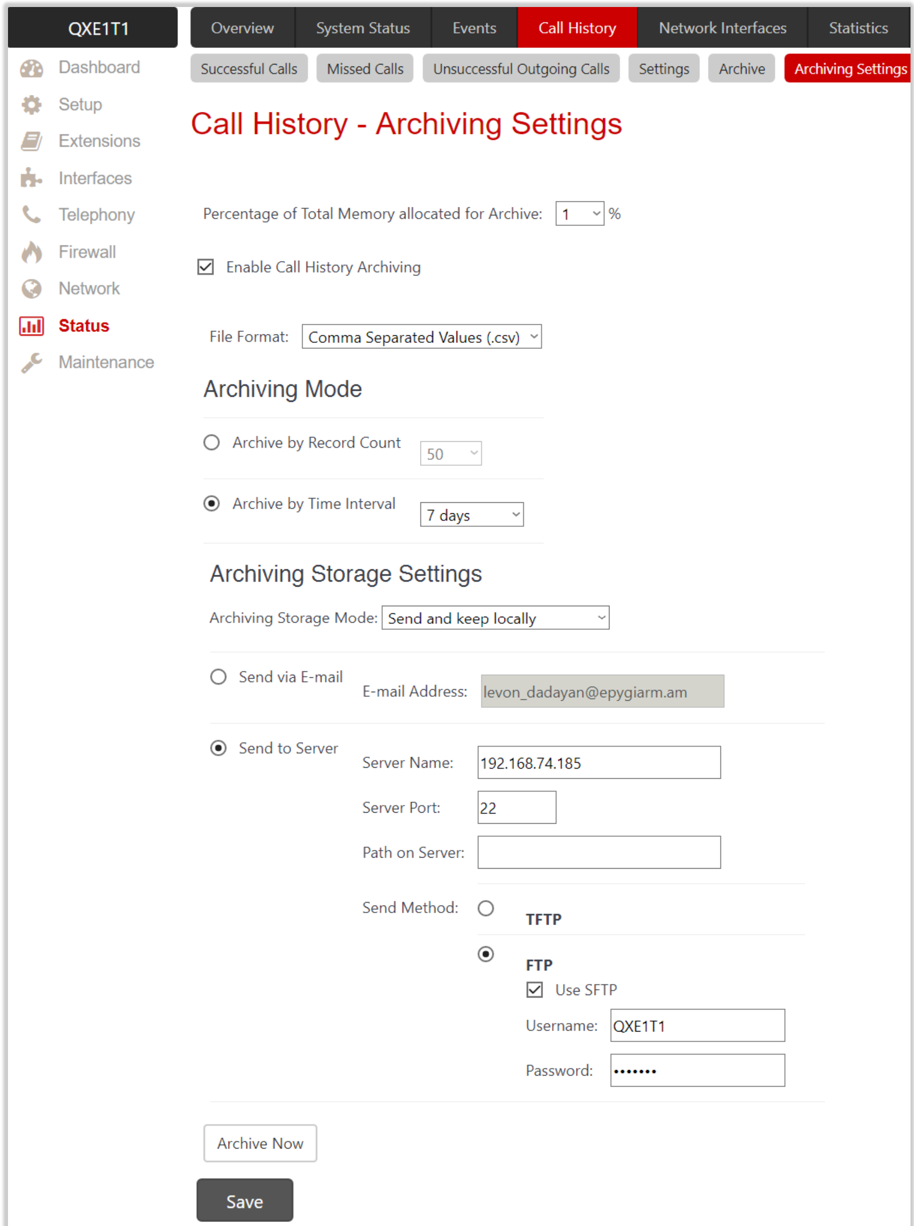


Figure 143: Call History – Archiving Settings page

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 options:
  - Do not send – the CDRs will be archived and kept locally only.
  - Send and keep locally – the CDRs will be sent to the server and kept locally.
  - Send and delete from archive – 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 sending 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 sending the archived files to an external server. This selection enables the following fields to be filled:
  - Server Name – the IP address or hostname of the server.
  - Server Port – the port of the server.
  - Path on Server – 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.
- The Archive Now button is used to archive CDRs immediately.

11.3.5 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. For example, when calling from an IP Phone attached to the QX IP line to an external SIP destination or from one external SIP destination to another through the QX Auto Attendant. Each group of parameters describes characteristics of a piece of RTP stream composing an overall SIP session. Normally, one leg describes the RTP stream from caller to the QX gateway and the other leg describes the RTP stream from the QX to the destination.

- **Quality** – indicates the call quality, which depends on RTP statistic. Below is the legend for Call Quality definitions on the displayed RTP Statistics:
  - **excellent** – RX Lost Packets < 1% & RX Jitter < 20
  - **good** – RX Lost Packets < 5% & RX Jitter < 80
  - **satisfactory** – RX Lost Packets < 10% & RX Jitter < 150
  - **bad** – RX Lost Packets < 20% & RX Jitter < 200
  - **very bad** – RX Lost Packets > 20% or RX Jitter > 200
- **Local** and **Remote** – indicate the two peers between which the RTP stream is transmitted. The characteristics in the table below describes to the piece of RTP stream between these peers.
- **Rx/Tx Codec** – codec for received and transmitted RTP stream respectively.
- **Rx/Tx Packets** – 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** – inter-arrival jitter is an estimate of the statistical variance of the RTP data packet inter-arrival time, measured in timestamp units.

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

$$D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)$$
$$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16, \text{ where } J(i) \text{ is Rx Jitter for packet i.}$$

For more details about Jitter calculations, please 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:

$$V(i) = |(Ri - R1) - (Si - S1)| = |(Ri - Si) - (R1 - S1)|$$
$$\text{Rx Maximum Delay} = \max V(i) / 8$$

- **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 notification specifics.
- **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 incoming from or addressed to the IP lines or remote extension.
- Calls from an external user are routed to another external user through QX's routing rules.

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

11.3.6 FAX Statistics

The **FAX statistics** page is accessed from the Call History page by clicking on the **FAX details** link in the **Details** column for the calls that contain T.38 FAX transmission. This page provides information about received and transmitted packets, lost, bad and duplicated packets. These statistics refers only to the T.38 FAX transmission. The FAX statistics is not available for the FAX transmitted with other protocols.

11.4 Network Interfaces

The **Network Interface Statistics** pages display the corresponding statistics.

- **LAN** – current activity of the LAN (Local Area Network).
- **WAN** – current activity of the WAN (Wide Area Network).
- **VLAN** – current activity of the VLAN.
- **PPTP/L2TP** – current activity of the PPTP/L2TP.

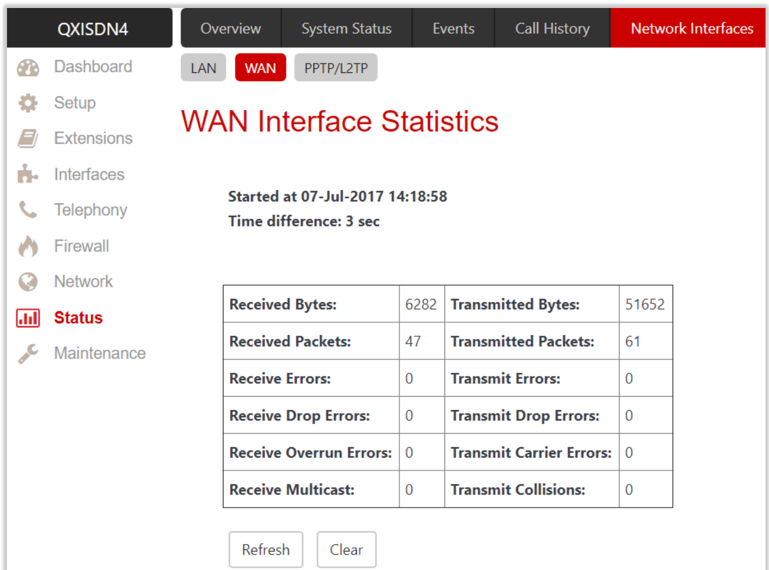


Figure 144: LAN Interface Statistics page

The table displayed here shows the number of receive and transmit events that occurred since the last resetting of the counters by clicking the **Clear** button. Depending on the **Watch LAN**, **Watch WAN**, **Watch VLAN**, **Watch PPP** link selected on the **Network Status** page, the LAN Interface Statistics, WAN Interface Statistics, VLAN Interface Statistics, PPTP or L2TP statistics page will be displayed. The page is automatically refreshed every minute. Additionally, **Refresh** allows to initiate manual.

11.5 Statistics

11.5.1 Network Transfer

The Transfer Statistics page shows a user-defined statistics table with the transmit/receive value (criteria), interface type and time period. It contains the following components:

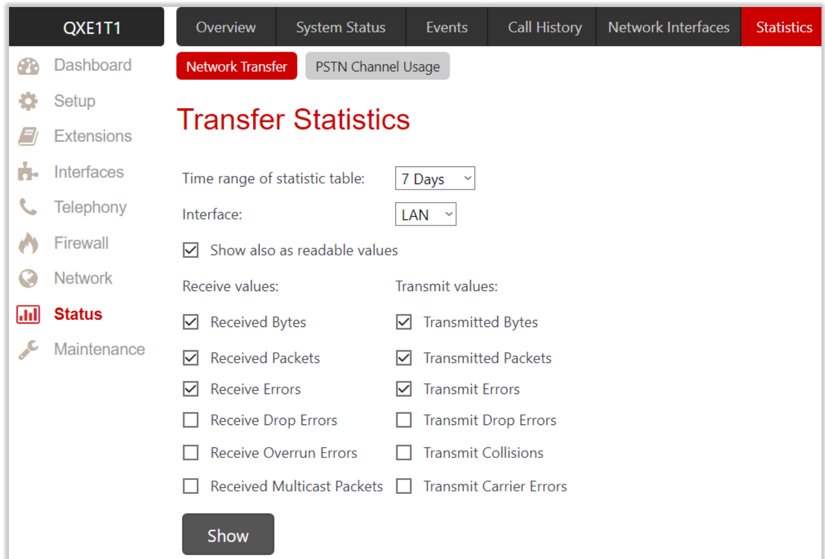


Figure 145: Transfer Statistics page

- Time range of statistic table – includes the period (in days) statistics data that is to be collected and the corresponding diagram charts that are to be built.
- Interface drop-down list offer the values:
  - LAN – show current activity of the LAN (Local Area Network).
  - WAN – current activity of the WAN (Wide Area Network).
  - VLAN – show current activity of the VLAN.
  - PPTP/L2TP – show current activity of the PPTP/L2TP.
- Show also as readable values – if selected, an additional table with statistics values will be displayed on the next page.
- Receive Bytes – number of received bytes.
- Receive Packets – number of received Ethernet packets.
- Receive Errors – number of received packets containing errors.
- Receive Drop Errors – number of received packets that have been discarded.
- Receive Overrun Errors – number of received overrun errors that occur when the receive buffer is not large enough to hold all incoming packets. This error usually appears due to a slow receiving system.
- Receive MultiCast Packets – number of received broadcast packets.
- Transmit Bytes – number of transmitted bytes.
- Transmit Packets – number of transmitted Ethernet packets.
- Transmit Errors – number of transmitted packets containing errors.
- Transmit Drop Errors – number of transmitted packets that have been discarded.
- Transmit Carrier Errors – number of transmit carrier errors that occur due to a defective or lost connection on the Ethernet link.
- Transmit Collisions – number of transfer errors that occurred during a simultaneous packet transmission from both sides.
- Reset Statistics – is used to reset the chart and the table (if enabled).

To see the Transfer Statistics Diagram Charts, select the desired criteria and click Save to generate the corresponding chart and the table showing the transfer statistics values (if enabled). The letters M (millions) and K (thousands) used in the legend of the displayed diagrams show the total number of specified criteria.

11.5.2 PSTN Channel Usage

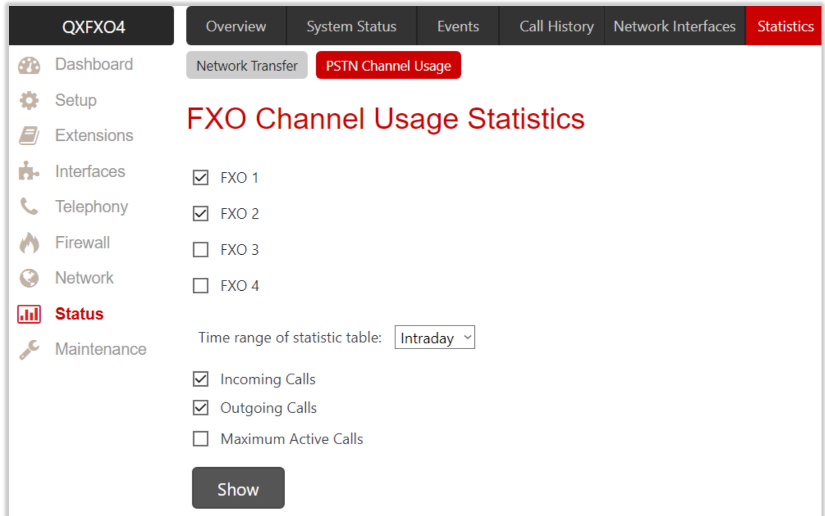


Figure 146: FXO Channel Usage Statistics page

The PSTN Channel Usage page (N/A on QXFXS24) is used to display diagram charts for the selected onboard lines and trunks.

- Line or trunk number – is used to select the line(s) or trunks for which the diagram chart will be generated.
- Time range of statistic table – lists the period (in days) statistics data that is to be collected and the corresponding diagram chart that is to be built.
- Incoming Calls and Outgoing Calls – are used to select whether the FXO, ISDN or E1/T1 (depending on the QX model) traffic statistics for only incoming or outgoing or for both type of calls should be displayed in the diagram chart.
- Maximum Active Calls – is used to have the number of maximum active calls displayed in the diagram chart. At least one of these checkboxes should be selected.

Click the Show button to generate an FXO, ISDN or E1/T1 (depending on the QX model) channels usage diagram chart for the selected parameters.

12 Maintenance Menu

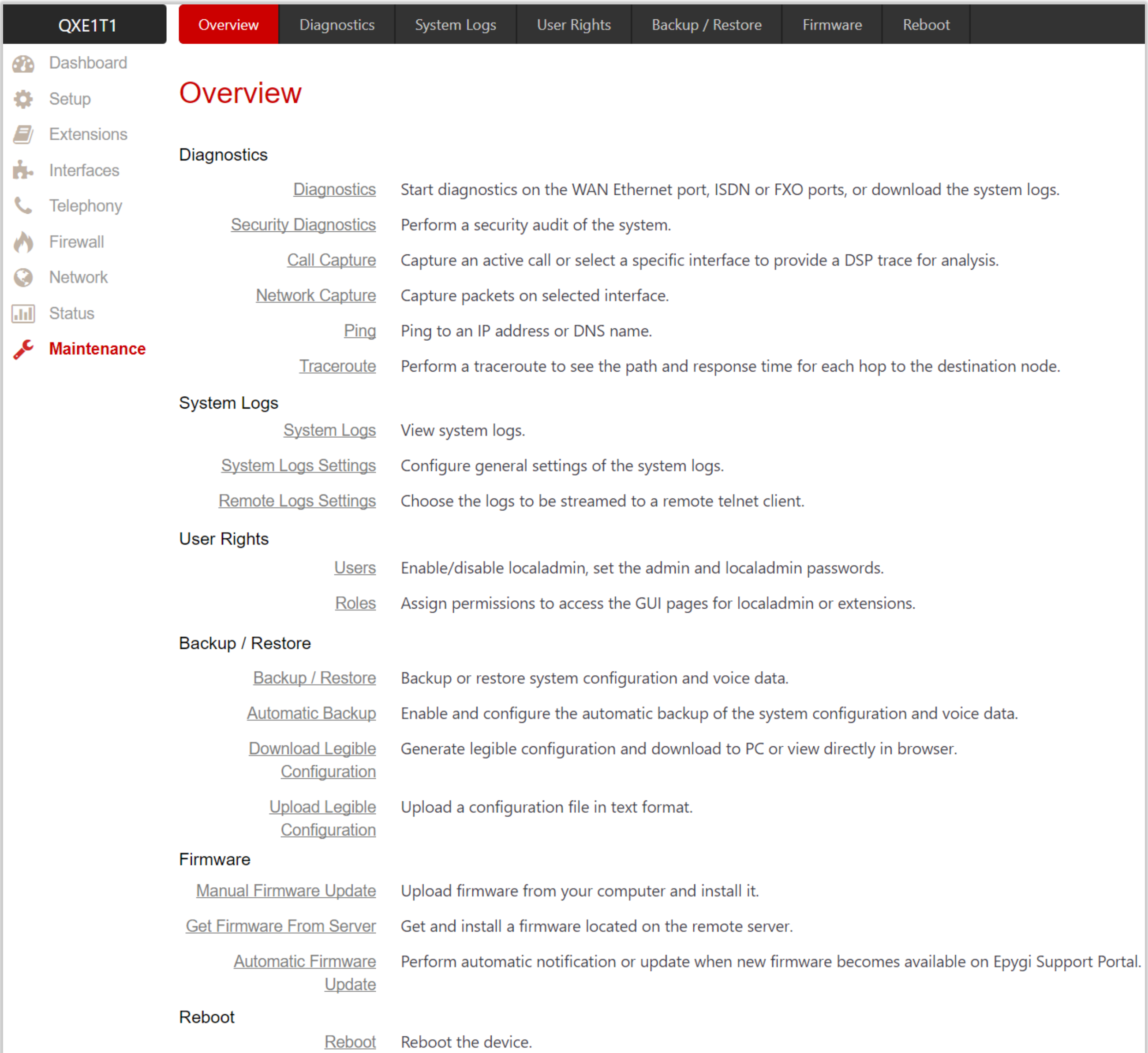


Figure 147: Maintenance Menu overview

12.1 Diagnostics

The **Diagnostics** page is used to run Network protocol diagnostics to verify QX's connectivity and download all system logs for possible problems recovery.

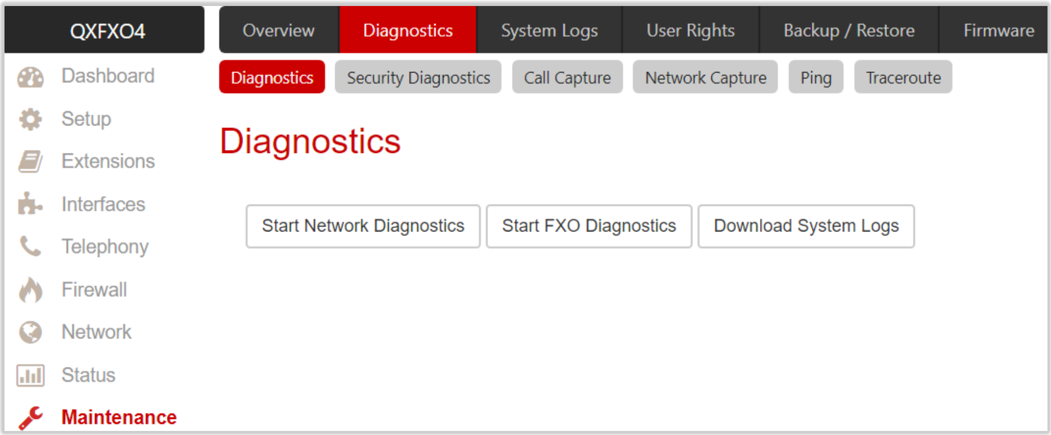


Figure 148: Diagnostics page

- **Start Network Diagnostics** – initiates network diagnostics, i.e., to check the WAN link and IP configuration, to verify gateway, DNS primary and secondary (if configured) servers' accessibilities.
- **Start FXO Diagnostics** (available on QXFXO4) – runs FXO diagnostic tests to determine the optimal value for the FXO country specific regional setting (CSRS) appropriate to your PSTN provider. Once the FXO diagnostic is complete, the recommended value should be set manually on the "**fxocfg.cgi**" hidden page. Setting this value may resolve echo or poor audio quality issues on FXO lines.
- **Start ISDN Diagnostics** (available on QXISDN4) – runs ISDN diagnostics test to initiate ISDN BRI low level diagnostic. With these tests, the ISDN physical link is checked and the Frame Synchronization is verified.
- **Start E1/T1 Diagnostics** (available on QXE1T1) – initiate E1/T1 **Link Diagnostic** and **Diagnostic Loopback**. With these tests E1/T1 physical link is checked, Frame Synchronization and Red Alarm states are verified. For successful **Link Diagnostic**, remote side should have Line_loopback or Payload_loopback settings configured or a loopback terminator should be plugged to the QX gateway's E1/T1 port. **Diagnostic Loopback** will be initiated if **Link Diagnostic** is failed or E1/T1 link is down.
- **Download System Logs** – is used to download all logs to the local PC as a (***.tar**) archive file. These logs can then be used by Epygi Technical Support to determine the problem that has occurred on your QX.

12.1.1 Security Diagnostics

The **Security Diagnostics** page allows running the security audit and getting the security reports.

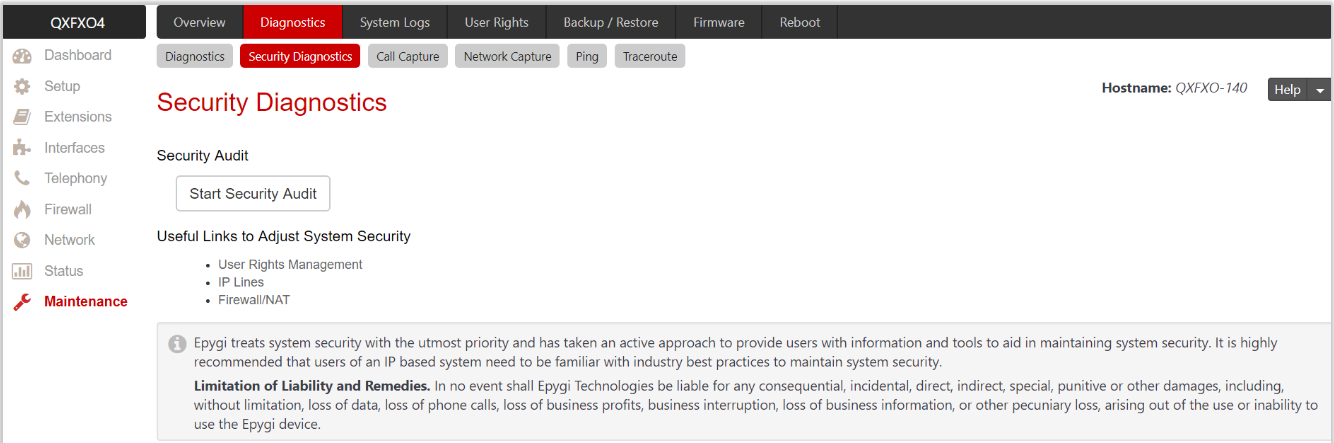


Figure 149: Security Diagnostics page

- **Start Security Audit** – is used for running the security audit. The QX Security Audit is a security reporting system, which generates the warnings regarding the QX gateway's weaknesses relative to the selected Security Level. Based on the selected global Security Level the warnings may vary. The Security Audit will detect the security related configuration issues in Firewall, IDS, Call Routing and extension settings.
- **Show Security Report** – displays the last security audit report.
- Following useful links are available to adjust the system security:
  - User Rights Management
  - IP Lines
  - Firewall/NAT

12.1.2 Call Capture

The **Call Capture** is used to capture the calls to/from onboard interfaces. You can capture calls on the following interfaces FXS, FXO or ISDN (**depending on the QX model**). This page consists of two sub-pages:

- **Active Calls** – sub-page lists all active calls on the QX for the certain moment.
- **Interfaces** – sub-page lists all available interfaces on the QX.

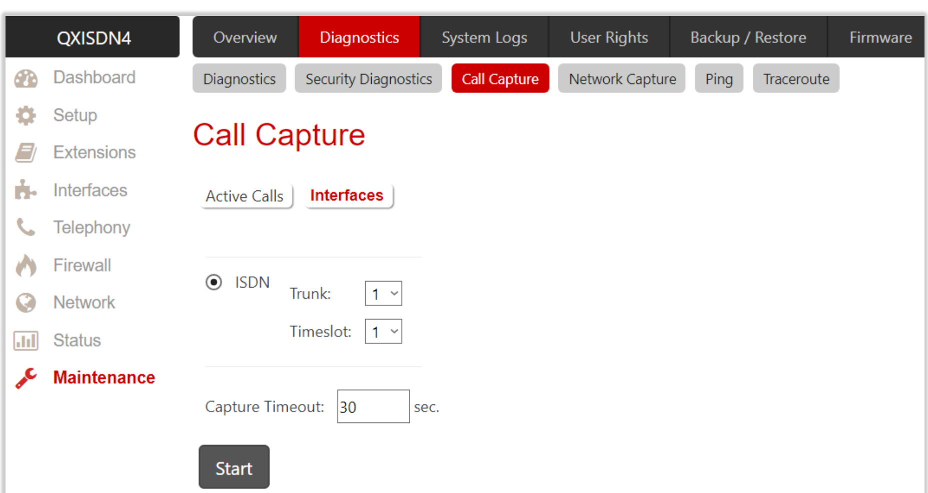


Figure 150: Call Capture - Interfaces subpage

To start the call capture:

1. Select 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 capturing.
4. Click **Stop**, to stop capturing and download the captured file.

The captured call will be downloaded in the (*.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

The **Network Capture** is used to capture packets for the selected network interface. The following options are available:

- **Capture on Interface** – 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** – number of packets to be captured.
- **Restrict to Host** – packets can be captured for only the specified IP address.

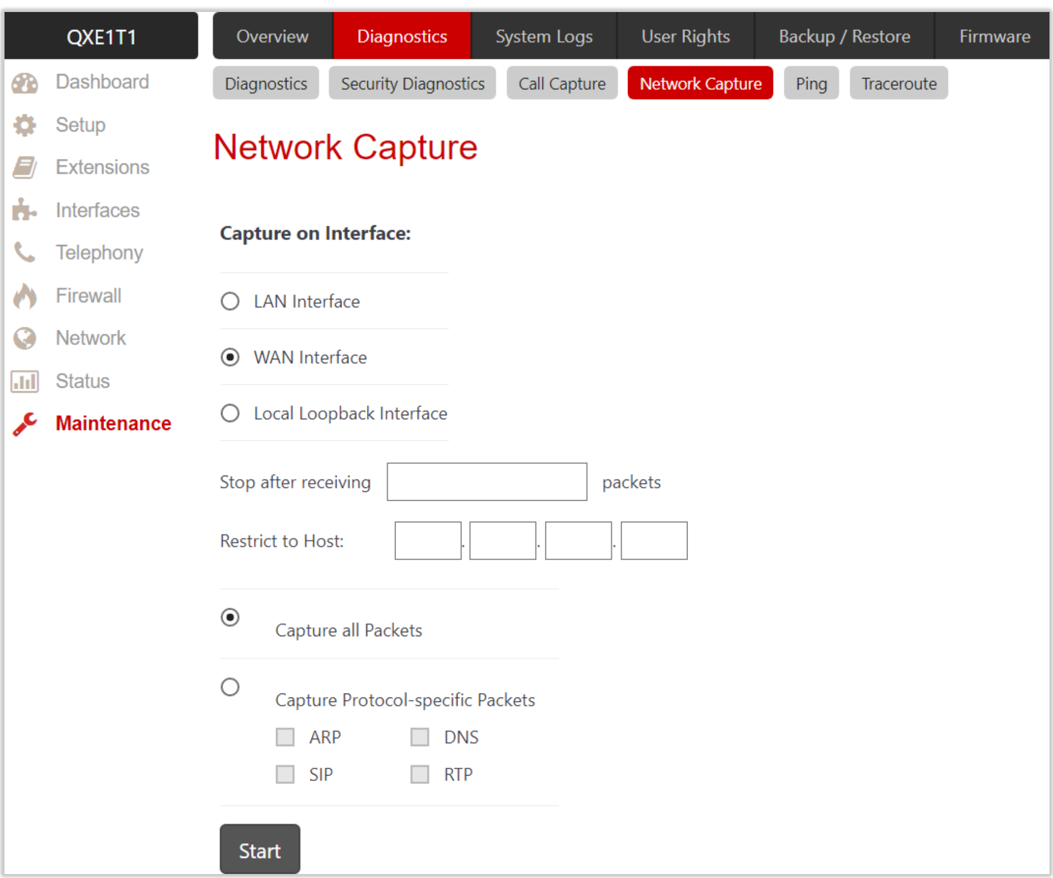


Figure 151: Network Capture page

- **Capture all Packets** – allows capturing all packets on the selected interface.
- **Capture Specific Protocol Packets** – enables restricting the capture to 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 capturing.
5. Click **Stop**, to stop capturing and download the captured file.

Note: The **Network Capture** size is limited to **24** MB. This will put a limitation on the duration of captured file.

12.1.4 Ping

Ping sends four ICMP (Internet Control Message Protocol) requests with a default size of 64 bytes to the destination (IP address or host name) specified in the **Ping Target**. The response times are logged, and the round-trip time (the time required from being sent until being received again) is measured. The minimum and maximum round trip time and its average as well as the percentage of lost and of received frames results are displayed in the lower area of the page.

To ping a target:

1. Enter the destination's 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.

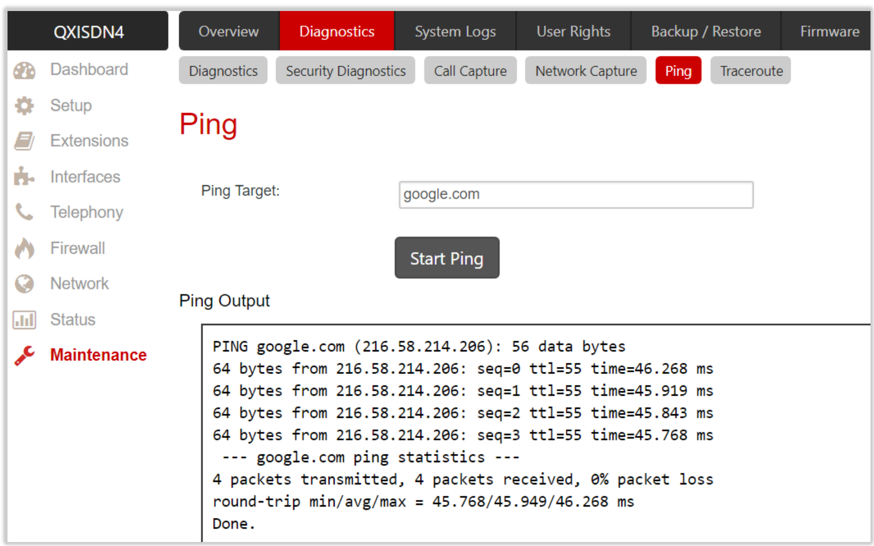


Figure 152: Ping page

12.1.5 Traceroute

Traceroute checks the Internet connection by triggering the routers (hops) that are passed to reach to the defined. Trace routing gives feedback on the routers passed by packets on the way toward the destination and the round-trip delay of packets to these routers.

To traceroute a target:

1. Enter the destination's IP address or hostname in the **Traceroute Target** field.
2. Select the **Use ICMP** checkbox to send an ICMP request the ping destination (MS Windows standard), otherwise a UDP request will be send (Linux standard).
3. Click **Start Traceroute**.
4. The results of the ping will be displayed in the **Traceroute Output** window.

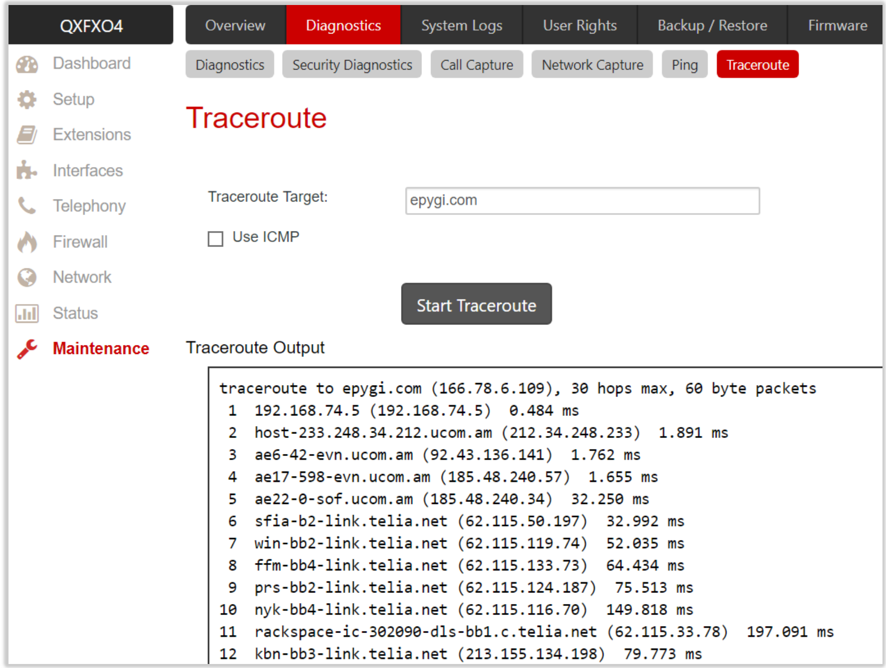


Figure 153: Traceroute page

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 frame is received by the first router, its IP address will be returned in its acknowledgement.

12.2 System Logs

The **System Logs** page displays the generated logs on the QX. **System logs** are useful to determine any king of problems on the QX as well as to monitor the user's access and the usage of it. On the left side of the page, a list of main logs is displayed. Clicking on the needed link will display the most recent log lines. The number of log lines displayed on this page is set on the **System Logs Settings** page.
The text field on the left side is dedicated for support personnel only and is used to search a custom log not listed on this page. To do so, enter a required log name to the text field and click **Show Custom Log**.

If the user has used **Logs Collection** *82 feature code after or during (from another phone connected to the same QX) the call, a special log file will be generated containing the details of that call and few last calls done in the system. This log file will be internally kept in the system until the next time someone used the **Logs Collection** feature code again. The collected logs will be a part of the **System Logs** when user downloads them next time. This could be used to collect the logs at the exact moment when a problem happens.

12.3 System Logs Settings

The **System Logs Settings** page is used to adjust system logging settings.

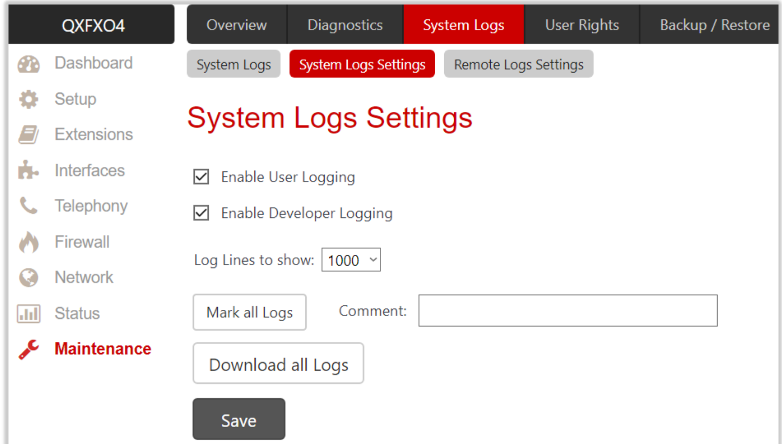


Figure 154: System Logs Settings page

- **Enable User Logging** – enables user level logging. This logging contains brief information about events on the QX.
- **Enable Developer Logging** – enables developer high level logging. This logging contains detailed information about events on the 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. If you need to follow a certain piece of log, push this button to set a starting mark in all logs and then perform the needed actions over the QX. When the actions are done, push this button again to set an ending mark in all logs. This way you shall clearly see a piece of log between the starting and ending marks generated during the certain actions taken over the QX.
- **Comment** – is used to enter some text information which will be displayed next to the marks entered in the logs. This comment may describe the problem captured in the following logs and may be useful for the Technical Support.
- **Download all Logs** – is used to download all logs to the local PC as a (***.tar**) archive file. These logs can then be used by the Epygi Technical Support to determine the problem that has occurred on your QX.

12.4 Remote Logs Settings

The **Remote Logs Settings** page is used to adjust the system logging settings and contains the following components.

Enable Remote Logging – enables remote monitoring of the QX's logs. When this option is selected, remote administrators may connect the QX with Telnet protocol (port number 645) and access the logs selected on this page. This is done for remote the QX's diagnostics and is mainly used by Epygi's Technical Support. To make the QX's logs open for remote access, appropriate Firewall level or Filtering Rules must be created. The options below are used to select those log types that should be accessible remotely. Select only those logs that you wish to have monitored remotely.

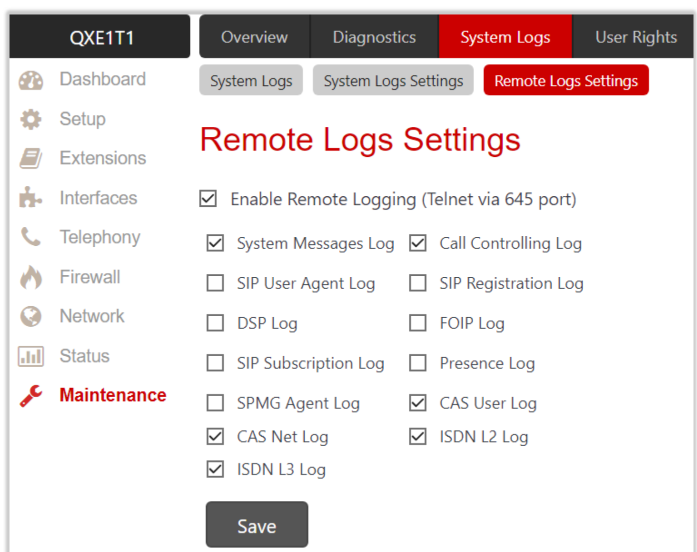


Figure 155: Remote Logs Settings page

12.5 User Rights Management

The **User Rights** service sets restrictions on the GUI access for various users, permits or denies the access to certain Web GUI configuration pages and creates multilevel user management of the QX.

12.5.1 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's account. The administrator has access to all Web GUI pages and no one else has configuration permission to adjust this account. The administrator is responsible for granting access to all other user groups. By default, as well as after factory reset of QX, the **admin password** is set to **19**.
- **localadmin** – this is a common sub-administrator's account. Local Administrator has permission to access and adjust each GUI management page. But the account of Local Administrator is disabled by default and after each factory reset. By default, as well as after factory reset of QX, the **localadmin password** is set to **19**.

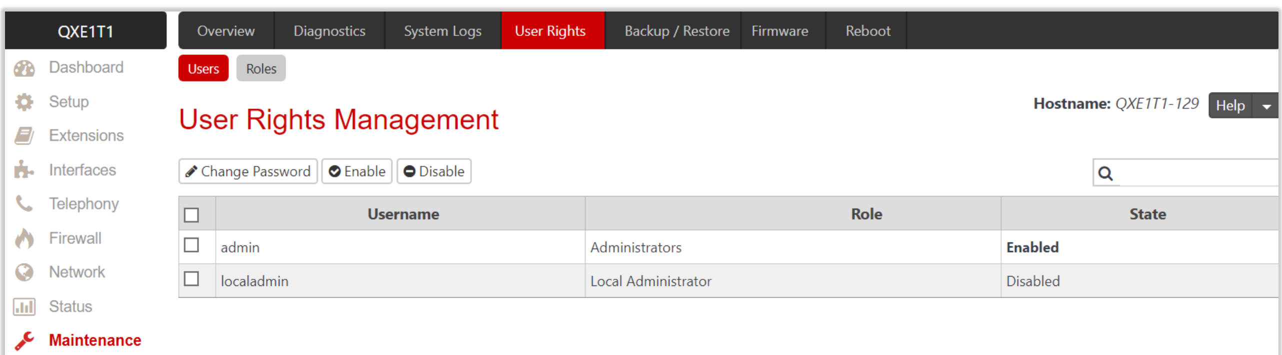


Figure 156: User Rights Management – Users page

To change the GUI Access Password:

1. Click the checkbox next to the **admin** or **localadmin** entry in the table and click **Change Password**.
2. The **Change Password** page appears for 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**. The password has now been changed.

The **Phone Access Password** which is required for Administrator Login (*75). The Administrator Login is used to review and modify the Auto Attendant greeting and recurring prompt, as well as the universal extension messages.

To change the Phone Access Password:

1. Click 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**. The password has now been changed.

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 the **Administrator's** password safe, do not write it down in public places and do not share it with other people.

12.5.2 Roles

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

- **Local Administrators** – this role can have permissions to adjust each GUI page.
- **Extension** (**N/A for QXFXS24**) – this role refers to all extensions created on the QX. Permissions for an extension to access each GUI page can be adjusted.

Figure 157: 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. Select the checkbox(es) next to **CGI Name**.
3. Click the **Grant Access** or **Deny Access** to grant/deny access to the corresponding page.

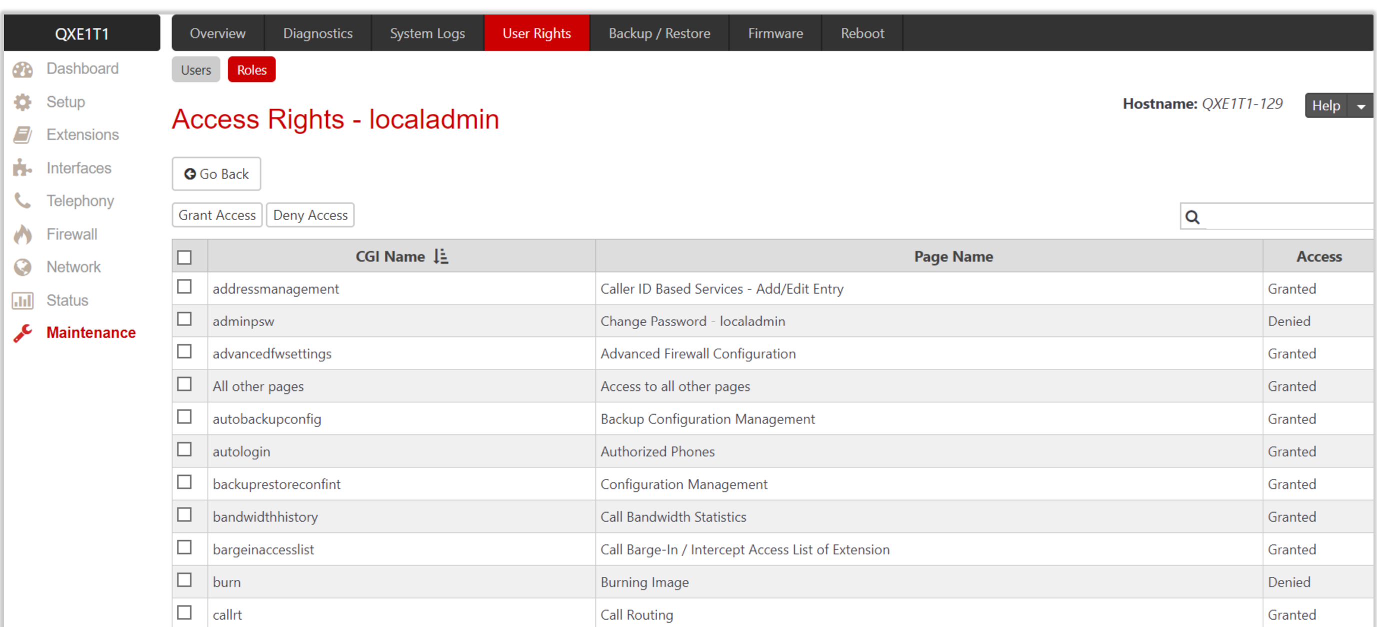


Figure 158: Access Rights – localadmin page

12.6 Backup / Restore

12.7 Backup / Restore

The **Configuration Management** includes the features allowing to back up and save the QX's current configuration, restore the configuration from backups created earlier, as well as to restore the system default configuration. The following options are available:

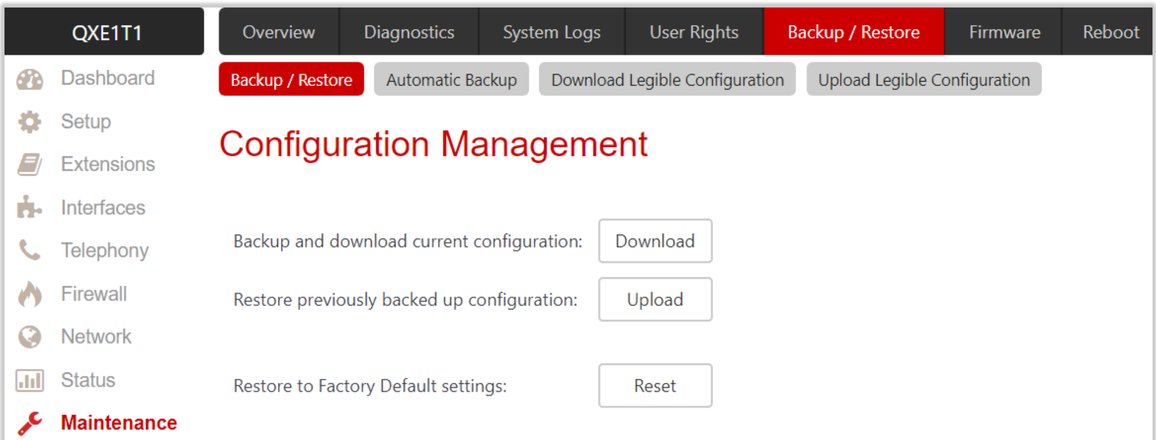


Figure 159: Configuration Management page

- **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**
- **Restore previously backed up configuration** – this option 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: The QX's 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** – this option is used to reset all configuration settings and restores the device's factory default settings.

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 the QX manually, this option will keep the following data:

- The device registration with Epygi Technical Support.
- The installed license keys.

12.7.1 Automatic Backup

The Backup Configuration Management feature allows to activate and configure the automatic backup of the current configuration and system voice messages (default and customized).

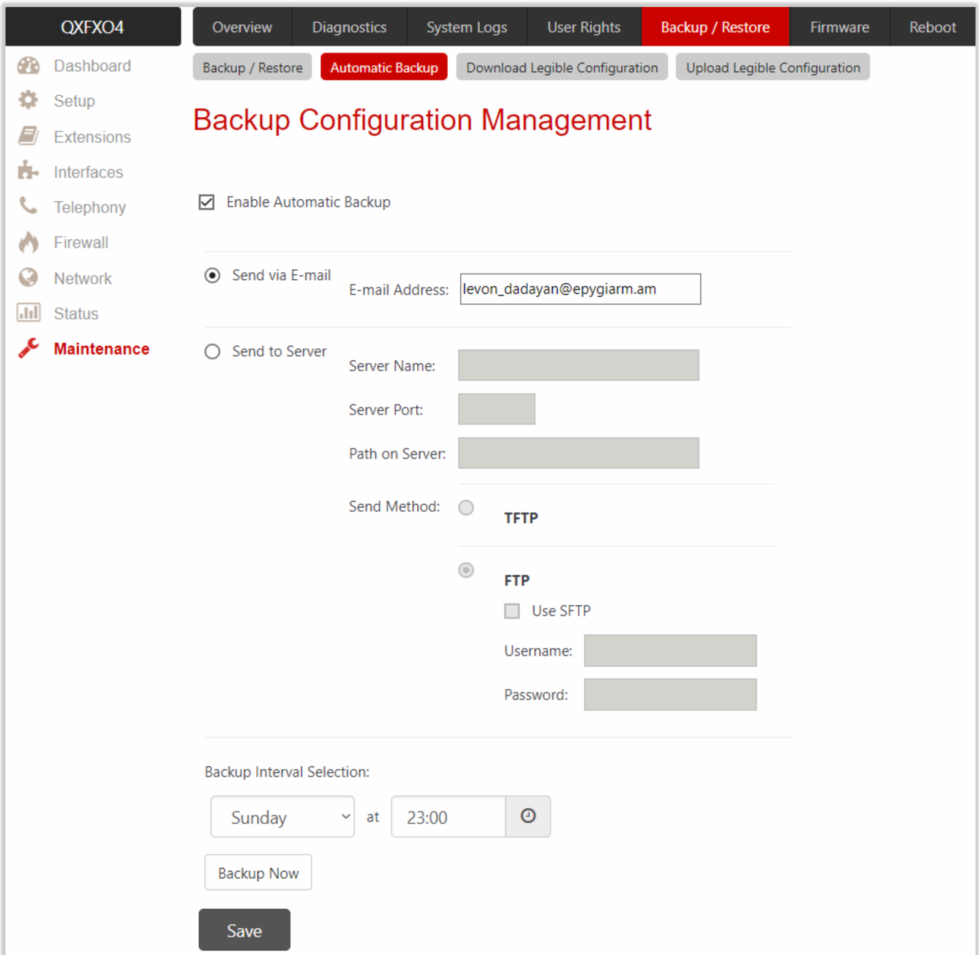


Figure 160: Automatic Backup page

The following options are available for automatic backup:

- Enable Automatic Backup – is used to enable the service.
- 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 – the IP address or the hostname of the server.
  - Server Port – the port of the server.
  - Path on Server – 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 backup of configuration and system voice messages (default and customized) immediately.

12.7.2 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(s) (LCF) contain QX configuration parameters in the (*.txt) file. LCF can be edited with any text editor and uploaded back to save the changes on the same or another QX system(s).

For information on how to configure and use Legible Configuration service, please refer to the Legible Configuration on QX IP PBXs guide.

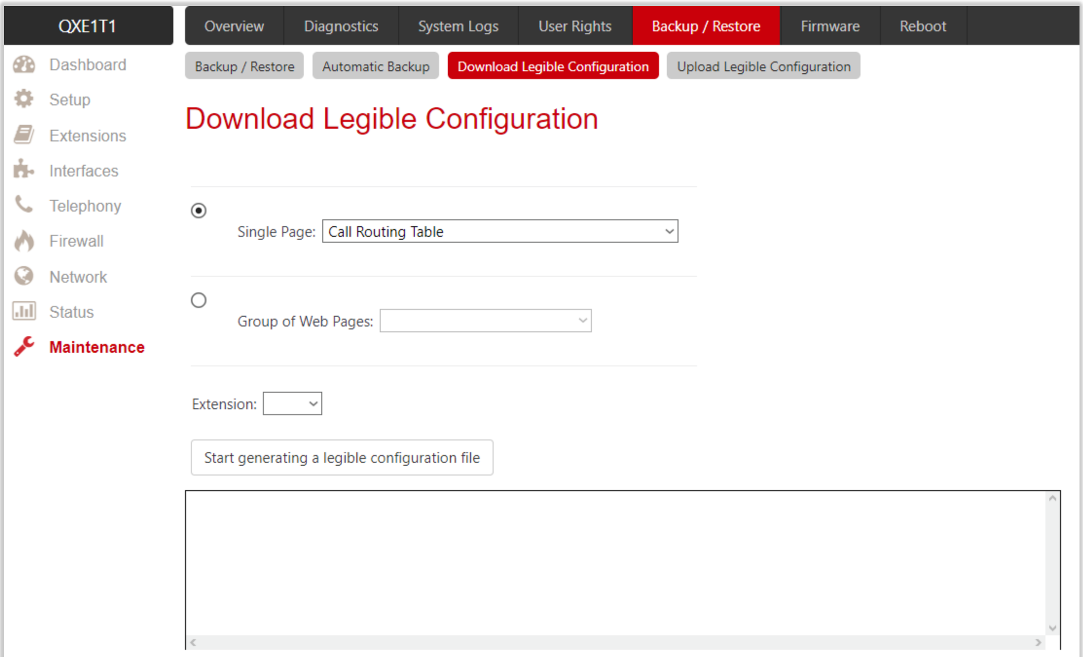


Figure 161: Download Legible Configuration page

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 QX's Web management pages for which the legible configuration can be manually managed. For example, selecting "**RTP Settings**" will generate a legible configuration file with parameters present on the RTP Settings page.
- **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 select the settings in the generated legible configuration file to one specific extension. For example, each of the extensions on the QX have own SIP settings or Codecs. To download the settings for a particular extension only, you need to choose the corresponding extension from the list. The drop-down may also have a blank selection. In that case, the legible configuration file will contain the parameter of all available extensions on the QX (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 – starts parsing the configuration structure of the device for the defined parameters. The progress will be displayed in the window.
- Cancel generation process – stops 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 when the legible configuration generation is finished.
- Restart generation! – is used to cancel the generated configuration file and start over. This button appears when the legible configuration generation is finished.

12.7.3 Upload Legible Configuration

The Upload Legible Configuration page is used to upload a configuration file in the (*.txt) format.

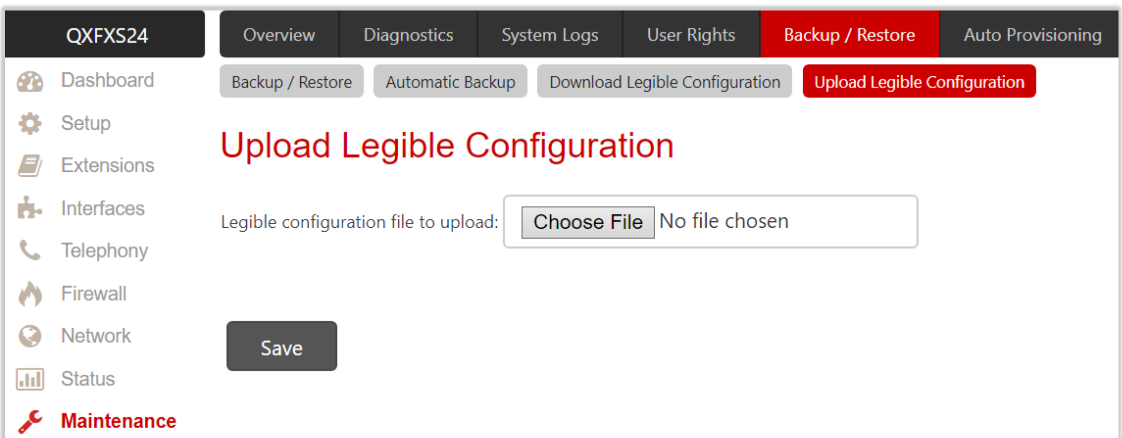


Figure 162: Upload Legible Configuration page

- Choose File – is used to browse certain legible configuration file to be uploaded and updated into the system. The file uploading progress will be displayed in the window.

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 the Save button to submit the changes. At any point, the QX detects a mistake – a version mismatch, the 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 an edited LCF, the QX will start to sequentially apply the changes.

12.8 Auto Provisioning

The **Gateway Operation Mode** page is used to select one of options for QXFXS24 operational mode. The following modes are available:

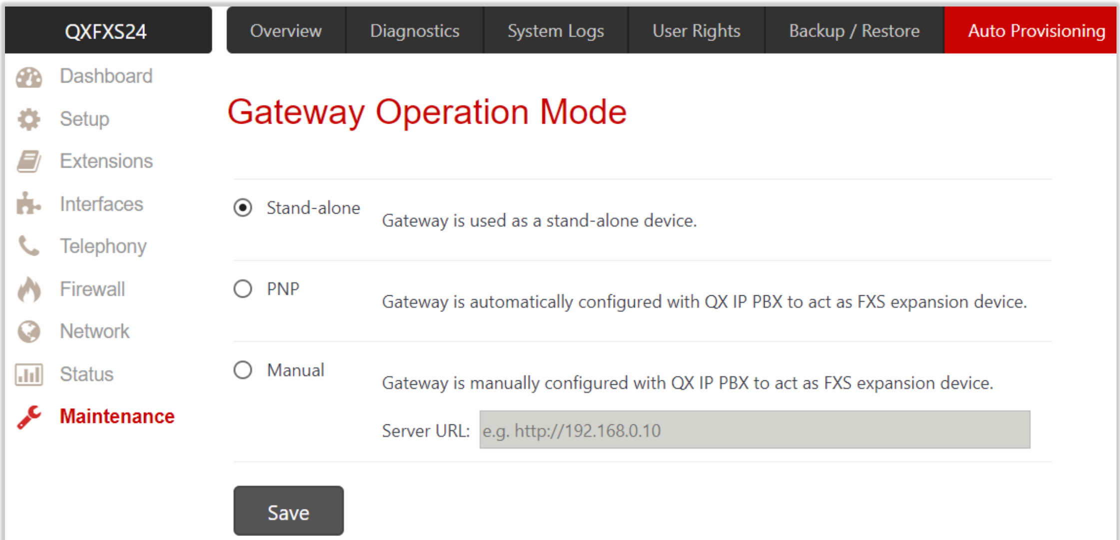


Figure 163: Gateway Operation Mode page

- **Stand-alone** – select this option to configure the QXFXS24 and use it as stand-alone VoIP getaway. You have to configure the device manually using the management GUI.
- **PNP** – select this option to configure the QXFXS24 automatically with any available in network QX IP PBX and use it as FXS expansion device. Some extra adjustment in configuration can be done manually, if needed.
- **Manual** – select this option to configure the QXFXS24 manually with the specified QX IP PBX and use it as FXS expansion device. TIP: The **Server URL** needs to be in the following format http://xxx.xxx.xxx.xxx.

For information on how to configure and use QXFXS24 with QX IP PBXs, please refer to the Configuring QXFXS24 with QX IP PBXs guide.

12.9 Firmware Update

The **Firmware** section is used to update the firmware of QXs. 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 firmware of QX, please 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 after the firmware update. Moreover, 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 the QX's Web GUI, connect to an QX again and login.
- The QX will factory reset and the system configuration will be lost while downgrading the firmware.

12.9.1 Manual Firmware Update

The Manual Firmware Update page is used to upload and update the QX firmware manually.

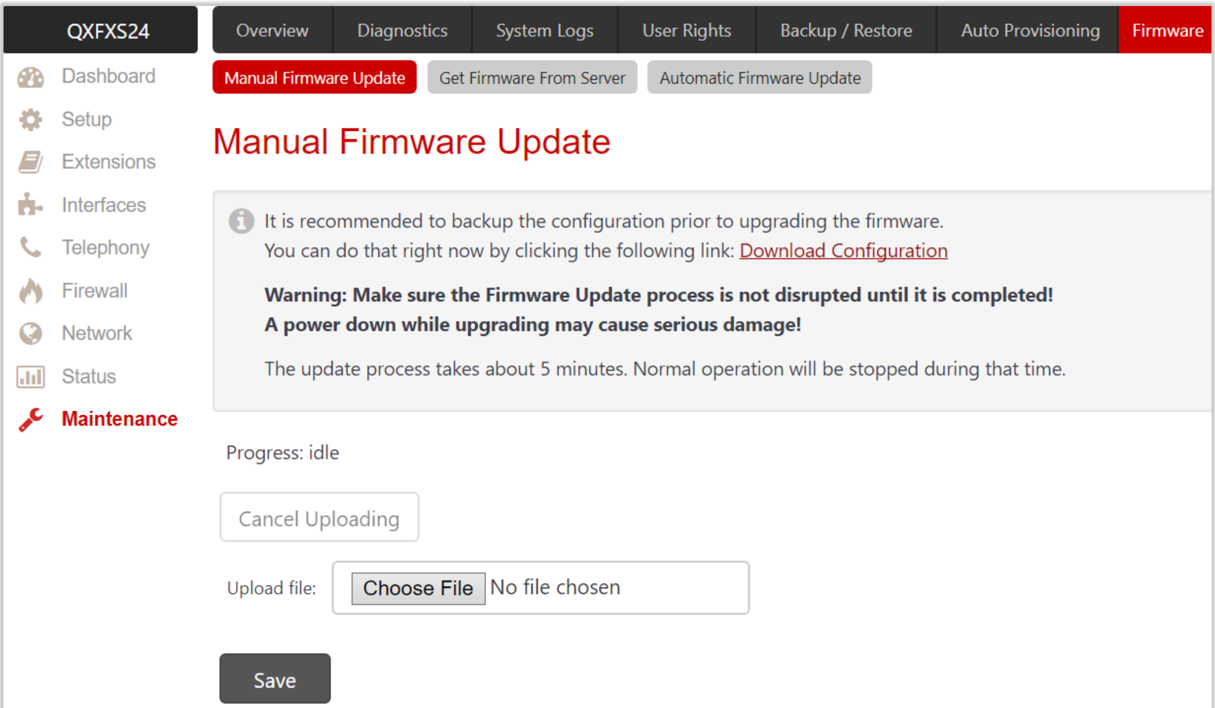


Figure 164: Manual Firmware Update page

The recommended manual firmware update procedure is:

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.
5. Click Yes to proceed the firmware upgrade.

Note: The update process takes about 5 minutes. Normal operation will be stopped during that time.

The following information will be displayed when firmware upload finished:

- Firmware check – show the status of uploaded firmware. Status Invalid means that the uploaded firmware is not compatible with the QX hardware version.
- Current Firmware Version/New Firmware Version – show the current/new firmware versions accordingly.
- Click Yes to proceed the update or click Discard this firmware to close the message without updating the device.

12.9.2 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.

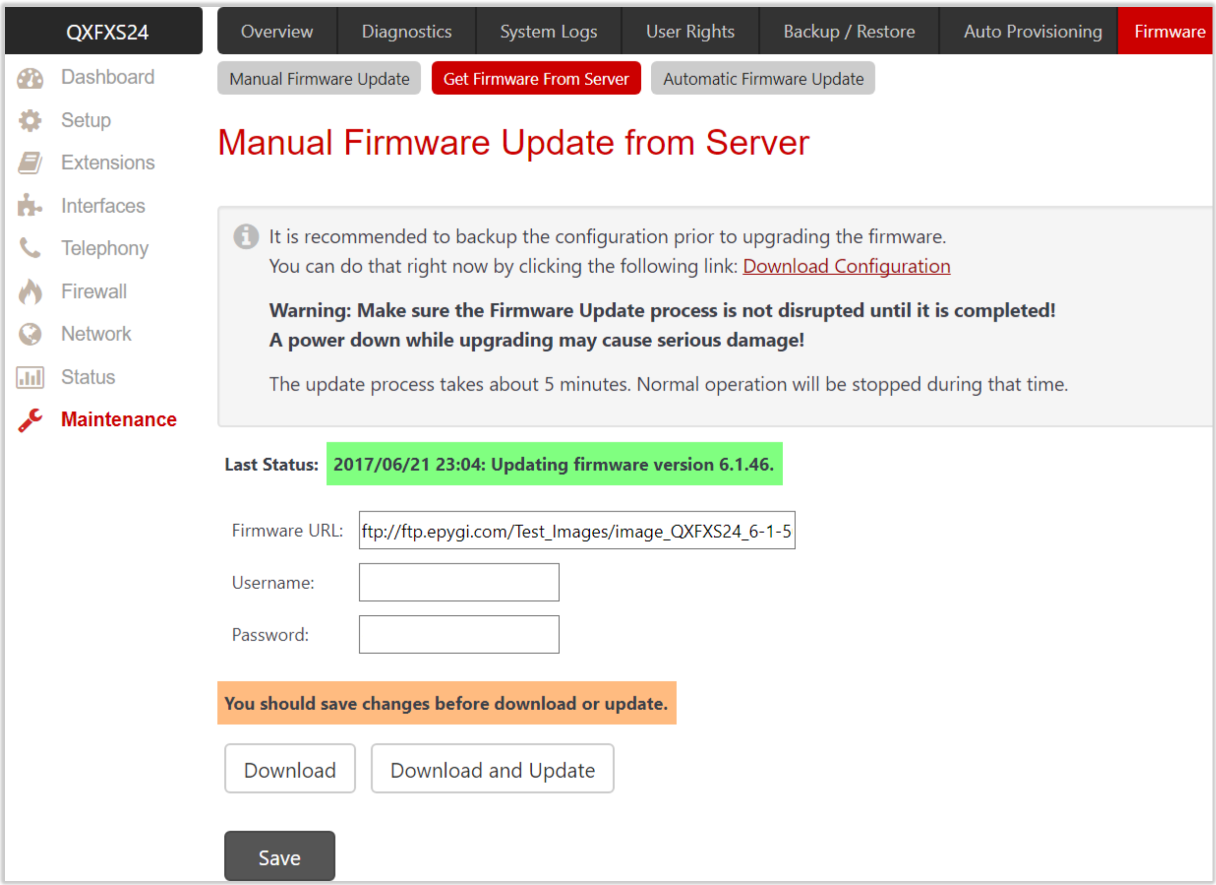


Figure 165: Manual Firmware Update from Server page

The following information and functions are available in this section:

- Last Status – displays the date/time and firmware version for the last update.
- Firmware URL – is used to define the URL for the firmware on the FTP server.
- Username and Password – are used to define the authentication parameters for the FTP server.
- Save – keeps the changes before Download or Download and Update.
- Download – starts downloading firmware from FTP Server.

The following information will be displayed when firmware download finished:

- Firmware check – shows the status of uploaded firmware. Invalid status means the firmware is not compatible with the QX hardware version.
- Current Firmware Version/New Firmware Version – show the current/new firmware versions accordingly.
- Update – is used to proceed the update or click Discard to close the warning message without updating the device.
- Download and Update – is used to automatically download and update the firmware from the FTP server.

12.9.3 Automatic Firmware Update

The **Automatic Firmware Update** page is used to enable and configure the automatic firmware update settings on the QX. When this service is enabled, on the scheduled time 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. The following components and functions are available:

- **Enable Automatic Firmware Update** – is used to enable Automatic Firmware Update service.
- **Server Name** – enter the IP address or hostname of the server.
- **Server Port** – enter the port of the server.
- **Update Method** – select the desired update method (FTP, HTTP or HTTPS).
- **Username** and **Password** – are used to define the server authentication parameters.

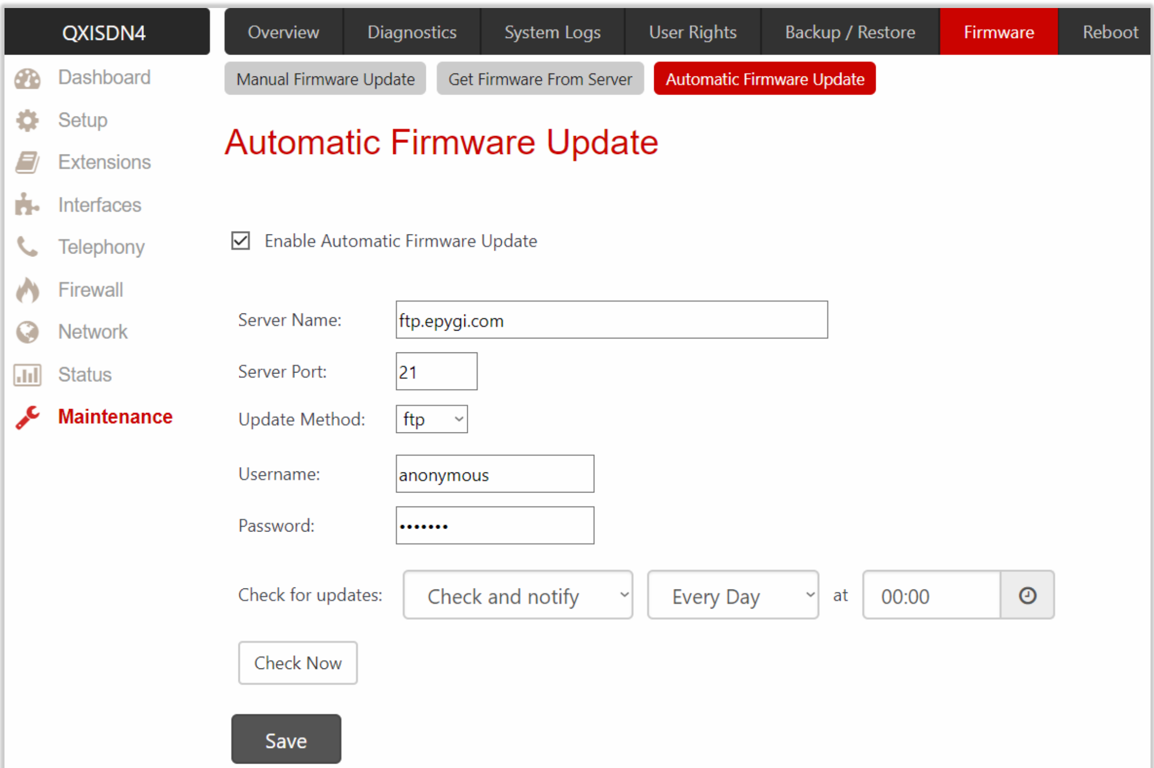


Figure 166: Automatic Firmware Update page

Note: The server configuration can be done manually. The recommended and simplest method is to use the Epygi's 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's FTP server:

1. Select the **Enable Automatic Firmware Update** option.
2. 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.
3. 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 scheduled time. If there is a new firmware available, the QX will download and update it automatically.

12.10 Reboot

The **Yes, Reboot Device** button is used to reboot the QX. TIP: The session with the QX will be closed, i.e., the QX's GUI should be newly opened and a new login will be required afterwards.

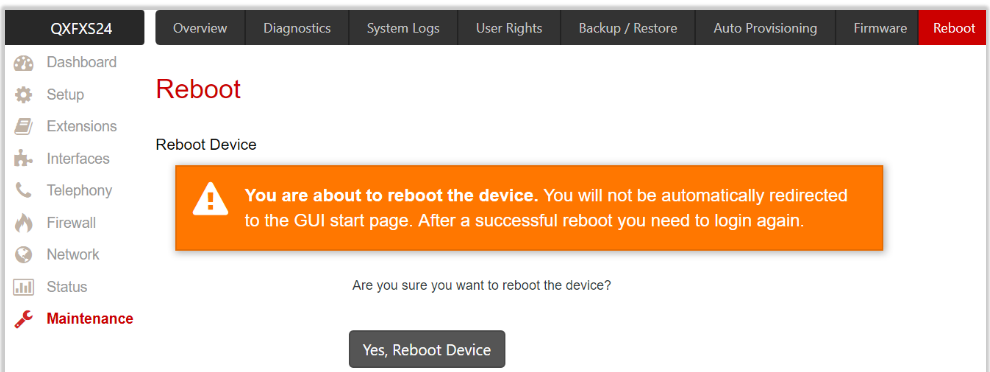


Figure 167: Reboot Device page

12.11 Registration Form

The **Register Your Device in Technical Support Center** page appears when administrating an unregistered QX, and it has been created for customer support purposes. The page requires customer registration at the **Epygi Technical Support Center**. It provides several links offering the following registration options:

Figure 168: Device Registration page

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

13 User Extension's Menu

QX configuration management may be accessed by users (extensions) and administrators. If you are a user, log in with the extension number and the password (if any) you received from your system administrator.

- **Log Out** – is used to close the session between the PC and QX and to leave the Extension Management.
- **Return** – this link is used to return back to Extensions Management page.
- **Extension #** menu – allows you to access the following settings to operate and perform actions that are private for each user.
    - Call History
    - General Information
    - Account Settings
    - Basic Services
    - Caller ID Services

13.1 Call History

The **Call History** allows to track and report the call detail records (CDR) for concerning the inbound/outbound calls, for the current extension.

The **Successful Calls**, **Missed Calls** and **Unsuccessful Outgoing Calls** pages lists successful, missed and unsuccessful outgoing calls and their parameters. The following components are available:

- **Filter** – allows searching for call records based on at least one of the criteria: Call Start Time, Call Duration, 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 the (***.log**) or (***.csv**) formats respectively.

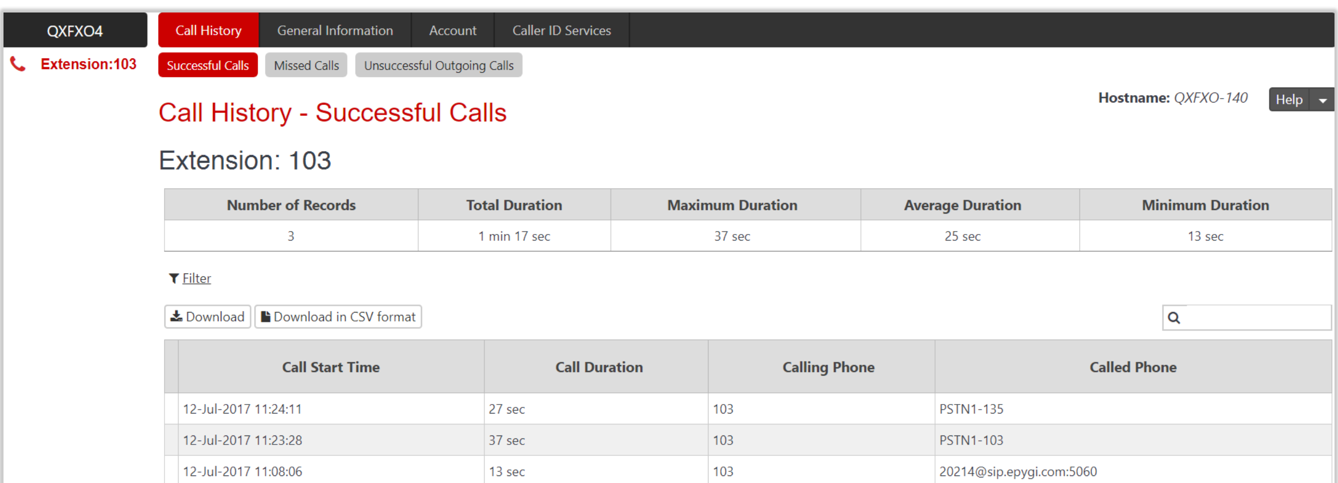


Figure 169: Call History – Successful Calls page

CDRs listed in the Call History tables are characterized by the following parameters:

- **Call Start Time** – shows the start date and time of the call.
- **Call Duration** – shows the duration of the call.
- **Calling Phone** – shows the caller's number and display name (if available).
- **Called Phone** – shows the callee's number and display name (if available).

The **Download Call Detail Records** / **Download Call Detail Records in CSV format** links are used to download the displayed CDRs for each page (Successful, Missed and Unsuccessful Outgoing) in the (*.log) or (*.csv) formats respectively.

13.2 General Information

The **General Information** page (N/A for QXFXS24) shows read-only information regarding the current extension, as well as some available resources on the QX. This page displays a list of activated codecs on the extension, the list of extensions on the QX **Extensions Directory**. Any available FXO lines, E1/T1 and ISDN trunks are also visible here.

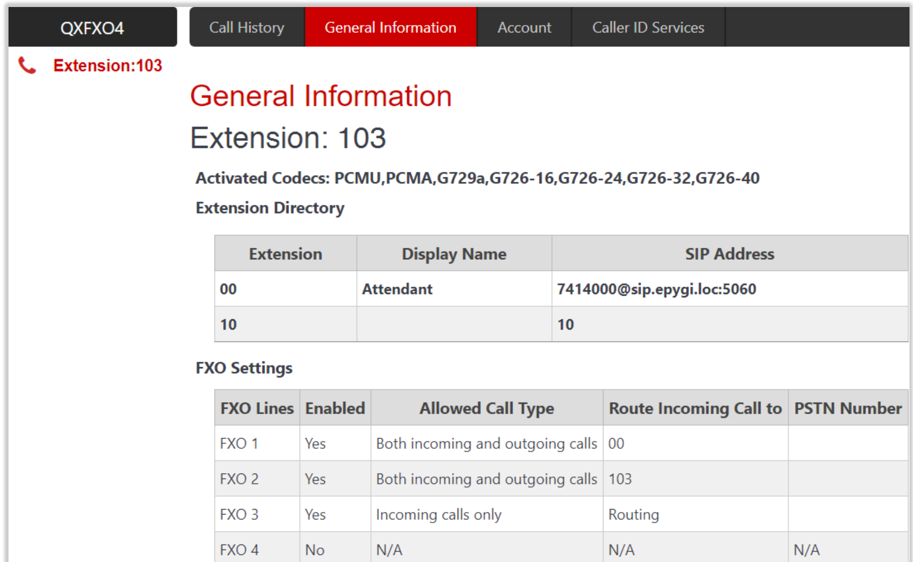


Figure 170: General Information page

13.3 Account Settings

The **Account Settings** page (N/A for QXFXS24) allows changing the extension display name, the user password and uploading the files with the user-defined messages. This page consists of the following components:

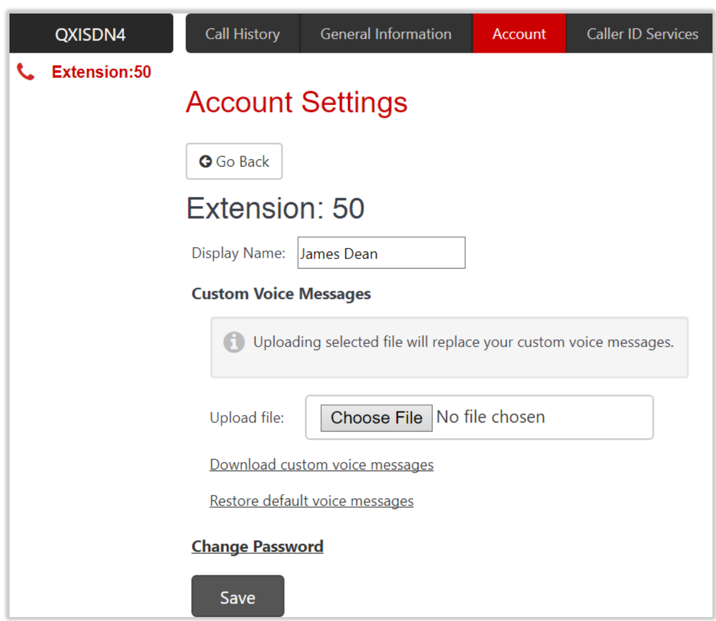


Figure 171: Account Settings page

- **Extension** – displays the current extension number.
- **Display Name** – allows to modify the extension's display name. The display name appears on the called phone display.
- **Enable Remote Extension** (N/A for QXISDN4) – this option is only visible when the **Remote Extension** service has been activated on the extension. With this option, the user can enable/disable the **Remote Extension** functionality.
- **Custom Voice Messages** – is used to upload custom voice messages for the extension. Uploading selected file will replace your custom voice messages. Uploading custom messages downloaded from the other QX will overwrite messages that have not been configured by the user with the current device default ones. This means that if some default messages were used on one QX, they may be completely different on another QX after uploading the voice data.
- The **Change Password** link leads to **Change Password** page where you can change your extension's password.

13.4 Basic Services

The Basic Services page (available only for QXFXS24 gateway) allows you to configure the basic telephony features of QXFXS24 gateway, such as Call Waiting and Hot Line service.

Note: Remember to save changes before moving between the configuration sections.

Call Waiting

The Call Waiting service allows to receive a call when you are currently on a call. The QX user will hear a special beeping on the phone when call arrives. For analog phones, to switch between the current and the new arrived call, use the appropriate calling code.

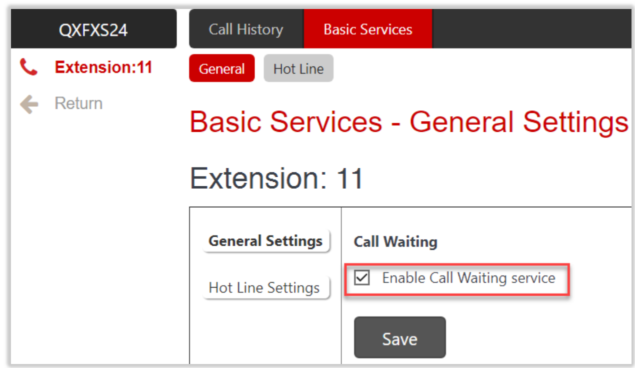


Figure 172: Basic Services – General Settings page

Hot Line Settings

The Hot Line service is used to call automatically the preconfigured number in case if no action for a predefined period after lifting the phone handset. This service is commonly used for emergency calls. The Hot Line Settings page consists of the following components:

- Enable Hot Line Service – activates the Hot Line service on the current extension.
- Timeout – is used to select the delay before the defined number will be dialed automatically.
- Call Type, Called Address – is used to define destination address.

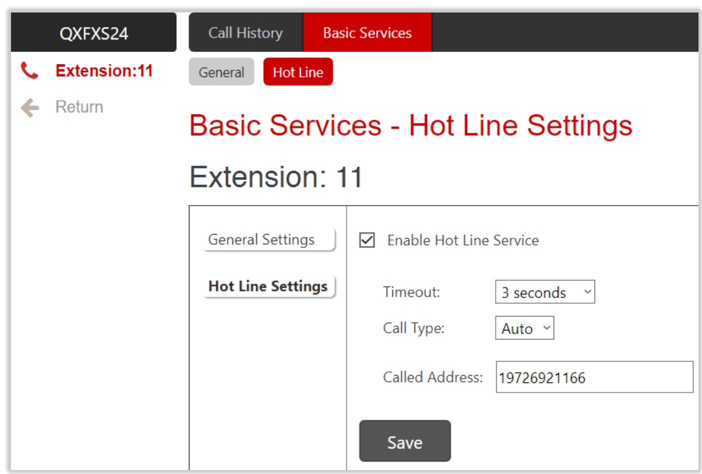


Figure 173: Hotline Settings section

13.5 Caller ID Services

The Caller ID Based Services page (N/A for QXFXS24) provides interface(s) to configure the telephony services for the extension. The configuration settings for Unconditional Call Forwarding, Incoming and Outgoing Call Blocking services are accessible from this page.

The Caller ID Based Services page lists all manually or automatically configured caller and called addresses with the ON/OFF status of their telephony services.

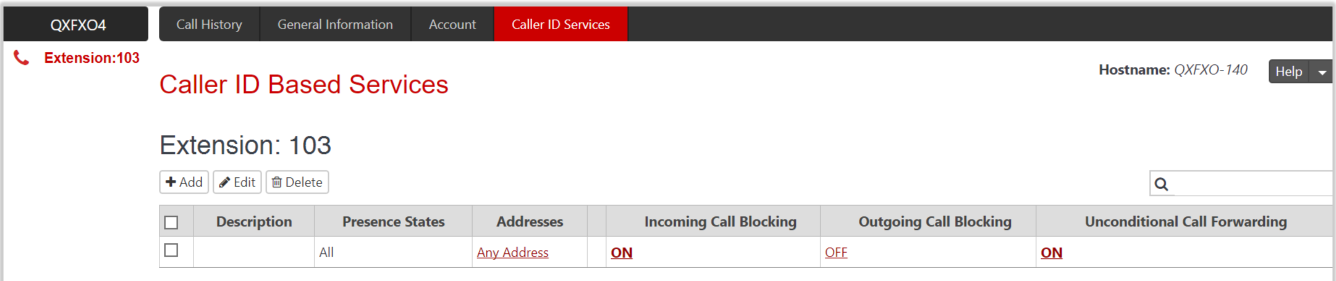


Figure 174: Caller ID Based Services for Any Address page

Note:

- **Any Address** – the **Any Address** entry in this page is undeletable. It is used to configure the Caller ID Based services for all addresses. Adding a new entry changes the **Any Address** to **Other Addresses**.
- Remember to save changes before moving between the caller ID based services configuration pages.

Add leads to the **Caller ID Based Services – Add Entry** page where a new address and presence states can be defined. The following settings are available:

- Enter a **description** about the address owner.
- **Presence State** allows to set the Presence State of an extension.
  - **All States** – is used to select and enable all states for the extension.
  - **Specific States** – is used to select the specified state(s) for the extension.

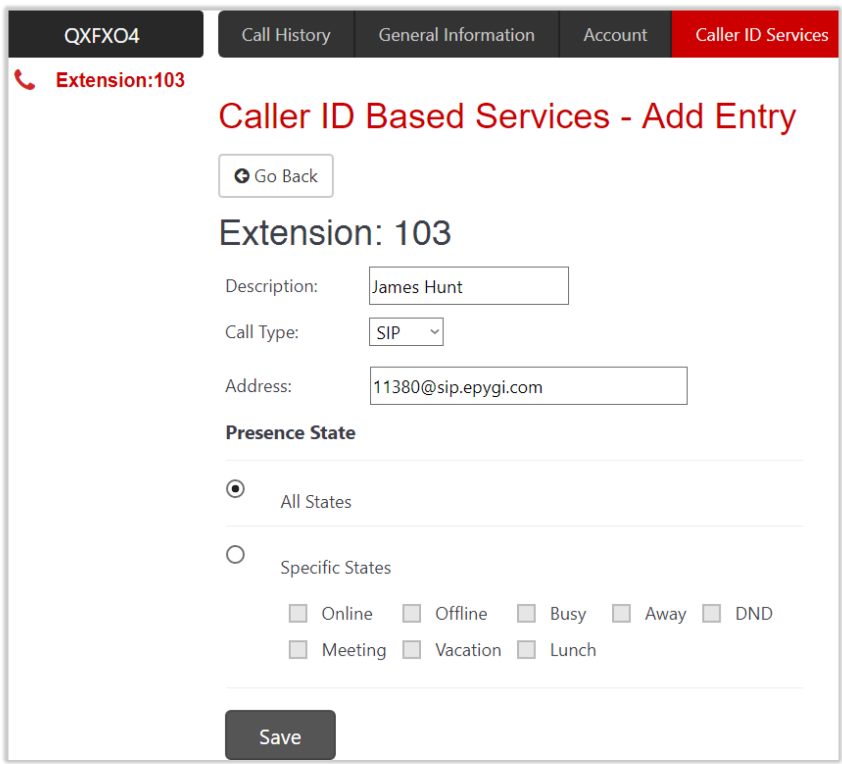


Figure 175: Caller ID Based Services – Add Entry page

To configure **Caller ID Based Services** for a specific address:

1. Click the **Add** button on the **Caller ID Based Services** page. The **Caller ID Based Services – Add Entry** page will open, where the address can be defined.
   - Enter **Description** for the address, if needed.
   - Select the call type from the **Call Type** drop-down list.
   - Enter the SIP address, extension or PSTN number (depends on the chosen call type) in the **Address** text field according to the entering rules.
   - Select the **Presence State** of an extension.
2. Click **Save**, the new address will be added to the **Caller ID Based Services** table.
3. Click on the newly created **Address** in the Caller ID Based Services table to open the **Caller ID Based Services for Address** page.
4. From the left frame, choose a **Caller ID Based Services**. From the right frame, enable, configure and adjust the corresponding service. Do this for each service.

13.5.1 Incoming Call Blocking

Incoming Call Blocking section allows blocking unwanted caller and informing the caller that the call is blocked.

- Enable Service – blocks the incoming calls to the current extension for any or for a specific address.
  - Send Message to Caller Party – if selected, announced the caller that his number is blocked, otherwise the calling party will be disconnected without notification.
  - Protect this Entry – if selected, the user will not be able to deactivate the Incoming Call Blocking service for the corresponding caller. This option is available only for administrators and is used to protect Incoming Call Blocking service from being disabled by the user.
- Incoming Call Blocking Message – is used to upload a new incoming call blocking message, download the message, as well as restore the default one.

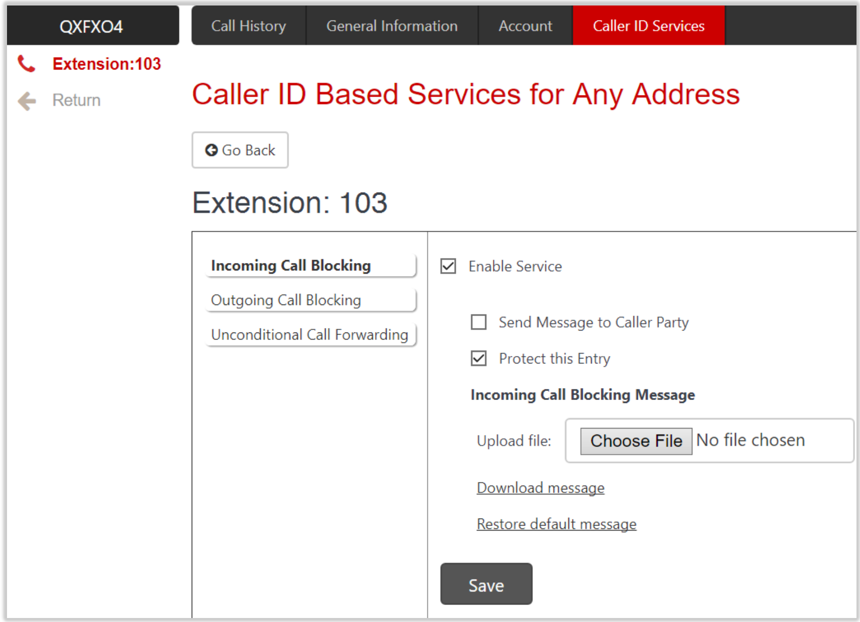


Figure 176: Incoming Call Blocking section

13.5.1 Outgoing Call Blocking

Outgoing Call Blocking section allows blocking the calls to unwanted numbers and informing the caller that the number is blocked.

- Enable Service – blocks the outgoing calls to any or to specific address.
  - Send Message to Caller Party – if selected, initiates a message to inform the caller that the called number is blocked, otherwise the caller will hear a busy tone.
  - Protect this Entry – if selected, the extension user will not be able to deactivate the Outgoing Call Blocking. This option is available only for administrators and is used to protect Outgoing Call Blocking service from being disabled by the user.
- Outgoing Call Blocking Message – is used to upload a new outgoing call blocking message, download the message, as well as restore the default one.

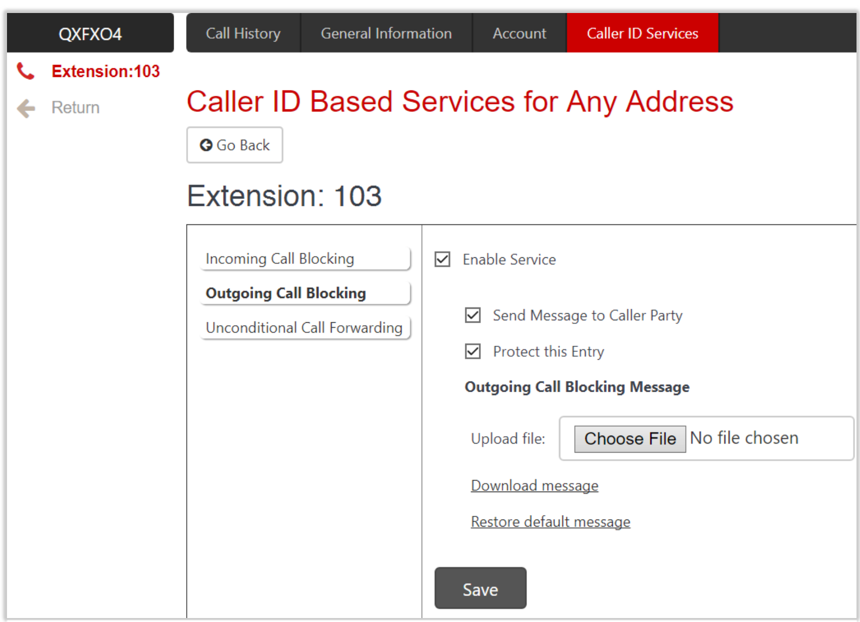


Figure 177: Outgoing Call Blocking section

13.5.2 Unconditional Call Forwarding

The **Unconditional Call Forwarding** section allows to forward all incoming calls to the defined destination(s). The **Forward to** table displays the list of destinations with the associated settings (Figure 179):

- **Enable Service** – activates the service for the current extension.
- **Enable/Disable** – is used to enable/disable the forwarding destinations in the **Forwarding** table.
- **Add** leads to the **Forwarding List – Add Entry** page where you can add forwarding destinations may be specified:
  - **External Party** – is used to call external number with options available:
    - **Call Type, Calling Address** – is used to define the forwarding destination.

Note: The QX allows to forward incoming calls through local **PSTN** lines. To do so, select PSTN from the **Call Type** drop down list and type **pstn** (capital and lower-case letters allowed) in the **Calling Address** field. Caller will connect to the available **PSTN** line, get the dial tone and be free to dial a number.

  - **Extension** – is used to call QX extension.

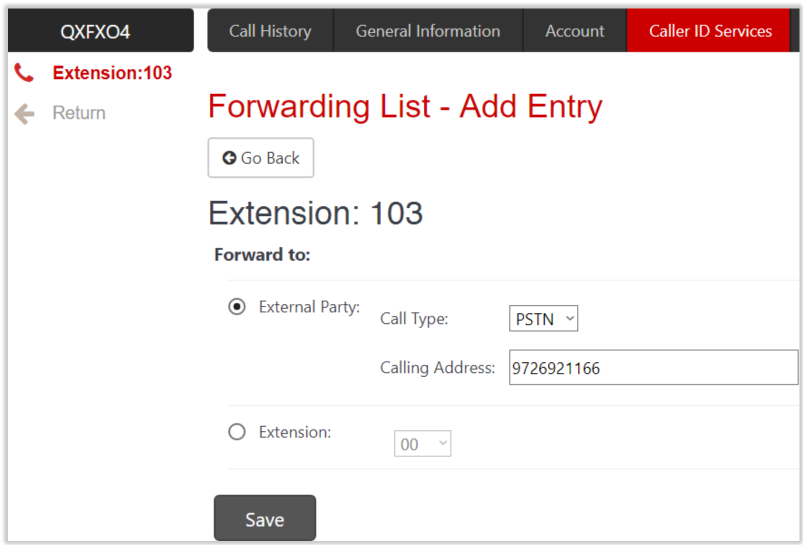


Figure 178: Forwarding List – Add Entry page

- **Send Notification via SMS** – is used to enable sending SMS notification to the specified mobile number when call forwarding takes place. If selected, the following options become available:
  - **Mobile Number** – enter the mobile number of the recipient. Use a space, semicolon or a comma to separate numbers in case of multiple recipients. TIP: This option will work when **SMS Service** is enabled on the QX.
- **Send Notification via E-mail** – is used to enable sending e-mail notification when call forwarding takes place. If selected, the following options become available:
  - **E-mail Address** – enter the e-mail address of the recipient. Use a space, semicolon or a comma to separate mailing addresses in case of multiple recipients. TIP: This option will work when **SMTP Service** is enabled on the QX.
- **Toggle from Handset** – is used to enable toggling the **Unconditional Call Forwarding** for a selected entry **ON/OFF** from the phone handset by the appropriate feature code. Dialing the *4 will toggle the **Unconditional Call Forwarding** for all entries in the Caller ID Based Services table that have the **Toggle from Handset** option enabled.

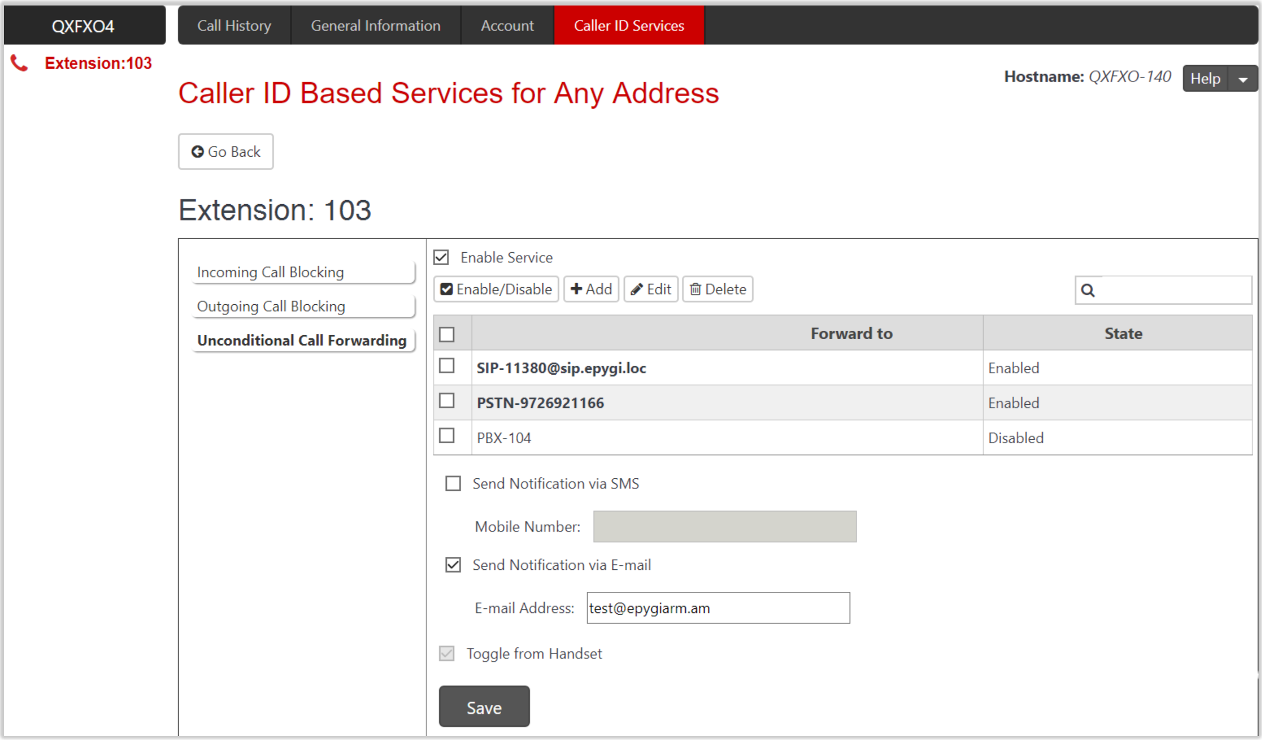


Figure 179: Unconditional Call Forwarding section

Attention: The Forwarding has higher priority over other Caller ID based services, except for Incoming and Outgoing Call Blocking. If the Incoming or Outgoing Call Blocking services are configured on the extension, these services will take effect.

14 Appendix: Needed Bandwidth for IP Calls

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

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–13.33	–	–	27	–	–	20
G.722	105	84	76	74	71	67
G.722.1	74	53	45	42	40	37

Table 6: 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–13.33	–	–	31	–	–	22
G.722	114	89	81	76	74	72
G.722.1	82	57	49	44	42	40

Table 7: 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–13.33	–	–	41	–	–	26
G.722	148	105	90	85	80	74
G.722.1	118	74	60	53	48	45

Table 8: Required Bandwidth for Encrypted Packets when using a VPN

15 Appendix: Feature Codes

15.1 PBX Services Accessible at the Dial Tone

This chapter describes the feature codes to navigate through the QX telephony services with the phone handset. These services are characterized by starting with the key *:

Automatic Redial

- Dial *1 to redial the last dialed number.
- If the called number is busy after dialing *1 keep the handset lifted to activate the auto redialing of the last called number. The connection will be established immediately when the called destination answers the call.

Note:

- ➢ This service is functional for SIP and PBX calls only. For PSTN calls, this feature works as a single redial (with no multiple attempts to reach the called destination).
- ➢ This service is not available on QXISDN4 and QXFXS24.

Call Back

Dial *2 to call back the last caller.

Unconditional Call Forwarding

Dial *4 to configure **Unconditional Call Forwarding**:

1. Press 2 to add a forwarding number.
2. Press 1 to toggle (enable or disable) the forwarding service.

After successful configuration, dial *4 to activate/deactivate the service.

Note:

- Using the "**Change the Forwarding Number**" option will update the first entry in the **Unconditional Call Forwarding** table with **Auto** call type. Any other entries with **Auto** call type, as well as with other call types will not be modified.
- Besides **Any Address/Other Addresses** entry of the **Unconditional Call Forwarding** table this toggling also affects all those entries that have **Toggle from Handset** option selected. The states of those entries will be set to the same as the state of **Any Address/Other Addresses** entry after toggling.
- This service is not available on QXFXS24.

Block Last Caller

- Dial *73 to block the last caller. The last caller will be blocked and added to the **Caller ID Services** table.
- To unblock the caller, go to the Incoming Call Blocking section and disable the **Incoming Call Blocking** service for the blocked address.

Note:

- This service can be activated within 10 seconds after the call termination.
- This service is not available on QXISDN4 and QXFXS24.

Line Information

Dial *74 to get information about the IP line, attached Extension number and SIP username. Note: This service is not available on QXISDN4 and QXFXS24.

Call Routing Management

The Call Routing Management is used to manage the routing entries in the Call Routing table, i.e. to enable/disable certain routing rule(s) by dialing key combinations pre-configured on each rule.

1. Dial *77 to enable the routing rule.
2. Enter the activation code and press #.

After successful activation, the state of the routing rule will be modified (enabled).

1. Dial again *77 to disable the routing rule.
2. Enter the deactivation code and press #.

After successful deactivation, the state of the routing rule will be modified (disabled).

Note:

- If the routing record has an authorization enabled on the enabler/disabler key, administrator's password (Phone Access Password) should be entered after the key. Once the password is entered, system plays a confirmation about the accepted configuration and the state of the certain routing rule(s) is getting modified. If the password has been entered incorrectly for 3 times, no status changes will be applied to any of the routing rule(s), even to those which have no authorization enabled.
- This service is not available on QXFXS24.

Hot Desking

If QX has limited number of IP phones connected, but much more users wishing to make and receive calls through the 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 first login with personal settings, such as the extension's number and password of previously configured and dedicated him virtual extension. Note: This service is not available on QXISDN4 and QXFXS24.

To access the public phone:

1. Dial *78 to login.
2. Enter the extension number and press #.
3. Enter the extension password and press #.

After successful login, the phone becomes a full featured phone connected to the QX. You can place and receive calls and use all supplementary PBX services of the QX.

When having finished using the phone, logout.

1. Dial *78 to logout.
2. Enter the password of the current logged in extension and press #.

When logged out, the public phone becomes available for other users.

Outgoing Call Blocking

Dial *79 to configure **Outgoing Call Blocking**:

1. Enter the extension's password and press #.
2. Press 1 to block a destination.
3. Enter the **number** to be blocked and press #.

After successful configuration, the service will be applied.

Dial *79 to unblock the destination:

1. Press 2 to unblock a destination.
2. Enter the **number** to be unblocked and press #.

Note: This service is not available on QXISDN4 and QXFXS24.

Mark the Last Call as Bad

You can **mark the last call as Bad** in the system logs, this can be used for diagnostics purposes only. Dial *81 after terminating the call. Note: This service is not available on QXISDN4 and QXFXS24.

Logs Collecting

You can collect system logs (user's failure log) from handset, this can be used for diagnostics purposes only. Dial *82 to collect the logs. Note: This service is not available on QXISDN4 and QXFXS24.

Call Codes available for QXFXS24

The table below presents the feature codes for PBX services accessible at the dial tone.

PBX Services	Keys
Call Hold (used both for call waiting and for switching from one line to another)	Flash 0
Call Blind Transfer and Call Transfer with Consultation	Flash
Call Conference	Flash 3
To terminate the call	Flash 4

Table 9: Feature Keys available on QXFXS24

15.2 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 login.
2. Enter the Phone access password.
3. Follow the voice prompts to review and change system messages.
4. Press *0 or hang up to logout.

System will notify about the messages that can be reviewed and modified.

<table>
<tr><th colspan="4">Administrator Login menu</th></tr>
<tr><td>❶
Review Attendant Greeting</td><td>❷
Review Attendant Recurring Prompt</td><td colspan="2">❸
Review Universal Extension Messages</td></tr>
<tr><td>Enter the Attendant Number (in case of multiple AAs)</td><td>Enter the Attendant Number (in case of multiple AAs)</td><td>❸
Incoming Call Blocking message</td><td>❹
Outgoing Call Blocking message</td></tr>
<tr><td>❶
Listen to the current greeting</td><td>❶
Listen to the current prompt</td><td>❶
Listen to the current message</td><td>❶
Listen to the current message</td></tr>
<tr><td>❷
Record a new greeting</td><td>❷
Record a new prompt</td><td>❷
Record a new message</td><td>❷
Record a new message</td></tr>
<tr><td>❸
Restore system default greeting</td><td>❸
Restore system default prompt</td><td>❸
Restore system default message</td><td>❸
Restore system default message</td></tr>
<tr><td>#
Stop recording or playback</td><td>#
Stop recording or playback</td><td>#
Stop recording or playback</td><td>#
Stop recording or playback</td></tr>
</table>

Table 10: Administrator Login menu

15.3 Auto Attendant

Auto Attendant can be accessed locally, remotely from the IP network (by dialing Auto Attendant's SIP address) and from the PSTN network if the calls from PSTN are routed to the Auto Attendant. TIP: Auto Attendant is not available on QXFXS24.

The following services are accessible from Auto Attendant by using appropriate feature codes:

Call Relay

When dialing on the IP phone connected to QX, the dialed digits are send directly to be processed by **Call Routing Table**. But when remote callers are dialing on the Auto Attendant prompt, the dialed digits are not send to Call Routing Table by default. This is done to prevent unauthorized calls. To send the Auto Attendant digits to Call Routing Table either the Auto Attendant "**Pass Dialed Digits through Call Routing**" option should be enabled or the Auto Attendant Call Relay service should be used. Using **Call Relay** gives privileges of PBX extensions to call directly to remote destinations.

The **Call Relay service** is accessible by feature code *2 on Auto Attendant prompt. After dialing *2 an authentication will be required (an extension number and password). Once successfully entered, the caller can use the routes available in the Call Routing.

Note: The **Call Relay** service cannot be used, if it is not enabled on at least one of the extensions on the QX. The **Allow Call Relay** option is enabled/disabled on a per extension basis. By default, this option is disabled on all extensions.

Call Relay allows the external user to make multiple calls to different destinations without the necessity of hanging up after each call and dialing the auto attendant again. To make a call to the new destination without disconnecting from QX, the external user has to enter ** rather than hang up. Upon receiving this service code, the QX terminates the current call to destination and sends the invitation to dial the new destination number.

Note:

- The ** service code is applicable at ringing and connected call stages.
- This service can only be used when accessing from PSTN to the external SIP destination through QX's AA or vice versa.
- This service is not available on the second QX Auto Attendant (calling from one Attendant to another).

Call Back

With the QX's Call Back service callers can save the call charge when calling to/through the QX to the remote destinations. The QX allows configuring a list of trusted callers that are allowed to make free of charge calls. Two types of Call Back configurations are available: **Pre-configured Call Back** and **Remote Call Back Configuration**.

Preconfigured Call Back

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

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

Remote Call Back Configuration

The **Remote Call Back Configuration** service is used by authorized callers to configure or reconfigure existing call back configuration on the QX. Remote Call Back Configuration is divided into two modes accessible from the QX's Auto Attendant:

- Permanent Call Back
- Non-Permanent (Instant) Call Back

Note: Remote Call Back Configuration services are only available when the **Automatically Enter Call Relay Menu** option is disabled in the Call Back settings for the trusted user.

Permanent Call Back

Permanent Call Back service allows callers registered in the Authorized Phones to create a new trusted caller with Call Back enabled. They can also modify the Call Back destination of existing callers in the Authorized Phones. By calling QX's Auto Attendant and entering the Auto Attendant menu, the caller can use the *6 code to create a new trusted caller as well as to modify the Call Back destination for the already registered callers in the Authorized Phones.

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

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

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

Non-Permanent Call Back

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

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

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

Other Services

You can also remotely access some QX telephony services through Auto Attendant after passing the authentication. The following services are accessible from Auto Attendant:

- Unconditional Call Forwarding
- Administrator Login
- Call Routing Management

16 Appendix: System Default Values

16.1 System Settings

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
User Rights Management	Username	Admin	All
	GUI Password	19	
	Phone Access Password	19	
	Users	admin – enabled	
		localadmin – disabled	
	Roles	Extension – all accessible pages are granted access	QXE1T1/QXFXO4/QXISDN4
		Localadmin – all accessible pages are granted access	All
System Configuration	Hostname	e1t1gw	QXE1T1
		fxogw	QXFXO4
		isdngw	QXISDN4
		fxsgw	QXFXS24
	Domain Name	epygi-config.loc	All
	LAN IP Address	172.28.0.1	All
	Subnet Mask	255.255.0.0	All
DHCP Settings for the LAN Interface	DHCP Server	Enabled	All
Regional Settings and Preferences	Your locale (location)	US	All
	Timezone	(GMT-06:00) Central Time (US&Canada)	
Uplink Configuration	WAN Interface Protocol	Ethernet	All
	Upstream	100.000 k/bits	All
	Downstream	100.000 k/bits	All
	Min Data Rate	0	All
WAN IP Configuration	IP configuration of the WAN interface	Obtain an IP Address automatically	All
WAN Interface Configuration	MAC Address	This device	All
	MTU	1500 Bytes	All

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
DNS Settings	DNS configuration	Obtain DNS Server Address automatically	All
Date / Time Settings	SNTP Server	Enabled	All
Date / Time Settings	SNTP Client	Enabled	All
Date / Time Settings	SNTP Server	ntp1.epygi.com	All
Date / Time Settings	Polling Interval	6 hours	All
E-mail(SMTP) Settings	SMTP Service	Disabled	All
Short Text Messaging (SMS) Settings	SMS Service	Disabled	All
System Security Management	Security Level	Medium	All
Licensed Features	–	No **feature** is activated.	QXE1T1/QXFXO4
Upload Language Pack	–	The **Custom Language Pack** isn't uploaded.	All
Extension Management	Extension Length	2	QXISDN4/QXFXS24
Extension Management	Extension Length	3	QXE1T1/QXFXO4
Extension Management	Extensions attachment	Ext. (11-34) attached to the FXS lines (1-24)	QXFXS24
User Extensions –General Settings	Display Name	None	All
User Extensions –General Settings	Password	Left blank	All
User Extensions –General Settings	Allow Call Relay	Disabled	QXE1T1/QXFXO4/QXISDN4
User Extensions –General Settings	GUI Login Allowed	Disabled	QXE1T1/QXFXO4/QXISDN4
User Extensions –General Settings	Show on Public Directory	Disabled	QXE1T1/QXFXO4/QXISDN4
User Extension – SIP Settings	Username / DID Number	Same as the extension number	All
User Extension – SIP Settings	Password	Left blank	All
User Extension – SIP Settings	SIP Server	Left blank	All
User Extension – SIP Settings	SIP Port	5060	All
User Extension – SIP Settings	SIP Registration Transport	UDP	All
User Extension – SIP Settings	Registration on SIP Server	Disabled	All
User Extension – SIP Advanced Settings	Authentication Username	None	All
User Extension – SIP Advanced Settings	Send Keep-alive Messages to Proxy	Disabled	All
User Extension – SIP Advanced Settings	RTP Priority Level	Medium	All
User Extension – SIP Advanced Settings	Do Not use SIP Old Hold Method	Disabled	All

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
User Extension – SIP Advanced Settings	Outbound Proxy	Left empty	All
	Secondary SIP Server	Left empty	
	Outbound Proxy for Secondary SIP Server	Left empty	
User Extension – Codecs	G711u, G711a and G729	Enabled	All
	Preferred Codec	G711	
	G726-16, G726-24, G726-32, G726-40, iLBC, G.722, G.722.1, TDVC	Disabled	
	Out of Band DTMF Transport	Enabled	
	T.38 FAX	Enabled	
	Pass Through FAX	Enabled	
	Pass Through Modem	Disabled	
	Force Self Codecs Preference for Inbound Calls	Disabled	
	SRTP Policy	Make unsecure calls, accept anything	
Attendant 00 – General Settings	Display Name	Attendant	QXE1T1/QXFXO4/QXISDN4
	Enable FAX forwarding	Disabled	
	Show on Public Directory	Enabled	
Attendant 00 – Attendant Settings	Scenario	Standard	QXE1T1/QXFXO4/QXISDN4
Attendant 00 – Attendant Scenario	Pass Dialed Digits through Call Routing	Disabled	QXE1T1/QXFXO4/QXISDN4
	Call Redirection	Disabled	
	ZeroOut Redirection	Disabled	
	Welcome Message	Enabled	
	Welcome Message and Recurring Prompt	Default message	
Attendant 00 – Attendant Ringing Announcement	Ringing Announcement service	Disabled	QXE1T1/QXFXO4/QXISDN4
Attendant 00 – SIP Settings	Username / DID Number	00	QXE1T1/QXFXO4/QXISDN4
	Password	Left blank	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
Attendant 00 – SIP Settings	SIP Server	Left empty	QXE1T1/QXFXO4/QXISDN4
	SIP Port	5060	
	SIP Registration Transport	UDP	
	Registration on SIP Server	Disabled	
Attendant 00 – SIP Advanced Settings	Authentication Username	None	QXE1T1/QXFXO4/QXISDN4
	Send Keep-alive Messages to Proxy	Disabled	
	RTP Priority Level	Medium	
	Do Not use SIP Old Hold Method	Disabled	
	Outbound Proxy	Left empty	
	Secondary SIP Server	Left empty	
	Outbound Proxy for Secondary SIP Server	Left empty	
Attendant 00 – Codecs	G711u, G711a and G729	Enabled	QXE1T1/QXFXO4/QXISDN4
	Preferred Codec	G711	
	G726-16, G726-24, G726-32, G726-40, iLBC, G.722, G.722.1, TDVC	Disabled	
	Out of Band DTMF Transport	Enabled	
	T.38 FAX	Enabled	
	Pass Through FAX	Enabled	
	Pass Through Modem	Disabled	
Attendant 00 – Codecs	Force Self Codecs Preference for Inbound Calls	Disabled	QXE1T1/QXFXO4/QXISDN4
	SRTP Policy	Make unsecure calls, accept anything	
Dialing Directories	Global Speed Dial	No file imported	All
Universal Extension Recordings	Percentage of System Memory	1%	QXE1T1/QXFXO4/QXISDN4
Authorized Phones	–	No entries	All
FXS Lines	FXS Lines attachment	FXS line 1-24 – enabled and attached to Exts. (11-34).	QXFXS24
Line Settings	Caller ID Type	Standard 2	QXFXS24
	Enable off-hook Caller ID	Disabled	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
Line Settings	Busy Tone and Power Disconnect indications	Disabled	QXFXS24
	Ringer Type	Type A	
	Hot Desking	Disabled	
FXS Lines Loopback Settings	–	Loopback is disabled for all FXS lines; Loopback timeout is 30.	QXFXS24
FXO Settings	4 FXO lines	All FXO lines enabled, incoming and outgoing calls are allowed and routed to 00 Attendant on all lines.	QXFXO4
E1/T1 Trunk Settings	1 E1/T1 Trunk	All incoming calls are allowed and routed to 00 Attendant.	QXE1T1
	Trunk Type	E1	
	Interface Type	User	
	Signaling Type	CSS	
ISDN Trunk Settings	4 ISDN trunks	All trunks enabled, incoming and outgoing calls are allowed and routed to 00 Attendant on all trunks.	QXISDN4+
	Interface Type	User	
	Connection Type	PTMP	
Shared PSTN Gateways	PSTN Gateway Operation Mode	Stand-alone mode	QXE1T1/QXFXO4/QXISDN4
	PSTN Lines Sharing	empty	
Call Routing Table	–	2 entries defined to call the default Auto Attendant 00, PBX extensions and SIP(sip.epygi.com).	QXE1T1/QXFXO4/QXISDN4
	–	An entry defined for a SIP calls.	QXFXS24
Call Routing	Route all incoming SIP calls to Call Routing	Disabled	All
Local AAA Table	–	No entries	All
SIP Tunnel Settings - Tunnels to Slave Devices	Tunnels to Slave Devices	Service is disabled, no entries.	All
SIP Tunnel Settings - Tunnels to Master Devices	Tunnels to Master Devices	Service is disabled, no entries.	All
NAT Traversal Settings	NAT Traversal for SIP	Automatic	All
NAT Traversal - SIP Parameters	UDP Parameters	Use STUN	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
NAT Traversal - RTP Parameters	RTP Parameters	Use STUN	All
NAT Traversal - STUN Parameters	Primary STUN Server	stun.epygi.com	All
	Primary STUN Port	3478	
	Secondary STUN Server	Undefined	
	Secondary STUN Port	Undefined	
	Polling Interval	1 hour	
	Keep-alive Interval	120 sec.	
	NAT IP checking Interval	300 sec.	
NAT Traversal Exceptions	–	No entries	All
RTP Settings	Packetization Interval	20 ms.	All
	Silence Suppression	Yes	
	–	No packetization interval and silence suppression values defined for G722, G722.1 and TDVC codec.	
	G726 Standard	Use ITU-T specification	
	RTP/RTCP port range	6000-6255	
	RTCP Support	Disabled	
SIP Settings	UDP and TCP Port	5060	All
	TLS Port	5061	
	Realm	Epygi	
	Session Timer	Disabled	
	DNS Server for SIP	Use default	
	SIP Timers	RFC3261	
Host Aliases for SIP	–	No entries	All
TLS Certificates	–	No certificate is generated and installed.	All
RTP Streaming Channels	–	No entries	QXE1T1/QXFXO4/QXISDN4
Gain Control Settings	FXS Lines	Transmit Gain: -6	QXFXS24
		Receive Gain: 0	
	FXO Lines	Transmit Gain: 0	QXFXO4
		Receive Gain: 6	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
Gain Control Settings	ISDN Trunks	Transmit Gain: 0	QXISDN4
		Receive Gain: 0	
	E1/T1 Trunk	Transmit Gain: 0	QXE1T1
		Receive Gain: 0	
	WAN Port	Not opened	
RADIUS Client Settings	–	The **Radius Client** service is disabled.	All
Dial Timeout Settings	Routing Dial Timeout	4 sec.	All
Configure Call Quality Event Notification	–	The **Call Quality Event Notification** service is disabled.	All
Hold Music Settings	Play Hold Music	Local Music	QXE1T1/QXFXO4/QXISDN4
	Hold Music	Default message	
	Percentage of System Memory	1%	
Firewall Configuration	IDS	Enabled	All
	NAT	Enabled	
	Firewall	Disabled	
	Firewall Level	Not selected	
Advanced Firewall Configuration	Ping Stealth	Enabled	All
	Fool Portscanner	Disabled	
Filtering Rules	Incoming Traffic / Port Forwarding	No entries	All
	Outgoing Traffic	No entries	
	Management Access	HTTPS (all IP addresses allowed).	
	SIP Access	All IP addresses allowed.	
	Blocked IP List	No entries	
	Allowed IP List	No entries	
Service Pool Configuration	–	No entries	All
IP Pool Configuration	–	No entries	All
SIP IDS Settings	SIP IDS	Enabled	All
	Add the IP address into the Blocked IP List in Firewall	Enabled	
	Discard SIP messages from IP address	Enabled, set to 32 sec.	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
SIP IDS Settings	Exceptions for SIP IDS	No entries	All
IP Static Routes	–	No entries	All
IP Policy Routes	–	No entries	All
PPTP/L2TP Routes	–	No entries	All
DHCP Advanced Settings	DHCP Options		
	Gateways	172.28.0.1	All
	Subnet Mask	172.28.0.1	
	Domain Name Servers	172.28.0.1	
	NBT Name Servers	0.0.0.0	
	NTP Servers	172.28.0.1	
	Domain Name	"epygi-config.loc"	
	Overload TFTP Server Name	172.28.0.1	
	DHCP Server Statements		
	Authoritative	Enabled	All
	Ping Check	Enabled	
	Ping Timeout	1 sec.	
DNS Server Settings	Zone	epygi.config.loc	All
	Time to Live (TTL)	86400 sec.	
	Mail Exchange (MX)	Undefined	
	Aliases	No entries	
Dynamic DNS Settings	–	The **Dynamic DNS** service is disabled.	All
PPP / PPTP Settings	–	The **PPP** service is disabled.	All
Global SNMP Settings	–	The **SNMP** service is disabled.	All
SNMP Trap Settings	–	No entries	All
VLAN Settings	–	No entries	All
IPSec Configuration	Connection	No entries	All
	RSA Key Management	1024-bit key is generated	All
PPTP/L2TP Configuration	Connection	No entries	All
	PPTP Server Configuration		
	Subnet	172.31.1.0/24	All
	Authentication	MSCHAPv2	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
PPTP/L2TP Configuration	Encryption	MPPE 128-bit	All
	L2TP Server Configuration		
	Subnet	172.31.2.0/24	All
OpenVPN	–	No files imported.	QXFXS24
Event Settings	–	"**Display notification**" for all events except Login and Firmware Update events. Those events have a "**Do nothing**" action assigned. Additionally, Fan Control critical and major failures have a **Flash LED** action assigned.	All
Call History – Settings	Call Reporting	Enabled	All
	Maximum Number of Successful Call Records	100	
	Maximum Number of Missed Call Records	100	
	Maximum Number of Unsuccessful Call Records	100	
	–	All CDR Parameters are included in CDR file.	All
Call History - Archive	–	No entries	All
Call History - Archiving Settings	Percentage of Total Memory allocated for Archive	0%	All
	Call History Archiving	Disabled	
System Logs Settings	User Logging	Enabled	All
	Developer Logging	Enabled	
	Log Lines to show	1000	
Remote Logs Settings	–	The **Remote Logging** service is disabled.	All
Backup Configuration Management	–	The **Automatic Configuration Backup** service is disabled.	All
Automatic Firmware Update	Automatic Firmware Update	Enabled	All
		Disabled	

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
Automatic Firmware Update	Server Name	ftp.epygi.com	All
	Server Port	21	
	Update Method	ftp	
	Username	anonymous	
	Password	Is left blank.	
	Check for updates	Check and notify every day at 0:00	

16.2 User Extension Settings

Page/Wizard/Section	Option/Parameter	Default Value	QX Model
Account Settings	Display Name	None	All
Basic Services – General Settings	Call Waiting service	Enabled	QXFXS24
Basic Services – Hot Line	–	The **Hot Line** service is disabled on FXS lines.	QXFXS24
Caller ID Services	–	All services are disabled for **Any Address** entry.	QXE1T1/QXFXO4/QXISDN4

17 References

Refer to the below listed recourses to get more details about the configurations described in this guide:

- Manual-I: Installation Guide for QX Gateways
- System Capacity of QX Gateways
- Licensable Features on QX IP PBXs
- Language Packs Overview for Epygi QX Line
- Auto Configuration of Epygi Supported IP Phones using OpenVPN
- OpenVPN Service on QX IP PBXs
- Extensions Bulk Import on QXFXS24
- Call Detail Records on the QX IP PBXs
- Firmware Update Service on Epygi QX Line

Find the above listed documents on Epygi Support Portal.

18 Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD.

Software License Agreement

THIS IS A CONTRACT.

CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE HARDWARE OR SOFTWARE.

1. **License.** Epygi Technologies, LTD. (the "Licensor"), hereby grants to you a non–exclusive right to use the Quadro or QX Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may use the Licensed Materials only in connection with your operation of your Quadro or QX. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.

2. **Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or the transfer of the Licensed Materials is subject to the terms of this Agreement.

3. **Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.

4. **No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language under penalty of law.

5. **Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro or QX product. If you sell your license rights in the Licensed Materials, you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

6. **Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.

7. **Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

   EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES AND ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON–INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

8. **LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OF OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.

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

9. **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.

10. **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227–19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.

11. **Entire Agreement.** It is understood that this Agreement, along with the Quadro or QX installation and administration manuals, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.
12. **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.

13. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.

14. **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.
If you have any questions about this Agreement, please write to Epygi at 1400 Preston Road, Suite 300, Plano, Texas 75093 or call Epygi at (972) 692–1166.

15. **Free Software.** Certain software utilized in the Epygi products is free software in its original form or in its modified form. Both types of free software are available to you free of charge for redistribution or modification under certain conditions. Permission is granted to copy, distribute and or/modify any free software you wish to download, whether in its original or modified forms, under the GNU General Public License or Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation. BECAUSE THE FREE SOFTWARE IS LICENSED FREE OF CHARGE, THERE IS ABSOLUTELY NO WARRANTY. Please make sure you download the GNU license from www.gnu.org . For a list of free software go to http://www.epygi.com/about/free–software–list.